# Data Protection Impact Assessment

A close up of a logo

Description automatically generated

|  |  |
| --- | --- |
| **Project name:** |  |
| **Project Lead:** |  |
| **DPIA Author:** |  |
| **Date created:** |  |

*You may be unfamiliar with some terms used within this document, therefore we have included a link to some key terms definitions* [*here*](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/)*.*

|  |
| --- |
| Step 1: Identify the need for DPIA |
| 1.1 Describe what the project aims to achieve and what things you will need to do with personal data, in order to achieve those aims. |
|  |
| 1.2 You may find it helpful to link to other relevant documents related to the project, for example a project proposal (Identify other documents here). |
|  |
| 1.3 Summarise why the need for DPIA was identified (Can draw on your answers from the screening question). |
|  |

|  |  |
| --- | --- |
| Step 2: Describe the Processing: What is it you will be doing that involves working with people’s personal data? | |
| *2.1 Describe the nature of the processing:* | |
| 1. How will you collect, use, store and delete data? |  |
| 1. What is the source of data? |  |
| 1. Will you be sharing personal data with anyone?  Please provide their address and say why you will need to share personal data with them. |  |
| *2.2 Describe the scope of the processing:* | |
| 1. What type of personal data (categories) will be collected and used?  E.g. Name; age; gender; geographical information; ID numbers; and online identifiers (ISP, cookies) |  |
| 1. Will it involve special or sensitive categories of data? This data will require more protection.  E.g. Racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; health; sex life; and sexual orientation. |  |
| 1. How much personal data will you collect (how many people), how frequently, what geographical area does it cover? |  |
| 1. How long will you keep the data and what will happen to it at the end of its use? |  |
| 1. What will happen to the data when it is no longer needed |  |
| 2.3 Describe the context of processing: | |
| 1. What is your relationship with the individuals whose data you will be using? |  |
| 1. Do they know how their data will be used and how much control will they have? |  |
| 1. Will you be processing data about children or other vulnerable groups? |  |
| 1. Has this, or similar processing been done before? Are there similar technologies already in use |  |
| 1. What is the current state of technology in this area? |  |
| 1. Are there any current issues concerning this type of processing or use of technologies to enable the processing that you should factor in? |  |
| 2.4 Describe the purpose of processing the personal data: | |
| 1. What do you want to achieve, and could it be achieved without using personal data? Why? |  |
| 1. What is the intended effect on individuals? |  |
| 1. What are the benefits of processing for you and more broadly? |  |

|  |  |
| --- | --- |
| Step 3: Consultation Process | |
| 3.1 Consider how to consult with relevant stakeholders: | |
| 1. Describe when and how you will seek individuals’ views – or justify why its not appropriate to do so. |  |
| 1. Who else do you need to involve within Loughborough University? |  |
| 1. Do you need to ask any of your Data processors to assist? And if so, who? |  |
| 1. Do you plan to consult information security experts or anyone else? |  |

|  |  |
| --- | --- |
| Step 4: Assess necessity and proportionality | |
| * 1. Describe compliance and proportionality measures, in particular: | |
| 1. What is your lawful basis for processing? Here is a [link](https://www.lboro.ac.uk/data-privacy/iwantto/checkthesixlawfulbasesforprocessingpersonaldata/) to the 6 lawful bases for processing personal data. |  |
| 1. Does the processing this data actually achieve your overall purpose? |  |
| 1. How will you prevent function creep (using the data for other purposes)? |  |
| 1. How will you ensure data quality? |  |
| 1. What information will you give individuals? |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Step 5: Identify and assess risk | | | |
|  |  | | | |
| Ref | **Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.** Consider the potential impact on individuals and any harm or damage your processing may cause – whether physical, emotional or material  *Examples: it is not possible to manage access to personal data, highly sensitive personal data is made publicly available, Individuals might be re-identifiable, project is capturing more data than is necessary for its purpose, individuals are unable to exercise their data protection rights, personal data is kept indefinitely without a lawful reason, individuals may target the data for malicious uses, data subjects would not expect their data to be used for the purpose intended by the project, or it would require the University to give up control of the personal data.* | **Likelihood of harm**  Probable: 3  Possible: 2  Remote: 1 | **Severity of harm**  Severe: 3  Significant: 2  Minimal: 1 | **Overall Risk**  Likelihood x severity  High = >6  Medium = 4-6  Low = <4 |
| *01* | *EXAMPLE: Data Subjects not expecting data to be processed in this way* |  |  |  |
| *02* | *EXAMPLE: The system not being used for the intended purpose* |  |  |  |
| *03* | *EXAMPLE: Collect more personal data than necessary for the specified purpose* |  |  |  |
| *04* | *EXAMPLE: University does not routinely obtain a signed form from the individual consenting to the collection and use of their personal data.* |  |  |  |
| *05* | *EXAMPLE: Staff may share personal data with other organizations or authorities over which they have no control regarding how the other organizations or authorities may use that data or further share it.* |  |  |  |
| 06 | *EXAMPLE: Data breach* |  |  |  |
| 07 | *EXAMPLE: Data Subjects not expecting data to be processed in this way* |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Step 6: Identify measures to reduce risk | | | | |
|  | Identify additional measures you could take to reduce or eliminate risks identified as Medium or High risk in Step 5. | | | | |
| Ref | Risk (Insert risk mentioned in Step 5) | Option to reduce or eliminate risk  Possible measure could include:   * *deciding not to collect certain types of data;* * *reducing the scope of the processing;* * *reducing retention periods;* * *taking additional technological security measures;* * *training staff to ensure risks are anticipated and managed;* | Effect on Risk  Eliminated, Reduced or Accepted | Residual risk  Low, Medium or High | Measure approved: Yes/No |
| *01* | *EXAMPLE: Data breach* | *Password protected files and only use SharePoint / workspaces. Ensure all accesses to the databases are logged into a register of processing operations. Set-up data breach notification procedures to inform the data subjects.*  *Encourage (warn) employees to avoid use of unsecured portable storage devices, such as memory sticks* |  |  |  |
| *02* | *EXAMPLE: Data Subjects not expecting data to be processed in this way* | *Clear privacy notices with use and clear pathways to opt out open to all parties* |  |  |  |
| *03* | *EXAMPLE: The system not being used for the intended purpose* | *A university wide/Partnership statement of purpose and an open door policy for users to report instances of the system being used in a way which is not aligned with purpose.* |  |  |  |
| *04* | *EXAMPLE: Collect more personal data than necessary for the specified purpose* | *Ensure the staff collects only the pieces of data which are necessary to achieve the purpose specified originally.* |  |  |  |
| *05* | *EXAMPLE: University does not routinely obtain a signed form from the individual consenting to the collection and use of their personal data.* | *Attempt, where possible, to get a signed informed consent form.*  *Ensure that the consent form is available in an appropriate range of languages for the target group.* |  |  |  |
| 06 | *EXAMPLE: Staff may share personal data with other organizations or authorities over which they have no control regarding how the other organizations or authorities may use that data or further share it.* | *Share personal information with other organizations or authorities only if a specific legal basis exists (consent, public interest etc.) Additionally, share personal information with other organizations or authorities only if there is an approved sharing agreement and if they observe adequate data protection such as high level training with Staff, do they clearly state staff expectations, is data kept encrypted* |  |  |  |
| 07 | *EXAMPLE: Data breach* | *Password protected files and only use SharePoint / workspaces. Ensure all accesses to the databases are logged into a register of processing operations. Set-up data breach notification procedures to inform the data subjects.*  *Encourage (warn) employees to avoid use of unsecured portable storage devices, such as memory sticks* |  |  |  |