

## What is Personal Data?

According to GDPR personal data means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, using one or more pieces of information.

---

## What types of data are covered?

Any type of record created by an employee or a person acting on behalf of the organisation which contains personal data including but not limited to email, video, handwritten material(including entries in a diary), audio recordings, social media posts, class lists etc.

---

## Relevant Definitions in GDPR

### Personal Data

Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information.

Examples of personal data include, but are not limited to:

- Name, email, address, phone number
- The contents of an individual student file or HR file
- A staff appraisal assessment
- Details about lecture attendance or course work marks
- Notes of personal supervision, including matters of behaviour and discipline
- Results of an interview panel
- Specific details about a student/staff illness
- Bank/Payroll details of a staff member

### Sensitive Personal Data

Sensitive Personal Data (or Special Categories of 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.

### Data Controller

A data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

## **Data Processor**

A data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

## **Processing Data**

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, adaptation 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.

## **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 Institute cannot constitute Consent.

## **Personal Data Breach**

GDPR defines a "personal data breach" in Article 4(12) 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." Examples of personal data breaches include:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

The Data Protection Commissioner must be notified without undue delay and not later than 72 hours after becoming aware of the breach.

## **Data Retention**

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed it should be disposed of securely. Retention periods are set based on good practice guidance and on a legal basis.

---

## What are my rights under GDPR?

The GDPR gives data subjects the right to access personal information held about them by the Institute. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any information that South East Technological University holds about them which includes copies of email correspondence referring to them or opinions expressed about them.

Data subjects have a number of rights under GDPR. These include:

Right of Access;  
Right to Rectification;  
Right to Erasure (sometimes referred to as the Right to be Forgotten, this is not absolute);  
Right to Restriction of Processing;  
Right to Data Portability;  
Right to Object to Direct Marketing;  
Right to Object to Automated Decision Making, including Profiling.

Any requests made to invoke any of the rights above must be dealt with promptly and in any case within one month of receiving the request. Members of staff should consult the Data Protection Office for all subject access requests (SAR's) which they receive as these are processed centrally .

---

## How do I make an access request?

Under Article 15 of the GDPR regulation you have a right to access information held by SETU Waterford about you. In order to receive this information you must make a subject access request (SAR) by filling in the request form available [here](#) and sending via email to [dataprotection.wd@setu.ie](mailto:dataprotection.wd@setu.ie) / [DPO.cw@setu.ie](mailto:DPO.cw@setu.ie), or by post to the Data Protection Coordinator, Room TL2.54 Tourism & Leisure Building, SETU, Cork Road, Waterford / the Data Protection Officer, SETU Carlow Campus, Kilkenny Road, Carlow.

You should provide any and all details which would help in progressing the request which might include student/staff ID, company name or any other details relevant. You should be as precise as possible as to the data you wish to access in order to ensure material is returned within the time limits as per legislation (1 month). There are some limited instances where there may be an extension of the timeframe as per GDPR regulations.

---

## What are the exemptions under which access can be refused?

There are some instances where a subject access request (SAR) can be refused. According to the Data Protection Act 2018 these are:

- to safeguard cabinet confidentiality, judicial independence and court proceedings, parliamentary privilege, national security, defence and the international relations of the State
  - for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties
  - for the administration of any tax, duty or other money due or owing to the State, a local authority or other public authority or body
  - in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure
  - for the enforcement of civil law claims, including matters relating to any liability of an organisation in respect of damages, compensation or other liabilities or debts related to the claim, or
  - for the purposes of estimating the amount of the liability of an organisation on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the interests of the organisation in relation to the claim.
- In addition, an access request may be refused if the data is:
- considered part of an expression of interest
  - likely to cause you serious mental or physical harm in the opinion of a medical practitioner
  - seen to safeguard certain aspects of public interest
  - likely to affect the rights of others

For more information on your rights you can consult the following [Rights of Individuals under the GDPR](#) produced by the Data Protection Commission.