Activity – GDPR Case Studies

1. **Case Study: Right to be Forgotten.**

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

The case study relates to the right to erasure, also called the right to be forgotten. Under Article 17 of the UK GDPR, the right to erasure (the 'right to be forgotten') allows individuals to have their data erased in certain circumstances. The right applies if the data is no longer necessary, the individual withdraws their consent, they object to processing, and there is no overriding legitimate interest, or if the data was processed unlawfully (ICO, 2023). The complainant, in this case, requested that links to webpages containing personal data that was inaccurate, incomplete, and outdated be removed (delisted) from search engine results (Data Protection Commission, N.D.)

1.2. How was it resolved?

The search engine operator complied with the request and removed the links. This fulfilled the complainant's right to erasure, ensuring that outdated and inaccurate information about the individual was no longer accessible through search engine results.

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

As an Information Security Manager, if this were my organisation, I would take the following steps to mitigate similar issues as Noss (2023) and Sengupta (2023) demonstrate:

- **Review and update policies:**

We must ensure our data retention policy is current and effective in preventing the retention of personal data beyond its necessary purpose. We must establish clear

guidelines for handling requests related to the right to erasure in a consistent and easy-to-understand manner (ICO, 2023).

- **Ensure data accuracy and quality:**

We must regularly audit and verify the accuracy, completeness, and relevance of personal data stored in our systems. We must also have processes to promptly update or delete outdated or incorrect data (ICO, 2023).

- **Conduct data protection impact assessments (DPIA):**

For any new data processing activities, we must conduct DPIA to assess potential risks to individuals' rights, including the right to erasure. We must evaluate the impact of data processing on individuals' privacy and take necessary measures (ICO, 2023).

- **Train employees and increase awareness:**

To ensure GDPR compliance, we must train employees, especially those handling personal data, on GDPR principles, including data subject rights. We need to make sure that all staff understand their responsibilities regarding data accuracy and erasure requests (ICO, 2023).

- **Improve incident response plan:**

Our incident response plan must be enhanced to include procedures for handling erasure requests. We must define roles and responsibilities for addressing such requests promptly (NCSC, 2019).

- **Communicate transparently:**

We must communicate our data handling practices clearly to individuals. We must provide information on how to request erasure and exercise other data subject rights in an easy-to-understand and transparent manner (Data Protection Commission, N.D.).

References:

- ICO (2023). *Right to erasure*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/.
- Data Protection Commission (N.D.). *Case Studies | Data Protection Commission*. [online] Available at: https://www.dataprotection.ie/en/pre-gdpr/case-studies#201804 [Accessed 25 Feb. 2024].
- Noss, S. (2023). *Data Risk Mitigation: How To Keep Your Organization's Data Safe*. [online] DataGrail. Available at: https://www.datagrail.io/blog/data-privacy/data-risk-mitigation/.
- Sengupta, N. (2023). *6 Essential Tips for Information Security Managers*. [online] Available at: https://www.bitraser.com/blog/6-essential-tips-for-information-security-managers/ [Accessed 25 Feb. 2024].
- ICO (2023). *Principle (e): Storage limitation*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/.
- ICO (2023). *Principle (d): Accuracy*. [online] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/.
- ICO (2023). *Data protection impact assessments*. [online] Available at: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/data-protection-impact-assessments/ [Accessed 25 Feb. 2024].
- ICO (2023). *Training and awareness*. [online] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/training-and-awareness/.
- NCSC (2019). *Plan: Your cyber incident response processes*. [online] Ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes.
- Data Protection Commission (N.D.). *The right to be informed (transparency) (Article 13 & 14 GDPR) | Data Protection Commission*. [online] The right to be informed (transparency) (Article 13 & 14 GDPR) | Data Protection Commission. Available at: https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-14-gdpr.