**Data Protection Impact Assessment (DPIA)**

A Data Protection Impact Assessment (DPIA) helps identify and minimise the data protection risks of a project, process or system implementation or research study whilst still allowing it to go ahead. A DPIA must be carried out for personal data processing that is likely to result in ahigh risk to individuals although it is good practice to do a DPIA for any project which requires the processing of personal data.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data. A DPIA must:

* + describe the nature, scope, context and purposes of the processing;
  + assess necessity, proportionality and compliance measures;
  + identify and assess risks to individuals; and
  + identify any additional measures to mitigate those risks.

In order to assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

You can complete the [DPIA checklist](https://herts365.sharepoint.com/sites/Legal-and-compliance/SitePages/Data-Protection-Impact-Assessment.aspx) first to assess whether a full DPIA is required.

Please complete the form below, in as much detail as possible, responding with ‘N/A’ to any questions which are not relevant to show you have considered each one. Once you have completed the form, please send it to the University’s Data Protection Officer at [dataprotection@herts.ac.uk](mailto:dataprotection@herts.ac.uk) who will contact you about next steps.

|  |  |  |  |
| --- | --- | --- | --- |
| Project Title: |  | | |
| Project Lead: |  | **SBU / Team** |  |
| Ref. No. (completed by DPO) |  |  | |

**Document Control**

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

|  |  |
| --- | --- |
| Step one: Summary of the project You may find it helpful to link to other relevant documents related to the project, for example a project proposal. | |
| Describe the project. What are the aims and objectives? |  |
| What are the benefits to UH, individuals, wider society or other stakeholders? |  |
| What is the investment in terms of resources, time and funding? (e.g. timescales, funding sources, staff / teams involved) |  |
| Status of project? (i.e. not yet started, in progress (since when), near completion (how long left). Please provide any key milestones / dates in the project, e.g. start date, and whether ethical approval has been sought / given |  |
| Step two: Describe the data processing  Please describe the collection, use and deletion of personal data here. This should include:   * Number and type of data subjects (e.g. students, participants (adults, children etc.), UH staff) * Types and volume of data being collected * Data collection methods * Storage, security and processing arrangements, including any sharing arrangements with 3rd parties * Retention periods and disposal   Please include a data flow diagram or table wherever possible in this section to clearly show the data processing details of the project. It may also be useful to attach any surveys or questionnaires. | |
|  | |

|  |  |
| --- | --- |
| Step three: Linking the DPIA to the data protection principles Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act. | |
| Principle 1: Fair, lawful, transparent  Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:  a) at least one of the conditions in Schedule 2 is met (see appendix A), and  b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met (see Appendix A) | |
| How will you tell individuals about the use of their personal data? |  |
| Do you need to amend existing privacy notices or create a new one? |  |
| Which conditions for processing apply? (See Appendix A) |  |
| If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?  How might this affect the project? |  |
| What are the social need and aims of the project?  Are your actions a proportionate response to these? |  |
| Will your actions interfere with the right to privacy under [Article 8](https://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/7) of the Human Rights Act? (Right to respect for private and family life) |  |
| Principle 2: Purpose  Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. | |
| Does your project plan cover all of the purposes for processing personal data? |  |
| Have you identified potential new purposes as the scope of the project expands? |  |
| Principle 3: Minimisation  Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. | |
| Is the quality of the information good enough for the purposes it is used? |  |
| Is there any personal data could you not use, without compromising the needs of the project? |  |
| Principle 4 : Accuracy  Personal data shall be accurate and, where necessary, kept up to date. | |
| How will you ensure that personal data obtained from individuals or other organisations is accurate? |  |
| If you are procuring new software does it allow you to amend data when necessary? |  |
| Principle 5: Data retention  Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes. | |
| What retention periods are suitable for the personal data you will be processing? |  |
| How will you ensure retention policies are implemented and actioned? |  |
| Are you procuring software that will allow you to delete information in line with your retention periods? |  |
| Principle 6: Security  Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. | |
| How will you ensure the security of the personal data, including protection against personal data breaches? |  |
| What training and instructions are necessary to ensure that staff know how to operate systems securely? |  |
| How will you ensure staff are trained appropriately?  Have you / staff had data protection training in the last 12-18 months? |  |
| Transfer outside the EEA  Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. | |
| Will the project require you to transfer data outside of the EEA? Please provide details |  |
| If you will be making transfers, how will you ensure that the data is adequately protected? |  |
| Third party Processors  Steps taken to ensure the reliability of third parties processing the data on the University’s behalf, and their compliance with data protection law | |
| Will any third parties be processing data? If so how will you ensure their reliability and compliance with data protection? (e.g. Data Sharing Agreements etc.) |  |
| Data Subjects Rights (See Appendix B)  Personal data shall be processed in accordance with the rights of data subjects under this Act. | |
| Will the systems and processes you are putting in place allow you to respond to Data subject rights requests more easily (e.g. right of access, right to erasure etc)? |  |
| If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose? |  |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Step four: Identify and assess risks (See Appendix C (example risks) and D (Risk scoring matrix)) | | | | |
| Ref No. | **Risk / Privacy issue**  Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. | **Likelihood of harm**  Remote, Possible or Probable | **Severity of harm**  Minimal, Significant or Severe | **Overall risk**  Low, Medium, HIgh |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| 4. |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step five: Identify measures to reduce risk** Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 4 | | | | |
| **Ref No.** | **Measure(s) to reduce or eliminate risk** | **Effect on risk**  Eliminated, reduced or accepted | **Residual risk**  Low, medium, high | **Measure approved by DPO (or DMG for Systems only)**  Yes/ No (DPO/DMG) |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |

**SECTION 3 – Sign off and record outcomes** (to be completed by the DPO and Initiative / Project Lead)

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/date** | **Notes** |
| Date measures approved by DPO: |  | Integrate actions back into project plan, with date and responsibility for completion |
| DPO advice provided: | page7image2371742192 | DPO should advise on compliance, step five measures and whether processing can proceed |
| Summary of DPO advice: | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will be kept under review by: |  | Person responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork and raising any privacy concerns that may arise in the future.  The DPO should also review ongoing compliance with DPIA |
| Next Review Date: |  |  |

**SECTION 4 – Sign off and record outcomes (New IT Systems only)** (to be completed by the Data Management Group (DMG))

|  |  |  |
| --- | --- | --- |
| Item | Name/date | Notes |
| Date measures approved by DMG: |  | Integrate actions back into project plan, with date and responsibility for completion |
| DMG advice provided: | page7image2371742192 | DMG should advise on compliance, step five measures and whether processing can proceed |
| Summary of DMG advice: | | |
| Comments: | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will be kept under review by: |  | The DMG should also review ongoing compliance with DPIA |

**Appendix A – 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 (more sensitive 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 Article 9 lawful bases are outlined here. 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 (this must be recorded)

(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) **Not-for-profit bodies**: processing is being done in relation to some specified activities of not-for-profit bodies

(e) **Made public by the data subject**: the data has deliberately been made available by the data subject and not by any other process or individual

(f) **Legal claims and judicial acts**: the processing is necessary to establish, exercise or defend legal claims.

(g) **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.

(h) **Health or Social Care**: the processing is necessary for the purposes of preventive or occupational health and medicine, or the provision of health care.

(i) **Public Health**: the processing is necessary for reasons of public interest in the area of public health, e.g. to stop spread of an infectious disease

(j) **Archiving, Research and statistical 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.

**Appendix B – Data Subject Rights**

|  |  |
| --- | --- |
| **Right** | **Description** |
| Right to be informed | Individuals have a right to know who is processing their personal data |
| Right of access | Individuals have a right to access any personal data collected on them |
| Right to rectification | Individuals have a right to have inaccurate personal data corrected |
| Right to erasure (to be forgotten) | Individuals have a right to have their personal data deleted |
| Right to restrict processing | Individuals have a right to restrict processing of their personal data |
| Right to data portability | Individuals can require organisations to transfer their personal data to another organisation |
| Right to object | Individuals have the right to withdraw their consent for processing their personal data |
| Rights related to automated decision making including profiling | Individuals can object to their personal data being used for automated decision making |

**Appendix C** **– Example risks associated with data processing**

Risks to data subjects

* Risk of processing being unlawful and/or regarded as unfair due to type / amount of personal data being collected
* Risk of personal data being inaccurate due to collection or processing methods
* Risk of ‘purpose creep’, e.g. data being used for purpose other than those expected by the data subject
* Risk of personal data being retained longer than necessary
* Risk of duplicate records being created due to data not being managed properly
* Risk of personal data being disclosed or accessed inappropriately due to inadequate access and security controls
* Use of new technologies or methodologies (e.g. biometrics) potentially causing an unjustified intrusion on the data subjects’ right to privacy
* Risk of processing being regarded as unfair due to the combination of matching of multiple datasets
* Re-identification of pseudonymised data (e.g. when linking with other data, small datasets)
* Affects data subject’s ability to access services or opportunities
* Detriment to data subject such as identity theft, financial loss or physical harm

Compliance risks

* Non-compliance with data protection law (i.e. UK GDPR, DPA 2018 and Privacy and Electronic Communications Regulations (PECR)
* 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 loss of public trust and confidence
* Risk of research or statistical objectives being compromised or skewed
* Risk of claims from individuals for compensation

**Appendix D – Risk Scores and matrix**

|  |  |  |  |
| --- | --- | --- | --- |
| **Likelihood score** | **1** | **2** | **3** |
| **Description** | **Remote** | **Possible** | **Probable** |
| **Frequency** | Would only happen in exceptional circumstances  (>25% chance) | Could happen or recur  (50% chance) | More likely to happen than not (75% chance) |

|  |  |  |  |
| --- | --- | --- | --- |
| **Impact score** | **1** | **2** | **3** |
| **Description** | **Minimal** | **Significant** | **Severe** |
| **Impact** | Minor impact | Likely to have some impact | May cause significant harm |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact** | **Severe (3)** | Medium | High | High |
| **Significant (2)** | Low | Medium | High |
| **Minimal (1)** | Low | Low | Low/Medium |
|  | | **Remote (1)** | **Possible (2)** | **Probable (3)** |
|