Data Protection checklist for researchers

This checklist is designed to guide researchers through their obligations under data protection legislation when planning to use information about individuals in their research project. The checklist is not part of any formal application or approval process. Instead it is intended as an aide memoire and guidance document.

Compliance with data protection legislation involves a range of requirements which should be considered at the design stage of a research project. This ensures adequate controls are in place before inadvertently infringing the legislation.

The checklist complements other governance requirements for research projects, particularly data management plans and applications for ethical approval. Working through the checklist will help researchers to ensure that data issues have been considered and addressed in the relevant process.

The checklist is below, with explanatory guidance on each question in the remainder of the document. It supplements the University's Data Protection policy and the Data Protection guidance pages on Staff Net.

For assistance with data protection requirements for a specific research project, please contact the Information Governance team at dpa@abdn.ac.uk.

1. **I understand whether my research data is personal data** ☐
2. **I have considered the need for a data protection impact assessment** ☐
3. **I have incorporated the necessary safeguards to use personal data** ☐
4. **I have a contract in place with processors of the personal data** ☐
5. **I have suitable arrangements for international personal data transfers** ☐
6. **I shall use personal data fairly to recruit research participants** ☐
7. **I understand research participants' rights over their personal data** ☐
8. **I have prepared the necessary privacy information for participants** ☐

1. I understand my project involves personal data

Data protection legislation applies only to information from which living people can be **directly or indirectly identified**. If the research involves the processing of personal data, the legislation will apply to the project.

Personal data

- Information that clearly identifies someone, e.g. you gather their name, photograph etc.
- Information from which a person could be identified, e.g. you gather a person's postal address, IP address, unique ID number etc.
- Information about identifiable people that you will anonymise during your research.
- Anonymised information about people where you have access to the key that identifies them or other identifying information.

Not personal data

- Information that does not relate to human participants.
- Information about deceased people.
- Information that includes an identifier but tells you nothing about the person; e.g. information that cites a name without revealing that person's behaviour, opinions, role, location, health etc.
- Anonymised information about people where you do not have reasonable access to any means to identify them.

2. I have considered the need for a DPIA

Data protection legislation requires that a **data protection impact assessment** (DPIA) is undertaken for any proposal to use personal data that may result in a high risk to individuals' privacy.

A DPIA is not the same as making an application for ethical approval of a research project. Data protection impact assessment and ethical approval are separate but complementary processes.

A DPIA will not be necessary for all research projects, even those involving personal data. It is a statutory requirement however if your project meets one of the mandatory circumstances.

Mandatory circumstances

A DPIA is required if the research project involves one or more of the following activities:

1. Systematic and extensive profiling of individuals, with significant effects on them.
2. Large scale use of special category personal data or criminal offence personal data.**
3. Systematic monitoring of individuals in a publicly-accessible area on a large scale.
4. Determining an individual's access to a product, service, opportunity or benefit based on an automated decision or special category personal data.
5. Profiling of individuals on a large scale.
6. Combining, comparing or matching personal data obtained from multiple sources.**
7. Using personal data of children or vulnerable individuals for marketing, profiling, automated decision making or to offer online services to them.
8. Processing personal data that would jeopardise the physical health or safety of individuals in the event of a personal data breach.

A DPIA is also required if the research project meets a condition in both List A and List B:

List A

9. Innovative use of technology to process personal data.
10. Processing biometric data (e.g. voice recordings, photographs, fingerprints).
11. Processing genetic data other than in the provision of health care.
12. Processing personal data from a source other than the individual without providing privacy information.**
13. Tracking individuals' location or behaviour, either online or offline.

List B

i. Evaluation or scoring of individuals.
ii. Automated decision-making with legal or similar significant effects on individuals.
iii. Systematic monitoring of individuals.
iv. Processing sensitive data or data of a highly personal nature.
v. Processing personal data on a large scale.
vi. Matching or combining datasets.
vii. Processing personal data of vulnerable individuals.
viii. Innovative use of new technological or organisational solutions.
ix. Preventing individuals from exercising a right or using a service or contract.

** Circumstances that apply more commonly to research projects

The following guidance may assist in deciding whether circumstances 2, 6 or 12 apply to your project.

2. Large scale use of special category personal data or criminal offence personal data

   'Special category personal data' is information about an individual's health, race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used to identify people), sex life or sexual orientation. Personal data relating to criminal convictions is also considered sensitive.

   'Large-scale use' depends on the circumstances. Typically, it involves personal data relating to thousands of individuals or to the whole of a defined population.

6. Combining, comparing or matching personal data obtained from multiple sources

   This circumstance arises when a research project brings together information about individuals in two or more datasets that are from different organisations, or that were compiled for different purposes, in a way that would exceed the reasonable expectations of the individuals involved.

12. Processing personal data from a source other than the individual without providing privacy information

    'Invisible processing' occurs when personal data is received from a third-party source without the research project giving privacy information to the individuals concerned.

    For information on the privacy information that is required by data protection legislation, see checklist point 8.

Early engagement with the Information Governance team about a DPIA helps to make sure it is approved quickly and does not hold up your research project. This includes advice on whether a DPIA is necessary for your research project.

If your research project requires a DPIA, use the template on the Data Protection DPIA page.

3. I have incorporated safeguards to use personal data

Data protection legislation supports the use of personal data in research subject to the incorporation of specific safeguards for individuals in the way personal data will be handled.

Data minimisation

Any use of personal data for research requires that the **principle of data minimisation** is respected. Compliance with this principle is a key part of the way you plan to collect, use and store personal data, and should be evident from your Data Management Plan.

You should,

- collect only the personal data elements that are necessary for your research.
- anonymise the data wherever possible.
- pseudonymise the data if you are unable to anonymise. Replacing personal details in a dataset with an identifier, and keeping the key separately from the dataset, is a recommended security measure.

Safeguards for use of special category personal data

There are three additional requirements for the use of special category personal data in research.

These requirements are likely to be met as part of any research ethics approval.

Research using special category personal data can proceed only if,

1. its use is unlikely to cause substantial damage or substantial distress to an individual;
2. the research does not involve making a decision that impacts on the individual concerned;

   NB: this condition does not apply to medical research that has been subject to ethical approval.
3. the research is deemed to be 'in the public interest'. Peer review, research ethics committee approval or research subject to an independent governance framework will meet this requirement.

4. I have contracts for processors of personal data

Data protection legislation requires that any external organisations engaged to process personal data on behalf of the University are capable of processing the data securely, and that their processing operations are governed by a written contract.

'Processing' activities that could be subject to this requirement include collection of personal data by a third party, outsourcing analysis or transcription of personal data, or engaging a supplier to store data.

NB: This requirement does not extend to sharing personal data with other universities or organisations in a joint research project, or to engaging an external organisation to process data that is anonymised.

If your research project involves a data processing arrangement, follow the supplier guidance on Staff Net.

5. I have suitable legal arrangements covering any international personal data transfers

Data protection legislation requires that any transfers of personal data to countries whose data protection regime is not deemed 'adequate' are subject to additional safeguards to protect the individuals concerned.

Unlike the contractual obligations described in checklist point 4, a legal agreement is required for collaborative or joint research projects that involve international transfers of personal data.

Adequate countries and territories

Agreements are required for transfer of personal data to anywhere other than the following countries:

Andorra	Denmark	Isle of Man	Portugal
Argentina	Estonia	Italy	Romania
Austria	Faroe Islands	Japan	Slovakia
Belgium	Finland	Jersey	Slovenia
Bulgaria	France	Latvia	Spain
Canada (transfers to commercial organisations only)	Germany	Lithuania	Sweden
	Greece	Luxembourg	Switzerland
	Guernsey	Malta	United States of America (transfers to Privacy Shield organisations only)
Croatia	Hungary	Netherlands	
Cyprus	Ireland	New Zealand	Uruguay
Czech Republic	Israel	Poland	

If your research project will involve international transfers of personal data, contact the Information Governance team at dpa@abdn.ac.uk for advice on an appropriate agreement.

6. I shall use personal data fairly to recruit participants

Data protection legislation requires that the use of personal information to contact or recruit research participants must be **fair and lawful**.

Recruitment methods that are not targeted to specific individuals using their personal information are not subject to data protection legislation.

- Personal details provided by individuals who volunteer direct to the University to participate in research will be fair to use. Make sure you respect any conditions agreed with the participant.
- Be careful about using contact details that have been provided by a third party. You need to be sure that the individuals concerned would expect their details to passed to the University and to be used in this way. Ask to see either the privacy information the third party provided to those people or a record of consent from the individuals.
- Be careful about using contact details that have been collected for a purpose other than research participation. You need to be sure that the individuals concerned would expect their details to be used in this way. Check the privacy information provided to them when their details were gathered.

7. I understand participants' personal data rights

Data protection legislation provides individuals with the following rights over their personal data:

- The right to transparency. (This is covered in more detail in checklist point 8.)
- The right of access to their personal data.
- The right to rectification of their personal data, i.e. correction of inaccurate data.
- The right to restriction of processing, i.e. to limit the way in which their personal data is used.
- The right to portability, i.e. to have their personal data transmitted to a different organisation.
- The right to object to their personal data being processed.
- The right not to be subject to a decision based on automated processing of their personal data.
- The right to erasure of their personal data, otherwise known as the right to be forgotten.

Applying these rights to research data

The legislation recognises that it may not be appropriate to uphold these rights for personal data used in research. This is not a blanket exemption for all rights and for all circumstances. The University can restrict some of these rights if granting them would prevent or seriously impair the outcome of the research, and when certain other conditions apply. Each case must therefore be judged on its own terms.

Key points for researchers

- Recognise and act when a research participant invokes one of their data subject rights, particularly if they cite the GDPR or the DPA.

Individuals can exercise their data subject rights verbally or in writing. They do not need to use a form or to pay a fee when making a request.

- Forward formal requests promptly to the Information Governance team at dpa@abdn.ac.uk. They will ensure relevant exemptions are applied and that the response meets statutory requirements.
- If you do not include the link to the University's privacy notice in your participant information, you will need to tell participants about their data subject rights. See checklist point 8 for further details.

8. I have prepared the necessary privacy information

Data protection legislation requires that the use of personal data is **transparent** to the participants. This involves providing specific information to participants about the use of their data in the research project.

General points

- There is no requirement to provide privacy information if the participants already have it. Other than in those circumstances, privacy information must be provided to participants regardless of whether you have direct contact with them.
- Provide the privacy information in a way that is appropriate to your project and meaningful for participants. Integrating the information into a participant information sheet is ideal. It does not need to be signposted or separated as 'GDPR information'.

- Privacy information does not replace your consent form. Ensuring participants have made an informed choice to take part remains a necessary part of ethical research involving people.
- The amount of additional information you provide can be minimised by providing a link to the University's overarching privacy notice for research in your privacy information. You can use or adapt the following form of words:

  For details of our legal basis for using personal data, the rights you have over your personal information, and the contact details of our Data Protection Officer for any data protection queries, please see our privacy information at www.abdn.ac.uk/privacy/.

- If you do not include a link to the overarching privacy notice in your privacy information, you must include the following additional details:
  - The identity and contact details of the University as controller of the personal data.
  - The contact details of the Data Protection Officer.
  - The legal basis under data protection legislation for processing personal data.
  - The rights that participants have to control the use of their personal data.

  Seek advice from the Information Governance team at dpa@abdn.ac.uk in these circumstances.
- Research projects that involve the use of clinical personal data should follow the GDPR guidance prepared by the Health Research Authority.
- Template privacy information notices for use by University research projects are in development, and will be published later in 2019.
- The privacy information that must be provided depends on how personal data is gathered.

If you intend to collect information directly from the research participants

- You must provide privacy information to the participant at the time you collect their personal information. The privacy information must include the following elements:
  1. The **purpose** for which the personal data will be used. This might include use of the personal data in future research studies.
  2. Any organisations or **recipients** outside the University to whom you intend to disclose the personal data. (NB: this does not apply if sharing or publishing anonymised data.)
  3. The safeguards that will apply to any **international data sharing arrangements**. See checklist point 5 and contact the Information Governance team at dpa@abdn.ac.uk if this applies to your project.
  4. Information about any **automated decision-making** that will affect participants. Contact the Information Governance team at dpa@abdn.ac.uk for assistance if this applies to your project.
  5. How long the personal data will be **kept**. This may be the storage period until the data is deleted, or a review period after which the research value of the data will be assessed.

If you intend to collect or receive personal data from a third-party source

- You must provide privacy information to participants within one month of receipt, before contacting participants or before disclosing the personal data to another organisation.
  You must include all the information described at 1. to 5. above, plus,
  6. The **categories of personal data** that will be used. Typical categories of personal data include; Basic personal identifiers (e.g. name, contact details), Health data, Financial data (e.g. bank details, credit card numbers), Political opinions, Genetic or biometric data, etc.
  7. The **source** of the personal data.