**Data Protection Impact Assessment**

A Data Protection Impact Assessment (DPIA) is designed to evaluate and mitigate data protection risks associated with the collection, processing, and storage of personal data for new projects or processing activities. Conducting a DPIA helps to ensure compliance with data protection laws, such as the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR), by systematically assessing potential privacy impacts and identifying safeguards to protect individuals' rights.

This assessment will provide an overview of the data processing activities, assess associated risks, and outline measures to mitigate or minimise identified risks. The DPIA should be regularly reviewed and updated to reflect changes in processing activities, technologies, or regulatory requirements, ensuring continued data protection compliance and accountability.

|  |  |
| --- | --- |
| **Step 1: Project Details** | |
| Name of project/proposed activity |  |
| Description of proposed activity |  |
| Project Lead / Principal Investigator  (Name, Job Title) |  |
| Department Responsible |  |
| Background  *Explain what the project aims to achieve, what the benefits will be to the University, to individuals and to other parties.*  *Summarise why the requirement for a DPIA was identified i.e. which screening questions were selected.* |  |

|  |  |
| --- | --- |
| **Step 2: Describe the processing** | |
| What type of personal data will be involved?  *Personal data is any data from which living individuals can be identified, including pseudonymised data,* |  |
| Will the project involve  sensitive/special category personal data?  *Special Category personal data includes personal data revealing: racial/ethnic origin; political opinions; religious/philosophical beliefs; trade union membership; biometric/genetic data; health data; sexual orientation.*  *Other sensitive data may include criminal convictions data.* |  |
| Who does the personal data relate to?  *E.g. Research Participants, students, staff etc.*  Does this include children or other vulnerable groups?  How many individuals are affected? |  |
| How much data will you be collecting and using? |  |
| What is the source of the data? i.e. will information be collected directly from the data subject or via a third party?  Would the individual(s) expect you to use their data in this way? |  |
| What information will you give data subjects? E.g. Participant Information Sheet, Privacy Notice  How will you help to support data subjects’ rights?  Will they have the right to make a Subject Access Request?  Will you be able to delete their data if they make a request for erasure? |  |
| How will you store the data?  Who will have access to the data? |  |
| How long will you retain the data?  *Please see the* [*University's Records Management Policy & Schedule*](https://www.sheffield.ac.uk/library/records-management-policy-and-guidance) *for further guidance on retention periods.* |  |
| How will the data be destroyed when no longer required? |  |

|  |  |
| --- | --- |
| **Step 3: Data Sharing/Data Processors or International Transfers** | |
| Will you be sharing data with anyone outside of the University? |  |
| Which IT Systems or third parties will be used to store/share/process the data? |  |
| What is the current state of technology in this area? Is it novel in any way?  Are there prior concerns over this type of processing or are there any security flaws? |  |
| Will there be any international data transfers? If so, which country/countries will the data be transferred to? |  |
| What technical security measures will be in place?  Examples include:   * Encryption, firewalls etc * Anonymisation, encryption, data partitioning * Integrity checks, backups, workstation management, malware * Secure communications * Certifications such as ISO27001, Cyber Essentials |  |
| How will you ensure that they comply with these measures? |  |
| Do you have a contract/Agreement in place with any third-parties? If yes, please provide a copy. |  |

|  |  |
| --- | --- |
| **Step 4: Consultation Process** | |
| How will you seek individuals’ views? If you are not going to ask individuals for their views, then please justify why it is not appropriate to do so. |  |
| Who else do you need to involve within your organisation? |  |
| Have you consulted the University’s [Information Security Team](https://staff.sheffield.ac.uk/it-services/risk-assessments)? Do you plan to consult any other experts? |  |
| Have you recorded the processing activity on your department’s Information Asset Register? |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Step 5: Lawful Basis for Processing** | | | |
| **Article 6 UK GDPR – Personal Data** | | **Article 9 UK GDPR – Special Category Data** | |
| Article 6(1)(a) – Consent |  | Article 9(2)(a) – Explicit consent |  |
| Article 6(1)(b) – Contract |  | Article 9(2)(b) – Employment, social security & social protection\*\* |  |
| Article 6(1)(c) – Legal obligation |  | Article 9(2)(c) – Vital interests |  |
| Article 6(1)(d) – Vital interests |  | Article 9(2)(d) – Not-for-profit body |  |
| Article 6(1)(e) – Public task |  | Article 9(2)(e) – Made public by the data subject |  |
| Article 6(1)(f) – Legitimate interests\* |  | Article 9(2)(f) – Legal claims |  |
| *\* If you have selected Article 6(1)(f) – Legitimate interests as your lawful basis, you must complete the Legitimate Interests Assessment at Appendix 1 of this document (please see below).* | | Article 9(2)(g) – Substantial public interest\*\* |  |
| Article 9(2)(h) – Medicine, Employee capacity, Medical Diagnosis, Health or Social Care\*\* |  |
| Article 9(2)(i) – Public health\*\* |  |
| Article 9(2)(j) - Archiving, Scientific and Historical Research or Statistical Purposes\*\* |  |
| *\*\* If you have selected (b), (g), (h), (i), or (j) as your lawful basis, you also need to select a condition under* [*Schedule 1 of the Data Protection Act 2018*](https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted)*. Please specify which condition you have selected:* | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Step 6: Identifying, Assessing and Mitigating Risks** | | | | | | |
| **Risk** | **Likelihood** (Remote/ Possible/ Probable) | **Severity** (Minimal/Significant/Severe) | **Risk** (Low/Medium/High) | **Mitigation measure** | **Residual risk** | **Measure approved** (Yes/No) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **Step 7: Sign off and record outcomes** | |
| **Part A: DPIA Sign-off** | |
| DPIA Approved (Yes/No): |  |
| Name of Data Protection Team officer: |  |
| Date of approval/rejection: |  |
| Comments/summary of advice: |  |
| DPIA to be kept under review by (Name/Date of agreement to keep DPIA under review): |  |
| **Part B: Review of DPIA Sign-off** (for use where the processing activity described in the DPIA has not been approved) | |
| **DPO Review of DPIA** | |
| DPIA Approved (Yes/No): |  |
| Name: |  |
| Date of approval/rejection: |  |
| Comments/summary of advice: |  |
|  | |
| **SIRO Review of DPIA** | |
| DPIA Approved (Yes/No): |  |
| Name: |  |
| Date of approval/rejection: |  |
| Comments/summary of advice: |  |
|  | |
| **UEB Review of DPIA** | |
| DPIA Approved (Yes/No): |  |
| Date of approval/rejection: |  |
| Comments/summary of advice: |  |

**Appendix 1**

**Legitimate Interests Assessment**

**Please note: You only need to complete this Appendix if you have selected “Article 6(1)(f) – Legitimate interests” as your lawful basis in Step 5 above.**

|  |  |
| --- | --- |
| **Part A: Purpose Test – you need to assess whether there is a legitimate interest behind the processing** | |
| Why do you want to process the data? |  |
| What benefit do you expect to get from the processing? |  |
| Do any third parties benefit from the processing? |  |
| Are there any wider public benefits to the processing? |  |
| How important are the benefits that you have identified? |  |
| What would the impact be if you couldn’t go ahead with the processing? |  |
| Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements, or e-privacy legislation)? |  |
| Are you complying with other relevant laws? |  |
| Are you complying with industry guidelines or codes of practice? |  |
| Are there any other ethical issues with the processing? |  |

|  |  |
| --- | --- |
| **Part B: Necessity test – You need to assess whether the processing is necessary for the purpose you have identified** | |
| Will this processing actually help you achieve your purpose? |  |
| Is the processing proportionate to that purpose? Please explain why. |  |
| Can you achieve the same purpose without the processing? |  |
| Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way? |  |

|  |  |
| --- | --- |
| **Part C: Balancing Test – You need to consider the impact on individuals’ interests and rights and freedoms and assess whether this overrides your legitimate interests.** | |
| **Nature of personal data** | |
| Is it special category data or criminal offence data? |  |
| Is it data which people are likely to consider particularly ‘private’? |  |
| Are you processing children’s data or data relating to other vulnerable people? |  |
| Is the data about people in their personal or professional capacity? |  |
| **Reasonable expectations** | |
| Do you have an existing relationship with the individual? |  |
| What is the nature of the relationship and how have you used data in the past? |  |
| Did you collect the data directly from the individual? What did you tell them at the time? |  |
| If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? |  |
| How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? |  |
| Is your intended purpose and method widely understood? |  |
| Are you intending to do anything new or innovative? |  |
| Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation? |  |
| Are there any other factors in the particular circumstances that mean they would or would not expect the processing? |  |
| **Likely Impact** | |
| What are the possible impacts of the processing on people? |  |
| Will individuals lose any control over the use of their personal data? |  |
| What is the likelihood and severity of any potential impact? |  |
| Are some people likely to object to the processing or find it intrusive? |  |
| Would you be happy to explain the processing to individuals? |  |
| Can you adopt any safeguards to minimise the impact? |  |
| Can you offer the individuals an opt-out? (Yes/No) |  |

|  |  |
| --- | --- |
| **Making the decision: This is where you use your answers to Parts A, B and C to ascertain whether or not you can apply the legitimate interests basis.** | |
| Can you rely on legitimate interests for this processing? (Yes/No) | |
|  | |
| Do you have any comments to justify your answer (Optional)? | |
|  | |
| LIA completed by: |  |
| Date: |  |
| LIA approved by: |  |
| Date: |  |