Collaborative Discussion 2

Initial post

The introduction of the General Data Protection Regulation (GDPR) in 2018 has imposed a greater demand on companies to address the rights of subjects who provide personal data (Breen et al., 2020). In 2019, tech giants Google were fined €50 million for a violation of GDPR obligations. The fine was issued after Google failed to provide customers with enough information about the data consent policies they have in place to be able to gain consent from the users (European Commission, 2019). Under the unambiguous indication of wishes characteristic of consent in the GDPR, the data subject is required to understand what their consent is for, what implications there could be and what the risks are of having their data processed (Breen et al., 2020).

The Ministry of Defence (MOD) privacy notice (2019) covers all aspects of data protection within the MOD. As a department of the government the MOD must ensure that the interests of the public comes first. For sensitive data the MOD will not collect, process or store this information without the necessary justification (Ministry of Defence, 2019). To ensure that all employees have the required knowledge and skills annual mandatory training is conducted with a graded test at the end and certification which has to be submitted as proof of completion.

An area that can be improved within the MOD relates to having multiple systems and networks that are unable to easily pass data between them. This violates the process of master data management (MDM) as data has to be stored on different networks which can easily cause there to be multiple versions of the same data which means any change in the data will cause multiple versions of the truth. To eliminate this the MOD could create a centralised system that connects to the different networks allowing for data to be passed between them efficiently while maintaining a single version of the truth as described in Martins et al. (2022).

References

Breen, S., Ouazzane, K. and Patel, P. (2020) “GDPR: Is your consent valid?,” *Business Information Review*, 37(1), pp. 19–24. Available at: https://doi.org/10.1177/0266382120903254.

European Commission (2019) *Communication from the Commission to the European Parliament and the Council. Data protection rules as a trust-enabler in the EU and beyond – taking stock* , *eur-lex.europa.eu*. Available at: https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html (Accessed: October 27, 2022).

Martins, J., Mamede, H. and Correia, J., 2022. Risk compliance and master data management in banking – A novel BCBS 239 compliance action-plan proposal. *Heliyon*, 8(6), p.e09627.

Ministry of Defence (2019) *Mod privacy notice*, *GOV.UK*. Available at: https://www.gov.uk/government/publications/ministry-of-defence-privacy-notice/mod-privacy-notice#data-protection-principles (Accessed: October 27, 2022).

Peer response Victoria Stapleton

Thank you for your very insightful post. Upon reading about your organisation's technical issues with the consent prompt I did some further research into how consent is gained.

Since the GDPR went into effect there has been a significant rise in the number of websites that contain consent requests upon entering the page, which has led to a significant improvement in the transparency of websites on how they use data (Degeling et al., 2019). However there is still great variation in the format of the consent prompts in terms of the user interface and the underlying functionality (Utz et al., 2019). Degeling et al. (2019) found that one of the main variations was the choice options that were presented to the users ranging from there being no option (in which the user continuing to use the website acts as consent) to category based notices (multiple options that can be accepted or rejected independently) and around 10% of websites block the user from having any access to the site until consent is given.

The style, choice of words and placement of consent prompts have a significant effect on how likely a user is to accept or even interact with the prompt (Utz et al., 2019). With this in mind do you believe that there should be a fixed template for the style and functionality of consent prompts?

Degeling, M. *et al.* (2019) “We value your privacy ... now take some cookies,” *Informatik Spektrum*, 42(5), pp. 345–346. Available at: https://doi.org/10.1007/s00287-019-01201-1.

Utz, C. *et al.* (2019) “(un)informed consent,” *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* [Preprint]. Available at: https://doi.org/10.1145/3319535.3354212.

Peer response Hamid Abdul

Thank you for your very insightful post.

You mentioned that the GDPR is standardising the data protection environment across the EU. However, the way that consent is gathered especially from web based sources still seem to vary in both the interface and underlying functionality and have a significant effect on how people respond (Utz et al., 2019). Research from Utz et al. (2019) showed that interaction and the

input of the user were affected by the placement and the options available to the user with consent banners being placed at top of the screen being the least likely to be interacted with. Combining this with the fact that a significant number of websites state that the user continuing to use the website acts as consent to use data, do you think that the GDPR should impose stricter guidelines to ensure that companies can not design consent prompts in ways to alter the users interaction?

Many employees are required to take part in mandatory training to ensure that they remain GDPR compliant. However, these employees may not have much interest in the training and therefore lack the required engagement and motivation to effectively learn the material. Phan & Phan (2020) found that serious games in the form of training scenarios had a positive effect on the engagement of employees. Do you think this type of training could help to increase awareness of GDPR policy?

Phan, Q. and Phan, T. (2020) “GDPR Staff Training in IT companies: A Game-Based Approach,” *NTNU* [Preprint].

Utz, C. *et al.* (2019) “(un)informed consent,” *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* [Preprint]. Available at: https://doi.org/10.1145/3319535.3354212.

Peer response Ruth Allison

Thank you for your very insightful post.

A survey in Poland was conducted which asked employees if their office fully complied with GDPR regulations to which 18% responded no with a significant number of employees refusing to respond (Lisiak-Felicka et al., 2021). The survey later asked what the most important elements were for implementing GDPR. The main responses were employee training and engagement (Lisiak-Felicka et al., 2021).

Many employers require their employees to take part in mandatory training to ensure that everybody at the company remains GDPR compliant. However, these employees may not have much interest in the training and therefore lack the required engagement and motivation to effectively learn the material, especially if data is not the main focus of their role (Phan & Phan, 2020). Phan & Phan (2020) found that serious games in the form of training scenarios had a positive effect on the engagement of employees. Do you think this type of training could help to increase awareness of GDPR policy? If not, what other methods could be used?

Lisiak-Felicka, D. and Szmit, M. (2021) “GDPR implementation in public administration in Poland – 1.5 year after: An empirical analysis,” *Journal of Economics and Management*, 43, pp. 1–21. Available at: https://doi.org/10.22367/jem.2021.43.01.

Phan, Q. and Phan, T. (2020) “GDPR Staff Training in IT companies: A Game-Based Approach,” *NTNU* [Preprint].

Summary Post

After discussing the MODs IT code of conduct with my peers I have been opened to new avenues of thought.

An area that can be improved within the MOD relates to having multiple systems and networks that are unable to easily pass data between them. This means that data has to be stored on different networks which can easily cause there to be multiple versions of the same data which means any change in the data will cause multiple versions of the truth, violating the process of master data management (MDM). To eliminate this the MOD could create a centralised system that connects to the different networks allowing for data to be passed between them efficiently while maintaining a single version of the truth as described in Martins et al. (2022).

In contrast to implementing a centralised system, my peers suggested the implementation of a data mesh. A data mesh supports the provision of complex data management and access allowing data from different locations to be connected, creating a decentralised data architecture that enables the extraction of large scale data (Machado et al., 2022). Implementing a data mesh will allow the different departments of the MOD to store and process their own data while a common platform allows homogeneous interactions with the data (Priebe et al., 2021). A limitation of data mesh is that it is crucial that each team is required to maintain data governance to extremely high levels, which can be time consuming (Ryan, 2022).

The centralised and decentralised (data mesh) approaches have their own benefits and limitations. Centralisation does not account for different sections of the MOD having separate interests and needs for data which suggests the decentralised approach could have the greatest benefits. However, at the expense of requiring more IT resources and potential connectivity issues (Haug et al.,2022).

Haug, A., Staskiewicz, A. M. & Hvam, L. (2022) Strategies for master data management: A case study of an international hearing healthcare company. *Information Systems Frontiers*, Available from: **https://doi.org/10.1007/s10796-022-10323-z**

Machado, I.A., Costa, C. and Santos, M.Y. (2022) “Data Mesh: Concepts and principles of a paradigm shift in data architectures,” *Procedia Computer Science*, 196, pp. 263–271. Available at: https://doi.org/10.1016/j.procs.2021.12.013.

Martins, J., Mamede, H. and Correia, J., 2022. Risk compliance and master data management in banking – A novel BCBS 239 compliance action-plan proposal. *Heliyon*, 8(6), p.e09627.

Ministry of Defence (2019) *Mod privacy notice*, *GOV.UK*. Available at: https://www.gov.uk/government/publications/ministry-of-defence-privacy-notice/mod-privacy-notice#data-protection-principles (Accessed: October 27, 2022).

Priebe, T., Neumaier, S. and Markus, S. (2021) “Finding your way through the jungle of Big Data Architectures,” *2021 IEEE International Conference on Big Data (Big Data)* [Preprint]. Available at: https://doi.org/10.1109/bigdata52589.2021.9671862.

Ryan, M. (2022) *5 operational challenges in adopting data mesh architecture*, *Amdocs*. Available at: https://www.amdocs.com/insights/blog/5-operational-challenges-adopting-data-mesh-architecture (Accessed: November 10, 2022).