GDPR: Use case study

UC is a large European company with a strategic role in its country. Direct references to UC have been redacted and anonymized.

UC does not have a single public document for the IT Code of Conduct concerning privacy. The foundations are laid by the current national and European legislation. The two fundamental documents are the collective agreement and the code of conduct. Further internal documentation defines additional rules and procedures. This documentation is not publicly available and it is relevant only for those who are in a position to handle personal data such as IT staff and HR.

The company has a Data Protection Officer and incidents must be reported to the ICT Service Desk that reports to National Data Protection Authority as defined in the Union Agreement and in the Employee’s contract. This is aligned with GDPR Regulation (European Parliament and Council, 2016: 33).

Specific rules are defined to monitor employees' electronic activity. Email and network can be used for limited personal use. Email may be accessed by the company only for proportionated business reasons. Network and Internet usage, and email exchanges are monitored for security threats and misuse. All collected personal data is immediately destroyed unless it requires further investigations. According to European regulations, this monitoring is possible, but it is important to take measures that are proportionated to the goal and transparently explained in policies. All these considerations should be taken via a DPIA (Working Party, 2017:

12-15). In UC it is always required to assess privacy and cybersecurity risks and to produce relevant documentation. For example, for any application containing personal data, it is required to document how the risk of data leaks is mitigated, who has access to the data and for which reason.

In UC, a strict policy is in place to segment the data based on confidentiality and, given the strategic role in the country, there is a strict limitation in where the data can be physically stored. This internal regulation is more strict than GDPR (European Parliament and Council, 2016: 41-48). For example, cloud providers outside the country are normally forbidden and on-premise solutions are always preferred.

Being a company under frequent scrutiny, all required norms are carefully respected.

It is my opinion that the only area of improvement can be found in how the monitoring of network and email is described. “An employer must have a transparent system of monitoring, of which all of the employees are fully aware”, such a system must be as less intrusive as possible, and the right to privacy must be recognized also at work (Keane, 2018). The description of the monitoring does not give sufficient details to understand in which cases monitoring ceases to be anonymized and it does not describe the tools in use to determine the kind of surveillance in place. Partial or complete understanding is the exclusive possibility of only part of the staff depending on their technical competence and position in the organization.

References

Consolidated text: 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 (General Data Protection Regulation) (2016). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN [Accessed on 14 August 2021]

Keane, E. (2018). The GDPR and Employee's Privacy: Much Ado but Nothing New. *King's Law Journal* 29(3): 354-363 Available from: https://www.tandfonline.com/doi/pdf/10.1080/09615768.2018.1555065 [Accessed on 14 August 2021]

Working Party. (2017) *Opinion 2/2017 on data processing at work – wp249.* Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=45631 [Accessed on 14 August 2021]