University of Edinburgh: Data Protection Impact Assessment guidance for research

# How to conduct a Data Protection Impact Assessment (DPIA)

This guidance is for all University students conducting research involving personal data. It accompanies the Student Research DPIA template and explains how to complete that template.

**Definitions**

- Personal data
- Special categories of personal data
- Data subject
- Processing
- Data processor
- Data controller

**How to carry out a DPIA**

**Stage 1: Preparing for the assessment**

Begin by describing your project and listing the purpose and objectives. As well as providing a clear and well-argued case for the project as a whole, it should also highlight those features that may have the potential for the biggest impact upon privacy.

**Stage 2: Mapping the information flow**

Next, make a preliminary assessment for data usage by mapping data flows:

- How is the information collected, stored, used and deleted?
- What information is used?
- What it is used for?
- Who will have access to it?

This gives you an understanding how the information is going to be used. The mapping can be done in the form of a flow chart, an information register, or a project design brief.

**Stage 3: Compliance with privacy laws**

Every project must be compliant with privacy laws. Even if after stage 4 you reach the conclusion that no full DPIA is required, your project must go through a data protection check. This third stage allows you to examine the project as a whole to ensure that you comply with all six data protection principles, that you have, for example, a legal basis and that what you want to do is covered in your Participant Information Sheet. Not all the legislation listed in the template will apply to your project – however, the GDPR most certainly will. By checking the legislation, you ensure that your project is compliant with all the relevant privacy and data protection legislation that apply.

*The 'motivated intruder test'*

One of the most frequently used methods of protecting datasets is by attempting to anonymise the data. The 'motivated intruder' test allows you to check if what you have done is sufficient or whether there is a real risk of individuals still being identified. Key question is the motivation: whether anyone would have the motivation to carry out re-identification.

The 'motivated intruder' is going to be a person who starts without any prior knowledge but who wishes to identify the individual whose personal data you have anonymised. This test is meant to assess whether there would actually be a 'motivated intruder' and whether the 'motivated intruder' would be successful. The basis is that this 'motivated intruder' has access to resources such as libraries and the internet, but does not have computer hacking skills and criminal intention such as burglary.

Thus, your deliberations will be:

- Is the data likely to attract a 'motivated intruder? This attraction could be
    - finding out personal data about someone else, for nefarious personal reasons or financial gain;
    - the possibility of causing mischief by embarrassing others – the more sensitive the data is (e.g. health information), the more likely it is to attract a motivated intruder
    - revealing newsworthy information about public figures;
    - o political or activist purposes, e.g. as part of a campaign against a particular organisation or person; or
    - curiosity, e.g. a local person's desire to find out who has been involved in an incident shown on a crime map.
- What is the risk of jigsaw attack, i.e. piecing different bits of information together to create a more complete picture of someone? Does the information have the characteristics needed to facilitate data linkage – e.g. is the same code number used to refer to the same individual in different datasets?
- What other 'linkable' information is available publicly or easily?
- What technical measures might be used to achieve re-identification?

**Stage 4: Screening**

Tick the box for all questions where your answer is 'yes'.

If you have ticked one or more boxes, you will need to carry out a full DPIA. Looking at the answers you've given, you should already get an understanding of where the privacy risks are. Always keep in mind: the purpose of the DPIA is to minimise privacy risk to the highest possible extent!

If all questions are answered with 'no' and you don't need to do a DPIA, remember that the privacy law compliance check will need to be a living document until your project is finished.

If you have concluded that a DPIA is warranted, the next stage is to make the preparations for the all-important risk analysis stage. This analysis is the core of any DPIA and is what distinguishes it from a straightforward legal compliance check.

**Stage 5: Risk identification and analysis**

Now identify the possible risks and begin the analysis. From this, you should start to form a clear picture about how significant the risks are, and whether there are previously unseen risks.

Next, list all measures you can take to either eliminate or mitigate the risks. There could well be more than one potential solution for each risk.

There are two types of solutions to privacy risks are avoidance measures and mitigation measures.

An avoidance measure is a means of completely eliminating a risk. It refers to the exclusion of technologies, processes, data or decision criteria, in order to avoid particular privacy issues arising. Examples are:

- Minimisation of personal data collection.
- Non-collection of contentious data items.
- Active measures to preclude the use of particular data items in the making of particular decisions.
- Active measures to preclude the disclosure of particular data items.

A mitigation measure is a feature that compensates for other, privacy intrusive aspects of a design. A mitigation measure may compensate partially or wholly for a negative impact. Examples are:

- Minimisation of personal data retention by not recording it, or by destroying it as soon as the transaction for which it is needed is completed.
- Destruction schedules for personal information which are audited and enforced.

- Limits on the use of information for a very specific purpose, which strong legal, organisational and technical safeguards preventing its application to any other purpose design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers.

Under some circumstances it may be appropriate to recognise and accept the privacy risk where the likelihood of it being realised or the impact would be low. However, this must be carefully considered, and must not be done simply as an alternative to taking action.

For each of the next three columns – impact of the risk on individuals, likelihood of it happening, likelihood of the situation escalating to reputational loss for the University through exposure – decide whether the risk is high, medium or low after implementation of the mitigation measures and enter this in the respective column.

**Stage 6: Approval**

Having completed the legal compliance checks and risk analysis, you should be in a position to clearly set out the options and to discuss with your supervisor about how best to proceed. If significant risks remain, you should explain what the problems are and why the risk analysis and mitigation process failed to resolve them. In extreme cases, your recommendation may be that your work needs to be re-thought because there is no viable solution that does not present an unacceptably high risk to the privacy of individuals. Your supervisor will finally give the approval. If you have answered 'yes' to question 11 in section 3, your supervisor will need to contact the Data Protection Officer, as your Head of School will need to approve that question.

If you require the guidance in an alternative format, please contact Records Management: recordsmanagement@ed.ac.uk or 0131 651 4099