# **Privacy impact assessment form (PIA)**

When you have identified that a PIA is necessary (by completing the PIA Screening forms), you should start to complete this document. You should start to complete this form at the **beginning** of the project planning stage, and **before you have made any commitment** to go ahead with the project. **Please refer to the PIA screening questionnaire available on the Legal Services DP page before completing this PIA. See Annex A for guidance on completing the PIA.**

|  |  |
| --- | --- |
| **Project Name:** |  |
| **PIA Completed by:** |  |
| **Job Title:** |  |
| **Date PIA Completed:** |  |

|  |
| --- |
| **1: Outline the Project & need for a PIA**  Explain what the project involves, the project aims, including the benefits to the University, to individuals and to other parties. Provide links to any relevant documents related to the project, e.g. a project proposal. Summarise why the need for a PIA was identified (draw on your answers to the screening questions). |
| For example;  The project involves [X] organisation sharing personal data about [X individuals] with MMU. MMU will also share personal data about [X individuals] with [X] organisation. The overarching purpose of the sharing is [XYZ]. The benefits of the share [to MMU/the external organisation/the wider public/students etc] are [XYZ].  The relationship between MMU and [X organisation] is (e.g. MMU are providing contracted services to X organisation [or vice versa] and [explain the role each party is playing and their responsibilities e.g. x organisation is delivering an IT system or MMU is providing research services].  The sharing of personal is due to take place [X project milestone] because [XYZ]. |

|  |
| --- |
| **2: Please explain below the type of personal data being processed under this project and detail the justification for processing this data.**  Explain the individuals or types of individuals to whom the personal data relates, the categories of personal data (e.g. names, dates of birth etc) and the reason why the personal data must be processed for your project or initiative. Please specify if your project involves the processing of sensitive personal data. |
|  |

|  |
| --- |
| **3: Please set out the relevant legal basis relied upon to process personal data under this project.**  In particular, please specify the Schedule 2 condition and if relevant Schedule 3 condition, you are relying upon in order to process personal data under this project. If you are relying upon consent from the relevant individuals please describe the method for obtaining consent. |
| *Under the 1st data protection principle you can only process personal data if a condition under Schedule 2 to the Data Protection Act 1998. For example, Schedule 2 processing conditions include that the individuals have consented to the processing of their personal data for this project, the processing is necessary for the performance of a contract with the relevant individuals, the processing is for a necessary for a legitimate purpose (provided those interest don’t override the privacy interests of the relevant individuals). If the project involves the processing of sensitive personal data a condition under Schedule 3 to the Data Protection Act 1998 must also be satisfied. The Schedule 3 conditions for processing are narrower or require a higher threshold is met. For example, Schedule 3 processing conditions include the individuals have given their explicit consent to the processing of their personal data for this project and the processing involves personal data which has been made public by the deliberate steps of the individuals.* ***For a full list of the DPA processing conditions please refer to Annex A.*** |
| **4: Describe the information flows**  Describe the collection, use and deletion of personal data. It may be useful to include a flow diagram or other way of explaining data flows. Include information about the volume of data involved, or number of individuals likely to be affected by the project. |
| **Please outline here the stages at which the parties will collect personal data, transfer personal data and destroy personal data. Please describe the methods of collection, transfer and deletion of the personal data.** |

|  |
| --- |
| **5. Consultation requirements**  Explain the practical steps you will take to ensure that you identify and address privacy risks. This should include: who you will consult internally and externally; and how will you carry out the consultation. Link this to the relevant stages of your project management process. You can use consultation at any stage of the PIA process. |
| E.g;  Legal for DPA assessment and review of Information Sharing Agreement  Information Security to agree requisite information security measures  Procurement team/Research and Ethics approval/Project Manager etc. |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **6: Identify privacy and related risks**  Identify the key privacy risks and the associated compliance and corporate risks.  Larger-scale PIAs might record this information on a more formal risk register.  A privacy issue involves a risk of breaching the Data Protection Act 1998. The guidance in Annex A will help with linking privacy issues to your particular project. **Examples of privacy issue are provided below for guidance only. Please review if applicable and include any other relevant privacy issues.**   |  |  |  |  | | --- | --- | --- | --- | | Privacy issue | Risk to individuals | Compliance risk | Associated organisation / corporate risk | | **For example;**   1. **Risk that the security of the data is compromised** 2. **Risk of unauthorised access to the data whilst in the University** 3. **Risk that the individuals would object to the processing if informed** 4. **Risk that the accuracy of the data is not maintained** 5. **Risk that personal data is retained for longer than is necessary** | Risk that sensitive personal data is lost or stolen or destroyed causing distress or damage to the data subjects  Risk that sensitive personal data is accessed by persons without authority causing distress or damage to the data subjects.  Risk of damage or distress to individuals without their consent or knowledge that their personal data could be processed in this manner.  Risk of damage or distress to individuals that their personal data is processed without their knowledge.  Risk that individual’s data is held for longer than is required and that security and other organisational methods applied to the personal data lapse | Risk that the 7th data protection principle is breached  Risk that the 1st and 7th data protection principles are breached  Risk that the 1st and 6th data protection principles are breached.  Risk that the 3rd data protection principle is breached.  Risk that 5th data protection principles is breached (and risk of breach of 7th data protection principles if security measures lapse over time) | Risk of reputational damage to the University and enforcement action brought against the University by the ICO. Risk to delivery of research objectives. Risk of complaints or litigation from affected individuals.  As above  As above  As above.  As above | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **7: Identify privacy solutions**  Describe the actions you could take to reduce the risks, and any necessary future steps (eg production of new guidance; security testing for systems). If personal data is to be transferred outside of the EEA, please ensure you include the solutions below for reducing any privacy risks associated with that transfer.  **Below are examples of the solutions which could be implemented.**   |  |  |  |  | | --- | --- | --- | --- | | **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? | | Risk 1 (table above)  Risk 2 (table above)  Risk 3 (table above)  Risk 4 above  Risk 5 (see table above) | Encryption measures are used  External body provides sufficient information security  E.g. Access to data is restricted to nominated individuals. IT controls to restrict access to systems storing personal data. Stored in locked cabinets in secure rooms.  E.g. The University’s publicly available data protection policy informs individuals that personal data may be used in this way.  E.g. data is stored in a secure environment (see risk 6 below). Accuracy will be reviewed periodically.  Appropriate retention periods have been agreed (e.g. in line with usual [JISC standards](http://bcs.jiscinfonet.ac.uk/he/default.asp)). |  |  | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **8: Integrate the PIA outcomes back into the project plan**  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 | |  |  |  |  |  | | --- | | Contact point for future privacy concerns | |  | |
| **9: Sign off and record the PIA outcomes**  Who has approved the privacy risks involved in the project?  What solutions need to be implemented?  Legal Services and Information Security should be consulted on the completion of the PIA and you should seek approval from your Head of Team or Deputy Director (who will be the Information Asset Manager for your team). |

# **Annex A Guidance:** **Identifying Risks: Linking the PIA to the data protection principles**

Answering these questions during the PIA process will help to identify risks that the project will fail to comply with the DPA or other relevant legislation, eg the Human Rights Act.

**Principle 1: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:**

**a) at least one of the conditions in** [**Schedule 2**](http://www.legislation.gov.uk/ukpga/1998/29/schedule/2) **is met, and**

**b) in the case of sensitive personal data, at least one of the conditions in** [**Schedule 3**](http://www.legislation.gov.uk/ukpga/1998/29/schedule/3) **is also met.**

1. What is the purpose of the project? Is this purpose included in the [University’s registration as a Data Controller](https://ico.org.uk/ESDWebPages/Entry/Z5710637)?
2. How will you tell individuals about the use of their personal data? eg, do you have a privacy notice for your service? Has your service privacy notice been updated to reflect this project?
3. Do you need to amend the University’s privacy notices, eg the [Data Protection Notice to Students](http://www.mmu.ac.uk/policy/pdf/policy_ref_dpanoticetostudents.pdf), or any MMU policies, eg CCTV policy, Data Protection Policy, etc?
4. Have you established which [conditions for processing](https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/) apply?

The processing of personal data must satisfy a condition for processing under Schedule 2 to the Data Protection Act 1998. The processing of sensitive personal data must satisfy a condition under Schedule 2 and a condition under Schedule 3 to the Data Protection Act 1998.

1. The conditions for processing personal data are set out in [Schedule 2](http://www.legislation.gov.uk/ukpga/1998/29/schedule/2) to the Data Protection Act 1998
2. The conditions for processing sensitive personal data are set out in [Schedule 3](http://www.legislation.gov.uk/ukpga/1998/29/schedule/3) to the Data Protection Act 1998

The processing conditions most commonly relied upon by the University to process personal data are the data subject has consented (paragraph 1 of Schedule 2), the processing is in pursuit of a legitimate purpose and the infringement of the data subject’s privacy rights and freedoms are not unwarranted (paragraph 6 of Schedule 2) and the processing is necessary for the performance of a contract with the data subject or entering into a contract with the data subject (paragraph 2 of Schedule 2). The processing conditions most commonly relied upon by the University to process sensitive personal data are the data subject has given their explicit consent to the processing (paragraph 1 of Schedule 3), the processing is necessary for research purposes (within the meaning of section 33 of the DPA 1998), is in the substantial public interest, does not support measures or decisions to be taken in respect of specific individuals and does not cause or is not likely to cause substantial damage or distress to the data subject (paragraph 9 of Schedule 1 to SI 2000/417 made under paragraph 10 of Schedule 3 to the DPA 1998).

1. If you are relying on consent to process personal data, how will this be collected? What will you do if consent is withheld or withdrawn? Have you checked that your methods of [collecting consent are adequate](https://ico.org.uk/about-the-ico/privacy-notices-transparency-and-control/transparency-consent-and-control/) for the purpose?
2. 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?

**Principle 2: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**

1. Does your project plan cover all of the purposes for processing personal data? What are the purposes?
2. Have you identified potential new purposes as the scope of the project expands?

**Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

1. Is the quality of the information good enough for the purposes it will be used?
2. Is there any personal data could you do without using, without compromising the needs of the project?

**Principle 4: Personal data shall be accurate and, where necessary, kept up to date.**

1. If you are procuring new software, does it allow you to amend data when necessary?
2. How are you ensuring that personal data obtained from individuals / other organisations is accurate?

**Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.**

1. What retention periods are suitable for the personal data you will be processing?
2. Have you checked the University’s Record Management Policy and Retention Schedule? Will this need to be amended?
3. How will you ensure that the data is destroyed at the appropriate time?
4. Are you procuring software that will allow you to delete information in line with your retention periods?

**Principle 6: Personal data shall be processed in accordance with the rights of data subjects under this Act.**

1. Will the systems you are putting in place allow you to respond to subject access requests (where a data subject requires copies of their personal data) more easily?
2. If the project involves marketing, have you got a procedure for individuals to **opt out** of their information being used for that purpose?

**Principle 7: 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.**

1. Do new systems provide protection against the security risks you have identified?
2. What training and instructions are necessary to ensure that staff know how to operate a new system securely?

**Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

1. Will the project require you to transfer data outside of the EEA?
2. Is the company you want to use based outside the EEA or does it store data in servers outside the EEA?
3. If you will be making transfers outside the EEA, how will you ensure that the data is adequately protected?