Collaborative Discussion 3

Failure by the Department of Justice and Equality to impose the correct access restrictions on access to medical data of an employee

- What is the specific aspect of GDPR that your case study addresses?
- How was it resolved?
- If this was your organisation what steps would you take as an Information Security Manager to mitigate the issue?

The case in question, related to confidential personal health information being accessible by co-workers in the US Department of Justice and Equality. The report shows that at least 1 person accessed the health records, while at least 80 people had unrestricted access to the records and may have accessed it. The records were available on the database for 3 years before being removed.

This health information public disclosure breached the GDPR guidelines in the following ways:

- Article 5: The processing and storage of data did not ensure adequate security of the data, leading to public disclosure (European Union, 2018a)

- Article 32: Pseudo-anonymisation and encryption of data was not followed. As the records were available for 3 years on the database, regular testing of security of data processing procedures were not followed (Intersoft Consulting, 2018).

- Article 33, 34: A breach of personal data was not reported to the subject, or the appropriate regulatory bodies (GDPR-info.eu, 2016).

- Article 82: No compensation was offered to the affected party. This was a clear failure by the data controller, and compensation should be offered as a result of negligence (*Art. 82 GDPR – Right to compensation and liability* | *General Data Protection Regulation (GDPR)*, no date).

The subject approached the courts for compensation, and an independent commissioner concluded that the department had contravened section 2A and 2B of the Data protection acts of 1988 and 2003. Personal data was not allowed to be processed and appropriate consent was not gained. In addition, the department shared personal data with at least 1 third party without consent.

This example is a clear failure of the data controller and data protection systems. All personal data should only be stored and processed with appropriate consent and where necessary. All stored data should be pseudo-anonymisation and encrypted. Regular data protection security checks should be done.

References

Art. 82 GDPR – Right to compensation and liability | *General Data Protection Regulation (GDPR)* (no date). Available at: https://gdpr-info.eu/art-82-gdpr/ (Accessed: 30 October 2021).

European Union (2018a) *Art. 5 GDPR – Principles relating to processing of personal data* | *General Data Protection Regulation (GDPR)*, *Intersoft Consulting*. Available at: https://gdpr-info.eu/art-5-gdpr/ (Accessed: 30 October 2021).

European Union (2018b) 'General Data Protection Regulation (GDPR) – Official Legal Text', *General Data Protection Regulation*, pp. 1–99. Available at: https://gdpr-info.eu/ (Accessed: 17 September 2021).

GDPR-info.eu (2016) *Art. 33 GDPR – Notification of a personal data breach to the supervisory authority* | *General Data Protection Regulation (GDPR)*, *GDPR-info.eu*. Available at: https://gdpr-info.eu/art-33-gdpr/ (Accessed: 30 October 2021).

GDPR compliance checklist - GDPR.eu (2021) *General Data Protection Regulation*. Available at: https://gdpr.eu/checklist/ (Accessed: 20 October 2021).

Intersoft Consulting (2018) *Art. 32 GDPR – Security of processing* | *General Data Protection Regulation (GDPR)*, *gdpr-info*. Available at: https://gdpr-info.eu/art-32-gdpr/ (Accessed: 30 October 2021).

Kan, Mi. (2017) 'Yahoo execs botched its response to 2014 breach, investigation finds', *Cso*. Available at: https://www.csoonline.com/article/3176181/yahoo-execs-botched-its-response-to-2014-breach-investigation-finds.html (Accessed: 31 October 2021).

Remember the 2013 Yahoo Data Breach? The Company May Owe You $375 | *Inc.com* (no date). Available at: https://www.inc.com/minda-zetlin/yahoo-data-breach-50-million-lawsuit-settlement-account-holders-375.html (Accessed: 31 October 2021).

Summary Post

We are living in the age of data. Data is collected, stored and used by all of us and from all of us. It is only appropriate that the old regulations which govern data have evolved into the GDPR. Stiff fines of up to 10 million Euros may be imposed on non-complying companies. This is a significant improvement, as in the past, the fines would essentially be a slap on the wrist, and companies could easily flout regulations without much oversight or penalties.

An example is the Yahoo data breach in 2013 and 2014, where an estimated **3 billion** user accounts were compromised (Kan, 2017). Compensation totalled around $375 dollars for each person, limited to the US and Israel (*Remember the 2013 Yahoo Data Breach? The Company May Owe You $375* | *Inc.com*, no date). Fines imposed did not reflect the negligence of the company, which failed to inform users of the breach for more than 2 years. If the GDPR regulations had applied in the Yahoo case, much more care would be taken by Yahoo and other companies when handling, storing and using user data.

Fortunately, the GDPR is a straightforward set of regulations for companies to take. 7 main principles for businesses to follow are (European Union, 2018):

- Lawfulness, fairness and transparency: The business must have a lawful reason for storing and or processing user data.
- Purpose limitation: User data will only be processed for the reason that they have been collected.
- Accuracy: User data should be accurate and up to date
- Storage limitation: Data should be kept in a form which is identifiable and portable, and only kept for as long as is necessary
- Data minimization: User data collected is to be relevant and limited to the purpose of the collection.
- Integrity and confidentiality (security): Adequate security and encryption to protect user data and limit unauthorized or unlawful use
- Accountability: Data controller shall be appointed to ensure compliance with the GDPR regulations and shall be held responsible for non-compliance.

All businesses should use the compliance checklist to ensure compliance (*GDPR compliance checklist - GDPR.eu*, 2021).

European Union (2018) ‘General Data Protection Regulation (GDPR) – Official Legal Text’, *General Data Protection Regulation*, pp. 1–99. Available at: https://gdpr-info.eu/ (Accessed: 17 September 2021).

GDPR compliance checklist - GDPR.eu (2021) *General Data Protection Regulation*. Available at: https://gdpr.eu/checklist/ (Accessed: 20 October 2021).

Kan, Mi. (2017) ‘Yahoo execs botched its response to 2014 breach, investigation finds’, *Cso*. Available at: https://www.csoonline.com/article/3176181/yahoo-execs-botched-its-response-to-2014-breach-investigation-finds.html (Accessed: 31 October 2021).

Remember the 2013 Yahoo Data Breach? The Company May Owe You $375 | *Inc.com* (no date). Available at: https://www.inc.com/minda-zetlin/yahoo-data-breach-50-million-lawsuit-settlement-account-holders-375.html (Accessed: 31 October 2021).