Data Protection Impact Assessment Guidance

DPIA & Privacy by Design Background

The General Data Protection Regulation (GDPR) has the mandatory requirement to complete a data protection impact assessment to ensure Privacy by Design.

Privacy by Design is an approach to projects that promotes privacy and data protection compliance from the start. Information needs to be protected against intentional and accidental disclosure, destruction, disruption, tampering or unauthorised access by identifying and protecting against the risks.

There are 3 main concepts that we protect against:

- confidentiality - the assurance that information is not disclosed to individuals or systems that are not authorised to receive it
- integrity - the assurance that information can't be modified by those who are not authorised to modify it, or that any such modifications will not pass undetected
- availability - the assurance that information is available when it's needed, and that mishap or malice cannot affect the ability of systems to provide information when requested

Security systems typically attempt to address one or more of these concerns through:

- physical controls, eg walls, locked doors, guards
- procedural controls, eg managerial oversight, staff training, defined processes
- regulatory controls, eg legislation, policy, rules of conduct
- technical controls, eg cryptographic software, authentication and authorisation systems, secure protocols

Not every system requires a full range of security controls. 'Completely secure systems' don't exist, and overly secure systems are often too expensive or thoroughly inconvenient for their users. The Data Protection Impact Assessment process is intended as a means for the University to identify and minimise information risks of new projects, changes or policies and to ensure measures that are implemented are appropriate and ensure compliance with relevant legislation

This process should be used for any new project or process change that involves University information to ensure we maintain confidentiality, integrity and availability of all Service information. Although the PIA section may not be required where no personal data in involved it is useful to go through this, not every question will be relevant but those such as retention, accuracy and other data quality questions should be considered.

Examples of such projects include (but are not limited to):

- Building new IT systems for storing or accessing data;

- Replacement of an existing data system by new packaged software with consequential changes to business processes and perhaps data storage;

- Plans to outsource business processes involving University information, or the storage and processing of University information;

- Embarking on a data sharing initiative; or

- Using data for new purposes.

The benefit of such an approach includes:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly;

- Increased awareness of information risk and data protection across the University;

- UoE is more likely to meet their legal obligations and less likely to breach relevant legislation;

- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

1. Executive Summary

Executive summary identifying the benefits and risks to enable the IAO, SIO, DPO and/or SIRO to make an informed decision.

2. Project Aims and Benefits

It is useful to capture what the project is aiming for, and what the business need is. By understanding what the aims, objectives and benefits are it is easier for IT to build/find a relevant solution. Sometimes a system used elsewhere appears to meet these needs but by fully understanding what is required, what the risks are and the business need an alternative solution may be more appropriate to fit within the University's infrastructure and avoid duplication.

You may find it helpful to link to other relevant documents related to the project.

3. Describe the Information Flows

You should describe the collection, use and deletion of data here and it may also be useful to refer to a flow diagram or other way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Use these questions to support your understanding of the information flow and points to consider:

- What information will be collected?
- What personal identifiers which will be used e.g. name, address, date of birth, postcode, health records, ethnicity etc.?
- Who will it be obtained from?
- How many individuals are likely to be affected?
- How will it be used?
- Is the information you are using of good enough quality for the purposes it is used for?

- Which personal data could you not use, without compromising the needs of the project?
- How do you amend data when necessary?
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?
- Who will have access to the information?
- Who will the information be shared with?
- Where will the information be stored?
- How will information be transferred (if being shared)?
- How will you ensure the security of information?
- Have University retention and disposal requirements been considered?

4. Stakeholder Engagement/Consultation Requirements

Explain what practical steps you will take to ensure that you identify and address information risks. Who should be consulted internally and externally? How will you carry out the consultation?

Stakeholder engagement / consultation should not be seen as a one step process but rather an activity which continues throughout the project.

Identifying those who should be consulted will be easier to determine when information flows are understood. Examples of relevant stakeholders include the project management team, Exeter IT, Legal, Colleges, suppliers and data processors.

External consultation should also be considered; this means seeking the views of the people affected by the project. There are two main aims. Firstly, it enables the University to understand the concerns of those individuals. Secondly the consultation will also improve transparency by making people aware of how information about them is being used.

Consultation should not be seen as a one step process but rather an activity which continues throughout the project.

5. Assessment Level Required

The University of Exeter follows best practice and a DPIA is required when any personal data is being processed. It considers the potential impact that a new or revised activity or proposed project will have on the individuals involved and ensures compliance with the Data Protection Act. This section will establish if you need to perform a full DPIA or just a ‘light’ version.

The full version will require completion of the DPIA and Risk Spreadsheet. The light version will require Appendix A to be completed.

In completing a DPIA you should consider the different aspects of privacy including:

- a physical perspective (eg from surveillance), or
- an informational perspective (eg collecting, disclosing or using personal data)

A DPIA enables us to identify and manage any data protection risks and supports compliance with the requirements of relevant legislation. Failure to recognise and mitigate privacy impact could result in reputational damage and possible enforcement action against the University.

The screening questions are intended to help you decide whether a DPIA is necessary.

Answering ‘Yes’ to any of these questions is an indication that a DPIA is required and that the checklist needs to be completed.

Regarding Risks (for full DPIA):

Identify the information and privacy risks and the associated compliance and corporate risks. Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems). Ensure the Information Asset Owner has signed off the risks and actions are integrated into project plans.

The Risks section helps identify the information, privacy and related risks, some will be to individuals e.g. inaccurate data, a security breach or upset caused by an unnecessary intrusion on privacy. Some risks will be to the organisation such as damage to the reputation, or the financial costs of a data breach. Legal compliance risks include the Data Protection Act and the Human Rights Act and may include other legislation.

Once risks have been identified the controls to treat or terminate these risks will need to be identified and evaluated. Some of these solutions will need to be treated by IT, so good stakeholder engagement is key here, e.g. Access control and change control processes. The University follows the HMG Security Policy Framework including the 114 ISO27001 baseline controls, therefore solutions that are integrated into University infrastructure will have security partially supported by controls already in place.

All risks will need to be signed-off by the information asset owner and added to the department risk register. Significant risks may need to be agreed and signed off by the Senior Information Risk Owner (SIRO) and added to the University Risk Register.

If you have any queries please contact the Information Governance Manager