

## Unit 8 – Summary

During Unit 8 we were reviewing Data Protection issues and breaches prior to the EU GDPR. My case study was regarding a Toll company and an agency employee. According to the individual (the complainant), the Toll company disclosed his personal data to his employer (in the form of an audio recording and CCTV footage) without his knowledge or consent (Data Protection Commission, n.d).

According to the Toll company, during their initial dispute, the individual threatened to take down all the toll plaza systems. This led to the Toll company requesting the termination of the individual's services as a service engineer at the Toll company's premises. After the employer agreed, the Toll company considered the matter to be concluded (Data Protection Commission, n.d). However, two months after the incident had occurred, the individual's employer requested from the Toll company the CCTV and audio footage, which the Toll company eventually did provide.

The commissioner assessed that this act did not comply with the Data Protection law because:

- 1) There was no legal ground for the processing of personal data,
- 2) There was not enough notice of the data collected (the company did not disclose the recording of audio),
- 3) There was no purpose to further process personal data as the matter was considered the matter to be concluded.

Following a review of my fellow students' case studies, it is clear that even while the GDPR provides clear guidance on how personal data should be handled, many companies still struggle to comply. Nevertheless, the EU GDP Regulation has raised awareness of the users' data, hopefully leading to fewer data leaks.

While the EU GDPR is one of the most comprehensive Data Privacy regulation, it is not compatible with novel technologies such as AI research, Big Data, IoT (i.e., insurance variable cost), etc. leading to compliance problems for innovative companies. In the future, a revision of the GDPR should be drafted to take into consideration these novel and emerging technologies.

## References:

Data Protection Commission (n.d.) Case studies. Available from: <https://dataprotection.ie/en/pre-gdpr/case-studies> [Accessed 29 June 2021]

EUR-Lex (n.d.) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available from: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 29 June 2021]

## Tutor Feedback:

Had I been requested to mitigate this situation by enforcing different and/or new practices in the organization, I would have proposed the following:

Hi Antonios,

These are excellent propositions. I just would add leaking CCTV data due to a backdoor hacking activity by employees is a greater threat than the regular potential danger of cybersecurity. I would think penalties and legislation need to be reinforced for non-compliance in addition to redrafting the usage policy guideline.

Regards,

Nawaz