Task ‘e-Portfolio Activity GDPR Case Studies Excessive Data Collection by An Post’ Unit 5

What is the specific aspect of GDPR that this case study addresses?

This case study addresses two cases related to the GDPR's data minimization principle, as defined in Article 5(1)(c). This principle requires organizations to collect only personal data that is adequate, relevant, and limited to what is necessary for the intended purpose. An Post's requirement for a copy of confidential, full bank financial information that appears on account holders' bank statements which may contain additional transaction information, was deemed excessive. This is because of the collection and handling of sensitive financial information.

How was it resolved?

The issue was resolved. This happened following intervention by the Data Protection Commissioner. The DPC advised An Post to allow applicants to submit only the relevant section of their bank statements or to redact all transaction information. An Post complied by updating their application forms, website guidance and internal processes, ensuring that customers were explicitly instructed to mask financial details was important. It is also committed to destroying statements after the first successful payment. The DPC considered these steps sufficient and compliant.

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

As an Information Security Manager, I would aim to mitigate such issues by reviewing the current data collection practices to ensure alignment with the data minimization principle, for instance I would be updating procedures and customer instructions to prevent the collection of unnecessary financial information, conducting a Data Protection Impact Assessment for verification processes, and implementing strict technical controls for secure handling and create retention policies for data, with more strict ones for sensitive data. Additionally, I would ensure training, awareness, regular compliance audits, and collaboration with the Data Protection Officer are being continually updated to ensure that data collection remains proportionate, transparent and GDPR-compliant.

(Data Protection Commission, 2014)

References

Data Protection Commission (DPC) (2014). Case Study 4: Excessive Data Collection by An Post, Available at: https://dataprotection.ie/en/pre-gdpr/case-studies [Accessed 22 November 2025].