Summary Post

With reference to the initial post and the peers' feedback, Information Security Manager (ISM) and Data Protection Officer (DPO) play a critical role in this case study for complying with the GDPR.

Besides of straighten their confidentiality, avoiding employees using personal devices, data protection policies for pursuing available remedies and. There are alternative mechanisms that could be considered such as data encoded as part of security precautions (Beran, 2022).

The organization should identify the sensitive data that requires to protect and separate them. In the human resources department, the resumes, background checks, paycheck records could be stored in a different location. Grant access to employees with the least privilege principle (CISA, 2013) and the Need-to-know security principle (Andreas, 2021) to limit the information accessing with confidentiality to their employees. Moreover, the data could apply granular encryption broadly to ensure sensitive data security even though it has been accessed by an improper person. In this scenario, the interviewer might not require having access to the interviewees’ photo, full name, and full home address. Personal information could be encrypted or partially masked which could mitigate the inappropriate behaviour from employees or even former employees mentioned in the case who causing data disclosure potentially (Data Protection Commission, 2020).

Indeed, Article 37(1) of GDPR requires the designation of a DPO where personal data processing is carried out by a public authority or body (Michael, 2022). Regarding the designation, GDPR does allow ISM to be DPO with “staff member of the controller or processor or fulfil the tasks on the basis of a service contract.” GDPR, Article 37(6) (EUR-Lex, 2016). However, the DPO function should be independent of all functions ideally, to avoid conflicts of interest with the staff members and be able to report to the executive independently. This retailer organization must nominate a DPO to instruct and advise the client and employees about their obligations under the GDPR regulation. The ISM of this retailer organization should governance the procedure and process to ensure all the above initiatives run smoothly, as well as data loss and fraud prevention.

In conclusion, to comply with the GDPR and mitigate the issue, ISM and DPO both act to protect the customer data and the organization. Organization as data controllers must secure their data from employees or even former employees to avoid inappropriate behaviour which causes data breaches.

References:

Andreas, W. (Feb 03, 2021) The Need-to-know security principle. *Security*. Available from: https://techcommunity.microsoft.com/t5/azure-sql-blog/security-the-need-to-know-principle/ba-p/2112393 [Accessed 5 February 2022].

CISA. (May 10, 2013) Least Privilege. Principles. Available from: https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege [Accessed 5 February 2022].

Data Protection Commission. (2020) Case Study 10: Disclosure of Personal Data via a Social Media App. *Pre-GDPR*. Available from: https://www.dataprotection.ie/en/pre-gdpr/case-studies#201710 [Accessed 5 February 2022].

EUR-Lex. (April 27, 2016) Regulations. *Official Journal of the European Union*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Accessed 5 February 2022].