GDPR strives to empower individuals to provide control over their data. It establishes a set of rules for organizations to ensure the effective protection of consumer rights and proper management of data. Numerous organizations have implemented privacy management automation to comply with GDPR requirements. This involves establishing a centralized consent system across all platforms, tailored to customer preferences. The implementation of Master Data Management (MDM) serves as a technical solution to ensure compliance with GDPR requirements by introducing essential modifications to processes and controls. Nevertheless, various challenges are encountered during the implementation related to conflicts in data or maintaining consistency (Haselden & Wolter, 2006).

While there exist best practices and controls for safeguarding data, there are still areas that can be improved. In recent cyber-threats, it has become apparent that many organizations need to carefully assess access and data-sharing practices. Enhancing contracts with agencies (Cobb, 2021), improving file sharing across systems, and implementing necessary access controls in all areas involving data transmission, along with ensuring proper data location, are critical areas for improvement. Administering and maintaining Kavya, 2021) access controls for data extraction, as well as ensuring control over data usage, is crucial.

I am currently employed as a developer in Siebel's Insurance Technology department. Siebel's operates as a Tech Vendor for their clients. I work for their clients as an IT engineer. During the MOVEit data breach in May 2023, one of our significant clients suffered an impact (Hayes, 2023). The stolen data comprises personally identifiable information (PII) such as names, dates of birth, phone numbers, etc. While the impact is substantial, the client has initiated the case filing process and maintained transparency with their customers. They have also advised the affected customers to remain vigilant and monitor their credit reports. We helped the client identify the issues with data transfer and remediated them by implementing complex encryptions with no access to the encryption key (Kavya, 2021), I have been part of this remediation team.

Classifying and linking data to particular user profiles, along with automating data subject access requests, could potentially heighten the risk of hacker attacks (Schrader, 2022). Complying with GDPR necessitates the careful management and protection of the movement of personal data. GDPR compliance efforts primarily contribute to enhancing the security of the IT infrastructure. This includes reviewing contracts with third parties and assessing their infrastructure to prevent issues related to data transfer. Implementing AI can serve as a differentiator, utilizing ML techniques to enhance the decision-making process for access controls by rendering decisions more comprehensible. Organizations should invest in assessing the risk within their data inventory using industry-standard PIA templates that align with privacy regulations. Relying solely on MDM as a technical solution may not address all issues; it might necessitate modifications to the business processes (Haselden & Wolter, 2006). Building trust with customers requires demonstrating that the organization prioritizes securing its infrastructure to address GDPR requirements, and places a high emphasis on data privacy and security.

References

Cobb, M. (2021) *7 best practices to ensure GDPR compliance: TechTarget*, *Security*. [online] Available at: https://www.techtarget.com/searchsecurity/tip/7-best-practices-to-ensure-GDPR-compliance

Haselden, K. and Wolter, R. (2023) *What is Master Data Management: Definition, tools, solutions*, *Enterprise Master Data Management, Profisee*. [online] Available at: https://profisee.com/master-data-management-what-why-how-who/

Hayes, M. (2023). *What You Need to Know About the MOVEit Data Breach - Experian*. [online] www.experian.com. Available at: https://www.experian.com/blogs/ask-experian/moveit-data-breach/.

Kavya (2021). *GDPR in the US: A Checklist for Compliance*. [online]. Available at: https://www.cookieyes.com/blog/gdpr-in-the-us-a-checklist-for-compliance/#:~:text=in%20the%20US.-

Schrader, D. (2022) *File integrity monitoring for PCI DSS compliance*, *Netwrix Blog*. [online] Available at: https://blog.netwrix.com/2022/03/17/pci-compliance-file-integrity-monitoring/