Unit 8 Collaborative Discussion Summary

Summary

Considering the specific GDPR case study undertaken in unit 8 (publishing job application cover letters to Snapchat) raised the point that employers are held liable for their employees' actions, mainly when the organisation handles data of non-employed individuals. While not favourable for those affected, the outcome digs deep into the notion of consent.

Consent is a theme identified by several students during the discussion about their GDPR case studies. Politou et al. (2018) state that informed consent is given based on "clear appreciation and understanding of the facts, implications and consequences of an action". This is an excellent definition of informed consent considering GDPR. Especially cases involving spam marketing and mail or CCTV recordings where "informed consent" might not be as evident as a signed document. For this reason, the GDPR study by Shan (2021) was interesting because it involved video footage and visible signage. The GDPR case study raised the question of whether signage erected on properties is considered consent.

Another consideration of the difficulties faced by implementing and adhering to GDPR concerns the case study by Smirnov (2021). In it, he considered that nurses have greater faith in physical paper records versus electronic ones due to the untrusted nature of electronic documents. Smirnov (2021) further pointed out that such mistrust is not unfounded, given that most health record breaches occur via electronic means. The difficulty in this scenario is related to the management of people and how easily processes can slip and the right data end up in the wrong hands (or in this study, address). The difficulty relates to a relevant question posted by Wong (2021) that questioned the likelihood of ensuring employee compliance. Such compliance must involve, I believe, the information security manager who is tasked with ensuring GDPR compliant information systems.

Lastly, a fellow student raised a thought-provoking question during the last module's seminar, namely, why data has become valuable in today's world (Swanlow, 2022). From this perspective, one cannot help but consider that, if data were not valuable (together with complete lack of consent), perhaps privacy regulations such as GDPR would not be required? However, since data is part of our modern lives, society can be thankful for GDPR that helps establish boundaries on how much access organisations are permitted to keep about individuals while attempting to balance the right of those individuals to privacy.

References

Keshta, I. & Odeh, A. (2021) Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal 22(2): 177-183.

Politou, E., Alepis, E. & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of cybersecurity, 4(1).

Smirnov, A. (2021). Collaborative Learning Discussion 3. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=293499 [Accessed 09 Feb. 2021]

Swanlow, S. (2021). Collaborative Learning Discussion 3. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=292900 [Accessed 09 Feb. 2021]

Swanlow, S. (2022) Conversation with Seminar 5 group held 5th February 2022.

Wong, M. S. (2021). Collaborative Learning Discussion 3. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=293038 [Accessed 09 Feb. 2021]