Ollscoil
Teicneolaíochta
an Atlantaigh

Atlantic
Technological
University

Data Breach Procedure

Version 2.0

Revision History:

Date of this revision: November 2024	**Date of next review**: November 2027

Version Number/ Revision Number	Revision Date	Summary of Changes	Pages
1.0		New Procedure	
2.0		Inclusion of links for more information Greater clarity on the process	

Consultation History:

Version Number/ Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0	n/a		
2.0	n/a		

Approval:

This document requires the following approvals:

Version	Approved By:	Date
1.0	Information Compliance Office	Nov 2022
2.0	UPT	Nov 2024

Quality Assurance:

Date Procedure to take effect: Nov 2024	Date Procedure be Reviewed: Nov 2027
Written by:	Information Compliance Office
Approved by:	UPT
Head of Function responsible:	VP for Finance & Corporate Services

Document Location:

Website – Policies and Procedures	X
Website – Staff Hub	X
Website – Student Hub	X
Other: - Information Compliance SharePoint	X

1.0 INTRODUCTION

ATU is obliged under data protection legislation to keep personal data safe and secure and to respond promptly and appropriately in the event of a personal data security breach. There is a legal requirement on the University to notify the Data Protection Commission within 72 hours of becoming aware of a breach where the breach presents a risk to the affected individuals, and to notify affected individuals without undue delay where there is a high risk to their rights and freedoms. It is therefore vital to take prompt action on foot of any actual or suspected security breach to avoid the risk of harm to individuals, damage to operational business and financial, legal and reputational costs to the University.

2.0 PURPOSE

The purpose of this procedure is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data held by the University. This procedure supplements the University's Data Protection Policy which affirms ATU's commitment to protect the privacy rights of individuals in accordance with data protection legislation.

3.0 SCOPE AND RESPONSIBILITY

This procedure applies to:

- All ATU stakeholders including staff, students, Governing Body Members, etc.
- All third parties that process the data of ATU data subjects.

4.0 WHAT IS A PERSONAL DATA BREACH?

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."*[1]

Personal data security breaches can happen in a number of ways, including via:

- disclosure of confidential data to unauthorised individuals
- inappropriate access controls allowing unauthorised use of information
- alteration or deletion of records without authorisation by the data owner
- transmission of emails containing personal or sensitive information in error to the wrong recipient
- unauthorised access to computer systems (e.g., hacking, etc)
- viruses or other security attacks on IT equipment systems or networks
- equipment failure
- loss or theft of data or equipment on which data is stored (e.g. laptop, etc)
- loss or theft of paper records
- access to confidential information left unlocked in accessible areas (e.g., leaving PC unattended when logged into user account, documents left at shared photocopiers)
- breaches of physical security (e.g., forcing of doors/windows/filing cabinets).

The General Data Protection Regulation (GDPR) identifies three categories of breaches:

- Confidentiality Breach – unauthorised or accidental disclosure of or access to personal data
- Availability Breach – unauthorised or accidental loss of access to or destruction of personal data
- Integrity Breach – unauthorised or accidental alteration of personal data.

[1] Article 4(12) GDPR

If there is any doubt as to whether a data breach has occurred, the Data Protection Officer (DPO) must be consulted immediately by emailing dataprotection@atu.ie.

5.0 PROCEDURE FOR REPORTING A PERSONAL DATA SECURITY BREACH TO THE DPO

All actual or suspected breaches must be reported to the DPO immediately by emailing dataprotection@atu.ie

Prompt reporting of an actual or suspected breach to the DPO is crucial to ensure compliance with data protection law.

The person reporting the breach will be required to complete a Breach Notification Form for assessment as soon as possible and no later than 24 hours after discovering the breach/ suspected breach. The urgency of reporting a breach/ suspected breach to the DPO is to enable the University to comply with statutory reporting obligations which require the University to notify the Data Protection Commission within 72 hours of becoming aware of the breach where the breach is likely to result in a 'high risk' to the rights and freedoms of the data subjects, and to inform the data subjects, where appropriate, without undue delay.

6.0 DPO MANAGEMENT OF A PERSONAL DATA BREACH

Upon receiving notification of a data breach, the following steps will be taken:

6.1 IDENTIFICATION & ASSESSMENT OF THE INCIDENT

The DPO will assess:

- Whether a personal data security breach has occurred
- The nature of the personal data involved
- The cause of the breach
- The extent of the breach (i.e. number of individuals affected)
- The severity of the consequences for the affected individuals.

Following this assessment, the DPO will determine the level of risk involved (None/Unlikely, Low, Medium, High, Severe) using the ENISA Personal Data Breach Severity Assessment Methodology[2] and other guidance from the Data Protection Commission[3] and European Data Protection Board[4]

In line with the accountability principle, an internal record of this assessment will be retained as well as a log of all data breaches.

6.2 CONTAINMENT & RECOVERY

Immediate and appropriate action will be taken to limit the breach, including:

- Relevant functions (e.g., IT Services, Buildings & Estates, Communications Office) will be informed to enable action to be taken to contain the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes on doors, etc.).
- Where possible, data losses will be recovered (e.g., physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data).

[2] https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool

[3] A Practical Guide to Personal Data Breach Notifications under the GDPR | Data Protection Commission

[4] Guidelines 9/2022 on personal data breach notification under GDPR | European Data Protection Board

- Where appropriate, Gardaí will be informed (e.g., in cases involving theft or other criminal activity).

6.3 NOTIFICATION

Based on the evaluation of risks and consequences, and where a risk to the rights and freedoms of individuals is identified, the DPO will notify the Data Protection Commission of the breach within 72 hours of the University becoming aware of the incident.

The University will also notify affected individuals in appropriate circumstances and certainly where the data breach is likely to result in a 'high risk' to their rights and freedoms. Affected individuals will be informed of:

- the nature of the breach
- the circumstances leading to the breach
- the steps taken to rectify the breach,
- an apology, and
- where applicable, the fact that the breach has been notified to the Data Protection Commission.

6.4 EVALUATION & RESPONSE

In the aftermath of a personal data security breach, the person responsible for the breach (and that person's line manager) will be provided with an update by the DPO.

A review of the incident may take place to ensure that the steps taken during the incident were appropriate and effective, and to identify any areas for improvement, such as updating policies and procedures or addressing systematic issues.

7.0 FURTHER INFORMATION

For further information, see the ATU Data Protection Policy or the Data Protection Commission website at www.dataprotection.ie