Framework for reporting and managing breaches involving personal data controlled and processed by the University.

**Management of a Data Breach**

Table of Contents

[1. Document Control Summary 2](#_Toc142042687)

[2. Introduction / Context 3](#_Toc142042688)

[3. Purpose 3](#_Toc142042689)

[4. Scope 3](#_Toc142042690)

[5. Definitions 4](#_Toc142042691)

[6. Procedure Details: 4](#_Toc142042692)

[6.1 What is a data breach? 4](#_Toc142042693)

[6.2 Reporting a personal data breach 5](#_Toc142042694)

[6.3 Managing a personal data breach 5](#_Toc142042695)

[6.3.1 Identification & initial assessment of the incident 6](#_Toc142042696)

[6.3.2 Containment & recovery 6](#_Toc142042697)

[6.3.3 Risk assessment 6](#_Toc142042698)

[6.3.4 Notification 7](#_Toc142042699)

[6.3.5 Evaluation & response 8](#_Toc142042700)

[6.4 How to contact us 9](#_Toc142042701)

[7. Related Documents 9](#_Toc142042702)

[8. Appendices 10](#_Toc142042703)

[9. Document Management 10](#_Toc142042704)

[9.1 Version Control 10](#_Toc142042705)

[9.2 Document Approval 10](#_Toc142042706)

[9.3 Document Ownership 10](#_Toc142042707)

[9.4 Document Classification 10](#_Toc142042708)

# 1. Document Control Summary

# 

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

# 2. Introduction / Context

TU Dublin (the ‘University’) is required under data protection legislation to keep personal data safe and secure and to respond promptly and appropriately in the event of a breach of security relating to personal data (hereinafter ‘data breach’).

# 3. Purpose

The purpose of these Procedural Guidelines (the ‘Guidelines’) is to provide a framework for reporting and managing breaches involving personal data controlled and processed by the University. The Guidelines supplement the TU Dublin Data Protection Policy which affirms the University’s commitment to protect the privacy rights of individuals in accordance with data protection legislation, namely the EU General Data Protection Regulation (‘GDPR’) and Data Protection Acts 1998 - 2018. It is imperative for all TU Dublin staff and students to immediately report any potential or suspected data breach to the Data Protection Office by phone or email – contact details are listed below. If unsure whether an incident is a data breach or not please refer to the guidance set out within this document and consult with the Information Governance Office.

# 4. Scope

The Guidelines apply to all processors of TU Dublin-controlled personal data, including:

Any individual who is employed by TU Dublin or is engaged by TU Dublin who has access to University-controlled or processed personal data in the course of their employment or engagement for administrative, research and / or any other purpose;

Any student of TU Dublin who has access to University-controlled or processed personal data in the course of their studies for administrative, research and / or any other purpose; or

Individuals who are not directly employed by TU Dublin, but who are employed by contractors (or subcontractors) and who have access to University-controlled or processed personal data in the course of their duties for the University.

These Guidelines apply to:

All personal data processed by TU Dublin in any format (including electronic and paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically, or accessed remotely;

Personal data held on all TU Dublin IT systems managed centrally by IT Services, and locally by individual Schools and Service Areas;

Any other IT systems, including email and Cloud-based platforms on which University-controlled or processed personal data is processed.

# 5. Definitions

**Personal data** is defined under GDPR as 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 held by TU Dublin.

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

* Name, email, address, home phone number
* The contents of a student record or an employee HR file
* Details about lecture attendance or assignment/exam grades
* Notes of personal supervision, including matters of behavior and discipline.

**Processing** is defined under GDPR as 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.

# 6. Procedure Details:

## 6.1 What is a data breach?

Under GDPR, a 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. This definition extends to breaches which result from malicious conduct, lack of appropriate security controls, system or human failure, or error.

Data breaches may occur in a variety of contexts.

For example:

* Loss or theft of data, including equipment on which data is stored (e.g. laptop, smartphone, tablet USB key etc.) or paper records
* Inappropriate access controls allowing unauthorised use of information (e.g. uploading personal data to an unsecured web domain, using unsecure passwords)
* Equipment failure
* Confidential information left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account)
* Disclosing confidential data to unauthorised individuals - Collection of personal data by unauthorised individuals
* Human error / accidental disclosure of data (e.g. emails containing personal or sensitive personal data sent to the wrong recipient)
* Hacking, viruses or other security attacks on IT equipment, systems or networks
* Breaches of physical security (e.g. forcing of doors / windows / filing cabinets)

Whether an incident giving rise to the suspected data breach involves personal data must be determined on a case-by-case basis. If an incident does not involve personal data, it is not a data breach per the per the GDPR definition. Furthermore, not all data incidents involving personal data will be data breaches.

For example:

* The personal data is securely encrypted or anonymised such to make the personal data unintelligible; and/or
* There is a full, up-to-date back-up of the personal data (in cases of accidental destruction).

If there is any doubt as to whether a data breach has occurred, the Information Governance Office should be consulted immediately.

## 6.2 Reporting a personal data breach

Under Article 33 of the GDPR, TU Dublin must report a data breach, if deemed reportable, to the Data Protection Commission within 72 hours of becoming aware of the breach. This timeframe includes weekends and bank holidays.

Article 34 of the GDPR states that TU Dublin must inform affected individuals without undue delay if the data breach is likely to result in a high risk to their privacy.

As such, any data breach must be dealt with immediately and appropriately. If a member of the University becomes aware of an actual, potential or suspected data breach, they must report the incident to their Head of School / Service Area immediately. The Head of School / Service Area must then immediately report the incident to the Information Governance Office. Early recognition and reporting is vital to ensure the breach can be dealt with swiftly and appropriately.

After reporting the incident, the relevant member of the University must complete the TU Dublin Breach Notification Form and forward it to the Information Governance Office as soon as possible.

The Information Governance Office is responsible for keeping a written record of all potential or suspected data breaches that are notified to them (including those that are not notified to the Data Protection Commission or the affected individuals). For this purpose, it is imperative that the Breach Notification Form contains as much detail as possible. This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

## 6.3 Managing a personal data breach

Upon receiving notification of a data breach, the Information Governance Office shall, in conjunction with appropriate members of staff, take the following five steps (in line with best practice) when responding to the incident:

1. **Identification and initial assessment of the incident**
2. **Containment & recovery**
3. **Risk assessment**
4. **Notification**
5. **Evaluation & response**

### 6.3.1 Identification & initial assessment of the incident

If any member of the University considers that a data breach has, or might have, occurred, they must report the incident immediately and complete the TU Dublin Breach Notification form.

The Breach Notification Form will assist the Information Governance Office in conducting an initial assessment of the incident. This assessment will take into account:

* Whether a data breach has taken place
* The nature of the personal data involved in the breach (i.e. whether sensitive or confidential personal data is involved)
* The cause of the breach
* The extent of the breach (i.e. the number of individuals affected)
* The potential harms to which affected individuals may be exposed
* Any steps that may be taken to contain the breach

Following this initial assessment of the incident, the Information Governance Office may, according to the severity of the incident, consult with the Data Protection Officer and decide if it is necessary to involve other relevant University stakeholders (e.g. IT Services, Human Resources, Academic Registry) to assist with the investigation and containment process.

### 6.3.2 Containment & recovery

In the event of a data breach, immediate and appropriate steps must be taken to limit the extent of the breach.

The Information Governance Office, in consultation with relevant staff, will:

* Establish who within TU Dublin needs to be made aware of the breach (e.g. IT Services, Communications Office) and inform them of their expected role in containing the breach (e.g. isolating a compromised section of the network)
* Establish whether there is anything that can be done to recover any losses and limit the damage caused by the breach
* Where appropriate, inform the Gardaí (e.g. in cases involving criminal activity)

### 6.3.3 Risk assessment

The Information Governance Office, in conjunction with relevant staff, will use the information provided in the Breach Notification Form to fulfil the requirement to assess the potential adverse consequences for individuals, including how likely such adverse consequences are to materialise and how serious or substantial they are likely to be.

This assessment should, in particular, consider the likelihood of risks taking place and the severity of such risks is to be categorised as no risk / low risk / medium risk / high risk in accordance with the detailed criteria below:

1. Type of breach: A data breach may include any unauthorised or accidental disclosure, loss, destruction, damage or any other form of unauthorised, accidental or unlawful access to, collection, use, recording, storing or distributing of personal data. What type of data breach has or may have occurred? Does the breach consist of a breach of confidentiality relating to personal data? Is there a temporary or permanent lack of availability or access to personal data and if temporary, how long will it be before it is restored?
2. Nature of personal data: Is the relevant personal data sensitive in nature? The more sensitive the personal data the higher the risk of the data breach. The utility of the relevant information may also indicate a higher risk to the affected individuals.
3. Scale and volume of personal data affected: The higher the volume of the personal data records and the number of individuals potentially affected will usually create a higher risk.
4. Ease of identification: The ease of identifying the relevant individuals based on the personal data will likely increase the risk of identity theft, fraud and reputational damage in particular.
5. Security measures: Are the risks arising from the breach limited as a result of inherent security measures, such as encryption, where the confidentiality of the key is still intact and the data is unintelligible to a third party?
6. Containment measures: Have any containment measures been implemented which mean that the data breach is unlikely to present a risk to the individuals affected?
7. Other factors: Other relevant factors in assessing the risk to individuals is whether those individuals affected by the data breach have any special characteristics (for example children or vulnerable adults).
8. Severity of risk: Based on the above criteria and any other relevant factors, the Information Governance Office should assess the severity of the risk in terms of the potential consequences to the individuals affected by the data breach.
9. Likelihood of the risk(s) materialising: Once the data breach has occurred, the Information Governance Office must objectively assess the likelihood of the potential risks actually materialising and this should form part of the risk assessment.

An assessment of the risks for the University, including strategic and operational, legal, financial and reputational risks may also be prepared.

### 6.3.4 Notification

**Data Protection Commission**: Under GDPR Article 33, TU Dublin must report a data breach, if deemed reportable, to the Data Protection Commission within **72 hours** of becoming aware of the breach. This timeframe includes weekends and bank holidays. If a breach is deemed reportable a Data Breach Incident Report form should be completed by the Information Governance Office in conjunction with a manager from the affected School/Service Area.

If the relevant details surrounding the data breach are not clear within the initial 72-hour notification period, an initial notification should be made to the Data Protection Commission. Subsequent notifications can be made to the Data Protection Commission in phases.

Consideration as to whether a communication to affected individuals is required should be addressed when notifying the Data Protection Commission.

All contact with the Data Protection Commission should be made through the Information Governance Office.

The decision to report a breach to the Data Protection Commission will ultimately be made by the Information Governance Office, in consultation with the relevant senior management.

**Affected individuals**: As per Article 34 of the GDPR TU Dublin must inform affected individuals without undue delay, if the data breach is likely to result in a high risk to their privacy. Where the Information Governance Office assesses that there is a high risk to rights and freedoms of individuals as a result of the data breach, then the existence of the data breach should be communicated to the affected individuals **without undue delay**.

Any such communication should inform the affected individuals on relevant measures that they can take to reduce the risks to them and any negative consequences arising from the data breach.

The Information Governance Office should determine the most appropriate and effective means of communicating the data breach to the affected individuals, if necessary engaging the assistance of communications advisors.

Notification should have a clear purpose, e.g. to enable individuals who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc.

In each case, the notification should include as a minimum:

* a description of the nature of the breach;
* a description of the likely consequences of the breach;
* how and when the breach occurred;
* what data was involved;
* a description of the measures taken or proposed to be taken by the University to address the breach;
* the name and contact details of the Data Protection Officer and other contact points.

**Other parties**: TU Dublin should consider, and seek advice as appropriate, as to whether there are any other relevant notification requirements are required (such as to the Gardaí, insurers, external legal advisers etc.).

### 6.3.5 Evaluation & response

Certain data breaches will require further detailed investigation after the initial investigation period, which may involve external IT, legal and other support, as appropriate to ascertain the full extent of the data breach, its causes, and likely consequences, in order to effectively contain the breach. The effect of the data breach must be monitored and the risks re-evaluated throughout this period. It may be necessary to agree a phased notification program with the Data Protection Commission in these instances.

In the aftermath of a reportable data breach, a post-incident review of the incident should take place. The findings should include the following;

* Weaknesses that require remediation
* Actions taken to prevent similar incidents in the future
* Actions to be taken to prevent similar incidents in the future e.g. updating of policies or implementation of a technical measure
* If a DPIA is required for the processing activity
* If there has been media coverage of the incident
* Recommendations from the DPC

## 6.4 How to contact us

For further information and advice about what to do in the event of a suspected data breach 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

**Office of the Data Protection Commissioner:**

* [www.dataprotection.ie](http://www.dataprotection.ie/)
* By email: info@dataprotection.ie
* In writing: Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28
* Tel: +353 57 868 4800 or +353 761 104 800

Comprehensive information on data breach notification is available from the [Data Protection Commission](https://www.dataprotection.ie/sites/default/files/uploads/2019-08/190812%20GDPR%20Breach%20Notification%20Quick%20Guide.pdf).

# 7. Related Documents

This procedure should not be viewed in isolation. This procedure supports the following compliance and IT security policies;

1. TU Dublin Data Protection Policy
2. TU Dublin Information Security Policy

# 8. Appendices

Data Breach Notification Form

Data Breach Post Incident Report

# 9. Document Management

## 9.1 Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSION NUMBER** | **VERSION DESCRIPTIN /**  **CHANGES MADE** | **AUTHOR** | **DATE** |
| *1.0* | *Initial Procedure* | *Information & Compliance Working Group* |  |
| *1.1* | *Review and Update* | *Information Governance Team* | *27.07.23* |
|  |  |  |  |

## 9.2 Document Approval

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