**TU Dublin Policy**

Data Protection Policy V1.1

Table of Contents

[1. Document Control Summary 2](#_Toc633028555)

[2. Introduction / Context 2](#_Toc1398022908)

[3. Purpose 2](#_Toc1765635259)

[4. Scope 2](#_Toc395050602)

[5. Common Terms and Definitions 3](#_Toc405317448)

[6. Policy Details: 5](#_Toc1297495137)

[6.1 Policy Overview 5](#_Toc2132580291)

[6.2 Roles and Responsibilities 5](#_Toc440806587)

[6.3 Personal Data Processing Principles 7](#_Toc1399903653)

[6.4 Principles of Lawfulness, Fairness and Transparency 7](#_Toc2028110232)

[6.4.1 Lawful basis for processing personal data 7](#_Toc2133711622)

[6.4.2 Direct Marketing 8](#_Toc1677402447)

[6.4.3 Processing of Special Categories of Personal Data 8](#_Toc181260084)

[6.4.4 Transparency – Data Protection Notices (Fair Disclosure Notices) 9](#_Toc2103167571)

[6.4.5 Data Collection from Third Party Sources 9](#_Toc1350051163)

[6.5 Principles of Data Minimisation 10](#_Toc1116447054)

[6.6 Principles of Purpose Limitation 10](#_Toc161689431)

[6.7 Principles of Data Accuracy 10](#_Toc589791946)

[6.8 Principles of Data Storage Limitation 10](#_Toc385148801)

[6.9 Security of Personal Data (Integrity and Confidentiality) 11](#_Toc1743153723)

[6.9.1 Information Security 11](#_Toc1550947872)

[6.9.2 Data Breach (Unauthorised Disclosure) 11](#_Toc1710622714)

[6.9.3 Data Encryption 12](#_Toc602442579)

[6.9.4 Data Anonymisation/Pseudonymisation 12](#_Toc1244016096)

[6.10 Principle of Accountability 12](#_Toc841070244)

[6.10.1 Data Protection by Design and by Default 12](#_Toc1458621058)

[6.10.2 Data Protection Impact Assessment (DPIA) 13](#_Toc2123126174)

[6.10.3 Record of Processing Activity and Data Inventories 13](#_Toc1266225722)

[6.10.4 Transfer and Sharing of Data 14](#_Toc1320359149)

[6.10.5 Third Parties Relationships and Data Sharing Agreements 15](#_Toc779852168)

[6.11 Data Subjects Rights 15](#_Toc473535236)

[6.11.1 Subject Access Requests (SARs) and Subject Rights Requests (SRRs) 16](#_Toc411861325)

[6.11.2 Fees and refusals of SARs under Data Protection Legislation 17](#_Toc2085788304)

[6.12 CCTV 17](#_Toc1256380393)

[6.13 Data Protection Officer (DPO) 17](#_Toc882947799)

[7. Related Documents 18](#_Toc561643914)

[8. Conclusions 18](#_Toc1587948052)

[9. Appendices 18](#_Toc1227069760)

[10. Document Management 19](#_Toc701415761)

[10.1 Version Control 19](#_Toc317173342)

[10.2 Document Approval 19](#_Toc2038467053)

[10.3 Document Ownership 19](#_Toc92770573)

[10.4 Document Classification 20](#_Toc405849833)

# 

# 1. Document Control Summary

|  |  |
| --- | --- |
| **Area** | **Document Information** |
| Author | Information Governance Office |
| Owner | Head of Governance and Compliance |
| Reference number |  |
| Version | 1.1 |
| Status | For Approval |
| Approved by | Governing Body |
| Approval date | 07/07/2023 |
| Next review date | 2024 |
| Document Classification | Public |

# 2. Introduction / Context

The University intends to meet all relevant data protection, privacy and security requirements, whether originating from legal, regulatory, or contractual obligations.

The University also embraces Privacy by Design and Privacy by Default principles in all its services and functions both current and future. This ensures that the public can maintain a high level of trust in the University’s competence and confidentiality while handling personal data.

This policy should not be viewed in isolation. Rather, it should be considered as part of the TU Dublin suite of compliance policies and procedures.

# 3. Purpose

Technological University Dublin (the University) as a data controller, has established this Policy to comply with all relevant European Data Protection requirements and has aligned same to relevant internal policies, procedures and controls. In particular this document sets out the University’s policy regarding personal data collection/processing/sharing for all Schools and Service Areas, staff and students.

# 4. Scope

This Data Protection Policy applies to:

* any person who is employed by the University who receives, handles, or processes personal data in the course of their employment.
* any student of the University who receives, handles, or processes personal data in the course of their studies for administrative, research or any other purpose.
* third party companies/individuals (data processors) that receive, handle, or process personal data on behalf of the University.

This applies whether you are on campus, travelling or working remotely.

# 5. Common Terms and Definitions

|  |  |
| --- | --- |
| **Consent** | Means any freely given, specific, informed, and unambiguous indication of the Data Subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her. In this context, “signifies” means that there must be some active communication between the parties. Thus, a mere non-response to a communication from the University cannot constitute Consent. |
| **Data Classification** | A process whereby information/data is classified in accordance with the impact of data being accessed inappropriately or data being lost. The resulting data classification needs to be applied when handling data. It is the responsibility of data owners to classify the data under their control. |
| **Data Controller** | Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed. A Data Controller can be the Sole Data Controller or a Joint Data Controller with another person or organisation or a Separate Data Controller. |
| **Data Processor** | ‘processor’ means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller;  It is possible for one University or person to be both a Data Controller and a Data Processor, in respect of distinct sets of Personal Data. |
| **Data Protection Commissioner** | Means the Office of the Data Protection Commissioner (DPC) in Ireland. |
| **Data Subject** | Refers to the individual to whom Personal Data held relates, including employees, students, customers, suppliers. |
| **Destruction** | Where the personal data no longer exists, or no longer exists in a form that is of any use to the Data Controller. |
| **Encryption** | The process of encoding information stored on a device that can add a further layer of security. It is considered an essential security measure where Personal Data is stored on a portable device or transmitted over a public network. |
| **GDPR** (General Data Protection Regulations) | Means EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the free movement of such Data. |
| **Loss** | Where the personal data may still exist, but the Data Controller has lost control of or access to it, or no longer has the data in its possession. |
| **Personal Data** | In Article 4 (1) of GDPR personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;  Examples of personal data include, but are not limited to:   * Name, email, address, home phone number * The contents of a student file or an employee HR file * Details about lecture attendance or course work marks * Notes of personal supervision, including matters of behaviour and discipline. |
| **Personal Data Breach** | In Article 4(12) of GDPR, a “personal data breach” is defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.” |
| **Processing** | Means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The terms “Process” and “Processed” should be construed accordingly. |
| **Restriction of processing** | means the marking of stored personal data with the aim of limiting their processing in the future; |
| **Sensitive Personal Data** | Sensitive Personal Data (or Special Category Personal Data) relates to specific categories of data which are defined as data relating to a person’s racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions, or the alleged commission of an offence; trade union membership. |
| **Third Party** | Means an entity, whether or not affiliated with the University, that is in a business arrangement with the University by contract, or otherwise, that warrants ongoing risk management. These Third-Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the University has an ongoing relationship. Third Party relationships, for the purposes of this Policy, generally do not include student or customer relationships.  In Article 4(10) of GDPR a ‘Third Party’ means a natural or legal person, public authority, agency, or body, other than the data subject, controller, processor, and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to Process Personal Data. |
| **Unauthorised or unlawful processing** | This may include disclosure of personal data to (or access to) recipients who are not authorised or do not have a lawful basis to have access to the personal data. |

All other terms used in the Data Protection Policy not referenced in this document, shall have the same meaning as in data protection legislation and/or local requirements.

# 6. Policy Details:

## 6.1 Policy Overview

This Data Protection Policy provides information about the ways in which TU Dublin (the University) collects, stores and uses personal data relating to individuals (data subjects). TU Dublin is the data controller of personal data and is subject to the [Data Protection Acts 1988 to 2018](http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html) and the [General Data Protection Regulation 2016/679](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN)

This Data Protection Policy relates to personal data received by the University where data subjects contact or provide personal data to the University directly and also to personal data received by the University indirectly (via a third party).

This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

The University is committed to complying with all applicable data protection, privacy and security laws and regulations. The suite of compliance policies adopted by the University create a common core set of values, principles and procedures intended to achieve a standard set of universal compliance parameters based on Data Protection Legislation.

Technological University Dublin (TU Dublin) is responsible for the processing of a significant volume of personal information across each of its Schools and Service Areas. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

* It is the responsibility of each School and Service Area to ensure that personal information is processed in a manner compliant with the relevant data protection legislation and guidance.
* The Information Governance office is available to Schools and Service Areas to provide guidance and advice pertaining to this requirement.
* All staff must appropriately protect and handle information in accordance with the TU Dublin Data Classification Policy.
* Personal Data is considered confidential information and requires the greatest protection level.

## 6.2 Roles and Responsibilities

|  |  |
| --- | --- |
| **Governing Body** | To review and approve the policy on a periodic basis |
| **Chief Operations Officer** | The Chief Operations Officer is the member of the University Executive Team with overall responsibility for the delivery of the regulatory objectives of the University including compliance with data protection and privacy obligations. |
| **University Executive Team** | The University Executive Team is responsible for the internal controls of the University, an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. Responsible for:   * Reviewing and approving all data protection policies and any updates to them as recommended by the Data Protection Officer. * Ensuring ongoing compliance with data protection legislation in their respective areas of responsibility. * As part of the University’s Annual Statement of Internal Control, signing a statement which provides assurance that their functional area is in compliance with data protection legislation. * Ensuring oversight of data protection issues either through their own work or the Information Compliance Group or other governance arrangement. |
| **Heads of Service/Heads of School[[1]](#footnote-2)** | * To lead the data protection compliance for their School/Service Area * Provide guidance to their staff * Ensure prompt reporting of data protection breaches originating from their School/Service Area |
| **Data Protection Officer (Head of Governance & Compliance)** | * To lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable data protection legislation and regulations, including the GDPR * To advise on all aspects of data protection and privacy obligations. * To monitor and review all aspects of compliance with data protection and privacy obligations. * To act as a representative of data subjects in relation to the processing of their personal data. * To report directly on data protection risk and compliance to Chief Operations Officer. |
| **Information Governance Team** | * To support the Data Protection Officer in leading the data protection compliance, with responsibility for advising how to comply with applicable privacy legislation and regulations, including the GDPR |
| **Staff/Students/External Parties** | * To adhere to the suite of compliance policies. * To report suspected breaches of policy to their Head of School/Service Area and/or Data Protection Officer. |

## 6.3 Personal Data Processing Principles

The following data protection requirements apply to all instances where personal data is stored, transmitted, processed, or otherwise handled, regardless of geographic location.

The University has established the following high-level principles relating to data protection in order to comply with relevant European requirements;

* Personal data shall only be processed fairly, lawfully and in a transparent manner (**Principles of Lawfulness, Fairness and Transparency)**
* Personal data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes **(Principle of Purpose Limitation**)
* Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (**Principle of Data Minimisation**)
* Personal data shall be accurate, and where necessary kept up to date (**Principle of Accuracy**)
* Personal data shall not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which the Personal Data are processed (**Principle of Data Storage Limitation**)
* Personal data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to prevent and / or identify unauthorised or unlawful access to, or processing of, personal data; and prevent accidental loss or destruction of, or damage to, Personal Data (**Principles of Integrity and Confidentiality**)
* The University whether serving as a data controller or a data processor, shall be responsible for, and be able to demonstrate compliance with, these key principles. (**Principle of Accountability**)

## 6.4 Principles of Lawfulness, Fairness and Transparency

### 6.4.1 Lawful basis for processing personal data

The University shall process personal data under an appropriate lawful basis, where at least one of the following conditions is met:

* the individual has consented to processing;
* processing is required due to a contract;
* processing is necessary for compliance with a legal obligation;
* processing is necessary to protect an individual’s vital interests;
* processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the University;
* processing is necessary for the legitimate interests of the University or a third party and does not interfere with the rights and freedoms of individuals.

TU Dublin is classified as a public body under the Technological Universities Act, 2018. As such, the use of the ‘legitimate interests’ condition is not applicable to TU Dublin’s statutory functions but may be relied-upon as a legal basis for processing that is not related to the University’s statutory functions.

Where TU Dublin relies on consent as a lawful basis for processing personal data, the University must:

* obtain the individual’s specific, informed and freely given consent;
* ensure that the individual gives consent by a statement or clear affirmative action;
* ensure any written consent request is clearly distinguishable from other matters and presented in clear and plain language
* retain evidence of that statement/affirmative action; and
* allow the individual to easily withdraw their consent at any time if they so wish.

Appropriate consent request methods include:

* clauses in contracts with students and vendors, and / or
* check boxes on replies to applications or forms, and / or
* click boxes on online forms where personal data is entered.

### 6.4.2 Direct Marketing

Any form of marketing to such audiences must follow the TU Dublin Direct Marketing Policy. For example, it must offer a way for people to ‘opt out,’ and this preference should be recorded to ensure that they do not receive future communications.

TU Dublin will communicate with alumni of the University who have consented to direct marketing within the last five years, or where the electronic contact details have been obtained in the course of a service (or event) within the last twelve months and the direct marketing material relates to a ‘similar product or service’, provided the individual was given an opportunity to refuse such contact at the time the data was collected, also known under electronic marketing rules as a ’Soft Opt–in’.

See TU Dublin Direct Marketing Policy in **Appendix A** for further information.

### 6.4.3 Processing of Special Categories of Personal Data

The University will not process special categories of personal data unless;

* the data subject expressly consents

and / or

* it is necessary to carry out data controller’s obligations or exercise data subject’s specific rights in the field of employment and social security and social protection law

and / or

* it is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity.
* it is in the vital interest of the data subject. The University may only process such data where it is necessary to protect a data subject’s vital interest in the event that this subject is physically or legally incapable of giving consent. For example, this may apply where the data subject may require emergency medical care. Only the Data Protection Officer may authorise this exemption and only in accordance with relevant national legislation.

Any exceptions to processing in the absence of one of these conditions requires the approval of the Data Protection Officer.

### 6.4.4 Transparency – Data Protection Notices (Fair Disclosure Notices)

To ensure fair and transparent processing activities, Schools and Service Areas must provide data protection notices to data subjects when directly collecting data. This policy includes Data Protection Notices for Students, for Staff and for Recruitment Candidates.

These notices must be:

* provided at the first contact point with the data subject or as soon as reasonably practicable.
* provided in an easily accessible form.
* written in clear language.
* made in such a manner as to draw attention to them.

If Schools and Service Areas use consent as the lawful basis for processing personal data, then this consent should, where possible, be obtained at the data collection point.

All Schools and Service Areas collecting personal data must establish technical or administrative means to:

* deliver the data protection notices and
* document that the University has provided these notices to the Data Subject at the time of collection, or document they were previously provided and
* record all obtained consents and ensure this information is up to date.

See **Appendix B, C, D and E** for Data Protection Notices for Students, Staff, Recruitment Candidates and Students Health Centres.

### 6.4.5 Data Collection from Third Party Sources

In addition to Section 6.4.4 above, when the University collects personal data from a third party (i.e., not directly from a data subject), the data controller must provide data protection notices to the data subject either at the time of collection or within a reasonable timeframe that is no more than 30 days post collection.

In addition to the content of the notice outlined above in Section 6.4.4, Schools and Service Areas shall provide the data subject with the following information necessary to ensure fair and transparent processing of their personal data:

* the personal data collected
* whether this was from a public source.
* the categories of personal data concerned.

The following are the only exceptions:

* if the data subject has already received this information or
* notification would require disproportionate effort or
* the law expressly provides for this personal data collection, processing, or transfer.

## 6.5 Principles of Data Minimisation

School and Service Areas should limit personal data collection to:

* what is directly relevant and
* what is necessary to accomplish a specified purpose.

School and Service Areas should identify the minimum amount of personal data needed for a particular purpose and then align collection volumes and associated retention periods to this purpose.

Please see **Appendix F** for the University’s Records Management, Retention and Destruction Policy.

## 6.6 Principles of Purpose Limitation

School and Service Areas must only collect personal data for specified, explicit and legitimate purposes. They are prohibited from further processing unless they have identified and documented additional legitimate processing conditions or if the personal data involved is appropriately anonymised and /or pseudonymised and used for statistical purposes only. Please see Section 6.9.4 below for further information.

## 6.7 Principles of Data Accuracy

Each School and Service Area must ensure that any personal data collected is complete and accurate and maintained in an accurate, complete, and up-to-date form as its purpose requires.

## 6.8 Principles of Data Storage Limitation

School and Service Areas must only keep personal data for the period necessary for permitted uses. They shall establish a destruction date and / or review schedule when defining a personal data permitted use under the stated purpose. This shall be recorded and aligned to the University’s Records Management, Retention and Destruction Policy which can be found in **Appendix F** of this document.

School and Service Areas should reasonably endeavor to erase any personal data that violates:

* data protection law
* data protection regulations
* contractual obligations
* requirements of this policy
* if the University no longer requires the data
* if the personal data no longer benefits the data subject in the relevant process

School and Service Areas should anonymise and / or pseudonymise personal data where possible rather than erase if:

* the law prohibits erasure
* erasure would impair the legitimate interests of the data subject
* erasure is not possible without disproportionate effort due to the specific type of storage or
* where the data subject has disputed the accuracy of the personal data, the University disagrees with that assertion and resolution has not been reached.

## 6.9 Security of Personal Data (Integrity and Confidentiality)

### 6.9.1 Information Security

Each School and Service Areas shall ensure personal data security through appropriate physical, technical and organisational measures. These security measures should be in keeping with standards appropriate to the University sector and prevent:

* alteration
* loss
* damage
* unauthorised processing
* unauthorised access

When implementing personal data security measures each School and Service Area must consider:

* technological developments
* implementation costs
* nature of relevant personal data
* inherent risks posed by human action/physical/natural environment

Technology Services must adequately address European data protection requirements in relevant University IT policies and procedures.

European data protection requirements specifically refer to personal data collected and processed within EEA. However, the University is committed to protecting all collected, processed, stored, and transferred personal data regardless of country of origin.

### 6.9.2 Data Breach (Unauthorised Disclosure)

No employee or agent shall disclose data subject’s personal data (including personal data or special categories of personal data), except where this policy allows such disclosures.

TU Dublin as a data controller is legally required to notify the Office of the Data Protection Commissioner within 72 hours of becoming aware of a data breach, where a personal data breach is likely to result in a riskto data subjects’ rights and freedoms. In addition, TU Dublin is legally required to notify the affected individuals (data subjects) where a personal data breach is likely to result in a high risk to their rights and freedoms

Staff must report all suspected incidents of unauthorised access to the Information Governance Office. Incidents include disclosure, loss, destruction, or alteration of personal data, regardless of whether it is in paper or electronic form.

For further guidance on recognising and managing a data breach, please see the Procedure for Management of a Data Breach in **Appendix G**.

**Types of Breach**

* Confidentiality Breach – where personal data is disclosed or accessed in an unauthorised or accidental manner.
* Integrity Breach – where personal data is altered in an unauthorised or accidental manner.
* Availability Breach – where personal data is lost or destroyed in an unauthorised or accidental manner.

Please see **Appendices H and I** for the University’s Data Breach Notification Form and Data Breach Post Incident Report.

### 6.9.3 Data Encryption

The University has published guidelines for staff on the encryption of personal data contained, processed, or transmitted within hardware and software resources that are owned and/or operated by the University. Please see **Appendix J** for these Guidelines on Data Encryption.

Situations requiring encryption – data at rest (servers, desktop computers, laptops, tablets, mobile phones and other smart devices and removable storage devices) and data transmission.

### 6.9.4 Data Anonymisation/Pseudonymisation

Anonymisation and pseudonymisation are two methods of processing personal data, in such a manner that the personal data in question cannot be traced back to the individual (data subject) to whom it originally pertained. The key difference between these methods as defined under data protection legislation, is whether the original data subject can be re-identified.

**Anonymisation** renders the data subject unidentifiable, even to the party that carries out the anonymisation of data. If the data is truly anonymised and identifying the subject is impossible, then the data falls outside the remit of data protection legislation.

**Pseudonymisation** renders the data subject unidentifiable without the use of additional information. Once the “additional information” and the pseudonymised data are held separately, the data processor/controller can use the data more freely, as the rights of the data subject under data protection legislation remain intact.

The University has published guidelines for staff regarding the treatment and use of aanonymisation and pseudonymisation. Please see **Appendix K** for these guidelines.

## 6.10 Principle of Accountability

### 6.10.1 Data Protection by Design and by Default

**Privacy by Design** is an essential requirement that involves minimising privacy risks to individuals. It is the consideration of data protection implications at the start or re-design of any product, service, system, IT application or process that involves the processing or personal data. It fosters a culture of embedding privacy by design into operations and ensuring proactivity instead of reactivity.

**Privacy by Default** promotes that, where possible, having regard to business implications and the rights of the data subject, the strictest data protection settings are applied automatically to any project.

The University has an obligation under data protection legislation to consider data privacy throughout all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data. This is of particular importance when considering new processing activities or setting up new procedures or systems that involve personal data. Data protection legislation requires a ‘privacy by design’ requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought. School and Service Areas engaged in projects, new courses, services, or systems development of any sort (including change to existing practices) through the relevant local project and change management processes must comply with the terms of this policy and any specific guidelines and requirements set by the Data Protection Officer or IT policies in furtherance of these principles.

### 6.10.2 Data Protection Impact Assessment (DPIA)

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.

A DPIA Initial Assessment should be conducted to ascertain if a full DPIA is required for your project/processing activity if you are unsure if your project processes personal data.

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.

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, employees, the public, patients, etc. they should conduct a DPIA of these risks and identify measures, which would help to reduce these risks. 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.

The University’s Data Protection Impact Assessment Template can be found in **Appendix N**, DPIA Initial Assessment Template can be found in **Appendix M.** For further information on conducting a DPIA, please see Criteria and Guidelines for the completion of a DPIA in **Appendix L**.

### 6.10.3 Record of Processing Activity and Data Inventories

The University as a data controller is required under data protection legislation to maintain a Record of Processing Activities (ROPA) under its responsibility. That record contains details of why the personal data is being processed, the types of individuals about which information is held, who the personal data is shared with and when such data is transferred to countries outside the EEA.

New activities involving the use of personal data that is not covered by one of the existing records of processing activities require consultation with the Data Protection Officer prior to the commencement of the activity.

The Data Protection Officer will review records of processing periodically and will update same accordingly. The Data Protection Officer will provide processing activity records to a Supervisory Authority on request.

See **Appendix O** for the University’s ROPA which is also published on the University Website.

**Data Inventories**

The University has created a Data Inventory Template (Data Processing Register) as part of the data protection compliance program. This details all business activities that involve the processing of personal data, the basis for doing so, retention periods for this personal data, what the personal data is used for, and whether this personal data is transferred to a third party. Please see **Appendix P** for the template.

Schools and Service Areas must maintain a written records of processing activity under its responsibility on a system accessible to the Data Protection Officer. The Data Protection Officer will review these records periodically and will update same accordingly. The Data Protection Officer will provide processing activity records to a Supervisory Authority (Office of the Data Protection Commissioner) on request.

### 6.10.4 Transfer and Sharing of Data

**Sharing with a Third Party or External Processor**

As a general rule, personal data should not be shared with or passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible e.g.

* The University may disclose student’s personal data and sensitive personal data (Special Category Personal Data) to external agencies to which it has obligations or a legitimate reason. Such sharing should be noted in the relevant data protection notices. Please see the Data Protection Notices in **Appendix B, C, D and E** for information on what third parties the University shares Personal Data with and for what purpose.
* The data subject consents to the sharing.
* The third party is operating as a data processor and meets the requirements of GDPR. Where a third party is engaged for processing activities there must be a written contract or equivalent in place which shall clearly set out respective parties’ responsibilities and must ensure compliance with relevant European and local member state data protection requirements/legislation. These are known as Data Sharing Agreements, an example of which is available in **Appendix Q**.

The Data Protection Officer should be consulted where a new contract that involves the sharing or processing of personal data is being considered.

**Transfer of Personal Data outside the EEA**

Transfers of personal data to third countries are prohibited without certain safeguards. The means the University must not transfer personal data to a third country unless there are adequate safeguards in place which will protect the rights and freedoms of the data subject. It is important to note that this covers personal data stored in the cloud as infrastructure may be in part located outside of the EU/EEA.

School and Service Areas must not transfer personal data to a third party outside of the EU/EEA regardless of whether the University is acting as a data controller or Data processor unless certain conditions are met.

Prior to any personal data transfer outside the EU/EEA, the Chief Operations Officer, (on the recommendation of the Data Protection Officer) must approve the transfer of such information and the Data Protection Officer will record the determination in writing.

### 6.10.5 Third Parties Relationships and Data Sharing Agreements

Where Schools and Service Areas engage a third party for processing activities, the data processor must protect Personal data through sufficient technical and organisational security measures and take all reasonable compliance steps. When engaging a third party for personal data processing, School and Service Areas must enter into a written contract, or equivalent. This contract known as a Data Sharing Agreement and must:

* clearly set out respective parties’ responsibilities
* ensure compliance with relevant European and local member state data protection requirements/legislation

and must give due consideration to the following items:

* management of data processors
* selection of data Processors
* contract Requirements
* sub-contracted data processors
* monitoring and reporting
* data transfers
* appropriate safeguards
* derogations for specific situations
* once off transfer of personal data
* Data Sharing Agreements
* review of data sharing arrangements
* data transfer methods
* email
* cloud storage and cloud applications
* telephone / mobile phone
* sending the information by post
* hand delivery / collection
* Data Breach Notification

Please see **Appendix Q** for a sample Data Sharing Agreement.

## 

## 6.11 Data Subjects Rights

The Data Protection Officer, supported by the Head of Schools and Service Areas, shall maintain appropriate processes and procedures to address data subject's rights under data protection legislation.

Data subjects have the following rights under data protection legislation, subject to certain exemptions, in relation to their personal data:

|  |  |
| --- | --- |
| **Right** | **Explanation** |
| Information | The right to be informed about the data processing the University does. |
| Access | The right to receive a copy of and/or access the personal data that the University holds about you. |
| Portability | The right to request that the University provides some elements of your personal data in a commonly used machine-readable format in order to provide it to other organisations. |
| Erasure | The right to erasure of personal data where there is no legitimate reason for the University to continue to process your personal data. |
| Rectification | The right to request that any inaccurate or incomplete data that is held about you is corrected. |
| Object to processing | The right to object to the processing of your personal data by the University in certain circumstances, including direct marketing material. |
| Restriction of processing concerning the data subject | The right to request the restriction of processing of personal data in specific situations where:   1. You contest the accuracy of the personal data; 2. You oppose the erasure of the personal data and request restriction instead; 3. Where the University no longer needs the data but are required by you for the establishment, exercise or defence of legal claims. |
| Withdraw Consent | If you have provided consent for the processing of any of your data, you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn. This can be done by contacting the Department who obtained that consent or the University’s Data Protection Office (contact details below). |
| The right to complain to the Data Protection  Commissioner | You have the right to make a complaint in respect of our compliance with Data Protection Law to the Office of the Data Protection Commissioner. |

In order to exercise any of the above rights, please contact a representative of the Data Protection Officer using the contact details in Section 6.15 below.

### 6.11.1 Subject Access Requests (SARs) and Subject Rights Requests (SRRs)

Employees and students of the University can contact the Information Governance Office to discuss their request requirements prior to making a formal request in order to maximise the likelihood that their request will be fulfilled in a timely, efficient and satisfactory manner. External requests for personal data should all be directed to the Data Protection Officer for response.

All SARs are requested to be made via the request forms that are available on the University website. All subject access requests shall be directed to the Data Protection Officer and all requests shall have an open status until an action by the Data Protection Officer sets a closed status.

Any information provided to a Data subject in response to a request must be:

* concise
* transparent
* intelligible
* in an easily accessible form, using clear and plain language
* free unless proven to be excessive (administration fee chargeable in this case) and
* provided in a timely manner.

School and Service Areas must notify the Data Protection Officer immediately when in receipt of a SAR and must provide the Data Protection Officer with all necessary support to allow a response in accordance with regulatory timelines.

See **Appendix R and S** for the University’s Data Subject Access Request Form and Data Subject Rights Request Form along with information regarding both processes.

### 6.11.2 Fees and refusals of SARs under Data Protection Legislation

There is no fee for subject access requests. However, under the GDPR and Data Protection Legislation, the University reserves the right where requests from a data subject are manifestly unfounded or excessive in nature to either:

* charge a fee to cover the administrative costs of providing the personal data or
* refuse to act upon the request.

The University may also refuse to act upon a subject access request under GDPR in the following circumstances:

* Where it would breach the rights of someone else.
* Where it is the subject of an ongoing legal case.
* It would be illegal to do so.
* The identity of the requester cannot be determined.
* Where existing processes exist to access personal data (a charge may be in place).

## 6.12 CCTV

All usage of CCTV other than in a purely domestic context must be undertaken in compliance with the requirements of the Data Protection Legislation.

All uses of CCTV must be proportionate and for a specific purpose. As CCTV infringes the privacy of the persons captured in the images, there must be a genuine reason for installing such a system and such purposemust be displayed in a prominent position.

Please see **Appendix T** for the University’s CCTV Policy.

## 6.13 Data Protection Officer (DPO)

The University, in meeting its data privacy commitments, has appointed a Data Protection Officer (DPO) as the point of contact for all data privacy queries that employees and students may have including subject access requests. The contact details of the Data Protection Officer are available on the University website and have been notified to the Office of the Data Protection Commissioner.

Contact details for the 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

Clean Desk Policy (in development)

[Cookies Notice & Website Privacy Policy](https://www.tudublin.ie/cookies-notice-and-website-privacy-policy/)

[Data Classification Policy](https://www.tudublin.ie/media/intranet/data-classification/TU-Dublin-Data-Classification-Policy.pdf)

[HEA](https://www.tudublin.ie/explore/gdpr/hea-data-collection-notice/) Data Collection Notice | TU Dublin

[Microsoft Forms | TU Dublin](https://www.tudublin.ie/connect/technology-services/guides/microsoft-forms/)

Privileged User Policy (in development)

Risk Management Policy and Framework

[TU Dublin Acceptable Use Policy](https://www.tudublin.ie/explore/policies-and-forms/technology-services/)

[TU Dublin IT Security Policy](https://www.tudublin.ie/explore/policies-and-forms/technology-services/)

# 8. Conclusions

All staff of the University are expected to:

* + acquaint themselves with, and abide by, the rules of the full suite of compliance policies;
  + read and understand all data protection documentation;
  + understand what is meant by ‘personal data’ and ‘sensitive category personal data’ and know how to handle such data;
  + not jeopardise individuals’ rights or risk a contravention of data protection legislation;
* report all suspected incidents of unauthorised access to the Information Governance Office. Incidents include disclosure, loss, destruction, or alteration of personal data, regardless of whether it is in paper or electronic form. Data Breach Management Guidelines are provided in Appendix G.
  + contact their Head of School or Service Area or the Information Governance Office if in any doubt regarding their responsibilities under this policy.

**Compliance**

Compliance with this policy will help protect the University against data breaches under data protection legislation, reputational damage to the University and/or an infringement of the rights of employees, students, or other relevant third parties.

**Compliance Exceptions**

Any exception to the policy shall be reported to the Data Protection Officer in advance.

**Non-Compliance**

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the University’s disciplinary procedures. Failure of a third-party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

The Office of the Data Protection Commissioner (DPC) is the Irish Statutory Authority for GDPR. Please see <https://www.dataprotection.ie/> for further information on the Office of the Data Protection Commissioner.

# 9. Appendices

Appendix A Direct Marketing Policy

Appendix B Data Protection Notice for Students

Appendix C Data Protection Notice for Staff

Appendix D Data Protection Notice for Recruitment Candidates

Appendix E Privacy Statement for Student Health Centres

Appendix F Records Management, Retention and Destruction Policy

Appendix G Procedure for Management of a Data Breach

Appendix H Data Breach Notification Form

Appendix I Data Breach Post Incident Report

Appendix J Guidelines on Data Encryption

Appendix K Guidelines on Anonymisation and Pseudonymisation

Appendix L DPIA Criteria and Guidelines

Appendix M DPIA Initial Assessment Template

Appendix N Data Protection Impact Assessment Template

Appendix O Record of Processing Activity

Appendix P Template Data Inventory / Data Processing Register

Appendix Q Sample Data Sharing Agreement

Appendix R Subject Access Request Form

Appendix S Subject Rights Request Form

Appendix T CCTV Policy

# 10. Document Management

## 10.1 Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSION NUMBER** | **VERSION DESCRIPTION /**  **CHANGES MADE** | **AUTHOR** | **DATE** |
| *1.0* | *Initial Policy* | *Information & Compliance Working Group* |  |
| *1.1* | *Review and Update* | *Information Governance Team* | *10/02/2023* |
|  |  |  |  |

## 10.2 Document Approval

|  |  |  |
| --- | --- | --- |
| **VERSION NUMBER** | **APPROVAL DATE** | **APPROVED BY (NAME AND ROLE)** |
| *1.1* | *07th July 2023* | *Governing Body* |
|  |  |  |
|  |  |  |

## 10.3 Document Ownership

Document Owner – Head of Governance and Compliance

Document Update - Information Governance Senior Manager

## 10.4 Document Classification

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

1. Terminology subject to change pending finalisation of organisation design structures [↑](#footnote-ref-2)