Summary Final Decision Art 60

Notification

Administrative fine, Compliance order

EDPBI:FR:OSS:D:2021:279

Background information

Date of final decision: 14 June 2021

Date of broadcast: 21 September 2021

LSA: FR

CSAs: BE, ES, IT, PT

Legal Reference: Article 5 (Principles relating to processing of personal data), Article 13 (Information to be provided where personal data are collected from the data subject), Article 17 (Right to erasure), Article 32 (Security of processing)

Decision: Administrative fine, Compliance order

Key words: Data retention, Transparency, Right to erasure, Data security, Password

Summary of the Decision

Origin of the case

The LSA carried out an own volition audit at the premises of the controller in order to verify its compliance with all the provisions of the GDPR. The audit focused on the processing of personal data relating to the company's customers and prospective customers. More specifically, the LSA investigated on the information provided to data subjects, compliance concerning data subject requests and data retention periods.

In order to complete these investigations, the LSA also carried out an online audit relating to all processing accessible from the controller's website, with a particular focus on, *inter alia*, the methods used for informing data subjects.

Findings

In the course of its investigation, the LSA noted that the active database of the controller contained personal data of 16.653 persons who had not placed an order in more than 5 years and 130,000 persons who have not signed in to their customer account in more than 5 years. In this regard, the LSA

ruled that, although the controller implemented a retention period policy, personal data were kept for much longer periods than those specified in this policy on the day of the audit and did not appear to be appropriate for the purposes for which the data were processed (Article 5(1)(e) GDPR).

Furthermore, following its on-site and online audits, the LSA founds that certain mandatory information provided for by Article 13 GDPR was missing, namely the contact details of the DPO, the data retention periods, the legal bases of the processing and information on certain data protection rights. Nonetheless, the LSA noted that the company had complied with all the point raised regarding the information of data subjects by the end of the investigation.

As to the controller's obligation to comply with requests to delete personal data (Article 17 GDPR), the LSA found that when an individual requested the deletion of its account, the company simply deactivated the account in question. In this regard, the LSA stressed that the email address used for marketing purposes should have been deleted in the event of withdrawal of consent insofar as its retention is not legitimate on any other basis. Measures were taken by the company in the course of the procedure but did not fully achieve compliance, so the LSA issued an injunction against the company.

Finally, the LSA found that the passwords format when both creating an account on the controller's website and accessing to the customer databases were insufficiently robust to ensure data security within the meaning of Article 32 GDPR (Security of processing). Violations of the same Article have been reported by the LSA due to the obsolete nature of the hash function used for the storage of passwords of employees using the controller's website and the use of the same account by several employees when accessing to a copy of the controller's production database.

Decision

The LSA imposed an administrative fine of 300,000 euros to the controller to be in breach of Articles 5(1)(e), 13, 17 and 32 GDPR

In addition, the LSA imposed a compliance order on the controller to remedy its breach of Article 5(1)(e) with a penalty payment of 500 euros per day of delay at the end of a period of 3 months following notification of the decision.