GDPR Compliance: Peer Responses

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: ePortfolio

Date: Saturday 30th October 2021

Student ID: 126853

Peer Response 1:

In response to:

Uzayr Parak

Initial Post

13 hours ago

1 reply

Last now

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, 2018)

- 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.

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 (2018) *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).

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).

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).

Post:

Hi Uzayr,

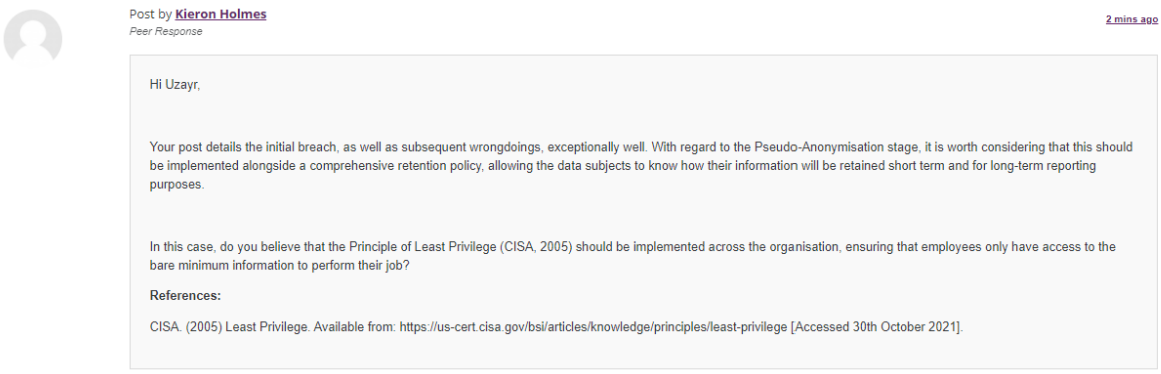
Your post details the initial breach, as well as subsequent wrongdoings, exceptionally well. With regard to the Pseudo-Anonymisation stage, it is worth considering that this should be implemented alongside a comprehensive retention policy, allowing the data subjects to know how their information will be retained short term and for long-term reporting purposes.

In this case, do you believe that the Principle of Least Privilege (CISA, 2005) should be implemented across the organisation, ensuring that employees only have access to the bare minimum information to perform their job?

References:

CISA. (2005) Least Privilege. Available from: https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege [Accessed 30th October 2021].

Screenshot:



Post by **Kieron Holmes** 2 mins ago

Peer Response

Hi Uzayr,

Your post details the initial breach, as well as subsequent wrongdoings, exceptionally well. With regard to the Pseudo-Anonymisation stage, it is worth considering that this should be implemented alongside a comprehensive retention policy, allowing the data subjects to know how their information will be retained short term and for long-term reporting purposes.

In this case, do you believe that the Principle of Least Privilege (CISA, 2005) should be implemented across the organisation, ensuring that employees only have access to the bare minimum information to perform their job?

References:

CISA. (2005) Least Privilege. Available from: https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege [Accessed 30th October 2021].

Peer Response 2:

In response to:

Sergio Rafael Zavarce Caldera

Initial Post

13 days ago

2 replies

Last 9 mins ago

In the Annual Reports published by the Data Protection Commission, a case in 2017 describes the use of CCTV footage in a disciplinary process. In this case, the complainant filed a claim at the Commission stating that his employer did not notify him about the possibility of using this footage in such proceedings (Data Protection Commission, 2020). The complainant was disciplined and dismissed by the company after reviewing the CCTV footage. They confirmed that he was away from the control room where he was assigned to monitor the cameras while on duty as a security officer, compromising the security of the client's premises.

The employer argued that before assigning the employee to the task where he was recorded, he was asked to read a document stating his responsibilities and signing a certificate of acceptance of these terms. The employer also argued that they had a legitimate interest to process the personal data from the CCTV footage, to protect its reputation and financial liability, since they had a contractual obligation to safeguard the client's premises.

The Commissioner considered that the employer had the legal basis to use the CCTV footage based on the Section 2A(1)(d) of the Data Protection Acts 1988 and 2003 (Data Protection Act, 1998), which states that "the processing is necessary for the purposes of the legitimate interests pursued by the data controller".

References:

Data Protection Commission. (2020) Case Studies. Available from:

https://www.dataprotection.ie/en/pre-gdpr/case-studies#201704 [Accessed 16 October 2021]

Data Protection Act 1998, c. 29. United Kingdom. Available from: https://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed 16 October 2021]

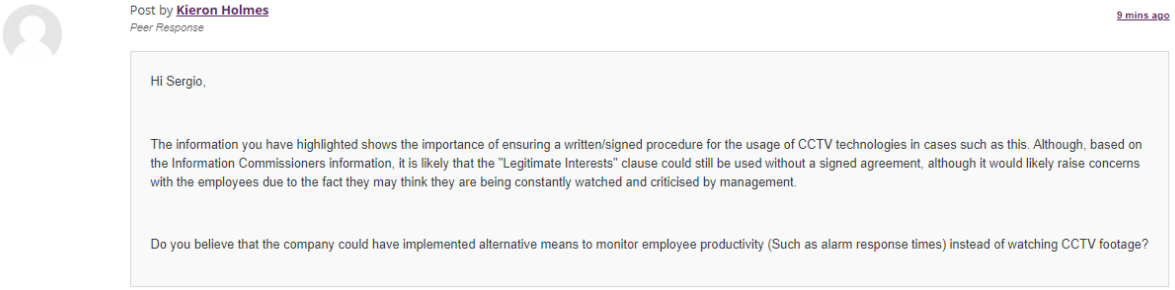
Post:

Hi Sergio,

The information you have highlighted shows the importance of ensuring a written/signed procedure for the usage of CCTV technologies in cases such as this. Although, based on the Information Commissioners information, it is likely that the "Legitimate Interests" clause could still be used without a signed agreement, although it would likely raise concerns with the employees due to the fact they may think they are being constantly watched and criticised by management.

Do you believe that the company could have implemented alternative means to monitor employee productivity (Such as alarm response times) instead of watching CCTV footage?

Screenshot:


Post by Kieron Holmes
Peer Response
9 mins ago
Hi Sergio,
The information you have highlighted shows the importance of ensuring a written/signed procedure for the usage of CCTV technologies in cases such as this. Although, based on the Information Commissioners information, it is likely that the "Legitimate Interests" clause could still be used without a signed agreement, although it would likely raise concerns with the employees due to the fact they may think they are being constantly watched and criticised by management.
Do you believe that the company could have implemented alternative means to monitor employee productivity (Such as alarm response times) instead of watching CCTV footage?