GDPR Case Study: Spartoo

Aryan Srivastava (asriva11)

Abstract

The European fashion retailer, Spartoo, was found to be in violation of Article 5(1)(c), Article 5(1)(e), Article 13, and Article 32 as a result of the investigation done by CNIL (France Data Protection Authority) after a dawn-raid on 31 May 2018 at SPARTOO's premises in France. The total fine against the company, decided at the final deliberation on 28 July 2020, was 250,000 euros.

1. Background

National Data Protection Commision ("Commission Nationale de l'Informatique et des Libertés", hereinafter referred to as CNIL) is an independent French administrative regulatory body. Its mission is to ensure that data privacy laws are complied with within its jurisdiction in France. [1] The CNIL's restricted committee (hereinafter referred to as "the restricted committee") can impose various sanctions on non complying data controllers. [5]

SPARTOO SAS (hereinafter referred to as "Spartoo"), headquartered in France, was created in 2006 and specializes in online shoe retail. The Spartoo group employs around 1000 people and operates 16 websites within thirteen countries of the European Union, namely France, Spain, Germany, Italy, the Netherlands, Slovakia, Denmark, Poland, Sweden, Finland, Belgium, the Czech Republic, Hungary, and the United Kingdom. [2]

The CNIL undertook a dawn-raid on 31 May 2018 in the premises of Spartoo with the purpose of verifying if the company complied with all the provisions of the General Data Protection Regulation (hereinafter referred to as GDPR). CNIL acted as the lead supervisory authority in cooperation with other EU supervisory authorities [4]. The investigation focused on the storage and processing of data, particularly of the company's customers and prospects. [2]

At the time of the dawn-raid, Spartoo was storing full and permanent recordings of telephone conversations between customer service representatives and clients, including the customer's bank details, address, and other private information. According to Spartoo, these calls were being used for the training of employees; however, only one recording was used per week and per employee for this purpose. For the purpose of fighting fraud, the company was collecting "health cards" in Italy, and storing scans of bank cards used during an order. [3]

Spartoo had not set up a retention period for customer data, and no procedure was set up for regular erasure and archival of personal data. Inconsistent information was provided in the privacy policy of the website. Employees were also kept out of light. Insufficient information was provided about the purpose of phone recordings, its legal basis, and the retention period. Lastly, Spartoo did not force customers to set up and use stronger passwords. [3]

In light of the preceding discussion, the following problem setting is revealed.

Data Subject: the clients, customers, and prospects of Spartoo

Data Controller: Spartoo. They got consent of the data subjects, stored their data, and decided how to use it. They also decided on the duration of the retention period.

Data Processor: Spartoo. They were using the data to train employees, keep old accounts active, and fight fraud.

2. GDPR Violations

Based on the investigation carried out by the CNIL following the dawn-raid, the restricted committee came to the conclusion that Spartoo had failed to comply with provisions of the GDPR. Following is a summary of the violations.

Article 5(1)(c) of the GDPR: the permanent recording of phone conversations between customer service representatives and clients - including the customer's banking information - given that only one recording was

being used per week and per employee for its stated purpose was excessive. The collection of health cards in Italy for the purpose of fighting fraud was also excessive. [6]

Article 5(1)(e) of the GDPR: No data retention policy was set up by the company and client data was not being regularly erased or archived. Spartoo informed the CNIL of the set up of a 5 year retention period, however the company was already retaining personal data of more than 3 million clients who had not connected to their account in more than 5 years. A 5 year retention period itself was considered excessive by the CNIL because Spartoo stopped sending digital marketing communication to its customers who did express any interest for 2 years. Moreover, Spartoo considered the data retention starting point to be the last time a prospective customer opened a marketing email. According to the CNIL, this is not sufficient evidence of a prospect being interested in Spartoo's products since emails can be accidentally opened. Lastly, the CNIL found that Spartoo was not deleting all data after 5 years, but would retain the email address and password of the client under a pseudonymized and not anonymous form in case a client were to reconnect with their account after 5 years. All these practices were non compliant with the GDPR. [6]

Article 13 of the GDPR: Spartoo's website's privacy policy had inconsistent and incorrect information. It claimed that consent was the legal basis of all personal data processing, however it could rely on other legal basis. The employees of the company were not informed about the purpose, legality, practices, and their rights with regards to the recording of phone conversations. This violates the transparency provisions of the GDPR. [6]

Article 32 of the GDPR: The required password strength for Spartoo's website was not strong enough. The company's claim that a simple password was more secure than a complex one because of its unpredictability to hackers and less reusability was rejected by the CNIL. Spartoo was also found to be infringing the security requirements as it collected clear scans of customers' credit and/or debit cards and retained them for 6 months. The company claimed that these practices were to fight fraud. [6]

The CNIL took into consideration the seriousness of the above infringements, the number of people concerned, and the fact that some of the infringements relate to obligations that already existed before the GDPR, and decided to announce a fine of 250,000 euros. The restricted committee also issued an injunction to comply with the GDPR and other data protection laws within 3 months under a penalty of 250 euros per day. [6]

Spartoo may appeal against the decision to the Council of State within two months of its notification, which is still ongoing. [2]

5. Prevention

Several of Spartoo's infringements of the GDPR could have been prevented if stricter policies were implemented company wide. As only one recording per week per employee was being used for training purposes, there was no reason to excessively record and store phone conversations. The company could also have explored other training approaches that do not require exhaustive recording of conversations. Parts of the conversation that included personal information like address, and banking details could have been censored or deleted. The company should have aimed to minimize data collection, and get permission for it wherever required.

For the purpose of fighting fraud, Spartoo should have explored options other than collecting health cards and storing clear scans of credit and debit cards.

The company failed to put in place policies for even simple issues, such as password strength. They should also have been more transparent and honest. Being inconsistent in their privacy policy and not being transparent to employees leads to a lot of questions about the leadership of the company.

6. Discussion

This was the CNIL's first decision of sanction as the Lead SA of an investigation in cooperation with 13 other European Data Protection Authorities, which makes it significant, at least in France. I believe the CNIL took impressive action by conducting a dawn-raid at Spartoo's premises. I believe that the dawn-raid which occurred on 31st May, 2018 - merely 6 days after the GDPR was implemented - was an excellent way for the CNIL to set the precedent that swift and imposing action can be taken on companies that do not comply with the GDPR. Even though it took more than 2 years for the final deliberation and judgement, I believe the judgement to be fair. Several of Spartoo's infringements are inexcusable and seem like the result of either mismanagement or malice. Whatever the case, this event hopefully prompted other French and EU companies to fix their acts.

References

[1] Institut Français FAQ - What is CNIL?
https://tinyurl.com/y2nvbdrt

[2] Deliberation of restricted training SAN-2020-003 of July 28, 2020 concerning the company Spartoo SAS
https://tinyurl.com/y53turwa

[3] SPARTOO : sanction de 250 000 euros et injonction sous astreinte de se conformer au RGPD
https://tinyurl.com/y6mjua6b

[4] CNIL Adopts its First Sanction as Lead Supervisory Authority, Fining French Online Shoe Retailer
https://tinyurl.com/y4c47gq3

[5] Status and Composition of the CNIL
https://tinyurl.com/y22dvj5w

[6] France: First sanction of an online shows company by CNIL acting as a lead authority for several infringements to GDPR requirements
https://tinyurl.com/y574vagv