

**Data Protection Impact Assessment (DPIA) relating to:**

**[Title of Initiative/project/process/study/system etc]**

DPIAs should be sent to the Information Governance Team at **data-protection@bristol.ac.uk**

DPIAs produced as part of the IT Services new service assessment procedure, or with an IT element, should also be send to the Information Security Team at**cert@bristol.ac.uk**

**Document control**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Summary of changes** | **Approver** | **Approval date** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| **Part A: Summary of the Initiative** |
| **Describe the scope of the Initiative** (to include its aims and objectives; business/research/other case; level of investment in terms of time, financial and other resources; duration and geographic reach; visibility within and outside the organisation) |
|  |
| **Status of the Initiative** (describe the current phase of development or implementation of the Initiative or, if the Initiative has already commenced, when it commenced and the extent to which the processing activities relating to the Initiative are still ongoing)  |
|  |
| **Part B: Description of the processing** |
| **Nature of the processing**  |
| **Method(s) of collection** (e.g. online or paper-based forms completed by data subjects or feeds from other systems)  |  |
| **Source(s) of the personal data being processed** (if personal data originates from third party sources, describe them) |  |
| **Matching or combination of datasets** (to what extent does the processing involve multiple datasets collected for separate purposes) |  |
| **Processing activities relating to the personal data** (how will personal data be processed after collection) |  |
| **Scope of data sharing with third parties** (you may want to refer to a data flow diagram or other materials explaining data flows)  |  |
| **Extent of automated decision-making** (describe extent to which decisions are made about data subjects without human intervention/review, e.g. through the use of automated algorithms) |  |
| **Scope of the processing** |
| **Categories of personal data** (identify each category of personal data processed, including any special category data and information relating to criminal convictions and offences) |  |
| **Categories of data subject** (e.g. staff, students, research participants, website visitors, device users, children, vulnerable adults) |  |
| **Format of the personal data** (e.g. paper records, electronic documents, spreadsheets, databases, system records or other files) |  |
| **Storage location** (e.g. locked filing cabinets, document repositories, on-premise servers or storage devices, cloud-hosted services in UK, EU or international) |  |
| **Duration and frequency of processing** (by reference to the relationship with the data subject or the nature of the Initiative) |  |
| **Volume of data subjects and records** (or an approximation where it is not possible to confirm precise numbers at present) |  |
| **Context of the processing** |
| **Relationship with data subjects** (describe the proximity between the University and the data subjects and how the relationship is established) |  |
| **Data subjects’ expectations** (describe the extent to which the data subjects are aware of and expect their personal data to be used in connection with the proposed processing activities)  |  |
| **Use of new technology or novel approach** (describe the extent to which the processing activities involve the use of any technology or other approaches that may be considered state of the art, novel or unexpected) |  |
| **Relevant matters of public concern** (describe any matters of public concern relating to the scope of the processing or the use of any particular technology or approach, if applicable) |  |
| **Purposes of the processing** |
| **Benefits to the data subject** (describe how the processing benefits the data subjects/individuals either directly or indirectly) |  |
| **Benefits to the organisation** (describe how the processing benefits the organisation either directly or indirectly) |  |
| **Benefits to third parties** (describe how the processing benefits any third parties either directly or indirectly) |  |
| **Part C: Consultation process** |
| **Input of internal stakeholders, experts and other professionals** (advice from parties including senior staff, specialists, IT experts, lawyers, security consultants, ethics advisers etc, where applicable) |  |
| **Advice from Data Protection Officer** (where applicable, obtaining the advice of the DPO is a mandatory requirement – this may be set out in a separate appendix/document) |  |
| **Input from data subjects (or their representatives)** (where relevant describe the views sought, consultation methodology or justification for not seeking input) |  |
| **Part D: Assessment of necessity and proportionality** |
| **Lawful basis for processing** (identify the most appropriate ground(s) for lawful processing, explaining the rationale - see Appendix 3 for permissible grounds. For legitimate interests a separate legitimate interest assessment is needed.) |  |
| **Fairness and transparency** (describe the means by which data subjects will be informed about the intended processing, e.g. fair processing notices, technical notifications, consent forms, participant information sheets) |  |
| **Data minimisation** (describe the steps that will be taken to ensure that the amount of personal data is minimised and limited to what is strictly necessary both initially and on an ongoing basis) |  |
| **Necessity of processing** (explain the extent to which the processing is necessary in relation to the purposes of the initiative) |  |
| **Accuracy** (describe the steps taken to ensure data quality in terms of accuracy and freedom from bias, both initially and on an ongoing basis, e.g. verification techniques and how individuals can update their data) |  |
| **Storage limitation** (describe the steps taken to ensure that personal data are not retained longer than necessary in connection with the intended purposes of the processing)  |  |
| **Security, integrity and confidentiality** (describe the steps taken to ensure the security of the personal data, including protection against personal data breaches) |  |
| **Data subject rights** (describe the steps taken to ensure that data subjects are able to exercise their rights fully and effectively. Individuals have the right to be informed, and rights of access, rectification, erasure, objection and to stop automated decision making) |  |
| **Third party processors** (where relevant, describe the steps taken to ensure the reliability of third parties processing the data on the University’s behalf, and their compliance with data protection law) |  |
| **International transfers** (identify any international transfers of personal data, whether or not to a third party processor, and the safeguards implemented in relation to such transfers) |  |
| **Part E: Identification and assessment of risks (see Appendix 1 and Appendix 2 for example risks and assessment process)** |
| **Ref No** | **Source of risk and potential impact on data subjects** (including associated compliance and organisations risks) | **Likelihood of harm** (see Appendix 2) | **Impact of harm** (see Appendix 2) | **Overall risk** (low, medium, high) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **Part F: Identification of controls and measures to eliminate or mitigate risk (of medium or high risks items in Part E)** |
| **Ref No** | **Controls or measures to eliminate or mitigate risk** (changes to design or additional safeguards and measures | **Effect on risk** (extent to which risk is eliminated or mitigated by the controls or measures) | **Residual risk** (any risk remaining after controls or measures have been implemented) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Part G: Implementation and integration of controls and measures**  |
| **Action** | **Approved by**  | **Person(s) responsible** | **Target completion date** | **Completed** |
|  |  |  |  |[ ]
|  |  |  |  |[ ]
|  |  |  |  |[ ]
|  |  |  |  |[ ]
|  |  |  |  |[ ]
| **Part H:** **Outcomes and sign-off** |
| **Residual risks that cannot be eliminated or mitigated (if any)** |  |
| **Consultation with ICO** (where there are any residual high risks that cannot be eliminated or mitigated) | **Date submitted** |  |
|  | **Submitted by** |  |
|  | **Outcome** |  |
| **Consideration of Data Protection Officer’s advice** (confirm whether advice accepted and implemented or rejected, and if rejected the reasons why) |  |
| **Sign-off** | **Name and role** |  |
|  | **Date** |  |
| **Frequency of review (usually at least annually)** |  |
| **Next review date** |  |

**Appendix 1** **– Example types of risk associated with the processing**

Risks to data subjects

* Risk of processing being unlawful and/or regarded as unfair due to more personal data being collected than is necessary for the intended purposes of the processing
* Risk of personal data being inaccurate due to collection or processing methods or the nature of the personal data being processed
* Risk of personal data being retained longer than necessary or not properly managed so that duplicate records are created
* Risk of personal data being inadvertently manipulated due to human error or otherwise
* Risk of personal data being disclosed or accessed inappropriately due to inadequate access and disclosure controls
* Collection of personal data may be regarded as unnecessary and/or overly intrusive having regard to the objectives of the Initiative
* Risk of processing being unlawful and/or regarded as unfair due to scope and purposes of processing being extended inadvertently
* Use of new technologies, approaches or methods may constitute an unjustified intrusion on the data subjects’ right to privacy
* Risk of processing being regarded as unfair due to complexity of processing activities/involvement of algorithmic analysis
* Risk of processing being regarded as unfair due to the combination of matching of multiple datasets
* Identifiers may be collected and linked which prevent data subjects from accessing or using a service anonymously
* Collection of personal data and linking identifiers may result in anonymisation being compromised
* Vulnerable data subjects may be particularly concerned about risks of identification or disclosure of personal data
* Processing of personal data may produce legal effects or similarly significantly affect the rights and interests of the data subject
* Processing of personal data may result in inappropriate inferences being made or discrimination being suffered by the data subject
* Disclosure of personal data may result in discrimination, victimisation and/or harassment

Compliance risks

* Non-compliance with data protection laws, including the GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations and other secondary legislation
* Non-compliance with common law duty of confidentiality
* Non-compliance with the Equality Act 2010 and other equality and human rights legislation
* Non-compliance with sector-specific legislation or standards

Associated organisational risks

* Risk of regulatory sanctions and fines
* Risk of reputational damage
* Risk of considerable financial expenditure to mitigate any risk that has materialised
* Risk of erosion of trust and confidence in processing activities resulting in loss of business
* Risk of investment returns being reduced or eliminated
* Risk of inaccurate, incomplete or outdated personal data having reduced value
* Risk of research or statistical objectives being compromised, skewed or false
* Risk of claims from individuals for compensation

**Appendix 2** **– Risk assessment methodology**

**Evaluation of likelihood of harm**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood score** | **1** | **2** | **3** | **4** | **5** |
| **Description** | **Rare** | **Unlikely** | **Possible** | **Likely** | **Almost certain** |
| **Frequency** | Will probably never happen | Not anticipated to happen, but possible | Might happen or recur occasionally | Will probably happen or recur, but not persistently | Almost certain to happen or recur, possibly frequently |

**Evaluation of impact of harm**

#

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood score** | **1** | **2** | **3** | **4** | **5** |
| **Description** | **Very Low** | **Low** | **Medium** | **High** | **Very High** |
| **Impact** | Unlikely to have any impact | May have an impact | Likely to have an impact | Highly probably it will have a significant impact | Will have a major impact |

**Overall evaluation of risk**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Impact** | **Very High (5)** |  |  |  |  |  |
| **High (4)** |  |  |  |  |  |
| **Medium (3)** |  |  |  |  |  |
| **Low (2)** |  |  |  |  |  |
| **Very Low (1)** |  |  |  |  |  |
|  | **Rare (1)** | **Unlikely (2)** | **Possible (3)** | **Likely (4)** | **Almost certain (5)** |
| **Likelihood** |

**Appendix 3 – Lawful basis for processing personal data**

**Personal data**

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. The University’s public tasks revolve around teaching and research. All research can come under this lawful basis.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. This cannot apply if the University is processing data to perform its public tasks. A legitimate interests assessment may be required.

**Special category data**

If you are processing special category data (information about an individual’s race, ethnic origin, political opinion, physical or mental health, religion, trade union membership, genetics, biometrics, sexuality or sex life) then you also need a further lawful basis set out in Article 9 of GDPR. At least one must apply whenever you process special category data. The main Article 9 lawful bases are outlined here, though others also exist. Please seek further advice from the Data Protection Officer if required:

(a) Explicit consent: the individual has given their explicit consent to the processing of their personal data for the specific purpose.

(b) Employment law: the processing is necessary for pursing obligations set out in employment law.

(c) Vital interests: the processing is necessary to protect someone’s life where they are incapable of giving consent.

(d) Substantial public interest: the processing is necessary for reasons in the substantial public interest where it will safeguard the rights and interests of the individual.

(e) Medical purposes: the processing is necessary for the purposes of preventive or occupational medicine, or the provision of health care.

(c) Research purposes: the processing is necessary for purposes of scientific or historical research in the public interest. This lawful basis will apply to all research conducted by the University involving special category data.