Selected Case Study: Failure to Honour Right of Access Request (Ireland)

a. Specific Aspect of GDPR Addressed

The selected case study focuses on the right of access under Article 15 of the General Data Protection Regulation (GDPR). This provision grants data subjects the right to obtain confirmation from data controllers as to whether their personal data is being processed, access to that data, and information about the processing purposes, recipients, and retention periods(Custers & Heijne,2022).

In this case, an individual submitted a subject access request (SAR) to a data controller seeking details of personal data held about them. The organization failed to provide a complete response within the statutory timeframe of one month, as stipulated under Article 12(3) of the GDPR. The complaint was escalated to the Data Protection Commission (DPC), which found that the organization breached its obligations by not fulfilling the SAR adequately and on time (Laurer & Seidl,2021).This case illustrates a crucial aspect of GDPR compliance—transparency and accountability which form the backbone of lawful data processing in enterprises (Labadie & Legner 2023).

b. Resolution of the Case

Upon investigation, the DPC determined that the organization had violated GDPR requirements regarding the right of access. Consequently, the Commission issued a formal reprimand and required the organization to improve its internal data handling and response procedures.

c. Mitigation Measures as an Information Security Manager

(i) Establish a GDPR Compliance Policy: Define clear internal procedures for handling SARs, including timelines, verification processes, and escalation paths.

(ii) Implement Automated Request Management Tools: Use workflow management software to log, track, and alert staff about pending access requests to prevent delays.

(iii) Conduct Staff Training and Awareness Programs: Regularly train employees on data subject rights and reporting obligations to reduce compliance errors.

(iv) Adopt ISO/IEC 27001 and 27701 Standards: Integrating these information security and privacy management standards ensures structured risk assessment, continual monitoring, and accountability (Allendevaux,2021).

(v) Perform Regular Data Audits and Impact Assessments: Conduct periodic Data Protection Impact Assessments (DPIAs) to identify potential weaknesses and ensure all personal data processing activities comply with GDPR.

References

Custers, B. and Heijne, A.S., 2022. The right of access in automated decision-making: the scope of article 15 (1)(h) GDPR in theory and practice. *Computer Law & Security Review*, *46*, p.105727

Laurer, M. and Seidl, T., 2021. Regulating the European data-driven economy: A case study on the general data protection regulation. *Policy & Internet*, *13*(2), pp.257-277.

Labadie, C. and Legner, C., 2023. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), pp.16-44.

Allendevaux, S., 2021. *How US State Data Protection Statutes Compare in Scope to Safeguard Information and Protect Privacy Using Iso/Iec 27001: 2013 and Iso/Iec 27701: 2019 Security and Privacy Management System Requirements as an Adequacy Baseline* (Doctoral dissertation, Northeastern University)