1-3 Discussion Forum

This discussion lasts three weeks, covering units 1, 2 and 3. This activity forms a component of the e-portfolio.

Discussion topic:

Download and read the **Communication: Data protection rules as a trust-enabler in the EU and beyond – taking stock (COM/2019/374)** and GDPR Regulation at **Regulation (EU) 2016/679**, and review an organisation's IT Code of Conduct and reflect on:

- Best practices.
- Areas that can be improved.
- Incidents and the role of a computing professional.
- What could have been done to improve the situation.

Demonstrate an understanding of the topic covered and critically appraise the emerging trends in the field, such as cloud computing, big data, cybersecurity, and the professional and ethical requirements for dealing with such contemporary computer-based technologies.

My reflection on the topic:

Since people worldwide increasingly value their privacy and data security, there is an international need to protect personal data. - By 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 (2019).

The General Data Protection Regulation (GDPR) is a set of laws governing data protection, personal information transfers, and privacy. Voss, W.G. & Houser, K.A.

(2019). The good news is that GDPR laws are simple to execute in business activities, despite how opaque they may appear on paper.

Incorporating GDPR practices puts businesses on the right side of the law whether you are in the European Union or another country; GDPR is about putting consumers' privacy first.

Best Practices:

The GDPR must be implemented with 'A privacy policy' that must include several crucial clauses because it is a legal document. Companies must create data policies that allow for some, but not excessive, freedom. Under laws like the GDPR, privacy rules must be expressed clearly, and intelligibly. An effective privacy policy will include a list of the many sorts of data the business gathers and the methods used to do so, such as:

- A list of the many kinds of data the company gathers and the methods it employs.
- The reason why the company is collecting the information. How is the data used to sell your products? Is it used to improve the customer experience? Is the purpose primarily to determine your target market?
- All the things the company plans to do with customer data, both positive and negative.
- Customers must be allowed to refuse to have their data sold and to have any information companies have collected about them erased. It would be best to outline how customers can do that in your privacy policy.

Areas that can be Improved:

To make a company's operations compliant, companies must complete GDPR training. However, GDPR training cannot simply be a "one-and-done" activity if it is to be truly effective. It must be continually updated and integrated into your onboarding procedure.

In my role as a computing professional, I must:

- Reactivate my ability to spot and track threats.
- Collect information about devices, sensitive information, and credentials that may be affected.
- Get timely information about threats and take appropriate action.
- Find resources that have malware on them and have got beyond endpoint security measures.
- Identify data exfiltration attempts and newly compromised user or system credentials.
- Test incident response plans regularly to ensure that the systems, procedures, and methods for detecting and resolving attacks and other emergencies are in place and working correctly. Show clients, partners, and regulators that the enterprise's security posture is strong enough to secure the personal data it retains or accesses and implement rigorous security measures.
- Keep track of risk factors, gaps, scheduled remediation, residual risk, and planned security and privacy controls.

What could have been done to improve the situation?

To maintain security and prevent processing in violation of the GDPR, the controller or processor should assess the risks inherent in the processing and implement risk-mitigation measures, such as encryption.

These measures should provide an appropriate level of security, including confidentiality, while considering state-of-the-art and implementation costs concerning the risks and nature of the personal data to be protected.

Consideration should be given to the risks posed by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed, which may result in physical, material, or non-material harm. - Team, I.G.P. (2020).

Reference:

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. (2019). [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0374&from=EN.

Voss, W.G. & Houser, K.A. (2019). Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal*, 56(2), pp.287–344. doi:10.1111/ablj.12139.

Team, I.G.P. (2020). *The fourth edition of EU General Data Protection Regulation (GDPR) – An implementation and compliance guide*. [online] *Google Books*. IT Governance Ltd. Available at: https://www.google.co.uk/books/edition/EU_General_Data_Protection_Regulation_GD/LicDEAAAQBAJ?hl=en&gbpv=1&dq=GDPR+improvements&pg=PA1&printsec=frontcover [Accessed 1 Feb. 2023].