Personal Data

Retention Policy

Contents

Introduction

This is the Personal Data Retention Policy of Dublin City University.

Purpose

The purpose of this policy is to state the University's position concerning the retention and destruction of Personal Data.

Scope

This Policy applies to all units of the University, both academic and support, including its research centres and its wholly owned campus companies. These are all hereinafter collectively referred to as either the 'University'' or "DCU".

Policy Statement

Retention Principles

Having regard to the principles contained in Article 5(1) of the General Data Protection Regulation (EU No. 2016/679) ("GDPR"), it is the policy of DCU to:

(a) retain personal data in identifiable form only for such period as is necessary in relation to the purpose for which the data are processed (the "storage limitation" principle);

(b) ensure that personal data retained by DCU is adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed (the "data minimisation" principle); and

(c) take all reasonable measures to ensure that personal data retained by DCU are accurate (the "accuracy" principle).

DCU Statutory Functions

Having regard to Article 24 of the GDPR, the storage limitation, data minimisation and accuracy principles must be considered in light of the nature, scope, context, purposes and the risks arising in the context of the data processing undertaken by DCU pursuant to its important statutory objects and functions as provided for under the University Act, 1997 (as amended) (the "University Act").

While sections 12 and 13 of the University Act state the general objects to be pursued and functions to be performed by DCU, section 13(1) specifically states that it is the function of a university to "do all things necessary and expedient in accordance with [the University Act] to further the objects and development of the university", which together are referred to as the "DCU Statutory Functions".

In performing its tasks in the public interest when discharging DCU Statutory Functions, DCU therefore has a lawful basis to undertake data processing, including the retention of personal data. Accordingly, it is the policy of DCU to retain and hold personal data in performing DCU Statutory Functions in a manner that is consistent with the principles of storage limitation, data minimisation and accuracy.

Data Ownership

All Data, irrespective of format, generated, created, received and/or retained by DCU in performing the DCU Statutory Functions is the property of the University and subject to its overall control. DCU Personnel leaving DCU or changing positions within DCU are not to remove any Data without the prior written authorisation of their Department/Unit Head.

Storing Data

DCU's records must be stored in a safe, secure and accessible manner to ensure the security and confidentiality of such Data in accordance with DCU's Data Privacy Policy and DCU's 'Information & Communications Technology (ICT) Security Policy'.

Special care is to be taken to ensure that information of a sensitive nature, in particular, information that constitutes a special category of personal data under the GDPR, is stored in a secure manner which may include, for example, locked filing cabinets and offices for hard copy Data and/or the use of password protection and encrypted files for Data stored in electronic form.

Destroying Data

Once Data has met its required retention period in accordance with the principles set out in this policy, such Data should then be transferred to the DCU approved archives or deleted, destroyed, or anonymized as follows:

(a) Hard copy files: to be destroyed by confidential shredding or by using the services of an approved confidential waste disposal firm.
(b) Electronic files: to be purged or deleted or anonymized from all relevant systems on which such Data is stored and/or data bases.
(c) Data stored in other media: to be deleted or destroyed or anonymized in a safe and confidential manner to ensure the content is not disclosed.

Litigation Holds and Other Scenarios

What is a Litigation Hold?

DCU requires all DCU personnel to fully comply with the general guidance set out in this policy and the specific retention periods set out in each unit's PDSS (see section below).

However, all DCU Personnel should note the following general exception to any stated destruction schedule: if you believe, or the DCU Chief Operations Office and/or the HR Department informs you, that certain Data held by DCU is relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit or other event, you must preserve and not delete, dispose, destroy or change such Data, including e-mails, until the DCU Chief Operations Office and/or the HR determines that such Data is no longer needed. This exception is referred to as a "Litigation Hold" and takes priority over any previously or subsequently established destruction schedule for those records.

If you believe this exception may apply, or have any questions regarding whether it may possibly apply, please contact the DCU Chief Operations Office and/or the HR Department

What to do when notified of a Litigation Hold?
The destruction of Data must stop immediately upon notification from DCU Chief Operations Office and/or the HR Department that a litigation hold is to begin due to ongoing or potential litigation or an official investigation. Destruction may begin again once DCU Chief Operations Office and/or the HR Department, as appropriate, has confirmed that the relevant litigation hold has been lifted.

Personal Data Security Schedule (PDSS)

To facilitate compliance with this policy, DCU Departments and Units are required to maintain a PDSS where one has been recommended or requested by the Data Protection Unit (DCU). A PDSS which contains information on the various categories pf personal data retained by the Department or Unit.

Where applicable, the PDSS is to be reviewed and updated by the Department or Unit on a regular basis. The updated PDSS shall be provided to the DCU Data Protection Unit.

Application of Policy

This policy applies to any type of Data created, received, transmitted and retained in the context of DCU's day to day activities in performance of DCU Statutory Functions and any other data processing undertaken by DCU, regardless of the format.

Therefore, any paper records or electronic files that are part of any of the categories listed in a unit specific Personal Data Security Schedule ("PDSS"), must be retained for the period indicated in the PDSS. Data should not be retained beyond the period indicated in the PDSS, unless a valid operational reason (or a litigation hold or other exceptional situation) calls for its continued retention.

Roles & Responsibilities

This Policy applies to all units of the University, both academic and support, including its research centres.

Ownership of the policy is within the remit of the Data Protection Officer.

It is the responsibility of all those engaged in the processing of personal data (e.g. DCU staff, students & researchers) to

- be aware of the policy;
- to implement its principles in all relevant areas of their work, studies or research;
  &
- to take and participate in the data protection training provided by the University.

Definition

Personal Data is any information relating to a living individual which allows the identification of that individual. The data can be by itself or combined with other data.

Examples of personal data in a university setting are:

- Documents & records
- Emails and correspondence
- Files, both electronic and paper, which hold details of individuals
- Audio visual files and recordings e.g. CCTV
- Consent forms, research participant files, patient records, interview notes etc.
- database or file containing research participant details, online survey returns, photos, IP addresses, diagnostic / clinical imaging etc.
- other e.g., genetic data, biometric data, clinical or medical samples etc.

Related Documentation

Additional guidance to support the understanding and implementation of this policy is available on the website of the DCU Data Protection Unit (DPU). The DPU is a sub-unit within the Office of the Chief Operations Officer.

Contact

Any queries regarding this policy can be directed to the Data Protection Unit.

Email: data.protection@dcu.ie

Policy Review

DCU will keep this policy under regular review.

Version Control

Document Name	Personal Data Retention Policy	
Unit Owner	Office of the Chief Operations Officer	
Version Reference	**Original Version – 1.0**	**Reviewed Version – 1.1**
Approved by	DCU Executive	Data Protection Officer
Effective Date	May 15th 2018	October 12th 2023

End