Unit 5: e-Portfolio Activity – GDPR Case Studies

Read the website at Data Protection Commission (2020) Case Studies: Data Protection Commission.

There are several case studies from 2014 – 2018 concerning GDPR related issues and breaches. Chose a case study (should be unique to each student) and answer the following questions:

- What is the specific aspect of GDPR that your case study addresses?
- How was it resolved?
- If this was your organisation what steps would you take as an Information Security Manager to mitigate the issue?

You can discuss your findings as a team and come prepared to share them in next week's seminar. Remember to also save to your e-portfolio.

---

16) October 2016 – Crypto Ransomware Attack on a Primary School

The following weakenesses were found which allowed the ransom attack to occur:

- No policies to maintain system backups
- No policies or procedures for system attacks like ransomware
- No contracts with data processors/ICT service providers
- Lack of staff training

GDPR Article 25 (EEU, 2018) appears to address this case:

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

The ransomeware case was resolved by implementing the following:

- Implementing a staff training and awareness program on email and personal USB key risks
- Implementation of contract review process with ICT suppliers
- Ensure any ICT support is performed by competent data processors

Recital 78 of the GDPR (EEU, 2019) includes several implentations that may be prudent to implement as an Information security manager.

- Minimising the processing of personal data,
- Pseudonymising personal data as soon as possible,
- Transparency with regard to the functions and processing of personal data,
- Enabling the data subject to monitor the data processing,
- Enabling the controller to create and improve security features.

Resources

EEU (2018) *Art. 25 GDPR – Data Protection by design and by default*, *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/art-25-gdpr/ (Accessed: December 7, 2022).

EEU (2019) *Recital 78 - appropriate technical and organisational measures*, *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/recitals/no-78/ (Accessed: December 7, 2022).