GDPR Case Study:

I reviewed a GDPR breach case in a public sector organisation where personal data was accidentally published online without data masking, violating core GDPR principles, especially **Article 5(1)(f)**, which requires integrity and confidentiality of personal data *(European Union, 2016)*.

Case Focus:

- **GDPR Aspect**: Article 5(1)(f), personal data shall be processed securely, including protection against unauthorised or unlawful processing (EU, 2016).
- **Issue**: A local authority uploaded documents containing unmasked names and contact details of data subjects, leading to reputational and privacy risks.
- **Resolution**: The Data Protection Commission (DPC) issued formal enforcement directions and mandatory staff training. (DPC, 2020).

Response Plan:

As an Information Security Manager, I would implement the following actions to mitigate the risk and ensure GDPR compliance.

- Audit internet facing publication workflows to identify high-risk data touchpoints (ICO, 2023a)
- Deploy automated tools to minimise human error (ENISA, 2021).
- Create a dual-approval checklist for pre-publication reviews (EDPB, 2020).
- Run annual GDPR refresher training for staff handling personal data.

- Integrate Data Loss Prevention (DLP) solutions to block sensitive data leaks (Gartner, 2022).

GDPR Response Workflow:

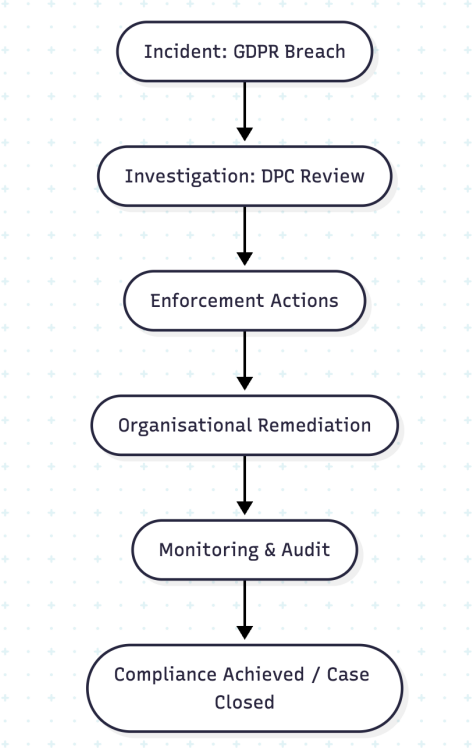

Figure 1: A linear model showing the response process from breach to remediation.

Learning Outcomes:

I learnt how to map GDPR principles to operational risks and recognised that even minor violations can trigger regulatory action and significant fines of up to 4% of global turnover. I also realised that compliance is not only legal but strategic governance.

References:

Data Protection Commission (2020) *Case Studies.* Available at: https://www.dataprotection.ie/en (Accessed: 18 October 2025).

EDPB (2020) *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR.* Available at: https://edpb.europa.eu/ (Accessed: 18 October 2025).

ENISA (2021) *Guidelines for Securing Personal Data.* Available at: https://www.enisa.europa.eu/publications (Accessed: 18 October 2025).

European Union (2016) *General Data Protection Regulation (EU) 2016/679.* Available at: https://gdpr.eu/ (Accessed: 18 October 2025).

Gartner (2022) *How to Implement Effective DLP Strategies.* Gartner Research.

ICO (2023a) *Accountability and Governance.* Available at: https://ico.org.uk/for-organisations/accountability-framework/ (Accessed: 18 October 2025).