Criteria and guidelines for conducting a DPIA

**Data Protection Impact Assessment (DPIA)**

Table of Contents

[1. Document Control Summary 3](#_Toc141451271)

[2. Introduction / Context 3](#_Toc141451272)

[3. Purpose 3](#_Toc141451273)

[4. Scope 3](#_Toc141451274)

[5. Definitions 4](#_Toc141451275)

[6. Procedure Details: 4](#_Toc141451276)

[6.1 Procedure Overview 4](#_Toc141451277)

[6.2 Identify the need for a DPIA 4](#_Toc141451278)

[6.3 When is a DPIA not necessary? 6](#_Toc141451279)

[6.4 Who must carry out the DPIA? 6](#_Toc141451280)

[6.5 Steps to carry out a DPIA 6](#_Toc141451281)

[6.5.1 Describe the project 6](#_Toc141451282)

[6.5.2 Describe the envisaged processing - information flows/lifecycle 6](#_Toc141451283)

[6.5.3 Consider the following - 7](#_Toc141451284)

[6.5.4 Consult with Stakeholders 7](#_Toc141451285)

[6.5.5 Assess Necessity and Proportionality: 8](#_Toc141451286)

[6.5.6 Identify and Assess Risks: 8](#_Toc141451287)

[6.5.7 Identify privacy solutions and controls to reduce or eliminate the risks: 8](#_Toc141451288)

[6.6 Ongoing management of a DPIA 9](#_Toc141451289)

[6.7 How to contact us 10](#_Toc141451290)

[7. Related Documents 10](#_Toc141451291)

[8. Appendix 10](#_Toc141451292)

[Appendix A – Examples of Risks and Potential Solutions 10](#_Toc141451293)

[Example of Risks to Individuals: 10](#_Toc141451294)

[Examples of Corporate Risks: 11](#_Toc141451295)

[Examples of Compliance Risks: 11](#_Toc141451296)

[Examples of data protection solutions (measures to address risks): 11](#_Toc141451297)

[9. Document Management 12](#_Toc141451298)

[9.1 Version Control 12](#_Toc141451299)

[9.2 Document Approval 13](#_Toc141451300)

[9.3 Document Ownership 13](#_Toc141451301)

[9.4 Document Classification 13](#_Toc141451302)

# 1. Document Control Summary

# 

|  |  |
| --- | --- |
| **Area** | **Document Information** |
| Author | Information Governance Office |
| Owner | Head of Governance and Compliance |
| Reference number |  |
| Version | 1.1 |
| Status |  |
| ~~Approved by~~ / to be approved by | Head of Governance and Compliance |
| Approval date |  |
| Next review date | 2025 |
| Document Classification | Public |

# 2. Introduction / Context

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks at the start of any **major project** involving the use of personal data, or if you are making a significant change to an **existing processing activity**. The final outcomes should be integrated back into your project plan.

# 3. Purpose

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of data subjects, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material, or non-material. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to eradicate the risks altogether but should help to minimise risks and assess whether or not any remaining risks are justified.

Therefore, a DPIA is a way to systematically and comprehensively analyse the processing and identify and minimise data protection risks. It is an important tool for building and demonstrating compliance with the GDPR principle of accountability.

# 4. Scope

The GDPR does not require a DPIA to be carried out for every processing operation. The carrying out of a DPIA is only mandatory where processing of personal data is “***likely to result in a high risk to the rights and freedoms****” of data subjects (the person to which the data relates)* (Article 35 GDPR). When a School or Service Area undertakes a processing activity which would be likely to have privacy impact upon students, staff, the public, etc. they should conduct a DPIA of these risks and identify measures, which would help to reduce these risks.

# 5. Definitions

Highlight, where needed, any new definitions for clarity.

# 6. Procedure Details:

## 6.1 Procedure Overview

DPIAs are mandatory for any new high-risk processing projects. It is also recommended for high-risk data processing which has taken place prior to May 2018 to ensure the privacy risks to individual are still mitigated. (For examples of risks please see Appendix A)

Even if there is no specific indication of likely high risk, it is good practice to conduct a DPIA at the start of any **major project** involving the use of personal data, or if you are making a significant change to an **existing processing activity** involving the use of personal data as a DPIA is a useful tool to comply with GDPR.

Please note that in some cases the DPIA will be an on-going process, for example where a processing operation is dynamic and subject to ongoing change. Carrying out a DPIA is a continual process, not a one-time exercise.

## 6.2 Identify the need for a DPIA

In order to determine whether the processing is likely to result in a high risk the factors below should be considered.

If you project involves any of the following you must carry out a DPIA.

* **Evaluation and scoring (including profiling and predicting) -** especially concerning a data subject’s performance at work, economic situation, health, personal preferences, reliability or behaviour, location, or movements. An example would be offering genetic tests in order to assess or predict disease/health risks or gathering social media profile data for generating profiles for contact directories or marketing. (GDPR recital 71 and 91).
* **Automated decision-making with legal or similar significant effects** a decision about a data subject producing legal effects concerning the natural person made by automated means without any human involvement. An example would be an online decision to award a loan or a recruitment aptitude test that uses pre-programmed algorithms and criteria.  (Article 35(3)(a). The processing may lead to the exclusion or discrimination against individuals.
* **Systematic monitoring -** processing used to observe, monitor, or control data subjects including through a publicly accessible place on a large scale. For example, using a camera to monitor driving behaviours on a road. (Article 35(3)(c)). The personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used, and it may be impossible for individuals to avoid being subject to such processing in frequent public space.
* **Sensitive data or data of highly personal nature -** this includes special categories of data - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data concerning a person’s sex life or sexual orientation, genetic data, biometric data (Article 9) as well as criminal data as defined in Article 10. An example would be a hospital keeping patient medical records or an organisation keeping offender’s details. This also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data and financial data. In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by an individual in the course of purely personal or household activity (such as smart technology, cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be perceived as very intrusive.
* **Data processed on a large scale -** while the term ‘large scale’ is not defined, the regulators recommend the following is taken into account: (a) the number of data subjects concerned; (b) the volume and range of data been processed; (c) the duration and permanence of the processing; (d) the geographic extent of the processing activity. (Recital 91)
* **Datasets have been matched or combined -** for example, two or more data processing operations performed for different purposes and/or by different data controllers been combined in way that would exceed reasonable expectation of the data subject.
* **Data concerning vulnerable data subjects -** because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data, e.g. children are considered as not able to knowingly oppose or consent to processing of personal data. Patients, elderly people, and asylum seekers would also be considered vulnerable data subjects
* **Innovative use or applying technological or organisational solutions -** for example combining use of fingerprint and face recognition for improved physical access control, using a video analysis system to single out cars and recognise licence plates. The GDPR makes it clear (Article 35(1) and Recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals’ rights and freedoms.
* **Data transfer across borders outside the** **EU -** taking into consideration the envisaged country/ies of destination, the possibility of further transfers
* **When processing prevents the data subject from exercising a right or using a service or a contract** - for example, processing a public area that people passing cannot avoid or processing that aims to refuse data subjects access to a service or contract (bank screens its customers against a credit reference database in order to decide whether to offer a loan). When the processing in itself “prevents data subjects from exercising a right or using a service or a contract” (Recital 91). This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or refusing data subjects’ access to a service or entry into a contract.

## 6.3 When is a DPIA not necessary?

Schools and Service Areas are **not** required to carry out a DPIA in the following cases:

* Where the processing is not likely to result in a high risk to the rights and freedoms of individuals.
* Where the nature, scope, context, and purposes of the processing are very similar to the processing for which a DPIA has already been carried out.
* Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out.

## 6.4 Who must carry out the DPIA?

It is the responsibility of the project team (Data Controller) to ensure that a DPIA is carried out for any new project, product, process, system, contract and/or use of end user or employee personal data or changes to existing data processing activities.

## 6.5 Steps to carry out a DPIA

### 6.5.1 Describe the project

Identify the purpose, scope, duration, and goals of the project, identify internal and external stakeholders. Include an assessment of the necessity and scale of the processing activity in relation to the purpose. Note the intended outcome for data subjects and the expected benefits for you or for society as a whole.

### 6.5.2 Describe the envisaged processing - information flows/lifecycle

Identify what information is collected, why it is collected, how it is collected, the intended use of the information, with whom the information is shared, the consent and choice rights of the data subjects and how the information will be managed, stored, secured, and destroyed. You should provide details of the assets on which personal data rely e.g., hardware, software, networks, or paper transmission channels. You may refer to a flow diagram. You should also say how many individuals are likely to be affected by the project and the nature, volume, variety, and sensitivity of the personal data including information on whether the data subjects include children or other vulnerable people.

You should identify the legitimate interest in carrying out the processing.   
When codes of conduct (outlined in the GDPR) are put in place, the description of processing will have to include measures taken to comply with these codes of conduct and period for which the personal data will be stored.

### 6.5.3 Consider the following -

* Will the project involve the collection of new information about individuals?
* Will the project compel individuals to provide information about themselves?
* Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
* Are you using information about individuals for a purpose it is not currently used or in a way it is not currently used?
* Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
* Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?
* 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 private.
* Will the project require you to contact individuals in ways that they may find intrusive?

### 6.5.4 Consult with Stakeholders

You should seek the views of data subjects (or their representatives) unless there is a good reason not to. In most cases it should be possible to consult individuals in some form, e.g., internal stakeholders such as project management team, IT, procurement, potential suppliers (processors), communications teams, customer facing roles, researchers, senior management, and then external stakeholders including people who will be affected by the project and members of the public.

However, if you decide that it is not appropriate to consult individuals then you should record this decision as part of your DPIA, with a clear explanation, e.g., you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts e.g., existing students or employees, you should design a consultation process to seek the views of those particular individuals or their representatives.  
If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process or targeted research. If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.  
If you use a data processor, you may need to ask them for information and assistance.

### 6.5.5 Assess Necessity and Proportionality:

You should consider -

* Do your plans help to achieve your purpose?
* Is there any other reasonable way to achieve the same result?
* What is your lawful basis for the processing,
* How you will prevent function creep i.e., using the data for more than the original purpose,
* How you intend to ensure data quality,
* How you intend to ensure data minimisation,
* How you intend to provide privacy information to individuals,
* How you implement and support individual’s rights,
* Have you implemented measures to ensure your processors comply
* Have you identified safeguards for international transfers

### 6.5.6 Identify and Assess Risks:

Identify the key privacy risks to the data subjects and the associated compliance and corporate risks, giving consideration to the likelihood and severity of the risk and the impact of the risk. Conduct a compliance check against legal, regulatory, industry and organisational standards. Schools and Service Areas are required to document the risks involved in the processing and identify the likelihood and severity of the identified risk (assessment of risks).   
Evaluate how information handling practices at each stage of the project may affect privacy as well as the potential impact on individuals and any harm or damage that might be caused by your processing, whether physical, emotional, or material. In particular, look at whether the processing could possibly contribute to:

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.

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 rating.

### 6.5.7 Identify privacy solutions and controls to reduce or eliminate the risks:

Identify appropriate measures in place to address and mitigate risks, identify alternatives to collection and handling processes, identify appropriate technical controls to mitigate privacy risks e.g., encryption, relevant security measures. Describe organisational measures e.g., robust policies staff training, etc. Describe the actions you could take to reduce the risks and any future steps which would be necessary. Schools and Service Areas are required to assess whether the impact on privacy is necessary and proportionate to the outcomes of the new product, process, system, contract, and/or use of end user or employee personal data (assessment of the necessity and proportionality).   
See the appendices below for examples of actions you could take to reduce the impact/likelihood and mitigate the risk.

**6.5.8 Document the Results / Signing off on the outcomes of the DPIA:**

Ensure appropriate sign off of outcomes is formally documented and retained.

Record what additional measures you plan to take, whether each risk has been eliminated, reduced, or accepted, the overall level of ‘residual risk’ after taking additional measures and whether the Data Protection Commission needs to be consulted.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, you need to contact the Information Governance Office who will consult with the Data Commissioner before you can go ahead with the processing. As part of the sign-off process, you should ask the Information Governance Office to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons. You should also record any reasons for going against the views of individuals or other consultees.

**6.5.9 Implement and Review**

**You must integrate the outcomes of your DPIA i.e., the data protection solutions, back into your project plans**. Create a summary describing the rationale for the final design choice or business process, ensure the controls and actions identified are tracked through to completion to ensure the rights of the data subject are upheld. If appropriate, publish the summary to provide transparency and accountability. This could help foster trust in your processing activities and improve individuals’ ability to exercise their rights by explaining the reasoning behind the design of systems and how they are engineered with privacy considerations in mind.  
You should identify any action points and who is responsible for implementing them. You should monitor the ongoing performance of the DPIA.

## 6.6 Ongoing management of a DPIA

The DPIA must be a living document throughout the lifecycle of the processing and Schools and Service Areas must ensure that it is kept up to date at all times. The revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over longer time. Where necessary, the Head of School or Service Area will conduct a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by processing operations e.g. where a significant change to the processing operation has taken place in terms of context, risks, purposes, personal data processed, recipients, data combinations, security measures and/or international transfers.

Where necessary, the Information Governance Office may also independently conduct a review to assess if processing is performed in accordance with the DPIA.

**Consultation -** Please note where the output of a DPIA indicates that the processing involves a high risk which a School or Service Area cannot mitigate or which the costs of mitigation are too high, the Head of School/Service is required, with the input of the Information Governance Office, to consult with the Office of the Data Protection Commissioner prior to commencing the processing.

## 6.7 How to contact us

For further information and advice about completing a Data Protection Impact Assessment please contact:

**Data Protection Officer, TU Dublin –**

* By email: [dataprotection@tudublin.ie](mailto:dataprotection@tudublin.ie)
* In writing: The Information Governance Office, TU Dublin, Blanchardstown Road North, Dublin 15, D15 YV78
* Tel: +353 1 220 7453 +353 1 220 7225 + 353 1 220 5243

# 7. Related Documents

DPIA Initial Assessment Template

Data Protection Impact Assessment Template

# 8. Appendix

# Appendix A – Examples of Risks and Potential Solutions

Example of Risks to Individuals:

* Inappropriate disclosure of personal data internally due to a lack of appropriate controls being in place.
* Data may be kept longer than required in the absence of appropriate policies.
* Loss of confidentiality, e.g., accidental loss of electronic equipment may lead to risk of disclosure of personal information to third parties.
* Breach of data held electronically by “hackers.”
* Discrimination, e.g., vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
* Re-identification of pseudonymised data.
* Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
* Loss of control over the use of their personal data, e.g., being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
* Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals and may inadvertently allow individuals to be identified from anonymised data.
* 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.
* inability to exercise rights
* inability to access services or opportunities
* identity theft or fraud
* financial loss
* reputational damage
* physical harm
* any other significant economic or social disadvantage.

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 customer expectations regarding privacy and personal data are likely to cause reputational risk.
* Public distrust of organisation’s use of personal information may lead to a reluctance on the part of individuals to deal with the organisation.
* Problems with project design identified late in the design process or after completion, may be expensive and cumbersome to fix.
* Unnecessary processing and retention of information can also leave you 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 organisation. Under the GDPR, the University may also be liable for non-material damage.

Examples of Compliance Risks:

* The organisation may face risks of prosecution, significant financial penalties, or reputational damage if it fails to comply with the GDPR. Individuals affected by a breach of the GDPR can seek compensation for both material and non-material damage.
* Failure to carry out a DPIA where appropriate is itself a breach of the legislation, as well as a lost opportunity to identify and mitigate against the future compliance risks a new project may bring.

Examples of data protection solutions (measures to address risks):

* Deciding not to collect or store particular types of information.
* Reducing the scope of the processing
* Devising strict retention periods, designed to minimise the length of time that personal data is retained.
* Planning secure destruction of information.
* Ensuring that staff are properly trained and are aware of potential privacy risks to ensure risks are anticipated and managed.
* Creating internal guidance and protocols for information handling within the project.
* Producing guidance for staff on how to use new systems, as a reference point in the event of any uncertainty relating to the handling of information and how to share data if appropriate.
* Making changes to Privacy Notices and Records of Processing Activities.
* Implementing appropriate and/or additional technological security measures.
* Consider using a different technology.
* Assessing the need for new IT systems to safely process and store the data and providing staff with training in any new system adopted.
* Assessing the possibility of using anonymised or pseudonymised data as part of the project to reduce identification risks.
* Ensuring that data subjects are fully informed about how their information will be used if appropriate.
* Offering data subjects, the chance to opt out where appropriate.
* Providing a contact point for individuals to raise any concerns they may have with the organisation.
* Implementing new systems to help individuals to exercise their rights.
* Adding a human element to review automated decisions.
* If using external data processors, selecting appropriately experienced data processors, and putting in place legal arrangements (Data Sharing Agreements) to ensure compliance with data protection legislation.
* Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks. You should ask the Information Compliance Office for advice.

# 9. Document Management

## 9.1 Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSION NUMBER** | **VERSION DESCRIPTIN /**  **CHANGES MADE** | **AUTHOR** | **DATE** |
| *1.0* | *Initial Guidelines* | *Information & Compliance Working Group* |  |
| *1.1* | *Review and Update* | *Information Governance Team* | *28.07.23* |
|  |  |  |  |

## 9.2 Document Approval

|  |  |  |
| --- | --- | --- |
| **VERSION NUMBER** | **APPROVAL DATE** | **APPROVED BY (NAME AND ROLE)** |
| *1.1* |  | *Head of Governance and Compliance* |
|  |  |  |
|  |  |  |

## 9.3 Document Ownership

Document Owner – Head of Governance and Compliance

Document Update - Information Governance Senior Manager

## 9.4 Document Classification

Document is classified as Public and is available to all staff, students and members of the public who wish to view it.