GDPR Violation Case Study: H&M Service Center in Germany

Livia Zhu, *Brown University*

Abstract

In October 2019, a configuration error exposed gigabytes of voice recordings and corresponding notes stretching back to 2014 containing personal information about the private lives of several hundred employees of an H&M Service Center in Nuremberg, Germany. These recordings and notes had been used in employee evaluations along with their work performance. On October 1st, 2020, the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) issued a €35 million fine against the company, citing GDPR Articles 5 and 6, and stating that this constituted unlawful data processing and was a severe violation of the civil rights of the employees. This hefty fine was imposed in the hopes of deterring future violations of employee privacy. In response, H&M took corporate responsibility, apologizing and paying compensation to the affected employees, appointing new management, and improving the storage of personal data, among other changes.

1. Background

H&M Hennes & Mauritz Online Shop A.B. & Co. KG is a fast-fashion chain founded in 1947 and currently headquartered in Stockholm, Sweden. It currently operates worldwide in 53 online markets and a total of 4,913 stores, with a revenue of €3 billion in Germany in the past year [1][2]. Hundreds of its employees worked in the Nuremberg Service Center, and the company retained information about them on their local network drives [3]. In this situation, H&M acted as both the *data controller* and the *data processor* of the employees' (the *data subjects*) data. As the service center is in Nuremberg, it was under the jurisdiction of the HmbBfDI.

Since at least 2014, management at the company collected voice recordings and detailed notes about many employees in the service center. These consisted of one-on-one conversations between employees and team leaders at meetings called Welcome Back Talks, which occurred after employee absences such as holidays and sick leaves. According to the press release by HmbBfDI after the fine was imposed, these conversations included sensitive health information and vacation experiences, and the related notes included detailed information about the private lives of employees such as family disputes and religious beliefs [3]. Up to 50 managers throughout the company had at least partial access to this information, and it was processed to create detailed profiles of the employees which were used in their work evaluations.

In 2019, the fact that this data was collected became public knowledge after a configuration error made the data accessible throughout the company. Through press reports resulting from this data breach, the HmbBfDI was alerted of this privacy violation and, after freezing the network drive, obtaining its 60GB contents, and further investigation, they imposed the €35 million fine against the company a year later [3].

2. GDPR Violations

According to the GDPR Enforcement Tracker, Articles 5 and 6, Principles relating to processing of personal data and Lawfulness of processing, were violated by H&M and the managers who collected and used the employee information [4]. This action was a gross violation of the principles of GDPR: the processing was not done transparently, data was not collected for a specific purpose, and the scope of data was unjustifiably broad. Furthermore, the processing of data had no legal basis as it did not fall under any of the categories listed in Article 6 of the GDPR [5].

The main privacy violation was not a result of a technical issue or data breach – rather, it was the result of a lack of compliance and misuse of technology by the managers within the company. However, the discovery of the violation, which in and of itself is another privacy concern, was in fact due to a data breach when a configuration error allowed employees throughout the company to view the collected data. The IT specialists at the service center were responsible for this secondary violation.

The principal violation could have been prevented by increased oversight over the data collected on employees, clearer guidelines on what data can be collected, retained, and utilized for employee evaluations, and increased training on privacy regulations and data protection. Technological solutions for this could include automated monitoring that reminds managers and employees what data they are allowed to process and detailed database specifications on what employee data can and cannot be stored. The secondary violation could have been avoided by more extensive testing and checks on the network configurations.

In response to the discovery of these violations, H&M released a press statement taking "full responsibility" for the violation. They made an "unreserved apology" and provided considerable financial compensation to those affected. Furthermore, the company took many additional steps to ensure data protection in the future, including:

- changes to management at the Service Center,
- additional trainings,
- creating a new role of data protection coordinator that audits and continuously improves data privacy,
- monthly data protection status updates,
- increased protection for whistleblowers,
- and improved data cleansing and other IT solutions to "support compliant storage" [3][6].

These changes were even commended by the HmbBfDI's press release as an "unprecedented acknowledgement of corporate responsibility", and the commissioner, Prof. Dr. Johannes Caspar, stated that their efforts "have to be seen expressly positively" [3].

3. Discussion

This case was scoped solely to the employees of H&M's Nuremberg Service Center, which consisted of several hundred employees, who were most likely German citizens, from the beginning of GDPR enforcement in May 2018 until the discovery of the data in October 2019. Despite this relatively small scope, as the amount of data they collected was so intrusive, H&M was fined €35 million, which at the time was the second-highest fine issued in Europe (it is, as of September 2021, the fourth highest fine) [4]. HmbBfDI's commissioner stated that the size of this fine was both proportional to the extent of the violation and useful as a deterrent for future company violations of employee data privacy, for both H&M and other corporations worldwide [3].

In this case, the GDPR enforcement process was effective, prompting extensive changes in how H&M handles employee data privacy within the company as outlined in Section 2. However, an interesting aspect of this case is that it was only discovered by chance, due to an unrelated data breach – despite the severity of the privacy violation, the practice of recording and retaining meticulous notes on the private lives of employees was allowed to continue for at least five years. This demonstrates an increased need for employee education on their data rights so that they can recognize violations, and improved whistleblower protections, so that they are able to make violations known. By educating and protecting employees, DPAs do not have to be reliant on chance occurrences like these to uncover cases.

Due to the COVID-19 pandemic, many companies began to collect a large amount of additional data on their employees to keep tabs on them during the work-from-home era – information that mirrors the data collected in this case, including health data and vacation information [7]. As a result, this case is becoming increasingly relevant and demonstrates to companies the severity of violating employee rights in this manner. Due to the recency of this case, it is hard to quantify whether it is effective as a deterrent. Ultimately, however, the case sets an important precedent emphasizing the importance of employee rights to data privacy.

References

[1] Market overview. *H&M Group.* 31 May 2021. https://hmgroup.com/about-us/markets-and-expansion/market-overview/,

[2] Revenues of H&M in Germany 2008-2020. *Statista.* 18 Feb 2021. https://www.statista.com/statistics/526859/handm-revenues-germany/

[3] 35.3 Million Euro Fine for Data Protection Violations in H&M's Service Center. *The Hamburg Commissioner for Data Protection and Freedom of Information*. 1 October 2020. https://datenschutz-hamburg.de/assets/pdf/2020-10-01-press-release-h+m-fine.pdf

[4] GDPR Enforcement Tracker. *CMS Law*. https://www.enforcementtracker.com/

[5] GDPR. *Official Journal of the European Union.* 27 April 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

[6] H&M has received a decision from the regional Data Protection Authority in Hamburg, Germany. *H&M Group*. 1 October 2020. https://hmgroup.com/news/hm-has-received-a-decision-from-the-regional-data-protection-authority-in-hamburg-germany/?s=regional

[7] H&M Germany fined $41.3M in one of largest GDPR penalties. *Compliance Week.* 1 October 2020. https://www.complianceweek.com/data-privacy/handm-germany-fined-413m-in-one-of-largest-gdpr-penalties/29556.article