UCD Office of the DPO
General Data Retention Guidance for Personal Data

1. Overview

Personal data must be stored for the shortest time possible. That period should take into account the reasons why the organisation needs to process the data, as well as any legal obligations to keep the data for a fixed period of time (for example employment, tax or anti-fraud laws requiring you to keep personal data about your employees for a defined period, etc.).

The organisation needs to establish time limits to erase or review the data stored and must also ensure that the data held is accurate and, where appropriate, kept up-to-date.

By way of an exception, personal data may be kept for a longer period for archiving purposes in the public interest or for reasons of scientific or historical research, provided that appropriate technical and organisational measures are put in place (such as anonymisation, encryption, etc.).

2. Introduction

This guidance document sets out the obligations of University College Dublin ("UCD") regarding the retention of records. The General Data Protection Regulation (GDPR) requires that UCD only retains personal data when there is a valid legal reason to do so. Data subjects must be informed about the planned period of retention when personal data is collected to enable them to make an informed choice about sharing their data. Exceeding allowable retention of personal data increases the risk that data will become inaccurate, lost, stolen, disclosed, shared too widely, and/or used inappropriately. Data storage is also costly, so it is important that all data is stored, managed and disposed of in accordance with this guidance document.

GDPR Article 5(1)(e), the storage limitation principle, outlines retention requirements and is one of the six core principles in the GDPR that is reflected in all relevant parts of the Regulation.

3. Definitions

The following definitions of terms used in this guidance document are provided to ensure clarity to the reader. What is:

"*Personal Data*"- Personal data is 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; Postal address; Date of Birth; Phone number; and more.

"*Special categories of personal data*" are more sensitive and therefore subject to stricter processing requirements. This includes personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; data concerning health; or data concerning a natural person's sex life or sexual orientation.

A **"*Record*"** refers to the different types of data that UCD processes, including financial information, personal data etc. This includes hard copy information and computer based.

The **"*Data Controller*"** is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data. This guidance document is aimed at UCD in its capacity as Data Controller.

The **"*Processor*"** is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of and the instruction of a data controller. e.g. UCD. The relationship between the instructing controller and the processor needs to be laid down in a binding contract (Data Processing Agreement), in line with Article 28 of the GDPR.

"*Processing*" is defined as any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated or non-automated means. Processing covers collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or the destruction of personal data.,

"*Accountability*" – The controller shall implement appropriate technical and organisational measures (TOMs) to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. The measures implemented shall be reviewed and updated where necessary ("Accountability Principle").

4. Defining data retention requirements

The legal basis for collecting and processing data and associated retention requirements must be identified and defined before data is collected. Information to be confirmed, and communicated to data subjects, before processing includes:

- The purpose(s) for collection of personal data e.g. to create a customer account, to manage the registration of a student, to enable product delivery, to enable marketing, to manage access to systems, to manage complaints and user service requests.
- The type and quantity of data to be processed for each defined purpose. In particular identifying subsets of;
    - o Special category data (these will be, for example, in the HR area)

• The minimum quantity of personal data and the minimum amount of personal data fields/data types required to serve the defined organisational or third-party purpose. Crucially UCD must consider:

o Can personal data collection and processing be reduced further to reduce risk to the data subject and comply with the data minimisation principle (Article 5(1) (c))?

o Can the purpose be served by using fully anonymised data? If yes, this removes the requirement for storage limitation and places the data set outside the scope of the GDPR.

o If it is essential to use personally identifiable data for this purpose, will that change in future? Switching to use fully anonymised data removes any applicable storage limitation requirement, and if the retention limit has been reached, it is an alternative to data deletion. But it is important to remember that data anonymisation is a processing activity in itself, and data subjects have to be informed, from the outset, of the intention to anonymise their data.

• One or more legal basis is/are needed to provide legitimacy to the processing of personal data for each defined purpose. Article 6 GDPR lists the following:

o Consent – Processing is on the basis of unambiguous, informed, and freely given consent from the data subject for the specified purposes. Consent can be withdrawn at any time.

o Contract - Processing is strictly necessary for performance of a contract with the data subject.

o Legal obligation - Processing is necessary for compliance with a legal obligation to which the controller is subject to.

o Vital Interest - Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

o Public Interest/Public Task - 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 controller.

o Legitimate Interests - Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (e.g. for information security purposes, or health & safety), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of their personal data, in particular where the data subject is a child.

5. Legal and regulatory defined retention periods

Where a statutory obligation to keep a particular category of records for a specific period of time applies, the relevant records must be kept for that prescribed period. There are numerous legislative provisions under which specific categories of records must be retained. Pre-defined mandatory retention requirements or formal recommendations associated with either the purpose, or the legal basis for processing include:

i. Processing data (including personal data) related to financial regulations, tax requirements, or legal proceedings. The retention period reflects government regulator, tax authority, or judicial/ legal requirements.
ii. Processing personal data, generally of pseudonymised/coded data, used for secondary purposes that are compatible with the original purpose, for example in the context of scientific research, where storage limitation, under certain conditions, as referenced to in GDPR Article 89(1), could be extended beyond the original purpose.
iii. Processing personal data to comply with separate legal requirements which specify their own retention requirements or exceptions e.g., anti-fraud and anti-money laundering requirements.
iv. Employment Law requirements in relation to staff records often specify retention requirements.

6. Recording and reviewing retention timeframes

A defined retention limit should be recorded for each data processing purpose. The retention limits are to be included in:

- UCD's Privacy Notices or Patient Information Leaflets (PILs) made available to data subjects before their personal data is processed, or if not feasible to include specific time limits, it should include the criteria used to decide upon those limits.
- UCD's Record of Processing Activities (ROPA), Article 30 of the GDPR, requires every organisation processing personal data to create and maintain a ROPA and Article 30(1)(f) states that time limits for retention of different categories of data in the context of specific processing activities should be included, where possible.

It is important to note that it is the obligation of the respective UCD 'business owner' of the processing activity to retain the data for the prescribed period. Any other UCD Unit or School that is not the official 'business owner' should not retain the data beyond passing it on to the 'business owner'.

7. Reviewing and managing retention requirements

Risks to the rights and freedoms of data subjects will evolve over time. Data processing techniques and technologies and data security threats all change rapidly and there are constant changes to legal and regulatory requirements.

Where data anonymisation or erasure may not be possible from the outset, without significant impact on data subjects or the wider operations of the organisation, it may become feasible at a later stage. The latter often is a useful tool to enable organisational planning and assessment of future resource needs, without impinging on individuals' privacy.

To reduce the risk of keeping personal data for longer than permitted, while accounting for different retention requirements and timelines, it is important for the University, but equally for individual Units and Schools within UCD, to review their processing activities, and related retention periods regularly, e.g.

annually. It is anticipated that reviews will involve liaising with other UCD stakeholders, and the UCD Office of the Data Protection Officer (ODPO).

8. Taking action when the retention limit is reached

All UCD Schools and Units, including the relevant University stakeholders, are responsible for ensuring that data is erased, securely destroyed or fully anonymised when the retention period is reached.

Data disposal and treatment at the end of a retention period should be a sustainable, business as usual on-going activity. When the retention period for a data set expires, that personal data will be either:

- Securely deleted from all systems and back-ups
- Fully anonymised, so that no individual can be directly or indirectly identified, or singled out
- Securely physically destroyed or shredded (paper records and/or data storage devices)
- Encrypted following current cryptographic best practice, before decryption keys are securely deleted.

9. Processor retention requirements

UCD, as controller, must formally specify data retention responsibilities and periods in third party contracts (DPAs), and service agreements., Each third party that acts as a data processor must comply with this guidance document and any specific retention requirements linked to different data processing purposes.

Where UCD acts as a data processor for another organisation that is the controller, UCD is obliged to know and follow their instructions. This includes adhering to 1) prescribed retention timelines, and b) either documented certified data erasure, or return of data to the controller. Which of the above applies should be included in the data processing contract (DPA) UCD signed with the instructing controller.

For further information on the different types of agreements and contracts that are required can be found at UCD GDPR Data Sharing.

10. Version history

- Rev 0. May 28th 2025.