**Data Protection Impact Assessment Form (DPIA) – Short Form**

This form should be completed after completing the DPIA - Screening Form. When submitting this form to the Data Protection Unit a copy of the Screening Form **must be attached**.

The purpose of completing a Data Protection Impact Assessment (DPIA) is to consider the risks and the potential harm that may arise both for the individuals concerned and the organisations involved. When considering your project please ensure that you are processing and sharing the minimal amount of personal data possible and ensure that the processing is fair, lawful and transparent. You must also ensure you have reasonable security measures in place to project the personal data you are processing.

Before completing this form please confirm the following:

| [ ]  I have read and understand the pertinent sections of the [Data Protection Guidance Handbook](http://www.stir.ac.uk/GDPR) (namely Section 11 – Data Protection Impact Assessments and Section 12 – Data Protection by Design and Default). |
| --- |

Please provide the information requested below (see sections in grey). The Data Protection Unit need to have a basic understanding of your overall project and more detailed information about how you will be processing personal data as part of that. Please try and keep your answers brief whilst addressing the points requested in the questions. It is your responsibility to complete the form with the required information. Once you have submitted the completed form to the Data Protection Unit (data.protection@stir.ac.uk), we will provide advice to assist you in progressing the form to being signed off.

|  |
| --- |
| **Project Title:** |
| **Name of responsible person:** |
| **Date form completed:** |

| **1) Project details** |
| --- |
| Provide a brief description in the box below of the project including an explanation of what the project aims to achieve (~half page, maximum one page). Your description should highlight those features that may have a potential impact on privacy. Your description should cover the following points (when you have completed your description please check the boxes to confirm these items have been covered in your text, or if it is not applicable record this):  |
| [ ]  A description of who the data subjects will be; or [ ]  Not Applicable[ ]  An estimation of the number of data subjects whose information will be processed; or [ ]  Not Applicable[ ]  Whether any vulnerable adults or children are involved; or [ ]  Not Applicable |
| Enter text here |

| **2) Justification, purpose and necessity** |
| --- |
| Please briefly explain why the processing is necessary, whether any alternative solutions have been considered, what the benefits of the processing are and what you hope to achieve that could not be achieved in other ways that did not involve the processing of personal data. |
|  |

| **3) Details of personal data** |
| --- |
| Please indicate what personal data will be collected/stored/processed. |
| *Administration data*[ ]  Name[ ]  Date of Birth/Age[ ]  Gender[ ]  Contact details[ ]  Unique identifier e.g. student number[ ]  Other data (please specify):*Special Categories of data (If you tick any of the boxes in this section please ensure you answer question 5 below)* [ ]  Racial or ethnic origin[ ]  Political opinion[ ]  Religious or philosophical beliefs[ ]  Trade Union membership [ ]  Physical or mental health condition[ ]  Sexual life and sexual orientation[ ]  Genetic data [ ]  Biometric data used to identify an individual*Other sensitive information* [ ]  Financial information/bank account details[ ]  Criminal convictions and offences *(If you tick this box please ensure you answer question 5 below)*[ ]  Other (please specify): |

| **4) Lawful Basis for processing (Article 6)** |
| --- |
| Under Article 6 of the [UK GDPR](https://www.legislation.gov.uk/eur/2016/679/contents) there needs to be a lawful basis for processing personal data. Further details about this are available in the University’s [GDPR Policy](https://www.stir.ac.uk/media/stirling/services/policy-and-planning/gdpr/documents/GDPRPolicy.pdf) (section iv). Having read the guidance please indicate the lawful basis that will apply to your project. If you need additional advice on this please speak to the Data Protection Unit (data.protection@stir.ac.uk) |
| [ ]  The individual who the personal data is about has given/will give unambiguous consent to the processing[ ]  The processing is necessary for the performance of a contract with the individual[ ]  The processing is necessary for a legal obligation[ ]  The processing is necessary for the vital interests of someone (i.e. life or death situation)[ ]  The processing is carried out in the public interests or in the exercise of official authority[ ]  The processing is in the legitimate interests of the University or another party and does not prejudice the rights and freedoms of the individual (if you select this option you must also complete a [Legitimate Interests Checklist](https://www.stir.ac.uk/about/professional-services/student-academic-and-corporate-services/policy-and-planning/legal-compliance/data-protectiongdpr/gdpr-policy-and-guidance/) and submit it with this form  |

| **5) Lawful Basis for processing special category or criminal conviction data (Article 9 or 10)** |
| --- |
| If you are processing ‘Special Category’ personal data or criminal conviction data (see question 3 above) you will require a separate lawful basis for processing this type of data under Article 9 of [UK GDPR](https://www.legislation.gov.uk/eur/2016/679/contents) and/or you will need to meet one of the conditions in Schedule 1 of the [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted). If this applies to your project we suggest you seek advice from the Data Protection Unit (data.protection@stir.ac.uk) to help identify a suitable condition of processing. |
|  |

| **6) Describe the Personal Data and Information flows** |
| --- |
| The collection, use and deletion of personal data should be described here. Where you have different groups of data subjects (e.g. staff and students) and their data will be handled in different ways please cover in your explanation the flows for each set of personal data. Your description should cover the following points (when you have completed your description please check the boxes to confirm these items have been covered in your text, or if it is not applicable record this): |
| [ ]  Explain where your personal data is coming from (new data or existing data); or [ ]  Not Applicable[ ]  How the data will be collected or obtained; or [ ]  Not Applicable[ ]  How the data will be stored securely; or [ ]  Not Applicable[ ]  What systems will be used; or [ ]  Not Applicable[ ]  How long the data will be retained for; or [ ]  Not Applicable[ ]  How will personal data be disposed of when no longer required; or [ ]  Not Applicable[ ]  Who will have access to the data; or [ ]  Not Applicable[ ]  What security measures will be in place; or [ ]  Not Applicable[ ]  Explain what third parties will have access to the data and confirm suitable contracts are in place; or [ ]  Not Applicable[ ]  Explain the context of any questions on the Screening Form which were marked as ‘Yes’; or [ ]  Not Applicable[ ]  Any other relevant information; or [ ]  Not Applicable |
| Enter text here |

| **7) Transparency, Privacy Notices and Consent** |
| --- |
| Please explain what arrangements will be put in place to inform individuals what you are planning to do with their personal data or get their consent. This will normally involve providing a privacy notice directly to the data subjects (see the [privacy notice template](https://www.stir.ac.uk/about/professional-services/student-academic-and-corporate-services/policy-and-planning/legal-compliance/data-protectiongdpr/gdpr-policy-and-guidance/) for guidance) or ensuring that your proposed activity is already covered within the scope of the University’s existing [privacy notices](https://www.stir.ac.uk/about/professional-services/student-academic-and-corporate-services/policy-and-planning/legal-compliance/data-protectiongdpr/privacy-notices/alumni-and-supporters/). If the lawful basis for processing personal data is consent (see section 4) please explain how you will be obtaining and recording consent. |
|  |

| **8) Identification of privacy and related risks and solutions** |
| --- |
| In this section you should identify the key privacy risks and associated compliance and corporate risks. Examples of risks are outlined below but they may or may not be relevant to your project. Please consider your project carefully to identify what risks should or should not be included and amend the grey text accordingly. In addition, there may be specific risks not mentioned below that require consideration. Risks could result in unnecessary intrusion on privacy, risks to physical safety, financial loss or distress caused.Privacy legislation for consideration may include:The Data Protection Act 2018 and UK General Data Protection Regulation (GDPR) – Regulate the processing of personal data – i.e. information about living identifiable individualsPrivacy and Electronic Communications Regulations 2003 (PECR) - Regulates electronic direct marketing e.g. email and text messagesHuman Rights Act 1998 – Individual’s right to respect for their private and family life, their home and correspondence.The Common Law Duty of ConfidenceYou should also identify solutions and thereafter balance the project’s outcomes with the impact on individuals. Whilst some risks might be eliminated altogether, other risks might be reduced and it may be appropriate to recognise and accept the risks. Each residual risk should thereafter be evaluated against the likelihood of harm to individuals and the severity of possible harm. |
| **Privacy issue/ Risk** | **Risk to individuals** | **Compliance/ organisation/ corporate risk (see table at the end of the form for examples of relevant privacy legislation)**  | **Solutions and actions to be taken** | **Evaluation of residual risks after implementing solutions** |
| **Likelihood of harm to individuals:****1 - Rare****2 - Unlikely****3 - Moderate****4 - Likely****5 - Almost Certain** | **Severity of harm:****A - Insignificant****B - Minor****C - Moderate****D - Major****E - Extreme** |
| Compliance with the data subject's right to be informed | The individuals will not be aware of how their personal data will be processed, who it will be shared with etc | Potential to breach the first data protection principle of ‘lawfulness, fairness and transparency’/reputational risk/financial risk | Explain how you will be informing the data subjects what will be happening with their personal data i.e. have you got privacy notice relating to the project. What are your arrangements for getting consent where required. |  |  |
| Personal data is used for a purpose which is incompatible with the purpose it was originally collected for. e.g. existing data is being used for a new purpose or there is a risk that data collected is used in a way that data subjects would not expect | The individuals will not be aware of how their personal data will be processed | Potential to breach the second data protection principle ‘purpose limitation’. This will result in potential reputational risk/financial risk to the University. | Explain what measures will be taken to prevent data being used for a purpose not outlined in the privacy notice. For data obtained from a different project or organisation will the individuals be re-contacted to explain how their information will be re-used?  |  |  |
| There is a risk that more personal information is gathered or held as part of the project than is actually needed.  | More information is collected from individuals than is required. This could lead to stress of the individuals concerned.  | Potential to breach the third data protection principle ‘data minimisation’. This will result in potential reputational risk/financial risk to the University | Explain the measures that will be taken to ensure only the minimal data is collected and what data minimisation techniques will be implemented such as anonymisation.  |  |  |
| The personal data held is inaccurate | Risk of holding incorrect data potentially leading to inaccurate conclusions or decision to be taken. | Potential to breach the fourth data protection principle ‘accuracy’. This will result in reputational risk/financial risk to the University. | Explain what processes will be in place to ensure data is accurate and kept up to date? For instance allowing data subjects to access their own data on a system to keep information up-to-date? |  |  |
| Personal data is held for longer than is necessary in breach of the storage limitation and data retention principle. | Personal information held by the University for longer than is needed causes distress to the individuals concerned. | Potential to breach the fifth data protection principle ‘storage limitation’ This could result in reputational risk/financial risk to the University. | Explain what the retention timescales will be and what methods will be used to delete or destroy data when it is no longer required? Confirm this information is in the privacy notice. |  |  |
| Personal data is not held securely. Confidentiality, integrity and availability of personal data. | The information is not held securely and is breached. This could lead to people having access to the information who should not have access putting the security of individuals at risk. | Potential to breach the sixth data protection principle ‘integrity and confidentiality’. This could result in a data breach and resultant reputational risk/financial risk to the University. | Outline here all the controls in place to safeguard the personal data against a data breach. For example, relevant training for people accessing the data, access controls, password protection, encryption, pseudonymisation/ anonymisation, storage location, locking procedures, details of how the personal data will transmitted/shared.  |  |  |
| Third parties having access to the personal data | Measures are not in place to protect the security of personal data when it is passed to third parties.  | Potential breach of Articles 24-43 (Controller and Processor responsibilities) | Are data processing contracts/data sharing/service agreements in place to assign responsibilities and liabilities?  |  |  |
| International Transfers. Personal data is transferred to a recipient outside of the UK/EU/EEA and located within a country that may not have adequate data protection laws. | The security of personal data could be put at risk as a result of the transfer leading to a risk for the individuals concerned. | Potential breach of Article 44 relating to transfers of personal data to third countries.  | Explain what safeguards are in place to meet the requirements for transferring data internationally, e.g. having an International Data Transfer Agreement (IDTA) in place. |  |  |
| Complying with data subject rights including subject access requests | There is a risk that individuals will not be able to exercise their rights such as right to access, rectification, erasure, portability and right to object. | Potential breach of the data subject rights Articles 15-23 | What measures are in place to ensure rights request could be handled, for instance extracting information relating to an individual from a system or deleting their information if it was no longer required. |  |  |
| Complying with Direct Marketing consent requirements | Correct consent is not obtained from individuals when their data is being used for direct marketing purposes. | Breach of Privacy and Electronic Communications Regulations (PECR) | Explain how you will obtain and record consent if you are contacting people electronically for marketing or promotional purposes. |  |  |
| Consider your own project and add additional risks as appropriate  |  |  |  |  |  |
| Add further risks here |  |  |  |  |  |
| Add further risks here |  |  |  |  |  |
| Add further risks here |  |  |  |  |  |

| **9) Sign Off** |
| --- |
| The proposed solutions to the risks identified above must be approved by a colleague who is ideally familiar with the project or well placed to assess whether the solutions are appropriate. This could be a senior colleague or peer who is familiar with the project.[ ]  The proposed solutions have been reviewed and agreed by an appropriate colleagueName:Position: |
| The Responsible Person for the project needs to confirm they will implement the agreed solutions and actions as specified in the risks section above.[ ]  I confirm that I will implement the agreed solutions and actionsName:Position: |
| To be completed by the Data Protection Unit. The Data Protection Unit has reviewed this submission and believes that the proposed actions appear to be reasonable based on the information provided. We will retain a copy of this form for our records.Name:Date: |

In the event that any aspect of the project changes then the form should be updated and resubmitted

Please submit a copy of the completed form to the Data Protection Unit at data.protection@stir.ac.uk

| **For Office Use only:** |
| --- |
| Overall Risk rating:IS consulted:Others consulted:LIA checklist submitted if required |

**Assessment of Overall Project Risk (for office use)**

|  |  | **Likelihood of harm** |
| --- | --- | --- |
|  |  | **1** | **2** | **3** | **4** | **5** |
| **Severity of Harm** | **Rare** **(<10%)** | **Unlikely** **(10-30%)** | **Moderate** **(31-50%)** | **Likely** **(51-80%** | **Almost Certain** **(> 80%)** |
| **A** | **Insignificant** | Low | Low | Low | Low | Moderate |
| **B** | **Minor** | Low | Low | Moderate | Moderate | High |
| **C** | **Moderate** | Low | Moderate | Moderate | High | High |
| **D** | **Major** | Low | Moderate | High | Critical | Critical |
| **E** | **Extreme** | Moderate | High | Critical | Critical | Critical |

Overall risk rating is based on the highest individual risk identified in section 8.