Ollscoil na Gaillimhe
University of Galway

Policies and Procedures

Code: **QA443**
Title: **Personal Data Breach Procedure**
Date: **25 November 2022**
Approval: **IT Security and Data Protection Committee**

1.0 Purpose

University of Galway are required to take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Any breach of the Data Protection Acts 1988 - 2018 and the European General Data Protection Regulation 2016 may render the University liable to action by the Data Protection Commissioner and by the person affected by the breach. This procedure is intended as one such measure to provide guidance on how to report and investigate a personal data breach.

All University of Galway users of personal data have a responsibility to ensure that they process such data in accordance with the Data Protection Acts 1988 - 2018 and in accordance with the General Data Protection Regulation 2016.

2.0 Procedure

All data breaches, whether accidental or not, should be reported to the Data Protection Officer so that appropriate advice can be given, and appropriate action can be taken, where possible to contain the breach or to advise any individuals likely to suffer distress or inconvenience as a result. Throughout the breach management process records should be kept of what action has been taken and by whom. Please note that in the case of a personal data breach, University of Galway shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Office of the Data Protection Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

A data security breach can happen for several reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking
- 'Misrepresentation' offences where information is obtained by deceiving the organisation who holds it.

Where a personal data breach has occurred, there are four important elements to any breach management plan:

1. Containment and recovery
2. Notification of Breach
3. Assessment of ongoing risk
4. Evaluation and response

2.1 Containment and recovery:

The unit where the breach occurred should consult immediately with the Data Protection Officer to confirm the breach and to identify and implement any steps required to contain the breach and to identify and implement any steps required to recover any losses and limit the damage of the breach. The unit where the breach occurred should consult with the Data Protection Officer and ISS to establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could for example involve the recalling of an email, the deletion of an email, isolating or closing a compromised section of the network, finding a lost piece of equipment or changing passwords or access codes. This will involve interaction with Chief Operating Officer, ISS, Internal Audit Office (Insurance Office) and other units across the University.

The unit concerned must assign a staff member to work with the above offices on resolving the matter.

The unit concerned should consult with the Data Protection Officer to establish whether there is anything can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff are alerted to recognise if someone tries to use stolen data to access accounts.

2.2 Notification of the Breach

2.2 (A) Notification to Data Protection Officer:

The responsibility for the notification to the Data Protection Officer will be completed by the unit where the breach occurred.

The notification should include details for each of the below:

- Please enter the time and date of the breach?
- When was the breach detected?
- What is the nature of the breach (lost device, misdirected email etc)?
- If not notified to the Data Protection Officer within 72 hours period as set out in GDPR the reasons why?
- How did the breach occur?
- How many people are affected and who are they?
- If you have not notified the Data Protection Officer immediately upon coming aware, why not?
- What processes or systems are affected?
- What consideration has been given to notifying third parties such as the police, insurers, bank or credit card companies, and the trade unions?
- What consideration has been given to discussing with the Press Office regarding the preparing and issuing a press release as necessary. When informing the media, it is

useful to report whether or not the Data Protection Commissioner's Office has been informed and what action is being taken?
- What are the possible adverse consequences of the breach?

2.2 (B) Notification to affected individuals:

The responsibility for the notification to affected individuals will be **completed by the unit where the breach occurred** with advice from the Data Protection Officer. The Data Protection Officer can advise if individuals need to be informed. Members of the unit may also need to meet with affected individuals.

An important element in managing a breach is informing the individuals whose data has been compromised. Notification will enable individuals affected by the breach to take steps to mitigate the risk. In deliberating the most appropriate way to notify those affected, the urgency of the situation and the security of the medium are key considerations.

Notification to the individual should include details on:

- A description of the data involved;
- Details of how and when the breach occurred;
- What action has already been taken to respond to the risks posed by the breach;
- Identify if there are any protections in place;
- An apology if necessary;
- Unit contact details for further information.

2.2 (C) Notification to the Office of the Data Protection Commissioner where required should include:

2.2(C)(1) Notification: The responsibility for the notification where required to the Office of Data Protection Commissioner will be completed by the Data Protection Officer with written input from the unit containing the below details where the breach occurred. Notification to the appropriate regulatory bodies will allow such bodies to provide advice, deal with complaints and perform their functions. Notification to the Office of the Data Protection Commissioner must be completed within **72 hours** from the time of becoming aware of the breach. Notification should include:

- The type of information and number of records;
- Circumstances of the loss, release or corruption;
- Action taken to mitigate effect on individuals;
- Whether individuals have been informed and whether any other organizations have been informed;
- Possible consequences of the breach;
- Details of the security measures in place and, where appropriate, details of the security procedures in place at the time the breach occurred;
- Remedial action taken to prevent future occurrences;

- Whether the media are aware of the breach so that the Data Protection Commissioners Office can manage any increase in enquiries from the public.

2.2(C)(1) Risk Assessment: One of the material changes impacting controllers under the GDPR relates to the mandatory notification of data breaches within 72 hours to the Data Protection Commissioner, unless the breach is unlikely to result in risk to the rights of individuals, and to affected individuals, where the breach is likely to result in a high risk.

There is a requirement under the Data Protection Acts for a risk assessment to be undertaken with regard to data breaches in a unit. The responsibility for conducting this risk assessment will rest with the Unit Head in conjunction with the Data Protection Officer.

In determining how serious the University considers the breach to be for affected individuals the University can take into the account the impact the breach could potentially have on the individuals whose data has been exposed. The following must be considered, the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place, and whether the data of vulnerable persons (a child, or a person who by reason of physical or mental capacity is unable to act on their own behalf) has been exposed.

The levels of risk can be defined as follows:
- Low: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
- Medium: The breach may have an impact on individuals but the impact is unlikely to be substantial.
- High: The breach may have a considerable impact on individuals.
- Severe: The breach may have a critical extensive or dangerous impact on the individual.

Low to medium will not be reported but mitigating actions shall be taken on the advice of the Data Protection Officer.

Medium, an assessment will be made by the Unit Head in conjunction with their Line Manager and on the advice of the Data Protection Officer.

Medium to High, High to Severe and Severe will be reported immediately.

2.3 Assessment of ongoing risk

Some data security breaches will not lead to risks beyond inconvenience to those who need the data to do their job e.g. where a device is lost but it can be remotely disabled, and where its files were backed up, can be recovered, albeit at some cost to the University. While these types of incidents can still have serious consequences, the risks are very different from those posed by, for example, the theft of a large research project database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary further to immediate containment, risks which may be associated with the breach need to be fully assessed. The assessment should include an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. Guidance should be sought from appropriate sources DPO/ISS to confirm the level of action required to reduce the risk of recurrence of similar events.

2.4 Evaluation and response

It is important not only to investigate the causes of any data breach but also to consider the effectiveness of the University's response in case there are systemic or ongoing problems e.g. lack of clear allocation of responsibility, inadequate policies or procedures. Monitoring of staff awareness of security issues may reveal gaps that can be filled through tailored advice or training. Risks will arise when sharing data with or disclosing data to others. The storing or transmission of personal data on portable or mobile devices is a weak point in security measures if encryption is not employed.

Where required, personal data breaches will be notified by the Data Protection Officer, the IT Security Committee, the Risk Management Group, University Secretary and/or Chief Operation Officer and/or the Registrar, who may appoint a member of staff to lead the investigation into the breach, ensuring that adequate resources are assigned to this task. The investigation will involve staff from school or department or unit where the breach occurred and potentially also from Information Services and Solutions, Human Resources, and Marketing and Communications (Press Office). Where the breach is serious, a written report will be prepared for the Chief Operation Officer and/or the Registrar and/or Secretary after the investigation is complete and mitigating action taken. Any action resulting from the investigation will fall under the normal agreed procedures.

3.0 Responsibilities

The following roles and responsibilities apply in relation to this Procedure:

Name/Title	Roles and Responsibility
ICT Security Committee	Procedure approver.
University Management Team (UMT)	Each member of UMT is responsible for ensuring compliance with the Data Protection Acts and this Procedure in their respective areas of responsibility.
Internal Audit	Monitoring and reporting compliance with the Procedure
Chief Operating Officer	Procedure Owner. Ensuring that appropriate policies and procedures are in place to support this Procedure. Liaising with the UMT as appropriate.
Data Protection Officer	Act as a contact point and support for and liaising with the Unit Heads. Notification of Breaches to Data Protection Commission Ensuring that this Procedure is reviewed and approved by the ICT Security Committee as appropriate: Organize targeted Procedure training and briefing sessions for University staff as required.
Heads of School/Unit	Ensuring compliance with this Procedure in their respective areas of responsibility; Notification of Breaches to the Data Protection Officer

	Notification of Breaches to affected Data Subjects if required. Ensuring Personal Data sharing is conducted in accordance with University guidance.
All Staff or Students or Members engaged in dealing with personal or Special Categories of Personal Data	Acquaint themselves with, and abide by, the rules of this Procedure and related policies and procedures. Understand what is meant by 'personal data' and 'special categories of personal data' and know how to handle such data. Notification of Data Breaches to Unit Heads or nominees. Must complete relevant training and awareness activities provided by the University to support compliance with this Policy. Should take all necessary steps to ensure that no breaches of information security result from their actions.

4.0 Related Documents
QA400 Data Protection Policy
QA402 Data Classification Policy
QA401 Data Handling Policy
QA442 Record Retention Policy
Data Rights Request Procedure
Records of Processing Procedure

5.0 Further Information
If you have any queries in relation to this policy, please contact:

The Data Protection Officer
Room A129 The
Quadrangle
University of
Galway
University Road
Galway
Email:
dataprotection@universityofgalway
.ie

6.0 Disclaimer
The University reserves the right to amend or revoke this Procedure at any time without notice and in any manner in which the University sees fit at the absolute discretion of the University or the President of the University.