Summary Final Decision Art 60

Investigation

EDPBI:FR:OSS:D:2024: 1100

Violation identified ; Administrative fine;

Background information

Date of final decision:	29 December 2023
Date of broadcast:	11 January 2024
LSA:	FR
CSAs:	DE, AT, BE, CY, DK, ES, FI, IE, IT, LU, NL, PL, PT, RO, SE, NO, EL SAs
Legal Reference(s):	Article 5 (Storage limitation) , Articles 12, 13 (Information to be provided), Article 32 (Security of processing)
Decision:	Violation identified, Administrative fine.
Key words:	Transparency; Data retention; Data security

Summary of the Decision

Origin of the case

The controller is a company that operates a website and a mobile application, which allow users to make online payments after registering for the service. At the end of September 2021, the LSA carried out two investigations of the company.

Findings

The LSA identified three infringements of the GDPR and an infringement of the French Data Protection Act by the controller.

Firstly the LSA held that the controller **failed to comply with the obligation to retain data for a period limited to the purpose for which it was collected (Article 5.1(e) GDPR)**. The company had set a period of ten years, after which user accounts were deactivated, but not deleted. Account data was therefore kept for an indefinite period. In addition, the ten-year retention period was applied to all user accounts, without sorting the data to be retained for instance in accordance with the rules of the

French Consumer Code. While the controller brought itself into compliance during the proceedings, the LSA still identified the past infringement.

Secondly, the LSA concluded that the controller **failed to comply with the obligation to inform data subjects (Articles 12 and 13 GDPR)**. Both on its website and on its mobile app, the controller informed data subjects through an incomplete and outdated privacy policy. In addition, this information was provided in English, whereas the company's target audience was mainly French-speaking.

Thirdly, the LSA held that the controller **failed to ensure the security of personal data (Article 32 GDPR)**. The complexity of the passwords for user accounts was insufficiently robust. In addition, almost 50,000 passwords were stored unencrypted in the database, together with the e-mail address and user ID. Lastly, the use of the SHA-1 function for the hashing of passwords was no longer deemed to comply with the state of the art. The LSA noted that the controller implemented compliance actions during the proceedings.

Lastly, according to the LSA, the controller failed to comply with obligations related to the use of cookies (Article 82 of the French Data Protection Act). The LSA noted that third-party analytics cookies were used on users' terminals without their consent. However, since these cookies may contain advertising functionalities and in any case enable the collection of data that may be used to maintain and protect the third-party analytics service, they cannot be used without user consent. In addition, the company used a captcha mechanism when users create an account and connect to the website and mobile app. This mechanism operates by collecting hardware and software information (such as device and application data). While the data collected was transmitted to the captcha provider for analysis, the company did not provide any information to the user and did not obtain their prior consent, either to access the information stored on their equipment or to write information on it. The failure to obtain consent for the use of third-party analytics cookies affected each individual browsing the website, i.e. several hundred thousand individuals. In the same way, the failure to obtain consent for the use of the captcha mechanism potentially affected each of the 700,000 account holders at the time of the investigations.

Decision

Consequently, the LSA imposed two fines against the controller:

- A fine of €90,000 for infringements of Articles 5.1(e), 12, 13 and 32 GDPR, within the framework of the one-stop shop procedure, as the website had users in several EEA Member States.
- A fine of €15,000 for non-compliance with the national legislation relating to the use of cookies. In this case, the authority had the jurisdiction to act alone.

In order to determine the amount of the fine, the LSA took into account the nature of the breaches, the categories of personal data (including banking details), the negligence of the company, the number of individuals concerned and the financial situation of the company.