Technological University Dublin

Data Breach Management Guidelines

Version 1

Document Location
Data Protection Officer, TU Dublin

Revision History

Date of this revision: September 2020	**Date of next review: September 2021**

Version Number/ Revision Number	**Revision Date**	**Summary of Changes**
Draft	July 2020	
1.0	September 2020	Update by Information & Compliance Working Group

Approval

This document requires the following approvals:

Name	**Title**	**Date**
Denis Murphy	Chief Operations Officer	24/11/2020

Table of Contents

Introduction

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'). 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 Act 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 and Compliance Officers.

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 Functions;

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

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 and Compliance Officer should be consulted immediately.

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 course work marks
- 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.

Procedure for reporting personal data breaches

Under Article 33 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.

Under Article 34 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.

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 / Function immediately. The Head of School / Function must then immediately report the incident to the Data Protection 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 Personal Data Breach Report Form (*see Appendix 2 below*) and forward it to the Data Protection Office as soon as possible. The Data Protection 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 Personal Data Breach Report Form is completed satisfactorily. 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.

Procedure for managing personal data breaches

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

Step 1: Identification and initial assessment of the incident

Step 2: Containment & recovery

Step 3: Risk assessment

Step 4: Notification

Step 5: Evaluation & response

Step 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 Personal Data Breach Notification form.

The Personal Data Breach Notification Form will assist the Data Protection 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 Data Protection Office may, according to the severity of the incident, consult with the Information and Compliance Working Group and decide if it is necessary to appoint a group of relevant University stakeholders (e.g. IT Services, Human Resources, Academic Registry) to assist with the investigation and containment process.

Step 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 Data Protection 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)

Step 3: Risk assessment

The Data Protection Office, in conjunction with relevant staff, will use the information provided in the Personal Data 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:

a) 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?

b) 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.

c) 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.

d) 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.

e) 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?

f) Containment measures: Have any containment measures been implemented which mean that the data breach is unlikely to present a risk to the individuals affected?

g) 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).

h) Severity of risk: Based on the above criteria and any other relevant factors, the Data Protection Office should assess the severity of the risk in terms of the potential consequences to the individuals affected by the data breach.

i) Likelihood of the risk(s) materialising: Once the data breach has occurred, the Data Protection 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.

Step 4: Notification

Data Protection Commission: Under Article 33 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.

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 Data Protection Office.

The decision to report a breach to the Data Protection Commission will ultimately be made by the Data Protection Office, in consultation with the relevant Head of School / Function.

Affected individuals: Under Article 34 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 Data Protection 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 Data Protection 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.).

Step 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 data breach, a post-incident review of the incident should take place to ensure that the steps taken during the incident were appropriate and effective, and to identify any areas that may be improved in future, such as updating policies and procedures or addressing systematic issues if they arise, in order to reduce the recurrence of similar data breaches and to ensure that appropriate technical and organisational security measures are put in place.

Guidance

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

Data Protection Office, TU Dublin –

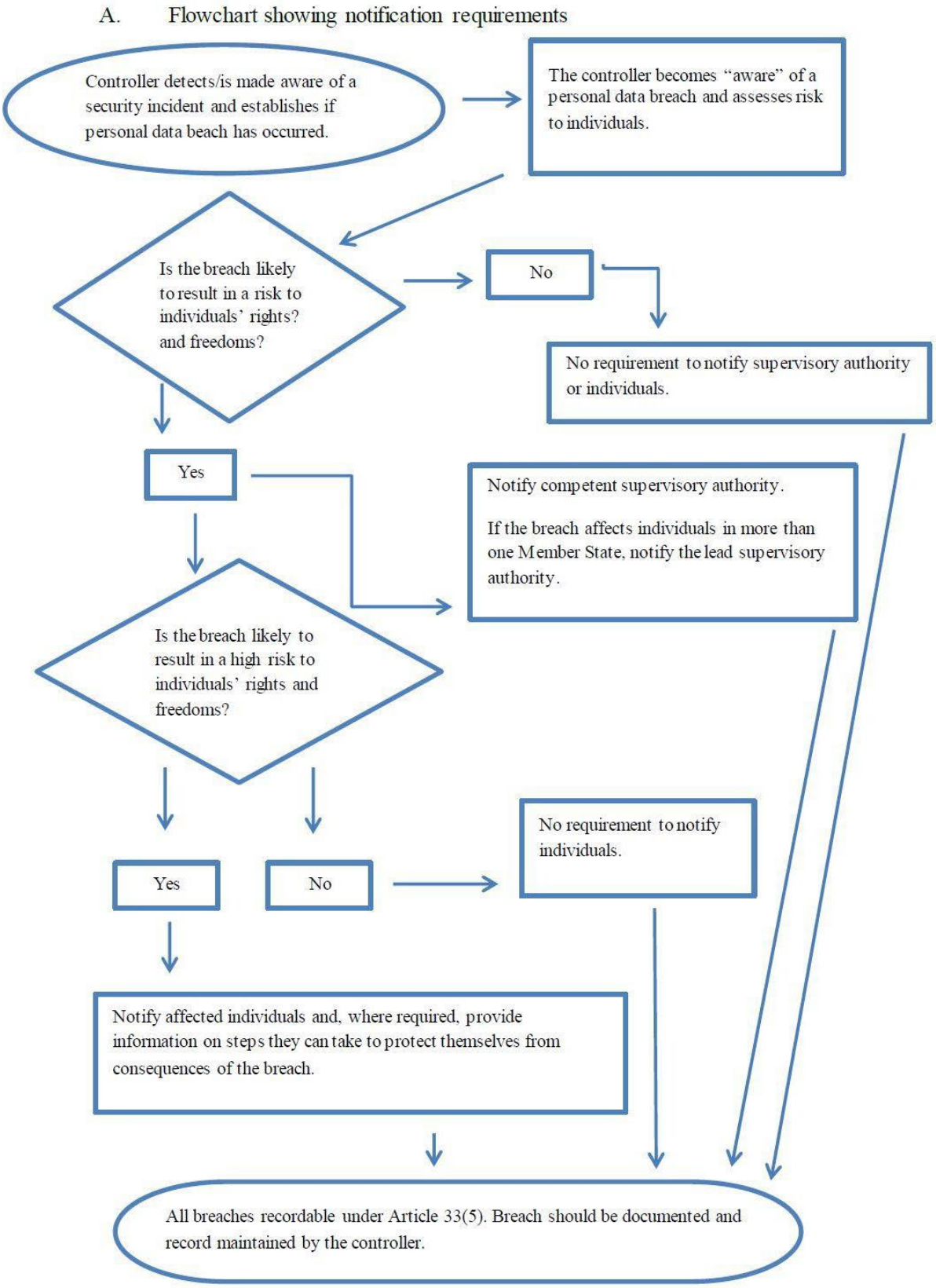
- By email: dataprotection@tudublin.ie
- In writing: The Data Protection Office, TU Dublin, Park House Grangegorman, 191 North Circular Road, Dublin 7, D07 EWV4
- Tel: Blanchardstown +353 1 8851503
  City +353 1 2205071
  Tallaght +353 1 4042530

Office of the Data Protection Commissioner:

- 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.

Appendix 1 – Data Breach Response Flowchart



Appendix 2 - Personal Data Breach Notification Form

Data Breach Incident Notification – Instructions for Completion

If you discover a personal data security breach, please notify your Manager immediately.
Please complete the Data Breach Incident Notification and return it to the Data Protection Officer **as soon as possible** **dataprotection@tudublin.ie** Please note that there is a very short period of time in which to notify the Data Protection Commissioner – 72 hours.
Please refer to Terms and Definitions for clarification on the data protection terminology used in some questions.

If you require assistance, please do not hesitate to contact your Information & Compliance Office

Blanchardstown –
Joanne Lumley, TU Dublin Blanchardstown, D15 YV78, Ireland
Email: Joanne.lumley@tudublin.ie Tel: +353 1 8851503

City –
Brian Forbes, TU Dublin Grangegorman, D07H6K8, Ireland
Email: brian.forbes@tudublin.ie Tel: +353 1 2205264

Tallaght –
Cecily Giles, TU Dublin Tallaght, D24 FKT9, Ireland
Email: cecily.giles@tudublin.ie Tel: +353 1 4042530

Data Breach Incident Notification

Initial Incident Report ***(To be completed by individual reporting the incident and/or Manager)***	
Name:	Function:
Date:	Staff Number:
Campus:	
Date of Incident:	Time of Incident:
Who was Notified?	Data and Time of Notification:
Description of Incident:	
Type of breach: Confidentiality breach, Integrity breach, Availability breach	
Estimated number of Data Subjects affected	
Estimated number of records affected	
Categories of Data Subject affected (e.g. employees, the public, suppliers etc.)	
Categories of personal data affected (e.g. Contact Details, Health Data, Bank Details, etc.)	
Any Sensitive Category personal data? (E.g. Health, Trade Union Membership, Ethnic Origin, etc.) Y/ N	
What device or system was the personal data held on?	
Are there any reasons to suspect that the passwords used to protect the personal data may have been compromised? (e.g. password stored with mobile device or weak password used)	
Any further information:	
Signed By individual reporting incident:	**Date:**
Signed By Manager:	**Date:**

Data Breach Incident Notification – Terms and Definitions

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 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 course work marks • Notes of personal supervision, including matters of behavior and discipline.
Personal Data Breach **Breach Incident**	GDPR defines a "personal data breach" 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."* A breach incident includes but is not restricted to the following: • **Unauthorised disclosure** of personal data (this includes disclosure to recipients that are not authorized to receive the data) • **Loss** or theft of confidential or sensitive personal data or the equipment used to store the data (e.g. laptop, USB key, tablet, paper record) • **Accidental or unlawful destruction** (e.g. failure of equipment) • Unauthorised use of access to or **modification/alteration** of personal data or IT systems • Attempts to gain unauthorised access to information or IT systems • Human error **Destruction –** where the data no longer exists, or no longer exists in a form that is of any use to the Data Controller. **Damage –** where personal data has been altered, corrupted, or is no longer complete. **Loss –** where the data may still exist, but the Data Controller has lost control of or access to it, or no longer has it in its possession.
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 Subject	Refers to the individual to whom Personal Data held relates, including employees, students, customers, suppliers.
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.
Unauthorised or unlawful processing	This may include disclosure of personal data to (or access by) recipients who are not authorised or do not have a lawful basis to have access to the personal data.

Appendix 3 - Personal Data Breach Report Form

Data Breach Incident Report Form

Reference No. _____ **Campus** _____

Investigation, Assessment and Response ***(To be completed by DPO Nominee in conjunction with the Staff Manager)***
Is this a Data Breach? Y / N
Potential risks to the Data Subject / Likely consequences of the personal data breach
Mitigating factors in place or proposed to be actioned
Assessment of likelihood of risks to data subject (none, low, medium, high)
Assessment of severity of risks to the data subject (none, low, medium, high)
Likely to result in a risk to the rights and freedoms of the data subject? (Y/N and justification). *Note: If yes, report to Data Protection Commissioner.*
Report to Data Subject? Y / N

Comments	
Signed By DPO Nominee:	**Date:**
Signed By Manager:	**Date:**

Post Incident Review

(To be completed by DPO Nominee in conjunction with the Staff Manager)

Potential weaknesses identified which are required to be remediated?
What action has been taken to prevent similar incidents in the future?
What action has been identified to be taken to prevent similar incidents in the future?
Has there been any media coverage of the incident?
Is a Data Protection Impact Assessment (DPIA) now required for the processing activity?
Have we recorded communications to Data Protection Commissioner and Data Subject where necessary? If so, please provide their details and an outline of their response.

Comments	
Signed By DPO Nominee:	**Date:**
Signed By Manager:	**Date:**