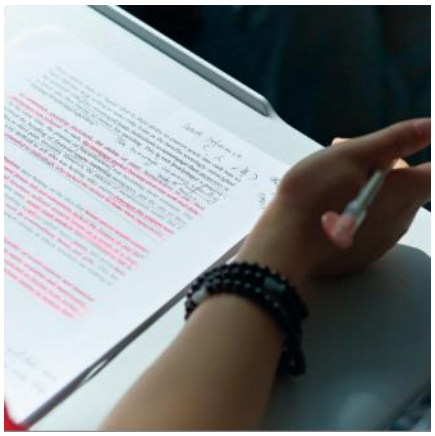
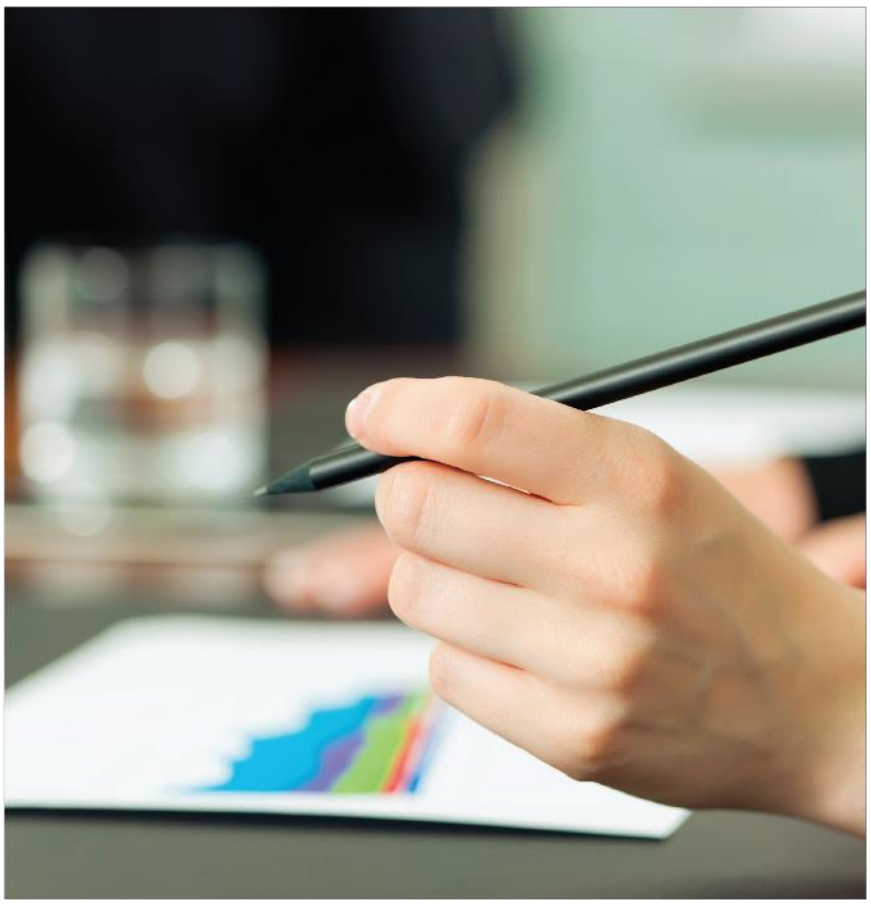
UNIVERSITY of BRADFORD

Data Protection

Procedure for conducting Data Protection Impact Assessments





1 What is a Data Protection Impact Assessment?

1.1 Data Protection Impact Assessments (DPIAs) assist organisations to identify and minimise the privacy risks of new projects or policies, comply with their data protection obligations as well as to meet individuals' expectations of privacy.

1.2 A DPIA must be done where processing is likely to result in a high risk to the rights and freedoms of individuals. This includes a number of specified types of processing and the screening checklist will help to determine when to do a DPIA.

1.3 It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

1.4 Effective DPIAs are an integral part of taking a privacy by design approach allowing organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

1.5 DPIAs can be used throughout the development and implementation of a project, using existing project management processes but can also be useful when an organisation is planning changes to an existing system.

1.6 DPIAs should be undertaken in consultation with people within the University and beyond including those affected in order to identify and reduce privacy risks.

1.7 Conducting a DPIA should not be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising and in the long term should benefit the University by producing better policies and systems.

1.8 To assess the level of risk, both the likelihood and the severity of any impact on individuals has to be considered. High risk can result from a high probability of some harm, a lower possibility of serious harm or a combination of a moderate probability of a moderate level of harm.

1.9 The University's data protection officer (DPO) must be consulted when completing a DPA as he can advise whether a DPIA is needed, how you should conduct one, what measures and safeguards can mitigate risk, whether the DPIA has been done correctly and whether the processing can go ahead. The DPO will also monitor the processing to ensure that the actions planned have been implemented and that they are effective.

1.10 Where appropriate other people, including those who may be affected by the processing should also be consulted with, this is covered below in paragraphs 5.11-5.16.

1.11 If the processing results in a high risk – even after the DPIA and any mitigating actions, the ICO must be consulted before starting the processing who will give written advice and may issue a formal warning not to process the data, or ban the processing altogether.

2 What sort of projects which might require a DPIA

2.1 DPIAs must be done where processing of personal data is likely to result in a risk to the rights and freedoms of individuals.

2.2 Examples of what constitutes such a risk includes:

- where processing could lead to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage;
- where individuals could lose control over their personal data;
- where racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership could be revealed;
- where there is processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, such as performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where the processing involves vulnerable people or children; and
- where processing involves a large amount of personal data and affects a large number of people.

2.3 DPIAs always have to be completed when the processing involves:

- Processing of sensitive data (i.e. special-category or criminal-offence data) on a large scale;
- systematic monitoring of publicly accessible places on a large scale;
- use of innovative technology;
- profiling or special category data to decide on access to services;
- profiling of individuals on a large scale;
- processing of biometric or genetic data;
- matching data or combining datasets from different sources;
- collecting personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- tracking individuals' location or behaviour;
- profiling or targeting marketing at children; or
- processing data that might endanger the individual's physical health or safety in the event of a security breach.

2.4 Screening whether a DPIA is needed should be done for every new project or any proposed new activity. To be effective it should be applied at a time when it is possible to have an impact on the project.

2.5 Conducting a DPIA of an existing project is possible but it will be less likely to make a positive difference unless it is possible for necessary changes to be implemented and there is an appetite to do it and so a DPIA should be done as early in a process as possible.

3 Who is responsible for conducting a DPIA?

3.1 Project managers and other managers without specialist data protection knowledge should be able to use the screening checklist to help them focus on privacy issues.

3.2 An effective DPIA must include consultation with others who will each be able to identify different privacy risks and solutions.

3.3 The University Data Protection Officer is available to assist conducting PIAs and in advising those signing off DPIAs on privacy matters.

4 DPIA process

4.1 When it becomes clear that a project will have some impact on privacy you should start to consider how you will address approach this. This does not mean that a formal DPIA must be started and finished before a project can progress further. The DPIA should run alongside the project development process and can be reviewed on a regular basis. What begins as a more informal early consideration of privacy issues can be developed into part of the PIA.

4.2 The key elements to a DPIA are:

- Identify the need for a DPIA;
- Describe the processing;
- Consider consultation;
- Assess necessity and proportionality;
- Identify and assess risks;
- Identify measures to mitigate risks;
- Signoff and record outcomes;
- Integrate outcomes into project plan;
- Keep your DPIA under review.

4.3 A form is available on the portal to assist with the completion of a DPIA.

4.4 A DPIA does not need to be time consuming although complex projects may require more in-depth DPIA than a simple one.

5 The DPIA Process

Identifying the need for a DPIA

5.1 The first step is to identify the need for a DPIA.

5.2 Use the screening checklist below to determine whether a DPIA is necessary. It is designed to be used by project managers or other staff who are not experts in data protection or privacy matters.

5.3 Not all projects will require the same level of DPIA; there is a greater impact on privacy when data is sensitive or when its uses are more intrusive.

5.4 When a need for DPIA is identified it is important that senior management support is sought for conducting the DPIA. Gaining this commitment at an early stage is an important factor in ensuring the DPIA is effective.

DPIA screening checklist

5.5 The checklist is intended to help you decide whether a DPIA is necessary.

5.6 Answering ‘yes’ to any of the first part of the checklist is an indication that a DPIA is needed and to any of the second part is an indication that a DPIA may be needed.

5.7 If you tick yes to any of the second part of the checklist, you should consult the DPO who will consider the processing and ascertain whether a DPIA is needed. If any processing is considered to be high risk or where two factors are in play, a DPIA will definitely be needed.

5.8 If in doubt a DPIA should be completed.

Describe the processing;

5.9 You need to describe what is it is seeking to achieve, why that is important, how and why you plan to use personal data.

5.10 include the nature, scope, context and purposes of the processing. You may wish to document for example:

Nature

- how you collect the data;
- where and when you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether you use any processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

Scope

- the types of personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

Context

- the source of the data;
- the nature of your relationship with the individuals;
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern; and
- in due course, whether you comply with any GDPR codes of conduct (once any have been approved under Article 40) or GDPR certification schemes.
- Whether you have considered and complied with relevant codes of practice.

Purpose

- The reason why you are asking for personal data;
- your legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for you or for society as a whole.

5.11 This step is a key part of any DPIA process as a thorough assessment of privacy risks is only possible if you fully understand how information is being used.

Consultation

5.12 You should seek the views of individuals who may be affected unless there is a good reason not to. In most cases it should be possible to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals then you should record this decision as part of your DPIA, with a clear explanation.

5.13 If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.

5.14 If you use a data processor (i.e. an external sub-contractor to do some of the data processing), you may need to ask them for information and assistance.

5.15 Consultation should be:

- Timely – at the right stage and allow enough time for responses.
- Clear and proportionate– in scope and focused.
- Reach and representative - ensure those likely to be effected have a voice.
- Ask objective questions and present realistic options.
- Feedback – ensure that those participating get feedback at the end of the process.

5.16 You should consult all relevant internal stakeholders, in particular anyone with responsibility for information security. Examples of internal stakeholders

- Project Sponsor/Senior Management
- Project management team
- Data Protection Officer
- Information technology (IT) particularly IT security
- Procurement
- Potential suppliers, contactors and data processors
- Legal
- Customer-facing roles
- Academic staff
- Students Union/Trades Unions
- HR
- Focus Groups

5.17 Legal advice or advice from other independent experts may also be required.

Assess necessity and proportionality

5.18 In order to assess the necessity and proportionality you need to think whether your plans actually do help to achieve your purpose and whether there is any other reasonable and less intrusive way to achieve the same result.

5.19 You need to be able to document how you ensure data protection compliance as this is a good measure of necessity and proportionality. In particular, you should include relevant details of:

- the lawful basis for the processing;
- how you will prevent function creep;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation;
- how you intend to provide privacy information to individuals;
- how you implement and support individuals rights;
- measures to ensure any data processors comply; and
- safeguards for any international transfers.

Identify and assess risks

5.20 When considering risks, think about the potential impact on individuals and any harm or damage that might be caused by the processing: be that risk physical, emotional or material.

5.21 In particular look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

5.22 You need also to look at security risks, including the sources of such risks and the potential impact of each type of breach.

5.23 Assess each risk using the table below.

Severity of Impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	*Reasonable*	*Probable*
		Likelihood of harm		

5.24 You should also look at the University's own corporate risks, such as the impact of ICO or OfS action, reputational damage etc.

Identify measures to mitigate risks

5.25 Examples of mitigations which may reduce risk include:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

5.26 Record whether the measure would reduce or eliminate the risk. You can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

5.27 You should then record:

- what additional measures you plan to take;
- whether each risk has been eliminated, reduced, or accepted;

- the overall level of 'residual risk' after taking additional measures

5.28 You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation.

5.29 If a risk remains high risk even after mitigation however, the ICO must be consulted before starting the processing. The ICO will provide written advice and may issue a formal warning not to process the data, or prevent the University from processing altogether.

Concluding and signing off the DPIA

5.30 Once you have completed the DPIA, it should be signed off by the Information Asset Owner (IAO), normally the Dean or Director of the relevant area although sometimes this may be delegated. In project work, this will be the project sponsor.

5.31 DPIAs must also be approved by the Data Protection Officer as the DPO has responsibility to ensure that the DPIA has been correctly carried out and whether its conclusions are in compliance with data protection requirements.

5.32 If you or the IAO decides not to follow the DPO's advice, this should be recorded with your reasons.

Integrate outcomes into project plan

5.33 You must integrate the outcomes of your DPIA back into your project plans. You should identify any action points and who is responsible for implementing them. You can use the usual project management process to ensure these are followed through.

Keeping DPIAs under review

5.34 You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

5.35 The DPO will monitor performance of the DPIA including how well you have implemented your planned actions to address the identified risks.

5.36 You need to make sure that you can prove that the actions have taken place and you should assess that they are effective in addressing the risks.