**Qsis Data Protection Impact Assessment (DPIA)**

|  |
| --- |
| **Title of Initiative:** |
| **Date:** |
| **Completed by:** |

Please forward the completed form to**qsisgovernance@qub.ac.uk**

|  |  |
| --- | --- |
| **Step 1** | Identify the need for a DPIA |
| **Explain what the initiative aims to achieve, what you need to do with the data in order to achieve those aims, what the benefits will be to the organisation, individuals and other parties***You may find it helpful to refer or link to other documents, such as a project proposal**Summarise why you identified the need for a DPIA, drawing on your answers from the screening questions* |

|  |  |
| --- | --- |
| **Step 2** | Describe the information flows |
| **Detail the flow of the data from the point of collection, through processing, storage, transfer/sharing and deletion of data***What is the source of the data? How will it be used? Where will it be stored? Will it be shared with anyone? How long will it be kept for? How will it be deleted? What is the duration and frequency of processing?* |

|  |  |
| --- | --- |
| **Note** | Consultation requirements |
| **Explainwhen and how you will seek individuals’ views – or justify why it’s not appropriate to do so***Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. You can use consultation at any stage of the DPIA process.* *e.g. Discussed storage with Information Security Team* |

|  |  |
| --- | --- |
| **Step 3** | Identify and assess the privacy and related risks |
| **Identify the key privacy risks and the nature of potential impact on individuals. Include the associated compliance and corporate risks***Annex 1 can be used to help you identify the GDPR related compliance risks*

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe privacy risk and nature of potential impact** | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|  |  |  |  |

 |

|  |  |
| --- | --- |
| **Step 4** | Identify and assess the privacy and related 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)***The aim is to identify sufficient controls to eliminate each of the risks identified in Step 3, or to reduce them to a level which is acceptable to the University*

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** (Is the risk eliminated, reduced or accepted?) | **Measure approved?** (is the final impact on individuals a justified, compliant and proportionate response to the aims of the initiative?) |
|  |  |  |  |

 |

|  |  |
| --- | --- |
| **Step 5** | Assign responsibility for implementing controls |
| **What solutions need to be implemented? Allocate the controls to appropriate individuals and record an agreed deadline for implementation**

|  |  |  |
| --- | --- | --- |
| **Action to be taken** | **Date for completion** | **Responsibility for action** |
|  |  |  |

 |

|  |  |
| --- | --- |
| **Step 6** | Reassess, signoff and accept the risks |
| **Who is responsible for integrating the DPIA 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?**

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/Date** | **Notes** |
| Measures approved by: |  | *Integrate actions back into project plan, with date and responsibility for completion* |
| Residual risks approved by: |  | *If accepting any residual high risk, consult the ICO before going ahead* |
| DPO advice provided by: |  | *Where the impact of a risk identified at Step 3 is severe or major and likelihood is likely or very likely, the University's Data Protection Officer must be consulted* |
| DPIA will be kept under review by: |  |  |

 |

# **Annex 1**

# **Linking the DPIA to the data protection principles**

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the UK GDPR and other relevant legislation, for example 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 is met, and**

**b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**

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?

**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.**

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?

**Principle 3**

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

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?

**Principle 4**

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

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?

**Principle 5**

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

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?

**Principle 6**

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

Will the systems you are putting in place allow you to respond to subject access requests more easily?

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.**

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?

**Principle 8**

**Personal data shall not be transferred to a country or territory outside the United Kingdom unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

Will the project require you to transfer data outside of the UK?

If you will be making transfers, how will you ensure that the data is adequately protected?