Summary Final Decision Art 60

Investigation

Compliance order, Administrative Fine, Publication of the controller's name

EDPBI:FR:OSS:D:2020:134

Background information

Date of final decision:	28 July 2020
Date of broadcast:	11 August 2020
LSA:	FR
CSAs:	AT, BE, BG, HR, CY, CZ, DK, DE, EE, EL, FI, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, RO, SK, SI, ES, SE, UK
Legal Reference:	Principles relating to processing of personal data (Article 5), Security of processing (Article 32), Transparency and Information (Articles 12, 13 and 14)
Decision:	Compliance order, Administrative Fine, Publication
Key words:	Data minimisation, Storage limitation, Transparency, Employees, Clients, E-commerce, Data security.

Summary of the Decision

Origin of the case

The controller conducted full and permanent recording of all phone calls from its customer service employees, and without their ability to object. The controller did not prove that it had limited this processing to what is necessary for the purposes of assessing and training its employees. The controller also recorded the bank details of customers placing orders by telephone when recording its employees' conversations for training purposes and stored such data in clear text in its database for fifteen days.

The controller collected copies of Italian health cards and valid identity cards for anti-fraud purposes.

The controller also stored a significant amount of personal data of customers who had not connected to their account in over ten years and of individuals that had never placed an order on the company's website. After the expiry of the storage period for customers' data, the company keeps some of their data such as their e-mail address, and password in pseudonymised form for the alleged purpose of enabling customers to reconnect to their accounts.

The controller did not inform its customers that their data were transferred to Madagascar. The controller only cited in its privacy policy one legal basis for processing: consent whereas it conducted several processing operations on different legal basis. The controller did not inform either its employees individually of the recording of their telephone calls.

The controller accepted to log into user accounts passwords comprised of eight characters and only one category of characters. It also requested its customers to provide it with a scan of the bank cards used on ordering for anti-fraud purposes, which were subsequently stored by the company in clear-text and containing all of the credit card numbers for six months.

Findings

The LSA considered that the controller's recording of all phone calls from its customer service employees, including the bank details of customers placing orders by telephone and the collection of Italian health cards, which contain more information than the identity card that is not relevant to combat fraud, was excessive and concluded that it was a breach of the data minimisation principle of Article 5.1.c. GDPR.

The LSA concluded that the company's storage of a significant amount of personal data of former customers and prospects over long periods that exceed the purposes for which data were processed violated the storage limitation principle of Article 5.1.e. GDPR.

The LSA considered that the controller had not informed customers up to a specific date of the transfers of data to Madagascar, provided for each processing operation the corresponding legal basis in its privacy policy and adequately informed its employees of the recording of their telephone calls. All these failings constituted a breach of Article 13 GDPR (information provided to data subjects).

The LSA considered that the company did not take sufficient security measures to ensure the security of its customers' bank data, which violated Article 32 GDPR (security of processing).

Decision

The LSA decided to impose a compliance order on the controller to remedy its breaches of the principles of data minimisation, data storage limitations, requirement to inform data subjects, and to ensure data security. It associated the compliance order with a periodic penalty payment of 250 euros per day of delay on expiry of a period of 3 months following the notification of this decision.

The LSA also imposed on the controller an administrative fine of 250,000 euros.

The LSA further decided to make its decision public on its website, identifying the company by name, for a period of two years.