Collaborative Discussion 1

Summary

Over the course of the last three units in this module, we looked at the various roles and responsibilities of IT professionals, computer architecture and emerging trends within the industry. These three units of discussion integrate with the discussion around GDPR and data privacy in today's world.

Computer science professionals possess skills that are not purely theoretical but also very much practical. They have a deep understanding of algorithms and how these are used with data to derive new insights and solutions to industry problems. However, with data processing comes additional threats to the data; data must be protected at all times. There are ethical, moral and possible legal implications for the misappropriation (whether intentionally or otherwise) of sensitive or confidential data. IT professionals have a responsibility to ensure such data breaches do not occur within their organisation, and such responsibilities are codified in a Code of Conduct policy.

The European Union's introduction of GDPR regulations in 2018 (EU_1, 2021) set a new world-standard as being the toughest collection of privacy laws in the world. This new Code of Conduct, so to speak, brings greater responsibility for IT professionals to consider each and every piece of user data they wish to process or manipulate in their chosen IT systems. No longer can organisations simply gather data freely and pay no heed to their *intended use* of the data. GDPR places heavy fines on organisations who fail to respect the fundamental rights of European citizens' right to privacy, with regulation supporting fines of up to ten million Euros or two percent of an organisation's revenue (EU_2, 2021). These are no small figures for organisations who wish to perform business in the EU.

Therefore, given the financial implications involved, IT professionals, driven by a sound Code of Conduct, ought to harness opportunities in their day-to-day tasks to watch for potential data breaches, regularly review data processing processes and assess the impact of providing third-party vendors with their organisation's data. Also, if data must be tested within IT systems, (as is good practice before production releases) Blair et al. (2019) recommend the data be (pseudo)anonymised in order to remain within the GDPR regulations.

Considering the impact of GDPR, discussions revealed there is a heavy financial and training cost involved to ensure compliance. Most organisations lack knowledge of what is required

or even how to implement GDPR policies. For this point, reference was made to ISO standard 27701 (Std_Iso, 2021) and BS 10012 2017 + A1 2018 (Std_BS, 2018). These standards serve are starting points for organisations to consider implementing data privacy. Due to the financial cost of GDPR policies, it was discussed that smaller companies very likely would implement the bare minimum to not risk fines (Holmes, 2021). However, the idea that training is essential was a key theme that can easily be deduced from the discussions: organisations must rise to the challenge of data privacy and enable better compliance through regular training of their staff. Improved compliance is achieved through greater awareness of an organisation's data privacy policies both internally and externally.

Users are realising the value of their data, and in the years ahead, they will demand greater responsibility for their data from Big Tech companies. As more and more businesses look to leverage new opportunities to profit from data, the concept of Big Data has become a major concern for existing regulations as well as users. Big Tech have the money and motivation to mine more data at an ever increasing pace while still trying to maintain a balance between their own needs and the need to respect their data privacy. The current implementation of GDPR may soon find difficulties among organisations as they move their operations over to Cloud Computing; users are not always aware of what they can or cannot do with the data they access. However, in due course, users too will gain the requisite knowledge concerning their right to data privacy, and as more organisations around the globe (EU_3, ND.) recognise the efforts of the EU's GDPR, data privacy may become an in-built quality of all systems consumed and produced.

References

Blair, T. & Campbell, P (2019) Anonymization and Pseudoanonymization under the GDPR. Available from https://www.morganlewis.com/pubs/2019/12/the-edata-guide-to-gdpr-anonymization-and-pseudonymization-under-the-gdpr [Accessed 14 February 2021]

EU_1, (2021) What is GDPR, the EU’s new data protection law? Available from https://gdpr.eu/what-is-gdpr/ [Accessed 14 February 2021]

EU_2, (2021) What are the GDPR fines? Available from https://gdpr.eu/fines/ [Accessed 14 February 2021]

EU_3, (ND.) Adequacy Decisions. Available from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [Accessed 02 February 2021]

Holmes, K. (2021) Initial Post (Posts 3-4) Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=239705#p861613 [Accessed on 14 February 2021]

Std_BS, (2018) BS 10012 2017 + A1 2018 Standard. Available from https://www.itgovernance.co.uk/shop/product/bs-10012-2017-a1-2018-standard [Accessed on 02 February 2021]

Std_Iso, (2021) The international standard for privacy information management. Available from https://www.itgovernance.co.uk/iso-27701 [Access on 02 February 2021]