1. **Introduction**

Where a project or proposal includes the processing of personal information, Oxford Brookes University (OBU) uses privacy impact assessments (PIAs) as a tool to help identify the most effective way to comply with our data protection obligations and meet individuals’ expectations of privacy.

Examples would be projects to implement a new system or to make substantial changes to an existing one. By undertaking a PIA, OBU will be able to identify and correct privacy issues at an early stage, reducing costs and risks of damage to reputation. This is called a ‘privacy by design’ approach, whereby we identify and treat problems or risks as part of the planning phase rather than coming across them afterwards and trying to retro-fit solutions. PIAs can be mandated by the Information Management Team or OBU’s Chief Information Officer in circumstances where they believe that the information risk footprint or landscape will change considerably.

**1.1 What is privacy?**

The Information Commissioner’s Office (ICO) defines both physical and informational privacy. OBU is concerned with informational privacy in its PIAs, defined as:

*‘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 consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages’*

Conducting privacy impact assessments code of practice - Information Commissioner’s Office

**1.2 Privacy risks**

The PIA will act as a tool to minimise the risk to informational privacy and the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

∙ Inaccurate, insufficient or out of date

∙ Excessive or irrelevant

∙ Kept for too long

∙ Disclosed to persons who do not need to know

∙ Used in ways that are unacceptable to or unexpected by the person it is about

∙ Not kept securely

**1.3 Privacy impact assessment template**

The PIA template on the following pages should be completed by the appropriate business owner or project manager. Where appropriate, the views of the data subjects concerned should be sought.

Once completed please send this template to the IT Services Information Management team for review at info.sec@brookes.ac.uk

The information management team can also provide further guidance on completing the PIA if necessary, please contact them on ext. 5420

Section 2

# **2.1 Project title**

|  |
| --- |
|  |

# **2.2 Brief description of project**

|  |
| --- |
|  |

# **2.3 Screening Questions**

If you answer yes to one or more of these questions please complete Sections 2-7.

|  |
| --- |
| 2.3(a) Will the project involve the collection of new personal information about individuals? |
|  |
| 2.3(b) Will the project compel individuals to provide personal information? |
|  |
| 2.3(c) Will information about individuals be disclosed to organisations or people who have not previously had access to the information? |
|  |
| 2.3(d) Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? |
|  |
| 2.3(e) Does the projects involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. |
|  |
| 2.3(f) Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? |
|  |
| 2.3(g) Is the information about individuals likely to be perceived as sensitive such as racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, details of criminal offences or biometric data or other data that the individual may find sensitive such as financial and educational data. |
|  |
| 2.3(h) Will the project require you to contact individuals in ways that they may find intrusive? |
|  |

Section 3

|  |
| --- |
| **3.1 Describe the information flows**You should describe the collection, use and deletion of personal data here. It may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project. Please identify any external organisations that data is shared with. |

|  |
| --- |
| **3.2 Consultation requirements**3.2(a) Who should be consulted internally and externally? 3.2(b) How will you carry out the consultation?  |

Section 4

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **4.0 Identify the privacy and related risks**4.1 Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on the University’s central or Faculty/Directorate risk registerThe guidance notes can be used to help you identify the DPA related compliance risks.

|  |  |  |  |
| --- | --- | --- | --- |
| Privacy issue | Risk to individuals | Compliance risk | Associated organisation / corporate risk |
|  |  |  |  |

 |

Section 5

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **5.0 Identify privacy solutions**5.1 Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Solution(s)** | **Result:** is the risk eliminated, reduced, or accepted? | **Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project? |
|  |  |  |  |

  |

Section 6

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **6.0 Sign off and record the PIA outcomes** 6.1 Who has approved the privacy risks involved in the project? What solutions need to be implemented?

|  |  |  |
| --- | --- | --- |
| Risk | Approved solution | Approved by  |
|  |  |  |

 |

Section 7

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **7.0 Integrate the PIA outcomes back into the project plan**  7.1 Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

|  |  |  |
| --- | --- | --- |
| Action to be taken | Date for completion of actions | Responsibility for action |
|  |  |  |

|  |
| --- |
| 7.2 Contact point for future privacy concerns  |
|  |

 |

# **Guidance Notes**

# **Linking the PIA to GDPR principles**

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with data protection legislation.

1. **Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject**

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

**(b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with** [**Article 89**](https://gdpr-info.eu/art-89-gdpr/)**(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);**

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

**(c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);**

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

**(d) Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);**

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

**(e) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with** [**Article 89(**](https://gdpr-info.eu/art-89-gdpr/)**1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);**

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

**(f) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?