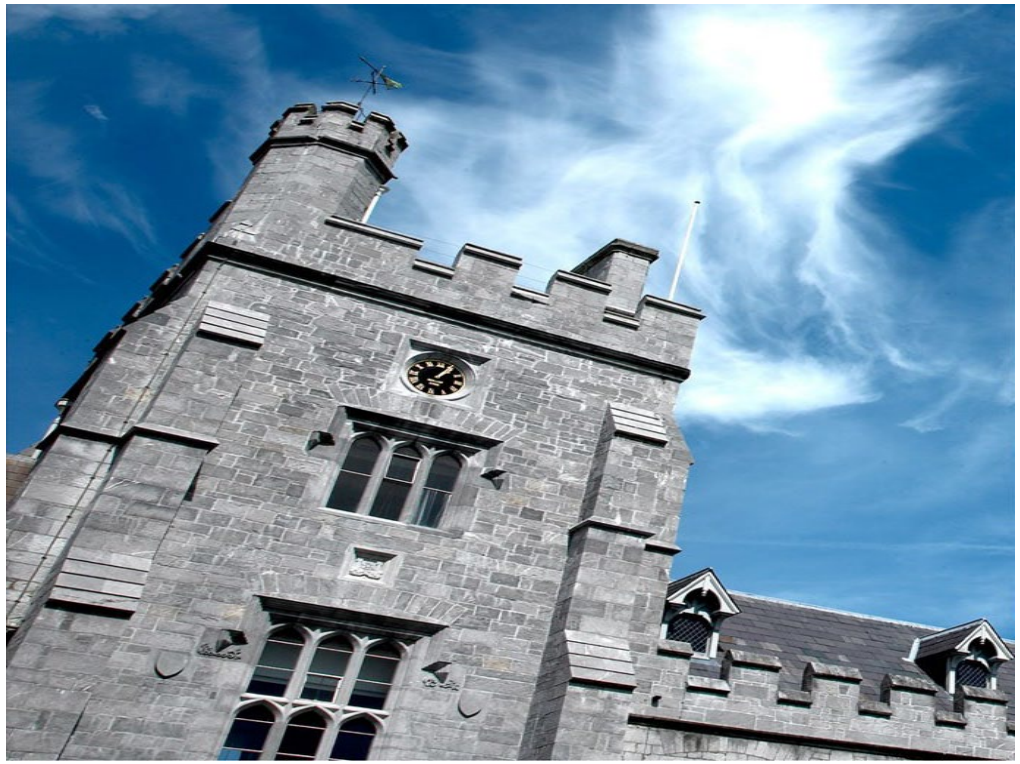

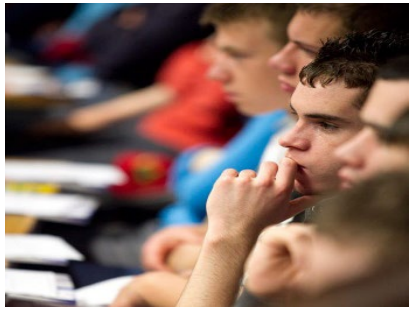

Managers' Insight Hub – Data Security Breaches
6th March 2025

Deirdre Cummins, Deputy Data Protection Officer
Audrey Huggard, Director of Legal and Information Compliance

A TRADITION OF INDEPENDENT THINKING

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

What is a data security breach?

A **data security breach** occurs when the personal data for which an organisation is responsible suffers a security incident resulting in a breach of **confidentiality**, **availability** or **integrity**

Data Breaches

- **Confidentiality breach** - unauthorised or accidental disclosure of, or access to, personal data.
- **Integrity breach** -unauthorised or accidental alteration of personal data.
- **Availability breach** - accidental or unauthorised loss of access to, or destruction of, personal data.

Examples of Types of Breaches

- Disclosure of confidential data to unauthorised individuals
- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls
- Hacking, viruses or other security attacks on IT equipment / systems
- Emails containing personal data sent in error to wrong recipient
- Emails sent to mailing list not using the BCC field

N.B. Applies to paper **and** electronic records

GDPR and Data Security

Principle of Integrity and confidentiality – keep data safe and secure! Do not permit unauthorised access, intentionally or accidentally.

Technical and organisational measures around processing of personal data. Includes physical, I.T. and policy measures.

Measures in place should be **appropriate** having regard to the nature of the data and resources available.

Sensitive data requires greater measures

What to do if you discover a breach

Report any suspected breaches immediately!

- **Report incident to your Head of School/Unit**
- **Head of Unit to report incident to Information Compliance Office (gdpr@ucc.ie)**
- **Section 1** of Personal Data Breach Report form to be completed by relevant unit and emailed to gdpr@ucc.ie
- Information Compliance team follow Data Breach Management Procedure:
    - Assess, contain and respond to the incident
    - Liaise with relevant parties
    - Assess whether notification to individuals and DPC is required.

Under GDPR, mandatory breach notifications:

- to Data Protection Commission within 72 hours
- to data subjects 'without undue delay'.

When in doubt, report it! gdpr@ucc.ie

Dealing with Data Breach Incidents

- **Act quickly** – we may be able to mitigate the consequences of the breach. Vast majority of reports do come in within a day or so of incident

- **Engage** with the Information Compliance Office

- **Prioritise the Breach Response** – time sensitivity of notification requirements

- **Timely cooperation** – same day responses required

- **Nature of data –** is there a particular sensitivity?

- **How many records?** – volume can influence assessment

- **How many affected (data subjects)?**

- **Potential consequences for data subjects?**

DPC Annual Report 2023

The DPC's annual report 2023 set out the amount / type of personal data breaches reported to the DPC.

"In 2023, the DPC received 6,991 valid GDPR data breaches. This represented a 20% increase (1,077) on the GDPR data breach numbers reported in 2022.

***Public sector bodies** and banks accounted for the 'top ten' organisations with the highest number of breach notifications recorded against them, with insurance and telecom companies featuring prominently in the top twenty.*

*Notably, **correspondence issuing to incorrect recipients because of poor operational practices and human error** – for example inserting a wrong document into an envelope addressed to an unrelated third party – continues to feature prominently."*

Internal Examples

Attachment error:

An external individual was sent an email attachment believed to be a blank form but the attachment in fact contained personal details relating to another external individual.

The details included in the attachment involved financial information and name and address of a third party.

Remedial action:

- Recipient requested to confirm deletion
- Data subject notified and apology extended
- GDPR Training
- Review of processes for providing access to forms

Internal Examples cont'd

Information leading to inference:

An email was sent, via bcc, to students. The email contained names of students, names and contact details of Practice Tutors, and location of Practice Placement sites.

Against the name of one student, was the comment: "*laptop use/other accommodations*".

Persons familiar with UCC's Disability Support (DS) procedures, may have drawn the inference that this student was registered with DS at UCC. The affected data subject notified the DPO.

Remedial action:

- Students were asked to permanently delete the email and to respond to confirm that they had done so.
- DPC was notified
- An email was sent to the data subject:
  - apologising for the incident
  - informing the data subject that UCC were treating it as a data breach and that the DPC was notified
  - assuring them that processes will be reviewed in light of the error
  - providing contact details should they wish to discuss further.

Case Studies

Maynooth University - €40,000 fine – December 2024

DPC inquiry into a personal data breach notified by Maynooth University where an unauthorised person gained control of the email accounts of six university employees. One such account was used to assist in the commission of a fraud, leading to a financial loss. The DPC found that there was:

- a failure to ensure appropriate security of personal data
- a failure to implement appropriate technical and organisational measures to ensure such security
- an infringement of the GDPR by failing to notify the DPC of the data breach within 72 hours.

Case Studies cont'd

Centric Health - €460,000 fine – January 2023

Ransomware attack affecting patient data. 70,000 data subjects. 2,500 patients were permanently affected as their data was deleted with no backup available. The DPC found that:

- there was a lack of appropriate measures to prevent the placement and execution of ransomware on the system
- Steps taken by Centric that permanently deleted some of the personal data amounted to an infringement of Article 5(1)(f) GDPR.
- there was a significant loss of availability of sensitive personal data and an inability to restore the availability for a subset of the data. There was a failure to appropriately address the identified risks and ensure ongoing integrity and availability, amounting to an infringement of Article 32(1) GDPR.

Case Studies cont'd

The Health Service Executive - €65,000 fine – August 2020

Documentation containing the personal data of 78 individuals, including special category personal data in respect of 6 of those data subjects, were disposed of in a public recycling centre.

Tusla - Child and Family Agency - €75,000 fine – November 2020

DPC conducted an inquiry in respect of three personal data breaches notified by Tusla which involved a failure to redact personal data when providing documents to third parties. DPC found that failed to implement appropriate organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data in respect of its sharing of documents with third parties. DPC also found that Tusla infringed Article 33(1) of the GDPR by failing to notify the DPC of the third breach without undue delay.

Consequences for Individuals

- Breach of confidentiality and privacy
- Financial loss
- Identity theft
- Personal or professional reputational damage
- Embarrassment, upset, even physical harm
- Availability breaches could lead to serious consequences e.g. where medical records cannot be accessed

Consequences for UCC

- Fines up to €1 million for public bodies
- Investigation / Audits by Data Protection Commission
- Litigation
- Reputational Damage – negative publicity – loss of confidence in the University

- Opportunity to learn and improve – University processes more agile and resilient

Other obligations under GDPR

Include:

- Complying with **rights** of the individual to seek access, erasure, rectification etc.

- **Transparency** measures

- **Data Protection Impact Assessments** - high risk processing

- Appropriate measures governing the **Transfer** of personal data

- Maintaining **Records** of Processing Activities
  and record **Retention Schedules**

- Kpersonal data safe and secure by implementing
  appropriate technical and organisational measures
- eep

Key Takeaways

- Staff training in GDPR

- Familiarise yourself and your staff with breach procedures

- Identify potential sources of breaches in your area and put mitigating measures in place

- Ensure you and your staff can identify a potential data breach

- Pay particular attention to any **special category data** you hold (e.g. disability data, health data, trade union membership)

- Take extra care when dealing with special category/sensitive personal data

Useful Links

- Data Protection (General) | University College Cork
- Data Security Breaches | University College Cork
- Data Breach Management Procedures
- Training | University College Cork
- Data Protection Notice procedure
- DPIA procedure