Summary Post

Summary Post

by Md Aminur Rahman - Saturday, 30 September 2023, 4:12 PM

In the era of data-driven operations, data protection and adherence to regulatory frameworks like the EU's GDPR are of paramount importance. My initial post and subsequent discussions with peers shed light on evaluating our organization's IT Code of Conduct in this context. The discourse encompasses best practices, areas for improvement, professional responsibilities, and data incident handling, all while drawing insights from academic literature.

My initial post underscores the alignment of our IT Code of Conduct with best practices in data protection, particularly emphasizing the significance of Master Data Management (MDM) in maintaining data accuracy and consistency (Redman, 2013). The post also calls for enhancing ethical clarity, comprehensive data privacy compliance, and a dedicated focus on data security within the code.

Jeffery Ng's response acknowledges the importance of encryption in data security but highlights potential performance impacts. Jeffery introduces an alternative approach involving a reconciliation process with file and password encryption to safeguard sensitive data. This practice adds an additional layer of security and aligns with GDPR's principles, ensuring data minimization and protection (European Parliament, 2016).

Diana Kangave's response commends my understanding of data governance and GDPR's significance. Diana emphasizes the need for ethical clarity and references the ACM Code of Ethics as a guide for ethical data practices (ACM, 2018). Furthermore, the response highlights the importance of professional responsibilities, emphasizing prompt incident reporting, collaboration in remediation, and staying updated on data regulations and security best practices (Gurses et al., 2018).

Courtney Sommerville's inquiry seeks details on the organization's MDM procedures, error resolution processes, and incident management protocols. This highlights practical aspects of data governance and security and underscores the significance of role-based access and password protection for sensitive data.

In conclusion, the discussions collectively emphasize the need for our organizations to continually evolve our IT Code of Conduct to address ethical considerations, data privacy compliance, and data security comprehensively. The role of computing professionals in upholding these principles and actively participating in incident management and data protection is critical.

Md Aminur Rahman

References:

1. Redman, T. C. (2013). Data Driven: Profiting from Your Most Important Business Asset. Harvard Business Press.

2. European Parliament (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union.

3. ACM (2018). ACM Code of Ethics and Professional Conduct. [Online] Available at: https://www.acm.org/code-of-ethics (Accessed 15 September 2023).

4. Gurses, S., Tuncay, B., & Vanden Bussche, J. (2018). "What Makes Data Privacy Hard? A Science of Privacy for a Data-Driven World." ACM Computing Surveys, 51(3), 1-38.

Turnitin ID: 2181421026

Maximum rating: -

Permalink Reply

◄ Summary Post

Initial Post ►