UNIT 5 - E-Portfolio Activity – GDPR Case Studies

Read the website at Data Protection Commission (2020) Case Studies: Data Protection Commission. https://dataprotection.ie/en/pre-gdpr/case-studies

There are several case studies from 2014 – 2018 concerning GDPR related issues and breaches. Chose a case study (should be unique to each student) and answer the following questions:

- What is the specific aspect of GDPR that your case study addresses?
- How was it resolved?
- If this was your organisation what steps would you take as an Information Security Manager to mitigate the issue?

You can discuss your findings as a team and come prepared to share them in next week's seminar. Remember to also save to your e-portfolio.

Chosen Case Study:

Year: 2017

Index 11: Failure by the Department of Justice and Equality to impose the correct access restrictions on access to medical data of an employee

Appendix A: Full Case study

11) Failure by the Department of Justice and Equality to impose the correct access restrictions on access to medical data of an employee

We received a complaint from an individual concerning an alleged disclosure of their sensitive personal data by the Department of Justice & Equality (the Department). It was claimed by the complainant, who was an employee of the Department, that a report containing information on the complainant's health had been uploaded to a general departmental open document management database in 2012 and that the report had remained on that database for up to three years where it could be accessed by approximately 80 employees. The complainant informed us that they had been notified of the accessibility of the report on the database by a colleague. The complainant told us that they had requested an explanation from the Department as to why the report had been placed on an open database but had not received official confirmation that the report had since been removed.

We commenced an investigation into the complaint. The Department confirmed that notes relating to a discussion which had taken place between the complainant and their line manager in 2012 (which included a note concerning the complainant's health) had been stored to the database in question and marked private. However,

the line manager had inadvertently omitted to restrict access to the document with the result that it could be accessed by approximately 80 staff members from the Department. The Department informed us that the document had been removed from the database in question some 3 years after having been saved to it. As the line manager in question had since left the Department, it had been unable to establish exactly why the document had been saved there in the first place but claimed that it was due to human error. The Department was also unable to establish how many staff had actually accessed the document during the 3-year period in which it was accessible as the Department's IT section had been unable to restore the historic data in question.

The Department made an offer, by way of amicable resolution, to write to the complainant confirming that the document in question had been removed from the database and apologising for any distress caused. The complainant chose not to accept this offer and instead sought a formal decision of the Commissioner. In her decision, the Commissioner concluded that the Department had contravened Section 2A(1) and 2B(1) of the Data Protection Acts 1988 & 2003 by processing the complainant's sensitive personal data without the required consent or another valid legal basis for doing so and by disclosing the complainant's sensitive personal data to at least one third party. These contraventions had occurred by way of the placing of a confidential document containing details of the complainant's health on an open database where it appeared to have remained accessible for 3 years and had been accessed by at least one co-worker.

This case is a stark illustration of the consequences for a data subject and general distress which can be caused where the data controller fails to ensure that its staff have adhered to, and continue, to adhere to proper document management protocols for documents containing personal data and moreover, sensitive personal data. While the controller in question was unable to identify how many times and by how many different staff members the document in question had been accessed during the 3-year period when it was accessible to approximately 80 staff members, the potential for further and continuing interference with the data subject's fundamental rights and freedom remained throughout this period. Had the controller in this case had adequate regular audit and review measures in place for evaluating the appropriateness of documents stored to open access databases, the presence of this confidential document would have been detected much sooner than actually occurred. Further, had the Department an adequate system of training and ensuring awareness by staff managers of basic data protection rules in place, this issue may not have arisen in the first instance.

Short summary of the issue:

An employee of the Irish Department of Justice & Equality discovered that a confidential document containing health information had been stored on an open

departmental database, accessible by about 80 staff for three years, and had been accessed by at least one co-worker.

QUESTIONS TO BE ANSWERED:

1) What is the specific aspect of GDPR that your case study addresses?

Under EU GDPR (EU, 2016) the issues directly addressed:

- **Article 5(1)(a) – Lawfulness, fairness and transparency**
  Processing was neither lawful nor fair, as no valid legal basis existed for storing health data in an open-access system.
- **Article 5(1)(c) – Data minimisation**
  More staff than necessary had access to highly sensitive personal data.
- **Article 5(1)(f) – Integrity and confidentiality (security of processing)**
  The Irish Department of Justice & Equality failed to ensure appropriate security of sensitive health data.
- **Article 6 – Lawfulness of processing**
  No valid legal basis for processing the complainant's health data.
- **Article 9 – Processing of special categories of personal data**
  Health data is "special category data." Its processing requires explicit consent or another lawful exception, which was absent.
- **Article 24 & 25 – Responsibility of the controller & data protection by design and by default**
  The Irish Department of Justice & Equality failed to implement adequate technical and organisational measures to prevent unauthorised access.
  - **Article 32 – Security of processing**
    No adequate technical or organisational measures were in place (e.g. access controls, regular audits and reviews, staff training).

2) How was it resolved?

- The Irish Department of Justice & Equality offered to send a written confirmation and apology to the complainant, but this was rejected.
- The Data Protection Commissioner issued a formal decision, finding the Department in breach of data protection law (Sections 2A(1) and 2B(1) of the Data Protection Acts 1988 & 2003).

3) If this was your organisation, what steps would you take as an Information Security Manager to mitigate the issue?

If this was my organisation, I would mitigate the risk by first establishing a management system based on ISO/IEC 27001 (ISO, 2022) and its privacy extension ISO/IEC 27701 (ISO 2019). This foundation provides governance, accountability, and

a structured risk management process that aligns directly with GDPR obligations. The steps would be:

- Establishing the management system (ISMS under ISO/IEC 27001) → governance, leadership commitment, risk management cycle.
- Extending with ISO/IEC 27701 → adding a Privacy Information Management System (PIMS) to address GDPR requirements and personal data risks.
- Implementing appropriate controls (access restrictions, classification, training, audits) guided by ISO/IEC 27002 and 27701 Annex A/B mappings to GDPR.
- Continuous improvement and accountability → audits, reviews, incident handling, and monitoring.

By embedding GDPR obligations within a recognised international standard, the organisation would both reduce recurrence risk and demonstrate accountability through a formal, auditable process.

Reference list

ISO (2019) *ISO/IEC 27701:2019 – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines.* Geneva: ISO.

ISO (2022) *ISO/IEC 27001:2022 – Information technology – Security techniques – Information security management systems – Requirements.* Geneva: ISO.