**UNIVERSITY OF DUNDEE**

**INFORMATION GOVERNANCE**

**Data Protection Impact Assessment**

**Guidance Note**

****

**Please read thIS GUIDANCE note before COMPLETING THE data protection impact assessment**

This is the Guidance Note for the University of Dundee’s standard template: Data Protection Impact Assessment (**DPIA**).

**Requirement to complete a DPIA**

DPIAs are used to ensure that the University complies with data protection laws. The main purposes of a DPIA are:

* to form a clear picture of how personal data is processed in connection with the University’s various activities and project;
* consulting relevant parties about how the University uses personal data; and
* to identify, consider and mitigate the risks in connection with such processing.

Under data protection laws the University has an obligation to complete, and keep updated, a DPIA in connection with any activities which are **likely to result in a high risk to individuals**. It may also be appropriate to complete a DPIA in connection with major projects or significant activities.

If the University fails to consider and address the risks involved in our activities, or to complete a DPIA where we have an obligation to do so, we may be subject to fines or other enforcement action by the Information Commissioner’s Office (**ICO**). Failure to comply with data protection laws could also have an impact on our reputation.

**Data protection and privacy should be considered as soon as possible**

You should consider the requirement for a DPIA as soon as possible in connection with each activity / project which involves personal data. The requirement for a DPIA should be considered in connection with both new and existing activities and where there are changes to the use of personal data. The University’s Data Protection Officer (**DPO**) should consulted as early as possible. The DPIA requires to be completed and tasks actioned before the commencement of the activity / project.

The standard template includes screening questions to assess whether a DPIA is required, and you should record the reasons why a DPIA either is or isn’t required. In both cases the DPIA should be signed off by the DPO.

**Data Protection Officer and further information**

Any questions about the DPIA should be directed to the DPO:

Alan Bell

Head of Information Governance and Joint Assistant Director, Culture & Information

a.z.bell@dundee.ac.uk

+44(0)1382 384441

Where the DPO is not available, please contact the University’s legal team with any questions.

**The content of the DPIA**

* sections 1-4 and section 20 should be completed always when considering whether a DPIA is required;
* section 5 outlines the scope of the DPIA;
* sections 6-9 include details about the data processing carried out by the University;
* sections 10-16 describe how the University will comply with data protection laws;
* section 17 contains a risk assessment;
* sections 18 and 19 are for recording actions and to provide further information;

* section 20 is used to record the decision reached on the basis of the completed DPIA;
* Annex 1 includes a list of documents relevant to the DPIA. Further Annexes may be added as required.

**It is essential to complete all the sections of the DPIA. Questions or sections should not be deleted from the standard template.**

**Process for completion and sign-off of the DPIA**

The DPIA and the screening questions should be completed by a person who is responsible for the data protection and privacy aspects of the activity / project. This should be a sufficiently senior member of the team involved in, and having good knowledge of both, the relevant activity / project in question and data protection law.

The University’s DPO, individuals and other relevant parties (such as stakeholders, Legal and any parties processing personal data on behalf of the University) should be consulted in the process of carrying out the DPIA. In certain cases, the University may be required to seek views from the ICO.

**Once you have completed the DPIA or (where there is no requirement to complete the DPIA), the screening questions please send this to the DPO for review and sign-off.**

A decision will be reached in connection with the relevant activity / project on the basis of the DPIA – i.e. whether:

* the relevant activity / project can proceed;
* specific actions require to be taken before the activity / project may proceed;
* it is not acceptable to proceed with the activity / project because it is not compliant with data protection laws or due to risks involved; or
* ICO should be consulted.

The completion of a DPIA is not a one-off exercise. The person responsible for completing the DPIA should **keep this updated** as the activity / project progresses, and particularly if there are any changes to the way in which personal data is used or where new risks emerge. The DPIA should be reviewed regularly at least once per year.

**Guidance Notes for completion of the DPIA:**

|  |  |
| --- | --- |
| **Note** | **INFORMATION REQUIRED**  |
|  | Insert the name of the activity / project. |
| 1. **Document management**
 |
|  | This section should be completed when an initial draft of the DPIA is signed off and each time it is reviewed. Insert details of: * the version;
* the date;
* any changes made to the document (if applicable);
* name and role of person completing / reviewing the DPIA; and
* the name and role of person signing off on the completed / amended DPIA.
 |
| 1. **Executive summary**
 |
|  | Insert a high level summary of the key outcomes / findings of the DPIA, including: * summary of the activity / project;
* summary of the way in which personal data is used in connection with the activity / project;
* summary of the purposes of data processing;
* summary of the benefits of the activity / project to the University, individuals, the society and other parties; and
* whether a DPIA requires to be completed and a summary of the rationale as to why.

The executive summary should be one of the last sections to be completed. |
| 1. **The Activities**
 |
|  | Insert the name of the relevant school(s) / departments carrying out the relevant activity / project. |
|  | Insert a description of the relevant activity / project.  |
|  | Insert details of the background or wider context of the activity / project. * As an example this will include the University’s relationship with the individuals, the control individuals will have over their data, expectations of individuals and other wider privacy considerations.
 |
|  | Insert description of the aims and benefits of the activity / project. Any benefits for the University, individuals and the society as a whole should be mentioned.  |
| 1.
 | Insert details of University personnel who have operational responsibility to carry out the activity / project.The table may be edited to add / remove spaces depending on the number of individuals.  |
|  | Insert the details of University personnel who are responsible for the data protection and privacy implications of the activity / project and for this DPIA. This may be the same individual as for Note 8 above. The table may be edited to add / remove spaces depending on the number of individuals. |
|  | Insert details of stakeholders and third parties (such as third party companies, processors or organisations) involved in the activity / project. The table may be edited to add / remove spaces depending on the number of parties. |
| 1. **Requirement to complete a DPIA**
 |
|  | The screening questions provide indication on whether University has a legal obligation to complete a DPIA. These should be completed **as soon as possible** in connection with each activity / project involving personal data, or where there is a change in the use of personal data. Even if a DPIA is not required, sections 1 to 4 and 20 should still be completed and signed off.**If you are unsure about any of the questions, or whether a DPIA is required, contact the DPO (in the first instance) or Legal.**  |
|  | A DPIA is a legal requirement where the relevant activity / project is likely to result in a high risk to individuals. To answer this question, consider the responses to the below screening questions 1-23. * If the answer to any question between 1 to 12 is ‘Yes’ then the processing DPIA will be required automatically.
* If the answer to any question between 13 to 22 is ‘Yes’ then processing may be high risk and a DPIA may be required.
* If the answer to question 23 is ‘Yes’ then a DPIA is required.
 |
| 1.
 | Insert ‘Y’ or ‘N’ as applicable. Automated decision-making and profiling have the following meanings: * **Automated decision-making** means making decisions by automated means without human involvement (for example through the use of IT, software or algorithms).
* **Profiling** means any automated processing of personal data to evaluate certain personal aspects relating to an individual (in particular to analyse or predict aspects concerning that individual’s performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements).

When considering whether processing is **systematic**, the following should be taken into account: * existence of any system to collect / process data;
* whether processing is pre-arranged, organised or methodical;
* whether processing occurs as part of a general plan for data collection;
* whether processing is carried out as part of a strategy.

When considering whether processing is **extensive**, the following should be taken into account: * geographical area affected;
* the range of personal data involved; and
* the number of individuals affected.
 |
| 1.
 | Insert ‘Y’ or ‘N’ as applicable. * **Special category data** includes personal data relating to race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for identification purposes), health, sex life and sexual orientation.
* When considering whether processing is **on a** **large scale**, the following should be taken into account:
* the number of individuals;
* the volume and/or range of data processed;
* the duration or permanence of the processing; and
* the geographical extent of the processing.
 |
|  | Insert ‘Y’ or ‘N’ as applicable. See Notes 13 and 14 for more information on “systematic” and “large scale.” |
|  | Insert ‘Y’ or ‘N’ as applicable. |
|  | Insert ‘Y’ or ‘N’ as applicable.See Notes 13 and 14 for further information on profiling, automated decision-making and special category data.  |
|  | Insert ‘Y’ or ‘N’ as applicable. See Notes 13 and 14 for further information on profiling and the meaning of “large scale” processing. |
|  | Insert ‘Y’ or ‘N’ as applicable. |
|  | Insert ‘Y’ or ‘N’ as applicable.This may involve personal data received / collected by the University from various sources or for various purposes.  |
|  | Insert ‘Y’ or ‘N’ as applicable.It should be checked whether an accurate privacy notice (also known as a fair processing notice) has been provided to the individual.  |
|  | Insert ‘Y’ or ‘N’ as applicable. |
|  | Insert ‘Y’ or ‘N’ as applicable.See Note 13 for further information on profiling and automated decision-making. |
|  | Insert ‘Y’ or ‘N’ as applicable. |
|  | Questions 13 to 22 are further screening questions to ascertain whether processing undertaken by the University is likely to result in a high risk to individuals. If the answer to any question is ‘Yes’ this does not automatically mean that a DPIA is required. In this case you should consult with the DPO. |
|  | Insert ‘Y’ or ‘N’ as applicable.* As an example, this may include automated decision-making, profiling or predicting (see Note 13).
* As an example, this may relate to individual’s performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
 |
|  | Insert ‘Y’ or ‘N’ as applicable.See Note 13 for further information on automated decision-making.* As an example, a significant effect may be a legal effect or another similarly significant effect on the individual.
 |
|  | Insert ‘Y’ or ‘N’ as applicable.Also see Note 13 for further information on systematic processing. |
|  | Insert ‘Y’ or ‘N’ as applicable.* As an example, sensitive data may include special category data (see Note 14) and criminal convictions data but may also include other sensitive data.
 |
|  | Insert ‘Y’ or ‘N’ as applicable.See Note 14 for further information. |
| 1.
 | Insert ‘Y’ or ‘N’ as applicable.* As an example, vulnerable individuals may include children and specific groups such as patients, mentally ill persons and the elderly. This may also include employees and students.
 |
|  | Insert ‘Y’ or ‘N’ as applicable.* As an example, this may include new forms of data collection or usage.
 |
|  | Insert ‘Y’ or ‘N’ as applicable.The University may wish to carry out a DPIA in connection with major activities to ensure that data protection is given due consideration. |
|  | Insert ‘Y’ or ‘N’ as applicable. |
|  | Insert ‘Y’ or ‘N’ as applicable. |
|  | Insert ‘Y’ or ‘N’ as applicable.If there is any other reason why the activity / project is likely to result in a high risk, then this should be indicated here. |
|  | Insert ‘Y’ or ‘N’ as applicable. |
|  | Insert the reasons why a DPIA either is or isn’t required. * This should draw on the responses to the screening questions.
* Insert an assessment of the risks and their likelihood.
* You should consult the DPO and record their views here.
* There are exceptions where a DPIA may not be required. If these apply, this should be discussed with the DPO and outlined here.
 |
|  | Insert the name and role of the person carrying out the screening. |
|  | Insert the name and role of the person authorised to make a decision on whether a DPIA is required. |
|  | Insert date decision made. |
|  | Insert signature of the person authorised to make a decision on whether a DPIA is required. |
| 1. **The scope of this DPIA**
 |
|  | Insert description of the relevant part(s) of the activity / project covered by this DPIA. If the DPIA covers the entire activity / project then this should be indicated.  |
|  | Insert description of the relevant part(s) of the activity / project which are not covered by this DPIA. |
|  | Insert details of any other similar University processing activities which are covered by this DPIA. |
| 1. **Details about the processing of personal data**
 |
|  | Insert a description of the processing of personal data in connection with the activity / project. A data flow map should be produced for this purpose.  |
|  | Insert a description of the means and methods used to process personal data. * As an example this may include technology/devices, paper/manual processes, networks, Cloud, cookies, software etc.
 |
| 1.
 | Insert the types of individuals whose data will be processed. |
|  | Insert the types of personal data processed (including whether this includes any criminal offence data or special category data – see Note 14.)  |
|  | Insert details of where the University receives the personal data.  |
|  | Insert details of the duration and frequency of processing. |
|  | Insert details of the volume of data processed, such as the number of individuals whose data will be processed.  |
| 1. **Purpose of processing**
 |
|  | Insert the purposes of processing, particularly in connection with issues identified in section 4 (*Requirement to complete a DPIA*). Purpose should also include the intended outcome for the University and the individuals. |
|  | Insert details of any benefits of the processing activities. Any benefits for the University, individuals or the society as a whole should be mentioned. |
| 1. **Disclosure / sharing of personal data by the University**
 |
|  | Details of parties who receive personal data from the University. Insert: * the name and role of these parties;
* details of the data disclosed;
* the reason why the University discloses personal data;
* details of the agreements the University has in place; and
* details of any monitoring activities and other action taken by the University to ensure that the recipient complies with its obligations.

The table may be edited to add / remove spaces depending on the number of parties. |
| 1. **Countries**
 |
|  | Details of international transfers of personal data, including where data is hosted on servers located abroad. Insert:* the name and role of the recipient;
* any countries that the personal data “touches” (whether located there or transferred via such country);
* reason for the international data transfer;
* details of any relevant agreements in connection with the transfer; and
* the legal ground for the international transfer (for example the use of model clauses).

The table may be edited to add / remove spaces depending on the number of recipients. |
|  | Insert the countries where the individuals (see Note 48) are located.  |

|  |
| --- |
| 1. **University’s legal basis for processing**
 |
|  | Insert details of the University’s legal grounds for processing personal data. Legal grounds are subject to additional conditions. Some of the possible legal grounds are:* individual’s consent;
* the processing is necessary for a contract with an individual, or because an individual has asked the University to take specific steps before entering into a contract;
* the processing is necessary for the University to comply with the law;
* the processing is necessary to protect vital interests; and
* the processing is necessary for the University to perform a task in the public interest or for its official functions.

Possible legal grounds in respect of special categories of data (see Note 14) are:* individual’s explicit consent;
* processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the University or the individual in the field of employment and social security and social protection law;
* processing is necessary to protect vital interests where the individual is physically or legally incapable of giving consent;
* processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body;
* processing relates to personal data which are manifestly made public by the individual;
* processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
* processing is necessary for reasons of substantial public interest, on the basis law;
* processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional;
* processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law; and
* processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with safeguard required by GDPR and based on law.

If you are unsure of which ground applies, contact the DPO (in the first instance) OF Legal. |
|  | * Insert details of how the University ensures data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
* Insert details of why the processing is necessary and proportionate in connection with the purposes outlined in section 7 (*Purpose of processing*). (As an example -does the processing help the University to achieve the purposes? Is there any other way the University could achieve the purposes?)
 |
|  | Insert details of how the University will meet the fairness requirements under data protection law. * As an example this may include details about privacy notices provided to individuals, the University’s Data Protection Policy, cookies policy and other relevant measures.
* As an example - would individuals expect their data to be used in this way? How can function creep be prevented?
 |
|  | Insert details of how the University ensures that the data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.  |

|  |
| --- |
| 1. **Security of processing and safeguards**
 |
|  | Insert details of practical and organisational safeguards in connection with the personal data.* As an example this may include access controls, identity verification, training, policies, etc.
 |
|  | Insert details of security measures and mechanisms in connection with the personal data. * As an example, security measures may include secure storage, encryption, authentication, data breach policy, etc.
* As an example, other mechanisms may include anonymisation, back-ups, arrangements for data destruction, etc.
 |
|  | Insert details of how the University can demonstrate that it complies with the legal requirements under data protection law.* As an example, this may include maintenance of processing records, safety certifications, use of privacy notices, etc.
 |
| 1. **Quality of data**
 |
|  | Insert details on the quality of data, including whether it is complete, up-to-date and accurate. |
|  | Insert details of steps to review or update the personal data. |
| 1. **Data subjects’ rights**
 |
|  | Insert details of arrangements to ensure that the University gives effect to the rights of individuals.* As an example, these may include policies and procedures adopted by the University.
 |
| 1. **Retention and disposal**
 |
|  | Insert details of how long different types of data will be used / stored. This should be in accordance with the University’s policies. |
|  | Insert details of any archiving, anomymisation, back-up, business continuity, decommissioning and other relevant measures relating to the personal data.  |
|  | Insert details of how data will be disposed of. This should be in accordance with the University’s policies.  |
| 1. **Vulnerable individuals**
 |
|  | Insert details of any vulnerable individuals / groups of individuals whose data is processed. See Note 31 for further information.  |
|  | Insert details of special arrangements required, if any.  |
| 1. **Consultation**
 |
|  | **The advice of the University’s DPO should be sought as soon as possible in connection with all DPIAs.** Insert the date of consultation and the advice provided by the DPO. Copy of the advice should be included as an Annex. * If the views of the DPO differ from decision reached in section 20 (*Outcome*) then reasons for reaching the outcome should be inserted.
 |
|  | Any relevant school or University department should be consulted in connection with the data processing. Insert the date of consultation and comments received.  |
|  | **The University has to seek views from individuals or their representatives, doing so does not cause prejudice to commercial or public interests or the security of processing.** * If individuals are consulted, insert date and method of consulting and comments received. If the views of the individuals differ from decision reached in section 20 (*Outcome*) then reasons for the outcome reached should be inserted.
* If decision is made not to consult individuals, then the reasons should be inserted.
 |
|  | If any third parties (e.g. processors, Legal, experts) are consulted, insert the name of the relevant party, date and comments received. |
|  | **Where high risks cannot be mitigated, the University has to consult the ICO.** Section 17 (*Risk Assessment*) should be completed to assess what the risks are and whether they can be mitigated. * Insert any details of communications with the ICO in connection with consultation.

If consultation required, insert date and advice received form the ICO. A copy of the advice should be included as an Annex.  |
| 1. **Risk assessment**
 |
| 1.
 | Insert the risks / potential impacts to individuals and their rights and freedoms. * As an example, these may include (but are not limited to):
* privacy risks;
* security risks;
* operational risks;
* financial risks;
* physical risks;
* social risks;
* loss of or unintended modification of data;
* loss of rights;
* loss of access to services / opportunities;
* loss of control over data;
* crime risks;
* reputational risks;
* risk of discrimination;
* risk of re-identification.
* Issues identified in section 4 (*Requirement to complete a DPIA*) should be used when completing the table.
* Include details about the source of risk, categories of individuals affected and the type of damage.
 |
|  | Insert the risks to the University in connection with the activity / project. * As an example, this may include compliance, corporate and organisational risks and other risks outlined at Note 78.
* Include details about the source of risk and the type of damage.
 |
|  | Insert details of any other risks identified. * This may include compliance/corporate risks and other risks outlined at Note 78.
* Include details about the source of risk, categories of parties affected and the type of damage.
 |
|  | Insert details of the severity of identified risks. |
|  | Insert details of the likelihood of identified risks. |
|  | Insert the level of overall risk based on the severity and likelihood of the risk.  |
| 1.
 | Insert details of solutions and mitigations for each identified high risk and how the solution reduces the risk.  |
|  | Insert the residual risk level after the solution / mitigation is applied.  |
|  | Insert whether the residual risk is eliminated, reduced or accepted.  |
|  | Insert assessment: after implementing the solution / mitigation, is the processing for the purposes compliant, necessary and proportionate considering the risks / impact on individuals? |
|  | Insert details of the relevant authorised person making the decision in connection with the risk. |
| 1. **Actions**
 |
|  | Insert actions arising out of this DPIA, including all solutions to be implemented under section 17 (*Risk assessment*) (see Note 84).  |
|  | Insert persons responsible for implementing actions. |
|  | Insert date action added to this list. |
|  | Insert due date for completing the action.  |
| 1. **Any other relevant information**
 |
|  | Insert any other relevant information in connection with this DPIA and the processing activities. |
| 1. **Outcome**
 |
|  | Insert decision in connection with the relevant activity / project on the basis of the DPIA – i.e. whether:* the relevant activity / project can proceed;
* specific actions require to be taken before the activity / project may proceed; or
* it is not acceptable to proceed with the activity / project because it is not compliant with data protection laws or due to risks involved; or
* ICO should be consulted.
 |
|  | Insert name of authorised person making the decision. |
|  | Signature of person making the decision. |
| **ANNEX 1 – RELEVANT DOCUMENTS** |
|  | Details of documents relevant to the DPIA. Insert the name, date and location of each document. Key documents (such as a data flow map and DPO advice) should be included in the DPIA as an Annex.  |
| **ANNEX 2 – DATA FLOW MAP** |
|  | Insert data flow map here.  |
| **ANNEX 3 – ADVICE FROM THE DATA PROTECTION OFFICER** |
|  | Insert copy of the advice / comments from the Data Protection Officer. Further Annexes may be added as required. |