Sheffield Hallam University

Data Protection for Researchers:
Data Protection Impact Assessments (DPIAs)

What is a DPIA?

A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan.

A DPIA does not have to eradicate all risk but should help you to minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

When used effectively a DPIA will help the University to assess and demonstrate compliance with its data protection obligations.

Are DPIAs just another risk assessment?

DPIAs focus on the impact of processing on the data subjects and their personal data.

When conducting a DPIA, you have to see the processing from the perspective of the data subjects, noting that you may need to think about different groups of individuals with a range of characteristics.

Unlike other risk assessments, you aren't looking at the impact of the activity on the University, its reputation or its finances.

Why are DPIAs important?

Legal accountability	DPIAs are an essential part of our data protection accountability obligations and are a legal requirement under the UK GDPR when the processing of personal data is likely to result in a high risk to individuals.
Data Protection by Design and Default	They help to promote the 'data protection by design' approach. Privacy and data protection issues should be considered at the design phase of any system, service, product or process and then throughout the lifecycle.
Identification of issues	They can help to fix problems at an early stage. An effective DPIA will raise awareness of data protection risks and allow problems to be identified and fixed at an early stage. Identifying problems early on can help simpler and less costly solutions or alternatives to be identified. This benefits the University and individuals and reduces the likelihood of complaints, reputational damage, fines and legal costs.
Relationship with stakeholders	DPIAs can help to improve the relationship with and reassure stakeholders. A DPIA can help improve understanding of stakeholders' needs, concerns and expectations, enabling trust to be built and better engagement. A comprehensive DPIA will reassure individuals and partner organisations that the University considers data protection in all its activities and is able to protect the personal data of participants in research projects.

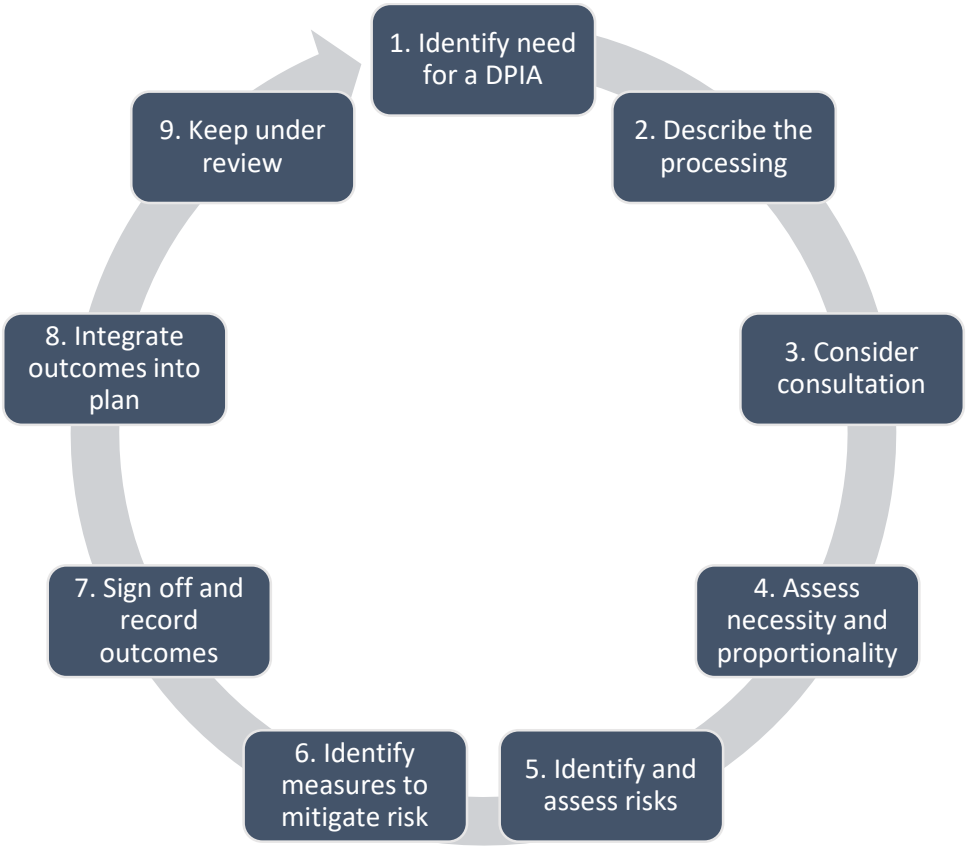
When do we need to carry out a DPIA? How do we know if a DPIA is required?

- DPIAs are required by law for higher risk data processing activities involving personal data.
- Screening questions will determine if a DPIA is required. A separate set of DPIA screening questions has been developed for academic research projects.
- Principal Investigators can also choose to carry out a DPIA if they would find this helpful in managing the project data.

- Funding bodies may request that a DPIA is carried out. They may be satisfied that screening questions have been completed and a DPIA is not indicated. They may require a DPIA regardless of the outcome of the screening questions.
- DPIAs should be carried out by the data controller, so if the University is the data processor in the relationship with a partner or funder, then we are only required to assist with a DPIA. The roles of data controller and data processor should be set out in the contracts and agreements relating to the project.
- For collaborative projects involving multiple organisations where each is a separate data controller, it may be helpful to work together on a DPIA. Where partners are joint controllers, all the partners must agree and sign off the DPIA.
- Where a DPIA is required, it should begin at the outset of a project and run alongside the planning and development process.

DPIA Process

1. First complete the screening questions to determine whether a full DPIA is required.
2. If a DPIA is indicated, complete the DPIA template. This is based on the template from the Information Commissioner's Office (ICO), and adapted slightly for academic research projects.
3. If you have any questions about how to complete the template, contact DPO@shu.ac.uk and a member of the Information Governance Team will be happy to provide support.
4. Consider whether you can seek the views of individuals who will be involved or their representatives, e.g. Patient and Public Involvement (PPI). If this is not feasible or appropriate, are there any other stakeholders, other researchers, or experts that could provide a view on the potential impact on data subjects?
5. The DPO must review the DPIA before you finalise it. The PI has responsibility for ensuring that the DPIA is complete and accurate, and that the controls to manage risks are implemented. The form contains a log to record who completed the DPIA and when they did so.
6. If the DPIA identifies a high risk to data subjects and there are no feasible controls to reduce that risk, the University is required to consult with the ICO and cannot begin the processing until the ICO has been consulted.
7. DPIAs should be submitted with ethics approval documents.
8. PIs and project managers should retain the DPIA with the rest of the project documentation and review and update the DPIA if any of the data processing changes.



A DPIA needs to describe the processing of personal data and assess potential risks to the data subjects:

Describe:

- The purposes of the proposed processing;
- The types of personal data to be processed, and the processing activities ;
- Who the data subjects are and would they expect their personal data to be used for these purposes ;
- How the data subjects' rights will be managed.

Assess:

- Whether the processing is necessary and proportionate to the aims;
- The potential risks to individuals and their interests, how those risks can be minimised and whether the level of risk is acceptable, taking into accounts any benefits of the processing;
- Whether the processing will comply with the data protection principles.

Do I need a new DPIA if the project changes?

You should update the DPIA if there are changes to the project, e.g. new types of data or data collection activities, new partners, new ways of transferring data between partners.

ICO Guidance:

Data protection impact assessments | ICO and Data Protection Impact Assessments (DPIAs) | ICO

Further Information and Support: Information Governance Team

Sharepoint: Information Governance

Email: DPO@shu.ac.uk