Summary Final Decision Art 60

Investigation

Administrative fine

EDPBI:FR:OSS:D:2021:310

Background information

Date of final decision:	30/12/2021
Date of broadcast:	05/01/2022
LSA:	FR
CSAs:	DE (BW, BY, BE, NI), ES, BE, IT, LU, NL
Legal Reference:	Article 5, Article 13, Article 17, Article 28 and Article 32.
Decision:	Administrative Fine
Key words:	Cooperation with the supervisory authority, Data retention, Data security, Data subject rights, Password, Personal data breach, Right to be informed, Right to erasure

Summary of the Decision

Origin of the case

The controller's is a company selling furniture online and in store. It has its main establishment in France. On 24 April 2019, 9 May 2019 and 5 June 2019 the LSA's team carried out an online investigation into the processing accessible from the company's domain and an on-site investigation. The purpose of these investigations was to verify the company's compliance with the GDPR and the national data protection law. The online investigations conducted by the LSA focused on the manner in which personal data for customers and prospective customers had been processed by the company.

In accordance with Article 56 GDPR, on 1 July 2020, the LSA informed all the European supervisory authorities of its competence to act as lead supervisory authority. In October 2020, the LSA submitted a draft order to the CSAs. The Berlin SA raised a relevant and reasoned objection within the meaning of Article 60(4) GDPR, requesting that the draft order be turned into a draft penalty, and more specifically an administrative fine. In support of this

request, the CSA pointed out the high number of data subjects concerned and the duration of the violations. The LSA then shared a revised draft decision, to which no CSA objected.

In its defence, the controller has contested the Berlin SA's objections and expressed its surprise at the importance given to them, bearing in mind the low percentage of the controller's sales in Germany. The company considers that it should have been the subject of an order, as initially proposed by the LSA, and not to a penalty.

Findings

Regarding the proceedings, the LSA recalled that the BE SA's objections had been expressed within the framework of the cooperation and consistency mechanism provided for under Chapter VII GDPR, which intends to ensure harmonisation of the SA's enforcement policy. Regarding the controller's obligations under Article 5(1)(e) GDPR, the LSA established a breach of this provision, in so far as the controller had not defined and implemented any satisfactory retention period policy on the date of the investigation.

Regarding the obligation under Article 13 GDPR to provide the data subjects concerned with information relating to the processing of their personal data, the LSA found that the information was not complete. In this context, the LSA pointed out that the link between the controller's failure to implement data retention period and the lack of information for individuals did not prevent these two breaches from existing as such.

Furthermore, the LSA established a breach of the obligation to comply with requests to delete personal data pursuant to Article 17 GDPR, because there were cases in which the controller had simply deactivated the customer's account without actually deleting the personal data. In addition, the controller's relationship with one of its processors had not been governed by any legal act, in breach of Article 28 GDPR.

Finally, the LSA also held that the controller had failed to ensure the security of personal data pursuant to Article 32 GDRP.

Decision

The LSA noted that, as part of the penalty proceedings, the controller has demonstrated having taken measures to ensure compliance with the GDPR. Nevertheless, the LSA held that this could not exempt the company from its responsibility for the past and imposed an administrative fine of EUR 120,000 in respect of the breaches of Articles 5(1)(e), 13, 17, 28 and 32 GDPR.