Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:FR:OSS:D:2021:313

Background information

Date of final decision:	28 December 2021
Date of broadcast:	11 January 2022
LSA:	FR
CSAs:	DEBW, DEBY, DEBE, DEHB, DEHH, DEHE, DEHI, DEMV, DENW, DERP, DESL, DESN, DEST, DESH, DESH, DETH, IT, NL, ES
Legal Reference(s):	Article 28 (Processor), Article 32 (Security of processing), Article 33 (Notification of a personal data breach to the supervisory authority), Article 34 (Communication of a personal data breach to the data subject)
Decision:	Administrative fine
Key words:	Clients, Personal data breach, Data security, Publicly available data, Finance

Summary of the Decision

Origin of the case

The controller is a payment service provider offering to its customers (merchants) solutions for managing recurring payments in SEPA. In order to provide these services, it processes personal data of its customers' debtors. In 2015, the controller carried out a research project on anti-fraud mechanism, for which it imported personal data of its clients' debtors on a dedicated server. Yet, the server was not subject to any special security procedures and the personal data remained freely accessible via a specific URL until 2020, when the breach was reported to the controller by one of its customers. Following this, the controller immediately took corrective measures and notified the LSA of the breach. The data of more than 12 million debtors was affected. It consisted of surname, first name, title, e-mail address, post address, telephone number, BIC/IBAN information.

Findings

The LSA carried out an investigation and received additional information from the company. It was established that the latter had acted as data processor hiring sub-processors for the processing carried out in the context of the services provided to merchants, and as data controller with regard to the research project resulting in the data breach. The LSA characterised a number of breaches. First, the company had failed to provide a formal legal framework for the processing carried out by the sub-processors and had merely sent them a questionnaire with no binding force. Furthermore, some of the contracts with its processors did not satisfy the requirements of Art. 28(3) and (4) GDPR. Second, the company had not ensured security of personal data within the meaning of Art. 32 GDPR. The continuous breach consisting of leaving personal data freely accessible online could not be explained by isolated human negligence, since security deficiencies were the result of repeated insufficiency and the controller should have ensured the security of the data in question at several stages. In addition, the LSA took the view that the lack of evidence of fraudulent use of the data did not affect the characterisation of the breach of the security obligation. Finally, the LSA also established a breach of the controller's obligation to notify data subjects of a personal data breach pursuant to Art. 34 GDPR. According to the LSA, given the nature of the personal data, the volume of data subjects, the ease of identifying the persons affected by the breach and the possible consequences for the data subjects, the risk associated with the breach could be considered high and communication to the data subjects should have been made.

Decision

In light of the above, the LSA decided to impose on the controller an administrative fine of EUR 180.000 for the infringement of Articles 28(3), 28(4), 32 and 34 GDPR and publish the decision, which will no longer identify the company at the end of a period of two years following its publication.