Unit 8

GDPR Case Study: Disclosure of Personal Data via Social Media Apps

This case study (Data Protection Commission, ND) addressed disclosure of personal data via the Snapchat instant messenger application. In this case study, copies of two job applicants' cover letters were photographed by a retailer's employee, who handled CV submissions, and posted to Snapchat, highlighting the similarities between both cover letters. Investigators found that the employee was aware that their action was contrary to their contract of employment and the retailer's policy.

The case study highlights the principle that data controllers are responsible for their employees' actions regarding the processing of personal data, whereby they act as data controllers. Whether or not their employees' actions are deliberate or accidental, Section 2A (1) of the Data Protection Act (DPA) of 2003 requires data processing to remain compatible with the purposes for which the data is provided. Such a requirement for data controllers applies regardless of their employee's first or last day of employment.

The case study does not state whether the photographs were removed after the investigation, but the retailer did terminate the employee's contract. Considering the GDPR-related investigation, I would highly recommend the retailer remove the Snapchat photographs as soon as possible to reduce further personal damage to the two applicants and the public opinion of the retailer. However, Snap (2021) shows that Snapchat has updated its data privacy policies.

An information security manager is required to take several steps to ensure data controllers adhere to GDPR policy regarding data processing. One step is to initiate a Privacy Impact Assessment (PIA) that helps to highlight issues that could occur from the collection and use of personal information and consider all measures required to mitigate or eliminate adverse data breach impacts. Conducting PIA aids organisations to support individuals' right to know what personal data will be collected about them and how their data is used. Mallory (2019) states that awareness of notification requirements laid out in Article 33 of the GDPR requires data processors to notify data controllers of data breaches or security incidents as soon as possible, often within 72 hours. Also, data collection security processes and policies need to be updated to meet compliance with GDPR. Additionally, O'Brien (2016) refers to the use of

security frameworks such as ISO/IEC27001:2013 to deliver continual improvements to information security.

References

Data Protection Commission (ND). Pre-GDPR Case Studies. Available from: https://dataprotection.ie/en/pre-gdpr/case-studies [Accessed 24 Jan. 2021].

Mallory, P. (2019). How has the GDPR changed the role of a security manager? Available from https://resources.infosecinstitute.com/topic/security-manager-roles-and-gdpr/ [Accessed 24 Jan. 2021]

O'Brien, R. (2016). Privacy and security: The new European data protection regulation and it's data breach notification requirements. *Business Information Review*, *33*(2):81-84.

Snap (2021). Snap and the GDPR. Available from https://businesshelp.snapchat.com/s/article/gdpr?language=en_US [Access 24 Jan. 2021]