**University of Dundee**

**Information Governance – Data Protection**

**Data Protection Impact Assessment – [SCHOOL/SERVICE] – [PROJECT TITLE – deploying new software/services]**

[Data Protection Impact Assessments should be completed for all new or modified uses of personal data. Data Protection Impact Assessments are mandatory for all high-risk or high-volume processing of personal data, for the introduction of any new systems or for monitoring and/or surveillance systems (such as CCTV).

This template should be used whenever new third-party products or services are implemented that require the storage, use or transfer of personal data.

The template includes instructions or comments in square brackets throughout to assist you in completion. Please contact the Data Protection Officer (DPO) - dataprotection@dundee.ac.uk - for assistance if you have any questions.

Your completed DPIA should be sent to the DPO for their comment. They will return it to you and the final version should be kept on file with the other information concerning the implementation of the system/service. Implementation of the controls should form part of your project checklists.]

**1. NAME OF PROJECT**

**2. BRIEF DESCRIPTION OF PROJECT**

[Explain the aims and objectives of the project. What the third-party software or services will do. Note where personal data will be processed, including the location of sub-processors or servers etc]

**3. DATA OWNER**

[Responsible officer (Member of UEG/Director/Dean/School Manager)]

**4. OPERATIONAL RESPONSIBILITY**

[Senior officer(s) with operational responsibility for the project/system/service etc]

**5. SCREENING QUESTIONS (is a DATA PROTECTION IMPACT ASSESSMENT REQUIRED?)**

If the answer to any of the questions in below is ‘yes’, proceed to step 6.

If the answer to any of the questions is unclear or you don’t know the answer, please contact dataprotection@dundee.ac.uk for guidance.

If the answer is ‘no’ to all the questions, a Data Protection Impact Assessment is not required. That decision and the authority for it should be documented and retained. No further steps are required.

1. Will the project involve the collection of new information about individuals?
2. Will the project compel individuals to provide information about themselves?
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics, facial recognition or surveillance technology such as CCTV or other monitoring systems.
6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
8. Will the project require you to contact individuals in ways which they may find intrusive?
9. Will the project require large volumes of personal data?
10. Will the project involve the use of personal data in a new setting or using different technology? For example, the transfer of a University system to the cloud or the use of a new cloud-based system or service?
11. Will any personal data be stored or otherwise processed outwith the European Economic Area?
12. Will the project involve children?

IS A DATA PROTECTION IMPACT ASSESSMENT REQUIRED?

IF A DATA PROTECTION IMPACT ASSESSMENT IS NOT REQUIRED PLEASE RECORD WHY:

NAME, SIGNATURE AND DESIGNATION OF DATA OWNER RESPONSIBLE FOR DECISION NOT TO COMPLETE A DATA PROTECTION IMPACT ASSESSMENT:

NAME: DESIGNATION: SIGNED: DATE:

**6. DESCRIBE THE TYPES OF PERSONAL INFORMATION TO BE USED IN THE PROJECT AND THE PURPOSE OF ITS USE?**

**6.1 Types of personal data**

[eg name, email address, postal address, date of birth, staff number, student number, gender]

**6.2 Purpose of use (personal data)**

[describe why using the personal data listed above is essential, noting the requirement that minimum amount of personal data is used for any purpose.]

**6.3 Types of special categories of personal data**

[eg racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health (in the broadest sense to include physical or mental health, disability etc), sex life, sexual orientation]

**6.4 Purpose of use (special categories of personal data)**

[describe why using the special categories of personal data listed above is essential, noting the requirement that minimum amount of personal data is used for any purpose.]

**7. NOTE ANY CONSULTATION THAT HAS TAKEN PLACE CONCERNING THIS USE OF PERSONAL DATA AND THE OUTCOME OF THAT CONSULTATION**

[Which University officers, committees etc have considered and agreed to the project? Has there been any consultation with a broader group of staff or students? Has DUSA been consulted? Have any other stakeholder groups been consulted? What was the outcome of the consultation in respect of the proportionate use of personal data in the project?]

**8. NOTE WHY THE INTENDED PROCESSING IS LAWFUL**

[Please discuss with DPO]

**8.1 Personal data**

**8.2 Special category personal data**

[The table in S.9 provides a series of example risks and usual UoD controls. If the risks apply to your project and the controls can be implemented **without modification** they should be included in your DPIA (and implemented accordingly). If you are unable to implement the controls for any reason please contact the DPO at dataprotection@dundee.ac.uk for guidance. Please include additional risks specific to project as necessary and risk assess those with the DPO.]

|  |
| --- |
| **9. DOCUMENT PRIVACY RISKS AND AGREED SOLUTIONS** |
| **PRIVACY RISK** | **LIKELIHOOD OF HARM****(Remote, possible or probable)** | **SEVERITY OF HARM****(Minimal, significant or severe)** | **RISK****(Low, medium or high)** | **CONTROLS** | **RESIDUAL RISK****(Low, medium or high)** | **IS THE RISK REDUCED, ELIMINATED OR ACCEPTED** | **AUTHORITY FOR THE DECISION** | **RESPONSIBILITY FOR IMPLEMENTING THE SOLUTION** | **EVALUATION: IS THE RISK TO INDIVIDUALS JUSTIFIED AND PROPORTIONATE WHEN CONTROLS ARE APPLIED?**  |
| **9.1 Inadequate controls around data collection /storage** | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | * UoD style data processing agreement (DPA) completed and signed by all parties. (Note UoD signatory must be per Schedule of Delegation). UoD style DPAs linked here - <https://uod.box.com/s/00xigbm3qvwq4ola0fnbrgdbhprthxei>
* UoDIT security assessment completed. UoDIT to warrant security of system/approach and/or data owner to accept risks/controls recommended by the UoDIT assessment.
 | [Where controls applied normal expectation is risk reduced to ‘low’ as likelihood reduced to ‘remote’ even though intrinsic data risk may remain high] | [Where controls applied normally ‘reduced and accepted’] | [Data owner] | [Senior officer(s) with operational responsibility for implementing the controls] | [To be agreed with DPO] |
| **9.2 Inappropriate access to personal data – UoD staff** | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | * Access to data must be role-appropriate.
* Contracted members of UoD staff required to adhere to UoD policies, procedures and expectations.
 | [Where controls applied normal expectation is risk reduced to ‘low’ as likelihood reduced to ‘remote’ even though intrinsic data risk may remain high] | [Where controls applied normally ‘reduced and accepted’] | [Data owner] | [Senior officer(s) with operational responsibility for implementing the controls] | [To be agreed with DPO] |
| **9.3 Inappropriate access to personal data by vendor/third party.** | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | * UoD DPA completed and signed, setting security expectations of third party.
* UoDIT security assessment completed and controls implemented.
 | [Where controls applied normal expectation is risk reduced to ‘low’ as likelihood reduced to ‘remote’ even though intrinsic data risk may remain high] | [Where controls applied normally ‘reduced and accepted’] | [Data owner] | [Senior officer(s) with operational responsibility for implementing the controls] | [To be agreed with DPO] |
| **9.4 Excessive retention of personal data** | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | * Data to be retained in accordance with normal UoD retention periods.
* Retention periods to be agreed via DPA.
 | [Where controls applied normal expectation is risk reduced to ‘low’ as likelihood reduced to ‘remote’ even though intrinsic data risk may remain high] | [Where controls applied normally ‘reduced and accepted’] | [Data owner] | [Senior officer(s) with operational responsibility for implementing the controls] | [To be agreed with DPO] |
| **9.5 Failure to communicate rights to data subjects.** | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | * Applicable privacy notice(s) to be updated and provided to data subjects OR new privacy notices to written and provided to data subjects. Advice must be sought from DPO.
 | [Where controls applied normal expectation is risk reduced to ‘low’ as likelihood reduced to ‘remote’ even though intrinsic data risk may remain high] | [Where controls applied normally ‘reduced and accepted’] | [Data owner] | [Senior officer(s) with operational responsibility for implementing the controls] | [To be agreed with DPO] |
| **9.6 Appointment of sub-processors by the vendor.** | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | * UoD DPA completed and signed. Cascades obligations to sub-processors.
 | [Where controls applied normal expectation is risk reduced to ‘low’ as likelihood reduced to ‘remote’ even though intrinsic data risk may remain high] | [Where controls applied normally ‘reduced and accepted’] | [Data owner] | [Senior officer(s) with operational responsibility for implementing the controls] | [To be agreed with DPO] |
| **9.7 Processing of personal data outwith the European Economic Area by the processor or their sub-processors.** | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | * UoD DPA completed and signed. Requirement to use the EU standard contract clauses (in the schedules) for non-EEA processing.
 | [Where controls applied normal expectation is risk reduced to ‘low’ as likelihood reduced to ‘remote’ even though intrinsic data risk may remain high] | [Where controls applied normally ‘reduced and accepted’] | [Data owner] | [Senior officer(s) with operational responsibility for implementing the controls] | [To be agreed with DPO] |
| **9.8 Vendor-side data incident** | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | [To be assessed per matrix below according to types of personal data being processed] | * UoD DPA completed and signed. Requirement to refer to UoD in the management of the incident.
* UoDIT security assessment and application of controls should reduce risk.
 | [Where controls applied normal expectation is risk reduced to ‘low’ as likelihood reduced to ‘remote’ even though intrinsic data risk may remain high] | [Where controls applied normally ‘reduced and accepted’] | [Data owner] | [Senior officer(s) with operational responsibility for implementing the controls] | [To be agreed with DPO] |

**RISK**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Likelihood of harm** | **PROBABLE** | **GREEN** | **RED** | **RED** |  | **RED** | **= HIGH RISK** |
| **POSSIBLE** | **GREEN** | **AMBER** | **RED** |  | **AMBER** | **= MEDIUM RISK** |
| **REMOTE** | **GREEN** | **GREEN** | **GREEN** |  | **GREEN** | **= LOW RISK** |
|  |  | **MINIMAL** | **SIGNIFICANT** | **SEVERE** |  |  |  |

**10. DATE OF CONSULTATION WITH DATA PROTECTION OFFICER**

[TBC by DPO noting key areas of attention for data owner and responsible officers.]