

**Data Protection Impact Assessment**

**< Project Title >**

Prepared by: < name of Author>

Version: 1.0

**Project Title DPIA**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document Owner: |  | | | |
| Status: |  | | | |
| Version: |  | | | |
| Current Version Date: |  | | | |
| Review date: |  | | | |
|  | | | | |
| Revision History | | | | |
| Author | | Description | Version | Date |
|  | |  |  |  |
|  | |  |  |  |
|  | |  |  |  |
|  | |  |  |  |
|  | | | | |
| Final Approval | | | | |
| Name - Position | | | Version | Date |
|  | | |  |  |
|  | | |  |  |
|  | | |  |  |
|  | | |  |  |
|  | | |  |  |

**Introduction**

You should fill out this document at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process.

To learn more about the process of completing a DPIA, please refer to the accompanying guidance document provided on the following webpage:

<https://www.qmul.ac.uk/governance-and-legal-services/governance/information-governance/data-protection/data-protection-impact-assessments/>

|  |
| --- |
| **Step 1: Identify a Need for a DPIA** |
| **Explain broadly what the project aims to achieve and what type of processing it involves.** 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. |
| **Project** **Aim**  **Processing Involved**  **Need for DPIA** |

|  |
| --- |
| **Step 2: Describe the Processing** |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved? |
| **Data Collection**  **Data Use**  **Data Storage**  **Data Deletion**  **Sources of Data**  **Sharing of Data**  **High Risk Types of Processing** |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| **Nature of Data**  **Amount of Data Collected and Used**  **Data Collection Frequency and Retention**  **Number of Individuals Affected**  **Geographical Area** |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| **Nature of Relationship with Data Subjects**  **Individuals’ Control**  **Individuals’ Expected Use of Data**  **Children and Other Vulnerable Groups**  **Prior Concerns and Security Flaws**  **Novelty of Processing**  **Relevant Processing Technologies**  **Potential Current Issues of Public Concern**  **Details of any Approved Code of Conduct and Certification** |
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? |
| **­­Desired Outcome of Processing**  **Effects on Participants**  **Benefits of Processing** |

|  |
| --- |
| **Step 3: Consultation Process** |
| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within Queen Mary? Do you need to ask any processors to assist? Do you plan to consult information security experts, or any other experts? |
| **Consultation with Individuals**  **Individuals Involved Within Organisation**  **Assistance from Data Processors**  **Consultation with Information Security Experts** |

|  |
| --- |
| **Step** **4: Assess Necessity and Proportionality** |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
| **Lawful Basis for Processing**  **Describe how Purpose Achieved**  **Function Creep**  **Data Quality**  **Data Minimisation**  **Informing Data Subjects**  **Supporting Data Subjects’ Rights**  **Ensuring Compliance with GDPR**  **Safeguarding International Transfers** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk Key** | | | | | |
| **Likelihood** | **Impact** | | | | |
| 1 - Negligible | 2 - Minor | 3 - Moderate | 4 - Major | 5 - Catastrophic |
| 1 – Rare | **Low**  **1** | **Low**  **2** | **Low**  **3** | **Low**  **4** | **Low**  **5** |
| 2 – Unlikely | **Low**  **2** | **Low**  **4** | **Low**  **6** | **Medium**  **8** | **Medium**  **10** |
| 3 – Possible | **Low**  **3** | **Low**  **6** | **Medium**  **9** | **Medium**  **12** | **High**  **15** |
| 4 – Likely | **Low**  **4** | **Medium**  **8** | **Medium**  **12** | **High**  **16** | **High**  **20** |
| 5 – Almost Certain | **Low**  **5** | **Medium**  **10** | **High**  **15** | **High**  **20** | **High**  **25** |

**Use this key to calculate the Risk Scores**

|  |  |
| --- | --- |
| **Risk Type** | **Risk Score** |
| Low | 1-7 |
| Medium | 8-14 |
| High | 15-25 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step 5: Identify and Assess Risks** | | | | |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | | **Likelihood**  1 - 5 | **Impact**  1 - 5 | **Risk Score**  Likelihood x Impact = Risk Score |
| **1** |  |  |  |  |
| **2** |  |  |  |  |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |
| **6** |  |  |  |  |
| **7** |  |  |  |  |
| **8** |  |  |  |  |
| **9** |  |  |  |  |
| **10** |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** **6: Identify Measures to Reduce Risk** | | | | |
| **Options to reduce or eliminate risk:** Identify additional measuresyou could take to reduce or eliminate risks identified as medium or high risk in step 5. | | **Effect on Risk**  (choose from Eliminated, Reduced or Accepted) | **Residual Risk** | **Measure Approved**  Yes/No |
| **1** |  |  |  |  |
| **2** |  |  |  |  |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |
| **6** |  |  |  |  |
| **7** |  |  |  |  |
| **8** |  |  |  |  |
| **9** |  |  |  |  |
| **10** |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Step 7: Sign Off and Record Outcomes** | |  | **Notes** |
| Approvals | Name - Position | Date |  |
| Measures Approved by: |  |  | Integrate actions back into project plan, with date and responsibility for completion |
| Residual Risk Approved by: |  |  | If accepting any residual high risk, consult the ICO before going ahead |
| DPO Advice Provided by: |  |  | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO Advice: | | | |
| DPO Advice Accepted/Overruled by: |  |  | If overruled, you must explain your reasons |
| Comments: | | | |
| Consultation Responses Reviewed by: |  |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | | |
| DPIA kept under review by: |  |  | The DPO should also review ongoing compliance with DPIA |

|  |  |  |  |
| --- | --- | --- | --- |
| **Integration of Risk Mitigation Measures** | | | |
| **Decide who is responsible for the integration of the risk mitigation measures** which weredecided and agreed upon in step 6. Record the completion status. | | **Responsibility** | **Status**  (RAG) |
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |
| **4** |  |  |  |
| **5** |  |  |  |
| **6** |  |  |  |
| **7** |  |  |  |
| **8** |  |  |  |
| **9** |  |  |  |
| **10** |  |  |  |
|  |  |  |  |