

EU Data Protection Authority Levies Its First Fine for Violations of the GDPR

September 08, 2020

The French Data Protection Authority, CNIL, has levied its first fine for enforcement of the General Data Protection Regulation (GDPR). The enforcement target, Spartoo, is a French online shoe retailer that makes its website available to a host of countries in the European Union.

In its August 5, 2020, enforcement decision, CNIL focused on violations of the following principles of the GDPR:

Failure to Employ Data Minimization Measures: CNIL's decision focused on Spartoo's practice of recording telephone calls for employee training purposes and the recording of credit card payment information from customers during these training calls, finding this data practice was not necessary.

Failure to Implement Adequate Measures Regarding Storage Limitation: Spartoo was found to be sitting on volumes of customers' personal information absent policies to scrub accounts no longer in use for upwards of 10 years. The records of over 25 million customers were kept for users who were not active for a period of more than three years. CNIL found the lack of meaningful data retention policies and corresponding time frames for deletion of customer information to be in violation of the storage limitation principle.

Failure to Provide Adequate Notice: Spartoo's privacy policies were found to be deficient in accordance with the GDPR notice requirement. The policy failed to appropriately provide notice regarding the legal bases for the processing of personal information.

Failure to Employ More Robust Data Security Standards: CNIL found that Spartoo's password practices and requirements for its customers were deficient, and that customers should have been required to create more secure passwords for their accounts.

CNIL's enforcement action may serve to open the floodgates for GDPR enforcement. As more EU data protection authorities issue guidance on specific provisions of the GDPR, whether it be cookies or the legality of data transfer mechanisms, businesses should be sure to expect investigations and enforcement actions from the various DPAs.

Related Practices

[Cybersecurity and Privacy
Technology](#)

Related Industries

[Technology](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.