GDPR Case Study – Right of Access (Unit 5)

The selected case for this analysis is **Case Study 6:** *The importance of data controllers having appropriate mechanisms in place to respond to access requests and document compliance* (Data Protection Commission, 2018). Although the case was published in 2018, it is classified as pre-GDPR because the events occurred before the GDPR became applicable in May 2018.

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

The case focuses on the data subject's right of access, which, in the current data protection law, is set out in Article 15 of the GDPR (European Union, 2016a). Under Section 4 of the Data Protection Acts 1988/2003, controllers were required to provide individuals with access to their personal data and to explain any information not provided. The issues raised in the case reflect the information requirements now set out in Article 15(1)(e)-(g), including the need to justify refusals, inform individuals of their right to file a complaint, and, where relevant, provide information on the source of the data. Legal commentary also highlights the importance of complete access. As noted in a recent analysis

"The right of access is necessary to enable the data subject to exercise the right to rectification, erasure, restriction of processing, objection and the right of action where he or she suffers damage" (Computer Law Review International, 2025, para. 58).

These obligations closely align with the GDPR standard and illustrate the continuity between pre-GDPR and GDPR access rights.

How was it resolved?

The Data Protection Commission required the company (data controller) to:

- Restart the access-request process because it could not demonstrate what data had been provided or omitted
- Review all personal data held on the individual across manual and electronic systems
- Issue a complete response within the specified timeframe
- Provide full access to all personal data and explain why certain information was being reissued
- Justify any refusals and identify the stature exemptions applied
- Copy the DPC on the correspondence

The complainant later withdrew the case, but the DPC emphasised the need for proper record-keeping and clear communication when responding to access requests.

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

I would follow the GDPR requirements applicable to data controllers, including the obligation to maintain clear and accurate records of processing activities. Article 30 requires controllers to document the personal data they hold, how it is processed, and who is responsible for it (European Union, 2016b). This supports consistent and complete responses to access requests.

Technically, I would use a simple system to track each request, keeping track of where personal data is stored, and enabling logging so actions can be traced.

The following GDPR articles support these steps:

- **Article 24 – Responsibility of the controller**

  Requires the organisation to have appropriate processes and to demonstrate how compliance is achieved.

  (European Union, 2016c)

- **Article 32 – Security of processing**

  Requires technical controls such as logging, access control and secure data handling (European Union, 2016d).

Together, these measures would help ensure that access requests are properly tracked, documented, and responded to responsibly.

References

- Computer Law Review International (2025) EU: Scope of the right of access to information according to Article 15 GDPR, 26(1), pp. 25–29. doi:10.9785/cri-2025-260105.
- Data Protection Commission (n.d.) Case Studies – Pre-GDPR. Available at: https://dataprotection.ie/en/pre-gdpr/case-studies#201806 (Accessed: 29 November 2025).
- European Union (2016a). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679 (Accessed: 29 November 2025).
- European Union (2016b) General Data Protection Regulation, Article 30: Records of Processing Activities (RoPA). Available at: https://gdpr-info.eu/art-30-gdpr/ (Accessed: 29 November 2025).
- European Union (2016c) General Data Protection Regulation, Article 24: Responsibility of the controller. Available at: https://gdpr-info.eu/art-24-gdpr/ (Accessed: 29 November 2025).
- European Union (2016d) General Data Protection Regulation, Article 32: Security of processing. Available at: https://gdpr-info.eu/art-32-gdpr/
- (Accessed: 29 November 2025).