University of Bolton

Teaching Intensive, Research Informed

GUIDANCE NOTES

DATA PRIVACY IMPACT ASSESSMENT

A Data Privacy Impact Assessment (DPIA) helps the University to assess the necessity and proportionality of processing personal data. A DPIA will enable the University to analyse how a certain proposal, project or processing operation will affect the privacy rights of those individuals involved by identifying, managing and minimising the risks. A DPIA should be used alongside any existing University project management and risk management processes and procedures.

DPIA's are important tools for accountability helping to ensure that potential issues are identified at an early stage and demonstrate that appropriate measures have been taken whilst providing the most effective way for the University to comply with its data protection obligations.

It has always been good practice to adopt a privacy by design approach and to carry out a DPIA as part of this. However, the General Data Protection Regulation makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes DPIAs mandatory in certain circumstances.

BENEFITS OF A DPIA

DPIAs benefit both the individual whose information is being used by the University and the University. Individuals can be assured that the University has followed best practice and can more easily understand how and why their information is being used; benefits to the University include increased trust with its stakeholders, better policies and systems and a reduced likelihood of the University failing to comply with its legal obligations under data protection and related legislation.

WHAT IS PERSONAL DATA?

Personal data is any information that relates to a living person who can be identified from the information itself or from using that information in connection with other information held or likely to be held by the University. This can include records of an opinion about an individual, details of education or employment records. For further guidance as to what constitutes personal data, see the flowchart at **Appendix 1**.

Sensitive or special category personal data is information which contains details on an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life or sexual orientation, genetic and biometric data including the commission of or proceedings of any offence committed or alleged to have been committed by an individual. Special care and secure safeguards need to be in place where sensitive or special categories of data is collected or used.

WHAT IS INFORMATION PRIVACY?

Information privacy is the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without lawful basis and misuse of such information.

Some of the ways that privacy risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those a person does not want personal information to be disclosed to;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

WHEN SHOULD A DPIA BE USED

A DPIA is required in situations where data processing is likely to result in high risk to individuals. To be effective a DPIA should be applied at a time when it is possible to have an impact on the project. This means that DPIAs are more likely to be of use when applied to new projects or where existing projects are revised.

For example, where a new technology is being deployed, undertaking a new research project that will use personally-identifiable information or where there is processing on a large scale of special categories of data. Whether you are collecting personal data or it is being given to you by a data provider, you should consider whether a DPIA is required.

The outcome of a DPIA should be a minimisation of privacy risk.

PROJECTS THAT MIGHT REQUIRE A DPIA

The following are examples of projects that may require a DPIA, although the list is not exhaustive each project should be considered on an individual basis:

- a new IT system for storing and accessing personal data.
- a data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- using existing data for a new and unexpected or more intrusive purpose.
- a new monitoring system or the application of new technology to an existing system.
- a new database which consolidates information held by separate parts of an organisation.
- legislation, policy or strategies which will impact on privacy through the collection of or use of information, or through surveillance or other monitoring.
- permitting a third party service provider access to University IT systems (e.g. for software maintenance etc.)
- permitting a third party service provider to access information held by the University.
- purchase of new software where the provider may have access to personal data (e.g. through maintenance or storage arrangements).

IDENTIFYING THE NEED FOR A DPIA

SECTION 1 - SCREENING QUESTIONS

This section asks questions designed to help you decide whether you need to complete Section 2 (Data Privacy Impact Assessment Form).

If you answer 'yes' or 'maybe' to any of the questions in Section 1, please complete Section 2 (Steps 1 – 3) and return it to the University Data Protection Officer at dpo@bolton.ac.uk who will complete Steps 4 – 5 in consultation with you.

SECTION 2 – DATA PRIVACY IMPACT ASSESSMENT FORM

STEP 1 –PROJECT OUTLINE

This section looks to clarify what the project aims are, what information you need to collect and why.

STEP 2 –DESCRIBE THE INFORMATION FLOWS

This section looks at what you will be doing with the data and to ensure that you are collecting the information in an appropriate way and storing and disposing of the information in a timely manner.

Collection

This section covers where the data comes from. For example: is it already held by the University, are we collecting it by questionnaires, online or will we be receiving data from a third party?

You also need to think how the individual will be made aware of the use of their data. Will you be asking the individual's permission to use the data; or does the University need to update its privacy notices, explaining how personal data is used by the University; or will a third party be responsible for this? If you do not think we need to inform the individual of the University's intended use of their data or gain their consent, explain why.

Storage

Under data protection legislation the University must ensure that data is kept securely, particularly if it is sensitive or special category personal data (such as education or medical records) or can easily be used to identify people. It is important that you think about how the information will be stored (electronically or otherwise) and the potential risks of unauthorised access.

Destruction

Detail in this section when you will have finished utilising the information and when the data should be destroyed. For more information on the University's standard procedures which may be applicable, see the University's **Records Retention and Disposal Policy** and **Records Retention Schedule.**

Ongoing monitoring

Ensuring the reasonable collection, use, storage and destruction of data is an ongoing obligation. You must ensure that before you begin the project you have thought about how you are going to continue to monitor the use, storage and retention of data. You should look to put in place a strategy to identify privacy risks and ensure they are dealt with effectively.

For example: removing users who are no longer authorised to access the data.

STEP 2 –CONSULTATION

You should think about who you need to consult with about the proposed project and detail how you intend to carry out that consultation. Who are the key stakeholders both internal and external to the University and whether there are any other third parties whose views should be taken into consideration on the project. List who you will be consulting and how you plan to do this.

For example: staff in procurement, marketing and communications, student data management, Students' Union, external funders, collaborative partners etc.

You should also confirm when you intend to consult them, whether this will be before or after you start collecting, transferring or using data.

STEP 3 –IDENTIFY THE RISKS

Having outlined what you intend to do, this step allows you to perform an analysis on the key risks and weaknesses in your project. Types of risks you may want to consider include:

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- Methods used for collecting information about individuals might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.
- Data being stored or processed outside EEA without appropriate safeguards.

Risks to the University

- Non-compliance with data protection or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched can result in expensive fixes.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the University and can increase administration.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Compliance Risks

- Non-compliance with data protection legislation.
- Non-compliance with the ePrivacy Regulation.
- Non-compliance with Higher Education sector specific legislation or standards.
- Non-compliance with human rights legislation.

Once the key risks in your project have been identified, you should identify what level of risk is posed, what steps could be taken to minimise the risk and what effect that is likely to have. The risks should be categorised as follows:

Eliminate	the risk can be totally eliminated by the proposed actions
Reduce	the risk will be significantly reduced by the proposed action
Accept	the risk cannot be reduced or removed but will be acceptable to the University

Reducing the Risks

There are many steps that the University can take to reduce a privacy risk. Some measures include:

- Deciding not to collect or store particular types of information.

- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise or pseudonymise the information when possible.
- Producing guidance for staff on how to use new systems and how to share data, if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Ensuring that University privacy notices are up to date and that individuals are fully aware of how their information is used.
- Select service providers who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on the University's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared, who it will be shared with and for what purpose.

Provide any additional comments on a risk, or where you are unable to eliminate a risk and state why you consider that it is justified for the University to continue the project despite the risk. Is the final impact on individuals after implementing each solution justified, compliant and a proportionate response to the aims of the project?

When you have completed STEP 3 send the form to the Data Protection Officer at dpo@bolton.ac.uk who will review the risks and set out what action should be taken in relation to the risks.

WHAT THE DATA PROTECTION OFFICER WILL DO

STEP 4 –RECORD THE DPIA OUTCOMES

This section will summarise and record the actions that the data protection officer will request be taken to make the data as secure as possible.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, the data protection officer will consult the Information Commissioner's Office (ICO) to seek its opinion as to whether the processing operation is compliant with the General Data Protection Regulation.

STEP 5 – INTEGRATE THE DPIA OUTCOMES BACK INTO THE PROJECT PLAN

The data protection officer will review the risks and set out what action should be taken in relation to the risks, set timescales for implementing these action points, if appropriate, and set dates to review the impact on privacy including detailing who is responsible for the ongoing monitoring and implementation of data protection.

PUBLICATION

A copy of the DPIA (redacted as appropriate) will be logged by the data protection officer so that interested parties will be able to review the use of information and security safeguards to be put in place. A copy of the DPIA (redacted as appropriate) will be provided to the project manager.

CONTACT DETAILS

Enquiries regarding completion of a DPIA should be sent to dpo@bolton.ac.uk

APPENDIX 1

PERSONAL DATA FLOWCHART

1. Can a living individual be identified from the data or, from the data and other information in your possession, or likely to come into your possession?

YES Go to Question 2.

NO The data is not personal data.

2. Does the data 'relate to' the identifiable living individual, whether in personal or family life, business or profession?

YES The data is 'personal data'

NO The data is not 'personal data'

UNSURE See Questions 3 – 8 below.

3. Is the information 'obviously about' a particular individual?

YES The data is 'personal data'

NO Go to Question 4

4. Is the data 'linked to' an individual so that it provides particular information about that individual?

YES The data is 'personal data'

NO Go to Question 5

Example: *a single named individual employed in a particular post, the salary information about the post will be personal data 'relating to' the single employee in that position.*

5. Is the data used, or is it to be used, to inform or influence actions or decisions affecting an identifiable individual?

YES The data is 'personal data'

NO Go to Question 6

6. Does the data have any biological significance in relation to the individual?

YES The data is likely to be 'personal data'

NO Go to Question 7

UNSURE Go to Question 7

7. Does the data focus or concentrate on the individual as its central theme rather than on some other person, or some subject, transaction or event?

YES The data is likely to be 'personal data'

NO Go to Question 8

UNSURE Go to Question 8

8. Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?

YES The data is 'personal data'

NO The data is unlikely to be 'personal data'

For further guidance and information see:
https://ico.org.uk/media/fororganisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf