

**Data Protection Impact Assessment**

## 

|  |  |
| --- | --- |
| **Name of Project/Initiative** |  |
| **Institute/Service** |  |
| **Project sponsor** |  |

**Step 1: Summary of the Project or Initiative**

|  |
| --- |
| Explain broadly what the project aims to achieve and what type of processing it involves. Include any high risk processing identified in the screening questions. You may find it helpful to refer to or link to other documents, such as a project proposal |
|  |

**Step 2: Describe the nature of the processing:**

|  |  |
| --- | --- |
| **Nature of the processing** | |
| **How will the data be collected?** E.g. online, forms completed by data subjects, other systems etc. |  |
| **What is the source of the data?**  E.g. third parties, other individuals |  |
| **What will be done with the data be after it is collected?** How it will be processed e.g. stored, transferred, used, and delete data – including any temporary storage and systems e.g. hardware, software, networks and paper systems that will be used |  |
| **Will it be combined with other data sets?** If so to what extent? |  |
| **Will data be shared with third parties**? If so, provide an explanation including details of the data flows, sharing/data processing agreements which will be in place |  |
| **Will there be any automated decision making?** If so describe the extent e.g. use of automated algorithms without human intervention. |  |
| **Scope of the processing:** | |
| **Categories of personal data-** identify each category processed including special category or criminal offences data |  |
| **Categories of data subjects** e.g**.** staff students, research participants, device users etc. Include geographical area or location of data subjects |  |
| **Storage location** e.g. cloud hosted services, UK, EU, storage devices etc. |  |
| **Duration and frequency of processing** e.g. How long it will be retained in an identifiable format and how often it will be collected |  |
| **Volume of data** - Approximate number of data subjects and volume of records |  |
| **Context of the processing** | |
| **Relationship with the data subjects-** how was the relationship with the University established |  |
| **Data subjects’ expectations-** are they aware of this processing and do they expect their data to be used this way, or feel that the processing is intrusive? |  |
| **Matters of concerns** – e.g. public concerns, security flaw, processing highly sensitive or private information. |  |
| **Use of new technology or novel approach-** describe the extent to which it involves new technology or novel a approach |  |
| **Purposes of the processing:** | |
| **Benefits to the University-** direct or indirect |  |
| **Benefits to data subjects-** direct or indirect |  |
| **Benefits to the third parties -** direct or indirect |  |

**Step 3: Consultation process**

|  |  |
| --- | --- |
| **Consider how to consult with relevant stakeholders:** | |
| **Internally stakeholders** e.g. IT and security, ethics, senior staff etc. |  |
| **Advice from** [**Data Protection Officer**](mailto:gdpr@cumbria.ac.uk?subject=DPIA)  This is mandatory |  |
| **Externally:**  Suppliers, partners, regulators |  |
| **Data Subjects** |  |

**Step 4: Assess necessity and proportionality**

|  |  |
| --- | --- |
| **Compliance and proportionality measures** | |
| **Lawful basis for processing**  Identify the most appropriate lawful reason for processing (refer to the [ICO Guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#what))  An additional assessment is needed if Legitimate interests is the identified lawful basis.  If you are processing [special category data](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/#scd1) and [addition condition](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/#scd3) is needed. | Consent  ​​​Contract  ​​Legal obligation  ​​Vital Interests  ​​​Public Task  ​​​Legitimate interests  Consent  Employment  Legal claims  Substantial Public interests  *Include the relevant substantial public interest conditions*  Statutory and government purposes  Equality of opportunity or treatment Preventing or detecting unlawful acts Protecting the public  Regulatory requirements Support for individuals with a particular disability or medical condition Safeguarding  Archiving, research, or statistical purposes in public interest |
| **Fairness and Transparency**  Describe how data subjects will be informed about the intended processing e.g. privacy notice, privacy statement, consent form, participant information sheets |  |
| **Data minimisation**  Describe how the amount of personal data will be limited to only what is necessary |  |
| **Necessity**  Explain why the processing is necessary and cannot be achieved in another way |  |
| **Accuracy**  Describe how accuracy and bias will be prevented e.g. verification, updating of data etc. |  |
| **Storage limitation**  Describe steps that will be taken to make sure that personal data will not be held longer than necessary for the intended purpose |  |
| **Security, integrity and confidentiality**  Describe steps that will be taken to make sure that personal data is secure, including at rest and in transit, including protection against any [personal data breaches](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatisa) |  |
| **Data subject rights**  How will you help to support their rights? |  |
| **Third party processors**  Where relevant describe measures taken to ensure that third parties processing personal data on the University’s behalf comply with data protection e.g. certification, IT assessment, checking their policies or privacy notices etc. |  |
| **International transfers**  Identify any transfers of personal data outside the UK and steps taken to safeguard them e.g. Standard Contractual Clauses, adequacy status |  |

**Step 5: Identify and assess risk**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk no.** | **Source of risk and potential impact on data subjects.** Include associated compliance and corporate risks | **Likelihood score** | **Severity score** | **Overall score** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |

**Step 6: Identify measures to reduce risk**

|  |  |  |  |
| --- | --- | --- | --- |
| **Additional measures to reduce or eliminate risks identified as medium or high risk in step 5** | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk**  Eliminated, reduced or accepted | **Residual risk**  any remaining risk |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |

**Step 7: Implementation of measures and controls**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Action** | **Assigned to** | **Due date** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |

**Step 8: Outcomes and Sign off**

|  |  |  |  |
| --- | --- | --- | --- |
| **Additional measures to reduce or eliminate risks identified as medium or high risk in step 5** | | | |
| **Residual risk**  (if any) and outcome of ICO consultation is applicable |  | | |
| **Data Protection Officer’s advice**  (Confirm if advice was accepted and implement or rejected and why) |  | | |
| **DPO comments** |  | **Date** |  |
| **Review date** |  | **Reviewer** |  |

## **Risk Assessment**

**Evaluation of Likelihood of harm (L)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Score & rating | 1  Very unlikely | 2  Unlikely | 3  Possible | 4  Likely | 5  Almost certain |
| Frequency | Will probably never happen | Not anticipated to happen but possible | Might happen more than once | Will probably happen | Will happen possibly frequently |

**Evaluation of Impact of harm (I)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Impact Score | 1  Insignificant | 2  Low | 3  Medium | 4  Significant | 5  Major impact |
| Impact | Unlikely to have an impact | May have an impact | Likely to have an impact | Most likely to have significant impact | Will have a major impact |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Likelihood** | 5  Almost certain |  |  |  |  |  |
| 4  Likely |  |  |  |  |  |
| 3  Possible |  |  |  |  |  |
| 2  unlikely |  |  |  |  |  |
| 1  Very unlikely |  |  |  |  |  |
|  |  | 1  Insignificant | 2  Low | 3  Medium | 4  Significant | 5  Major i |
|  |  | **Impact** | | | | |

**Overall Risk = L x I**