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

This form should be completed after completing the [DPIA - Screening Form](https://www.stir.ac.uk/about/professional-services/student-academic-and-corporate-services/policy-and-planning/legal-compliance/data-protectiongdpr/gdpr-policy-and-guidance/). 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).  I understand the difference between anonymised or pseudonymised data (see section 6 and 12 of the [Data Protection Guidance Handbook](http://www.stir.ac.uk/GDPR)). (You are only required to tick this box if you are using anonymised or pseudonymised data.) |

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](mailto: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, there is no need to repeat the information provided in the project summary on the Screening Form. You may find it helpful to refer to other documents such as a project proposal. 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  What is the nature of the relationship with the data subjects; or  Not Applicable  What geographical area is covered; or  Not Applicable  Will there be any risk of physical harm to the data subjects; 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. What is the intended effect on the individuals? |
|  |

| **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](mailto: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 from |

| **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](mailto: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  Will people be compelled to provide personal data and if so why; or  Not Applicable  How the data will be stored securely; or  Not Applicable  How will you ensure data quality and data minimisation; 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  Whether you will be carrying out any data matching using data from different sources; or  Not Applicable  How will you support data subject rights; or  Not Applicable  How will you safeguard any international transfers; or  Not Applicable  What control will the data subjects have over the processing of the data; 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) Third parties** |
| --- |
| Please list any third parties you will be sharing personal data with or who will be sharing personal data with you e.g. service providers, transcribers, partners, collaborators, software providers, videographers or others. |
| Enter text here |
| If you have specified any third parties above please confirm you have relevant contracts or agreements in place. For instance   * A data processing contract is required if a third party is processing data on our behalf such as an external transcriber, external photographer, service provider such as online services or survey providers. * A data sharing agreement should be in place for collaborators and partners with whom we are sharing personal data or who are sharing personal data with us. * A service contract that covers data protection issues (such as terms and conditions for online service providers)   Further advice can be obtained from [contracts@stir.ac.uk](mailto:contracts@stir.ac.uk) |
| I confirm that I have the appropriate contracts or agreements in place; or  Not Applicable |

| **8**) **Technology** |
| --- |
| If you are using new technology or technology which might be perceived as being privacy intrusive please provide details. For example the using of biometrics, facial recognition, monitoring via CCTV, tracking of individuals online or offline, automated decision making or profiling. |
|  |

| **9) 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. |
|  |

| **10) Consultation** |
| --- |
| Describe when and how you will seek individuals’ views - or justify why it is not appropriate to do so. Who else will be consulted internally or externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. If your project involves the use of information technology systems or software that accesses or makes use of the University’s network that has not previously been used by the University, you must consult with Information Services ([information.centre@stir.ac.uk](mailto:information.centre@stir.ac.uk)). This refers to both systems or software hosted on site within the University services or in the cloud (external provider). |
| I confirm that I have consulted IS about the use of new information technology systems or software; or  Not Applicable |
| Enter text here |

| **11) 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 (UK GDPR) – Regulate the processing of personal data – i.e. information about living identifiable individuals  Privacy and Electronic Communications Regulations 2003 (PECR) - Regulates electronic direct marketing e.g. email and text messages  Human Rights Act 1998 – Individual’s right to respect for their private and family life, their home and correspondence.  The Common Law Duty of Confidence  You 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, is the activity covered by an existing privacy notices (such as the staff or student notice) or will an existing privacy notice be amended to take account of the new activity. Could the processing be considered unfair or unexpected by the data subjects? Are there special arrangements in place to ensure young children and vulnerable adults are informed. Include links to the privacy notices of third-party sites or other organisations that will be involved during the project. |  |  |
| Personal data is used for a purpose which is incompatible with the purpose it was originally collected for. | Personal Information that is collected or processed during the project is used for a purpose other than the purpose stated in the privacy notice and therefore the data subjects are not aware of how their personal information is being used. Alternatively, personal data is being used that was originally collected for a different project or another organisation and is now being used for a new project | Potential to breach the second data protection principle ‘purpose limitation’. This will result in potential reputational risk/financial risk to the University. | Is there any risk of personal data being used in a way that was not originally intended? If so, explain what measures will be taken to prevent the people who have access to the data from using data for a purpose no 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 | Is there a possibility that more information will be gathered, processed or stored than is actually needed? If less information held then this reduces the risks in the event of a breach. Data minimisation techniques include anonymisation, pseudonymisation, deletion, collection minimisation, user access controls etc. In your response explain the measures that will be taken to ensure only the minimal data is collected and what data minimisation techniques will be implemented. If you are using audio or visual recordings how are you ensuring you don’t record information about other people? |  |  |
| The personal data held is inaccurate | Risk of University holding incorrect data about a data subjects 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. | Are there any risks of data being or becoming inaccurate? For instance, the risks of inaccuracies are higher when data matching is taking place or during longitudinal studies over a period of time. What processes will be in place to ensure data is accurate and kept up to date? Are there ways the data subjects can 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. | What measures are in place in relation to retention of data? Are retention timescales outlined in the privacy notice? At what point in the project will personal data be pseudonymised/anonymised? Please list the retention timescales of separate categories of personal data. What methods will be used to delete or destroy data when it is no longer required? |  |  |
| Personal data is not held securely. Confidentiality, integrity and availability of personal data. | The information is not held securely and is breached. This leads to the danger that people have access to this personal information who should not have access to it, either internally or externally and puts 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. | How are you keeping the personal data secure? Outline here all the controls in place to safeguard the personal data against a data breach. For example, relevant training for the people who have access to the personal data, access controls, password protection, encryption, pseudonysation/ anonymization of data, storage location, locking procedures, details of how the personal data will transmitted/shared. Will portable devices be used? Will personal devices be used? Is the information deemed particularly desirable or useful to someone? |  |  |
| 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) | How is the access by third parties being controlled? Are data processing contracts/data sharing/service agreements in place to assign responsibilities and liabilities? Have terms and conditions been reviewed by the University or data subjects? |  |  |
| International Transfers. Personal data is transferred to a recipient outside of the UK/EU/EEA and located within a country that may not be viewed as having adequate data protection laws by the European Commission. | 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. | Are you transferring data outside of the UK/EU/EEA? This can include the use of some cloud-based services. Have you checked the terms and conditions/privacy notices for any services being used to ensure data will not be transferred outside the UK/EU/EEA? ? What safeguards are in place/do we have an International Data Transfer Agreement (IDTA) in place? Are data subjects aware? |  |  |
| Data matching. Data from more than one source is being matched | There is an increased risk of creating inaccuracies in the data if the data has been matched from more than one source | Potential to breach the fourth data protection principle ‘accuracy’. This will result in reputational risk/financial risk to the University. | What safeguards are in place to ensure data accuracy of original files and the data matching process? |  |  |
| Complying with subject access requests | There is a risk that individuals will not be able to access the information about themselves that they are entitled to access | Potential breach of the Article 15 ‘Right of access by the data subject’ | What measures are in place to ensure a subject access request could be handled? How would information relating to an individual be identified and extracted in an accessible format? Will it be possible to handle a subject access request within a short time period? Will it be possible for users to access their own information on a system? |  |  |
| Complying with other data subject rights | There is a risk that we are not able to comply with data subject rights such as right to rectification, right to erasure (right to be forgotten), right to restrict processing, right to data portability, right to object. | Potential breach of data subject rights in Articles 16 to 23 | What procedures will be in place to ensure we could handle a data subject rights request? What would happen if someone asked for the information about them to be corrected, deleted or transferred to a different organisation? What would happen if an individual said they did not want their personal information processed in the proposed way? |  |  |
| 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) | If you are contacting individuals directly for marketing or promotion purposes via electronic means i.e. email, telephone, text, what measures do you have in place to obtain their consent? How is a record of the consent kept? Is the consent broken down so they can opt-in or out of different forms of communication? Do you continue to give them options to opt-out on all future communications? |  |  |
| Consider your own project and add additional risks as appropriate e.g. additional risk associated with audio/visual recordings, vulnerable people, use of portable devices, training, other risks highlighted by the questions on this form or the screening form etc. |  |  |  |  |  |
| Add further risks here |  |  |  |  |  |
| Add further risks here |  |  |  |  |  |
| Add further risks here |  |  |  |  |  |

| **12) 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 colleague  Name:  Position: |
| The Responsible Person for the project needs to confirm they will ensure the implementation of the agreed solutions and actions as specified in the risks section above. Where appropriate outcomes are integrated back into the project plan.  I confirm that I will implement the agreed solutions and actions  Name:  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](mailto: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 11.