LATHAM & WATKINS LLP

Global Privacy & Security Compliance Law Blog

Commentary on Global Privacy and Security Issues of Today

French Data Protection Authority Hands Down First Sanction as Lead Authority

By Latham & Watkins LLP on September 2, 2020

Posted in GDPR

The CNIL has imposed a €250,000 fine on an online retailer for GDPR infringements in cooperation with other EU supervisory authorities.

By Myria Saarinen and Charlotte Guerin

Founded in 2006 and headquartered in France, Spartoo SAS (Spartoo) is one of the leaders of the European online shoe retail market. On 31 May 2018, a week after the entry into application of the GDPR, the French Data Protection Authority (the CNIL) launched an on-site investigation of Spartoo in cooperation with other EU supervisory authorities. The CNIL eventually handed down its decision on 28 July 2020, imposing a €250,000 fine on Spartoo for the infringement of four different provisions of the GDPR. Spartoo may appeal the CNIL's decision within two months. The decision illustrates how the GDPR's "one-stop shop" mechanism can operate, and also provides insight to online retailers and other businesses on what to expect regarding GDPR enforcement in practice.

The CNIL as Lead Authority

Under GDPR Article 56, the supervisory authority of the main or single establishment of a data controller is competent to act as lead supervisory authority for cross-border processing carried out by that controller.

Spartoo is incorporated in France and operates 16 retail websites for customers in 13 EU Member States[1] and the UK. The CNIL found that it was competent to act as the lead supervisory authority in regard to Spartoo's cross-border data processing activities. Consequently, the CNIL followed the cooperation mechanism provided in GDPR Article 60, meaning that the authorities in the Member States in which Spartoo operates had the opportunity to contribute to the CNIL's investigation and decision. In this case, the authorities of Italy, Portugal, and Lower Saxony (Germany) all presented reasoned objections to the CNIL's draft decision, which the CNIL took into account.

The proceedings carried out by the CNIL were concluded relatively quickly, given the number of authorities involved, and the final decision was adopted 26 months after the investigation opened. The deadlines provided by GDPR Article 60 are indeed quite short: the lead authority must submit a draft decision to the other authorities concerned "without delay"; the latter may express relevant and reasoned objections within four weeks; and their consultation of the revised draft must take place within two weeks.

The CNIL's Decision

The CNIL held that Spartoo was in violation of four different provisions of the GDPR:

- Data minimization under Article 5.1(c)
- Storage limitation under Article 5.1(e)
- Right to be informed (transparency) under Article 13
- Security of processing under Article 32

As a result, the CNIL imposed a €250,000 fine and ordered Spartoo to comply with the GDPR within three months of the decision, under penalty of an additional €250 fine per day.

Although Spartoo's financial statements are not publicly available, several press articles reported an annual global turnover of €250 million for the 2018 fiscal year. On this basis, the fine imposed by the CNIL would correspond to approximately 0.1% of Spartoo's annual global turnover, well below the 4% maximum limit set by GDPR Article 83.

The CNIL referred to a number of factors in its decision on the level of fine:

- The fact that most of the violations related to data protection principles that existed prior to the GDPR
- The high-risk nature of some of the personal data (in particular bank details)
- The number and severity of the infringements (especially the systematic recording of employees' calls without a legitimate purpose or adequate information)
- The large number of data subjects impacted (several thousand)

The CNIL's order to remediate the breaches within three months was issued on the basis that it found Spartoo to still be in breach at the investigation's close (notwithstanding certain corrective measures already implemented).

Data Minimization

Under GDPR Article 5.1(c), personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

The CNIL found that Spartoo's practice of collecting and storing all calls between its customers and employees for the purpose of employee evaluation and training was disproportionate and particularly invasive of employees' privacy. The CNIL also noted that while customers are given the opportunity to object to the recording at the beginning of each call, employees are not given the same option.

Furthermore, the CNIL noted the absence of technical measures to ensure that calls including customers' banking information were not recorded. The CNIL deemed the banking information to be unrelated to the stated purpose of the processing (i.e., employee training) and high risk given the potential harm to individual customers (i.e., accidental or unlawful disclosure of their banking information to third parties).

Storage Limitation

Under GDPR Article 5.1(e), personal data may only be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."

The CNIL noted that Spartoo initially did not have a retention policy, and stored the personal data of its 25 million prospects indefinitely. Spartoo later adopted a retention period of five years from the date of last contact, which the CNIL found to be excessive.

During the investigation, Spartoo claimed to have implemented a new policy of contacting its former customers and clients for marketing purposes for up to two years after the date of their last activity. Although this retention period was deemed proportionate, the CNIL held that Spartoo was nonetheless in breach of the storage limitation principle by relying on the opening of a marketing email as customer "activity". The CNIL found this to be an insufficient indication of the interest of the data subject in the products and services, unlike, for example, clicking on a hyperlink included in a marketing email.

Furthermore, Spartoo's practice of retaining customers' and prospects' email addresses and passwords beyond the retention period was found to be noncompliant with the GDPR. The CNIL made clear in its decision that, at the expiry of the retention period, all personal data must be deleted and not simply made pseudonymous through, for example, a hash function.

Transparency and Right to Be Informed

Under GDPR Article 13, the data controller must provide data subjects with certain information, including the controller's identity, the purposes and legal bases of data processing, and the recipients or categories of recipients. The data controller must also specify whether personal data will be transferred outside of the European Union.

The CNIL found that Spartoo breached its obligations under this Article by failing to inform data subjects of the transfer of their personal data to Madagascar when calling customer service.

In addition, the CNIL held that consent should not be indicated as a blanket legal basis for all of the processing activities carried out by Spartoo pursuant to its privacy policy, as other legal bases, such as contractual necessity or legitimate interest, were also relied upon in practice and should therefore be specified in the company's privacy policy. The CNIL emphasized the need to identify and specify the legal basis for each specific data processing activity. Notably, the misidentification or failure to specify a legal basis did not appear to impact the CNIL's view on the lawfulness of the processing activities themselves, as long as a valid legal basis did in fact exist.

Finally, the CNIL found that Spartoo did not provide sufficient information to its employees regarding the existence and characteristics of the recording of their calls with customers, both with respect to data protection laws and applicable labor laws. The CNIL considered this lack of information particularly egregious as the practice lasted many years and could be regarded as a form of constant surveillance.

Security Obligations

According to GDPR Article 32, the controller or processor must implement security measures "to ensure a level of security appropriate to the risk".

In assessing Spartoo's compliance with this Article, the CNIL noted that banking information is a type of personal data that can severely impact individuals in case of a security breach. In light of this, the CNIL found Spartoo's use of eight-character-long passwords, without any requirements regarding character types, to be insufficient, as such passwords are vulnerable to brute force attacks.

The CNIL referred to the French Information System Security Agency guidelines regarding passwords as well as its own recommendations from 2017 to justify this assessment. Specifically, the CNIL states that a password must be at least 12 characters long and include a minimum of four different types of characters if no other security measures are implemented at the log-in stage. If additional security measures are implemented, such as captcha or account locking after multiple unsuccessful attempts, the CNIL considers a password of at least eight characters including at least three different types of characters to be secure enough.

According to the investigation, Spartoo requested that, for purposes of fraud prevention, customers send a scan of their credit or debit card by email, showing at least half of the card's numbers, the name of the holder, and the expiry date. The CNIL found that this practice encouraged customers to send, in an unencrypted form, the entirety rather than a truncated version of their bank card numbers. The CNIL considered such collection and storage of full customer card details to be in violation of Spartoo's security obligations, notwithstanding Spartoo's prior authorization from the CNIL to store bank card details in their truncated form.

Practical Implications

The CNIL decision sends a strong signal to online retailers and other businesses regarding the level of scrutiny that the CNIL and other supervisory authorities are likely to apply when investigating potential GDPR infringements. Whilst each supervisory authority has its own approach to enforcement, the CNIL decision was supported by a number of other supervisory authorities via the GDPR's cooperation mechanism, and gives a good indication of the standards expected by the supervisory authorities in practice. To minimize the risk of GDPR enforcement, online retailers and other businesses should:

- Adopt a consistent high-water-mark approach to GDPR compliance when engaging in cross-border dat processing, as the designation of a lead authority does not shield entities from scrutiny by other supervisory authorities, including those with potentially stricter approaches
- Consider prioritizing any compliance remediation efforts on longstanding data protection requirement that pre-date the GDPR, as supervisory authorities may be less tolerant of breaches in this context
- Ensure that each data processing activity has a clear and justified relationship with its underlying purpose, i.e., the nature and scope of the processing must be tailored to its purpose, not the other way around
- Define a sufficiently detailed and transparent data retention policy, and ensure the effective deletion of personal data at the end of the applicable retention period; supervisory authorities are taking an increasingly strict approach to long and unlimited retention periods of personal data (e.g., the highest GDPR fine imposed to date by a German data protection authority was in relation to the unlimited retention of customer data)
- Ensure that any local, or industry or technology specific, information security requirements, guidance, and best practices are properly integrated into the organization's systems and processes, to ensure adequate protection of personal data
- Be mindful that the obligations under GDPR apply equally to internal as well as external data subjects; how an organization uses its employee personal data can be subject to just as much scrutiny as its use of

customer personal data

This post was written with the assistance of Alex Park in the Paris office of Latham & Watkins.

Endnotes

[1] These websites target customers in France, Spain, Germany, Italy, the Netherlands, Slovakia, Denmark, Poland Sweden, Finland, Belgium, the Czech Republic, and Hungary.