Julius Cloos
Security and Risk Management
Tutor: Dr. Siddiqui

GDPR Case Study

In the case study on eir, Data Protection Commission (N.D.) describes a case where a complainant wasn't given all the information on which personal data was stored by eir on the complainant and wasn't given useful information about the stored data. During the investigation, it turned out that eir wanted to hold back information on which data it had stored about the complainant by relying on legal exemptions. Furthermore, it was uncovered that eir didn't know what data was stored on the user.

This case study addresses the right of access by the data subject (Article 15 GDPR) which states that a user has the right to know what data is stored on them, how it is processed and obtain a copy of the stored data (Intersoft Consulting, N.D.).

Eventually, the complainant withdrew the complaint (Data Protection Commission, N.D.). Therefore, this specific case had no real consequences for eir.

Given that right to access stored information on a user is a right of users according to the GDPR, an Information Security Manager would have to take multiple steps to prevent violations like this from causing the company large fines:

- Employee sensitizing: The Information Security Manager would need to make sure employees (and management) know about the rights of the users and responsibilities of the company according to GDPR (Aigner Business Solutions, 2020).
- Implementing a new system: Given the investigation by Data Protection Commission (N.D.) brought to light that the company doesn't even know what personal data is stored on different data subjects, it's necessary to implement a new system to ensure the company knows about which data they are storing and processing in the future. This would involve better documentation processes and developing efficient procedures to gather all data stored on a data subject to be sent to this person when they request it (Data Protection Commission, N.D.).
- Auditing: The ISM's job would also be to make sure that employees and management continue to adhere to the user's right to access information stored on them and to make sure that old habits (such as lack of documentation) don't return after the new system that allows users to access data stored on them has been implemented.

References

Aigner Business Solutions (2020) Tasks of the information security officer (ISO). Available from: https://aigner-business-solutions.com/en/blog/tasks-of-the-information-security-officer-iso/ [Accessed 02 August 2024].

Data Protection Commission (N.D.) Case Studies. Available from: https://dataprotection.ie/en/pre-gdpr/case-studies [Accessed 02 August 2024].

Intersoft Consulting (N.D.) Right of access by the data subject. Available from: https://gdpr-info.eu/art-15-gdpr/ [Accessed 02 August 2024].

Winheller (2024) German Data Protection Officer: Tasks, Rights and Duties. Available from: https://www.winheller.com/en/business-law/privacy-law/data-protection-officer.html [Accessed 02 August 2024].