**NUI Galway DPIA template 2019**

**Project or Unit Name:**

**Date:**

**Principal Investigator or Head of Unit Name:**

**Version number:**

1. **Purpose**

The purpose of a Data Protection Impact Assessment (DPIA) is to determine if the concept of ‘privacy by design’ is adequately embedded into NUI Galway processes, systems or projects that will affect or bring about high risk to individuals or high-volume processing of personal data**.** It is the responsibility of the NUI Galway Project Principal Investigator, Head of School or Head of Unit as applicable to ensure the required controls are put in place and to sign off on any risks arising from the processing of personal data. **A DPIA must be completed by the NUI Galway project owner, Head of School or Head of Unit for personal data processing that is likely to result in a high risk to the rights and freedoms of individuals.** Please use the checklists at **Appendix 1** to help a unit or project owner to decide when to do a DPIA.

1. **What is a privacy risk?**

A privacy risk can be defined as the probability that the fundamental rights and freedom of a data subject may be put at risk through the data processing activities of NUIG. Recital 4 of the General Data Protection Regulation defines the fundamental rights of a data subject as:

* respect for private and family life,
* respect for home and communications,
* protection of personal data,
* freedom of thought, conscience and religion,
* freedom of expression and information….”

Privacy related risks can include one or all of the following:

* Risks to students, staff, patients, research participants, or other third parties (for example, ill-use or overuse of research participant data, loss of anonymity, intrusion into the private lives through monitoring activities, lack of transparency, fairness and lawfulness of data processing activities etc.).
* Compliance risks e.g. breach of the General Data Protection Regulation (GDPR) or other health related legislation
* inherent or residual risks to NUIG (for example, project failure and associated costs, legal penalties or claims, damage to NUIG’s reputation, loss of trust of patients or the public).

1. **Health Research**

**NB:** Please note that specific conditions attach to the conducting of Health Research. A NUI Galway A Researcher must have the explicit consent of a patient of a project participant for Health Research or seek a Declaration from the Consent Declaration Committee. Please note that for Health Research there are other mandatory requirements which must be complied with which are set out in the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018.If you are conducting Health Research, you must additionally fill out Appendix 4 of this DPIA.Please see the Health Research Board for Guidance on Health Research : [**https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/health-research-regulations-2018/**](https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/health-research-regulations-2018/)

1. **Instructions for completion**

Once you have completed all the questions on the DPIA you should forward to the Data Protection Officer who will provide feedback on any risks identified and recommendations on the actions or controls needed to address those risks.

It is the responsibility of the project owner, Head of School or Head of Unit to ensure the required controls are put in place and to sign off on any risks arising from the processing.

The DPIA should be updated to reflect any material changes to the processing as the project or activity progresses.

|  |  |  |
| --- | --- | --- |
| step | Question | Answer*Please include your responses in the column BELOW:* |
| 1. | IDENTIFY the NEED FOR A dpia | |
|  | Explain broadly what the project/service or proposed research project aims to achieve and what type of processing of personal data it involves. Please summarise why your unit has identified the need for a DPIA. |  |
|  | DESCRIBE THE PROCESSING | |
|  | **Describe the nature of the processing:**  The nature of the processing is what a project plans to do with the personal data.  **Please describe:**   1. how the personal data is collected? 2. how the personal data is stored? 3. how the personal data is used? 4. who has access to the personal data? 5. who the personal data is shared with? 6. whether the project, unit or process will use any third-party processors? 7. how long will the personal data be kept? 8. what security measures are in places? 9. whether the project, unit or processes are using any new technologies; whether you are using any novel types of processing? 10. which screening criteria you have flagged as likely high risk?   Please refer to a flow diagram or other way of describing data flows, if relevant. |  |
|  | **Describe the scope of the processing:**  The scope of the processing is what the processing covers.  **Please describe:**   1. the nature of the personal data; 2. the volume and variety of the personal data; 3. the sensitivity of the personal data; 4. the extent and frequency of the processing; 5. the duration of the processing; 6. the number of data subjects involved; and the geographical area covered. |  |
|  | **Describe the content of the processing:**  The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. **Please describe:**   1. the source of the data; 2. the nature of the University relationship with the individuals; 3. the extent to which individuals have control over their data; the extent to which individuals are likely to expect the processing; 4. whether they include children or other vulnerable people; 5. any previous experience of this type of processing; 6. any relevant advances in technology or security; 7. any current issues of public concern; and 8. Identify where your project or unit have signed up to any approved code of conduct or certification scheme (if applicable or once any have been approved). |  |
|  | **Describe the purposes of the processing:**   1. Outline what is to be achieved by the processing activity. 2. Outlined the intended effect on data subjects. 3. Identify any benefits of the processing both for the University, data subjects and generally. |  |
|  | conSULTATION PROCESS | |
|  | **Consider how to consult with relevant stakeholders.**   1. Please consult with any relevant **internal stakeholders** (eg ISS, TTO, Research Office, Procurement or other?), with a view to identifying the technical aspects of information collection, storage and processing and how the difference elements of the project will fit together in operation. 2. Please consider if any **external data processors** who may be engaged or to whom personal data might be disclosed as part of the project should also be consulted with. 3. Please seek the views of individuals (or their representatives) unless there is a good reason not to. In most cases it should be possible to consult individuals in some form. If you decide that it is not appropriate to consult individuals then please record this decision as part of your DPIA, with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable. |  |
|  | ASSESS NECESSITY AND PROPORTIONALITY | |
|  | **Describe compliance and proportionality measures in particular:**   * What is the lawful basis for processing (please see **Appendix 2**)?   Under data protection legislation, organisations must have a valid legal basis in order to process personal data. For example, the University relies on legal and contractual obligations for the processing of student data for educational purposes and related administration and for the processing of staff data. The University relies of consent for other types of processing eg research participation, marketing etc.  **NB:** Please note for Health Research, you must have the explicit consent of the individual project participant or seek a consent declaration from the Consent Declaration Committee.  **Please describe:**   1. If/how the project plans will help to achieve the project purpose. 2. Is there another reasonable way to achieve the same outcome? 3. how function creep will be prevented (eg potential (“*the gradual widening of the use of technology or system beyond the purpose for which hit was originally intended especially when this leads to potential invasion of privacy*”)? 4. how data quality will be achieved/ensured; 5. how data minimisation will be achieved/ensured; 6. how privacy information will be provided to data subjects; 7. how individuals’ rights will be implemented and supported; 8. the measures to ensure that data processors (where relevant) are compliant with data protection obligations; 9. the safeguards for international transfers (where relevant) (please see NUI Galway Data Protection website FAQ Section on the protections which can be put in place for international transfers). |  |
|  | IDENTIFY AND ASSESS RISKS  This step involves examining the project design to assess what data protection issues arise in the project and to identify any risks it may expose individuals to as well as any data protection related risks that the project might create for the University. Please consider the potential impact on individuals and any harm or damage that might be caused by the personal data processing – whether physical, emotional or material. Please identify whether the processing could possibly contribute to: inability to exercise rights (including but not limited to privacy rights); inability to access services or opportunities; loss of control over the use of personal data; discrimination; identity theft or fraud; financial loss; reputational damage; physical harm; loss of confidentiality; reidentification of pseudonymised data; or any other significant economic or social disadvantage You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data). To assess whether the risk is a high risk, please consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.  Having identified the risks it is then necessary to assess which are going to pose the greatest threat by looking at both the likelihood of the risk occurring and the impact that might result. This provides the overall risk assessment.  **Practical examples of risks to be considered are provided at Appendix 3** | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe the source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary.  **Has the identified risk been placed on your Local Risk register?** | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|  | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | IDENTIFY MEASURES TO REDUCE RISK  This Section following on from the identification of data protection risks at Section 5 above with the aim of minimising the data privacy risk associated with the project insofar as possible. Please seek to identify data protection solutions to reduce the impact of the project on data protection. This can be done by looking at each of the risk identified as part of Section 5 above and seeking to address it individually or as part of a privacy solution which may address a number of risks together.  In some cases, data protection solutions may be able to eliminate some risks for example by abandoning unnecessary parts of a project which create unique risks. In other cases, data protection solutions may simply mitigate against risk or reduce the significance of data breaches. The nature of the solutions will depend on the types of risks that have been identified and the aims of the project. Options for reducing that risk might include for example: deciding not to collect certain types of data; reducing the scope of the processing; reducing retention periods; taking additional technological security measures; training staff to ensure risks are anticipated and managed; anonymising or pseudonymising data where possible; writing internal guidance or processes to avoid risks; using a different technology; putting clear data sharing agreements into place; making changes to privacy notices; offering individuals the chance to opt out where appropriate; or implementing new systems to help individuals to exercise their rights. This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks.  Under GDPR if there are remaining high risks then the University’s Data Protection Officer will need to be consulted in the first instance. If, during the DPIA process, the University as the Data Controller has identified and taken measures to mitigate any risks to personal data, it is not necessary to consult with the Data Protection Commissioner before proceeding with the project. Should the DPIA suggest that any identified risks cannot be managed, and the residual risk remains high the Data Protection Commissioner should be consulted with before moving forward with the project. | | | | | |
|  | Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in Step 5 | | | |  | |
|  | **Risk** | **Options to reduce or eliminate risk** | **Effect on risk**  **(select one)** | **Residual risk**  **(select one)** | | **Measure approved** |
|  |  |  | Eliminated  Reduced  Accepted | Low  Medium  High | | Yes  No |
|  |  |  | Eliminated  Reduced  Accepted | Low  Medium  High | | Yes  No |
|  |  |  | Eliminated  Reduced  Accepted | Low  Medium  High | | Yes  No |
|  |  |  | Eliminated  Reduced  Accepted | Low  Medium  High | | Yes  No |
|  |  |  | Eliminated  Reduced  Accepted | Low  Medium  High | | Yes  No |
|  |  |  | Eliminated  Reduced  Accepted | Low  Medium  High | | Yes  No |

## Practical examples of risk reduction are available at: http://gdprandyou.ie/DATA-PROTECTION-IMPACT-ASSESSMENTS-DPIA/

## Please send your completed Data Protection Impact Assessment (DPIA) form to the Data Protection Officer at: [dataprotection@nuigalway.ie](mailto:dataprotection@nuigalway.ie)

## 

|  |  |  |  |
| --- | --- | --- | --- |
|  | SIGN OFF AND RECORD OUTCOMES  The primary aim of conducting a DPIA is to identify and minimise the data protection risks involved in a project.  If the data privacy risks which have been identified are not capable of mitigation consistent with the goals of a project and it would not be proportionate to accept them, this stage should be used for re-evaluating the viability of the project. | | |
|  | **Item** | **Name/date** | **Notes** |
|  | Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion |
|  | Residual risks reviewed/approved by: |  | If accepting any residual high risk consult the Data Protection Commission before going ahead |
|  | DPO advice provided: |  | DPO should advise on compliance Step 6 measures and whether processing can proceed |
|  | Summary of DPO advice: | | |
|  | DPO advice accepted or overruled by: |  | If overruled you must explain your reasons |
|  | 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 DPO should also review ongoing compliance with DPIA |

INTEGRATE OUTCOMES INTO PLAN

Once the DPIA has been signed off it is necessary to put the findings of the DPIA into action by integrating any necessary changes into the plans for the project

KEEP UNDER REVIEW

As part of the implementation of the DPIA you should keep data protection issues under regular review. In particular you should assess whether the data protection solutions implemented are having the intended effect of mitigating data protection risks.

**Appendix 1**

**NUIG will carry out a DPIA where it plans to:**

* Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
* Process special category data or criminal offence data on a large scale.
* Systematically monitor a publicly accessible place on a large scale.
* Use new technologies processing personal data.
* Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit.
* Carry out profiling on a large scale.
* Process biometric or genetic data.
* Combine, compare or match data from multiple sources.
* Process personal data without providing a privacy notice directly to the individual.
* Process personal data in a way which involves tracking individuals’ online or offline location or behaviour.
* Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
* Process personal data which could result in a risk of physical harm in the event of a security breach.

**We consider whether to do a DPIA if we plan to carry out any other:**

-Evaluation or scoring.

-Automated decision-making with significant effects.

-Systematic

-Processing of sensitive data or data of a highly personal nature.

-Processing on a large scale.

-Processing of data concerning vulnerable data subjects.

-Innovative technological or organisational solutions.

-Processing involving preventing data subjects from exercising a right or using a service or contract.

* We consider carrying out a DPIA in any major project involving the use of personal data.
* If we decide not to carry out a DPIA, we document our reasons.
* We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

**Appendix 2**

**Legal Base for using**

**Personal Data and Special Categories of Personal Data**

The legal reasons for processing Personal Data are as follows:

1. **Consent:** Any consent must Be “freely given, specific, informed and unambiguous”. Be expressed affirmatively “either by a statement or by clear affirmative action”, i.e. they must check the box, not un-check it. Be revocable and scalable Be sought for a given purpose - where data is used for different purpose re-consent is required, i.e. the wording of the original consent statement is important.
2. **A contract with the individual**: for example, to supply goods or services they have requested, or to fulfil an obligation under an employee contract. This will cover anyone employed by the institution, including external examiners and visiting and honorary academic post holders, as well as any circumstance involving students’ contractual obligations to the institution.
3. **Compliance with a legal obligation**: when processing data for a particular purpose is a legal requirement.
4. **Vital interests**: for example, when processing data will protect someone’s physical integrity or life (either the data subject’s or someone else’s).
5. **A public task**: for example, to complete official functions or tasks in the public interest. This would include for example fulfilling the objects and functions as set out in the Universities Act 1997:
6. There is another lawful ground – **legitimate interests** – but it only applies to private sector units. Some aspects of what the University does may not fall within the public task therefore we might be able to use it for commercial activities.

The legal reasons for the processing of “Special Categories of Personal Data” are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as “special categories” of personal data. The special categories are:

1. personal data revealing racial or ethnic origin,
2. political opinions,
3. religious or philosophical beliefs,
4. trade union membership,
5. genetic data and biometric data processed for the purpose of uniquely identifying a natural person,
6. data concerning health,
7. data concerning a natural person’s sex life or sexual orientation.

Processing of these special categories is prohibited, except in limited circumstances as set out in summary below:

1. explicit consent (unless law prohibits the processing and that prohibition cannot be over ridden by the person)
2. legal obligation on the controller in respect of employment, social security etc.
3. protection of the vital interests of the data subject or another person where the data subject is legally or physically incapable of giving consent
4. legitimate activities of a non-profit making organisation with a political, philosophical or trade-union aim
5. the personal data is manifestly made public by the data subject
6. necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
7. substantial public interest (based on a Union or State law which is proportionate to the aim pursued, respects the essence of the right to data protection and provides specific measures to protect the fundamental rights and freedoms of the data subject)
8. necessary for the purposes of preventative or occupational medicine, assessment of working capacity, medical diagnosis, provision of health or social care or treatment or the management of health and social care systems and services on the basis of Union or State law
9. public health (on the basis of Union or State law)
10. archiving in the public interest, research and statistics.
11. Processing of personal data relating to criminal convictions and offences may only be carried out under the control of official authority or when authorised by Union or State law (A new and separate EU Data Protection Directive applies to the processing of such personal data).

Recitals 41-50 of the GDPR provide additional guidance on sensitive personal data.

**Appendix 3**

**Examples of the types of risks that we should be alert for in the DPIA process are outlined below.**

**Examples of risks to individuals:**

* Inappropriate disclosure of personal data internally within the University due to a lack of appropriate controls being in place.
* Accidental loss of electronic equipment by University’s personnel may lead to risk of disclosure of personal information to third parties.
* Breach of data held electronically by “hackers”.
* Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
* Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
* Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
* Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
* Personal data being used for automated decision making may be seen as excessively intrusive.
* Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
* Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
* Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
* Collection of data containing identifiers may prevent users from using a service anonymously.
* Data may be kept longer than required in the absence of appropriate policies.
* Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
* Data may be transferred to countries with inadequate data protection regimes.

**Examples of Corporate Risks:**

* Failure to comply with the GDPR may result in investigation, administrative fines, prosecution, or other sanctions.
* Failure to adequately conduct a DPIA where appropriate can itself be a breach of the GDPR.
* Data breaches or failure to live up to student, staff or other service users expectations regarding privacy and personal data are likely to cause reputational risk.
* Public distrust of the University’s use of personal information may lead to a reluctance on the part of individuals to deal with the University.
* Problems with project design identified late in the design process, or after completion, may be expensive and cumbersome to fix.
* Failure to manage how the University keeps and uses information can lead to inefficient duplication, or the expensive collection and storage of unnecessary information.
* Unnecessary processing and retention of information can also leave the University at risk of non-compliance with the GDPR.
* Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against the University.

**Appendix 4**

**NUI Galway Data Protection Impact Assessment (DPIA) additional Mandatory Questions required under the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018****. You must answer all questions in this section as their fulfilment is a mandatory requirement if you are conducting Health Research.**

|  |  |  |
| --- | --- | --- |
|  | Please specify which arrangements are in place to ensure that personal data will be processed as is necessary; a) to achieve the objective of the health research and; b) to ensure that shall not be processed in such a way that damage or distress to the data subject? |  |
|  | Please specify the data controller; joint data controllers (if applicable) and any data processors involved in the research. |  |
|  | Please specify any person or organization who provides funding for, or otherwise supports, the project. |  |
|  | Please specify any person other than the named data controller, joint controllers or processors with whom it is intended to share any of the personal data collected (including where it has been pseudonymised or anonymised) and the purpose of such sharing. |  |
|  | The provision of training in data protection law and practice to anyone involved in carrying out the health research is a mandatory legal requirement. Please specify the provision of training. |  |
|  | Has a “risk assessment” and/or “data protection impact assessment” been carried out, taking in to account local policy and/or legal requirements? |  |
|  | Please specify the measures in place that demonstrate compliance with the data minimisation principle (Is it adequate, relevant and limited to what is necessary?) The data minimisation principle specifies that Data Controllers must limit personal data collection, storage, and usage to data that is relevant, adequate, and absolutely necessary for carrying out the purpose for which the data is processed. |  |
|  | Please specify the controls in place to limit access to the personal data undergoing processing in order to prevent unauthorised consultation, alteration, disclosure or erasure of personal data. |  |
|  | Please specify the controls in place to log whether and by whom personal data has been consulted, altered, disclosed or erased. |  |
|  | Please specify measures to protect the security of the personal data concerned. |  |
|  | Please specify the arrangements to anonymise, archive or destroy personal data once the health research has been completed. |  |
|  | Please specify other technical and organisational measures designed to ensure that processing is carried out in accordance with the Data Protection Regulation, together with processes for testing and evaluating the effectiveness of such measures. |  |
|  | Please specify which arrangements are in place to ensure that personal data is processed in a transparent manner. |  |