Discussion Post 3: Summary and Reflection

This series of discussions focused largely on case studies where companies were found to be in violation of one or more of the broad range of regulations and policies observed under the General Data Protection Regulations (GDPR). The design of GDPR is intended to be a policy blanket, covering most industries, including health care, e-commerce and finance. It's therefore no surprise that topics were broad, ranging from unauthorized access to documents containing health data; as was the case with the Justice Department to marketing firms' unsolicited use of marketing emails being distributed without the ability to unsubscribe (Data protection Commission, nd).

What can be gained from case studies such as these is an appreciation of the breadth of these regulations and the complexities surrounding data protections and rights. A recurring theme seen throughout the case studies is intention (or lack thereof) as well as a general lack of preparedness. In the case of the Justice Department having a better paper trail on document access as well as role based access control (RBAC) could have helped to avoid penalty (Koot and SantAnna, 2018). This case study also shows that many companies are likely totally unaware they are in violation of one or more GDPR compliance rules. In the case of the justice department, it took three years for the violation to be discovered, and only after a colleague noticed they had unauthorized access to the file and notified the person who at that point was no longer with the department. GDPR regulation is also intended to give some measure of power back to the individual, focusing on user rights, such as the "right to erasure" of personal data. In the case of the justice department, the complainant measured her "right to lodge a complaint with a supervisory authority" under article 77 (General Data Protection Regulation (GDPR), n.d.).

In total the GDPR covers 99 separate articles that outline the rights and responsibilities of both users and data handlers. This is why it is in a company's best interest to either hire a compliance specialist to carry out routine audits and compliance checks or to outsource the task to a company with the legal and technical expertise to check and facilitate compliance across a business.

References:

Case Studies | Data Protection Commission. (n.d.). *Case Studies | Data Protection Commission*. Available at: https://www.dataprotection.ie/en/pre-gdpr/case-studies#201711 [Accessed 6 Jul. 2021]

General Data Protection Regulation (GDPR). (n.d.). *Art. 77 GDPR – Right to lodge a complaint with a supervisory authority*. Available at: https://gdpr-info.eu/art-77-gdpr/ [Accessed 7 Jul. 2021].

Koot, A. and SantAnna, V. (2018). *Effective GDPR and RBAC using role engineering*. Nixu Cybersecurity. Available at: https://www.nixu.com/blog/effective-gdpr-and-rbac-using-role-engineering-0 [Accessed 6 Jul. 2021].