Summary Final Decision Art 60

Investigation

EDPBI:FR:OSS:D:2023:802

Administrative fine Violation identified

Background information

Date of final decision:	08 June 2023
Date of broadcast:	19 June 2023
LSA:	FR
CSAs:	BE, LU, IT, ES, PT, BG, DE, IE
Legal Reference(s):	Article 5 (Principles relating to processing of personal data) , Article 6 (Lawfulness of processing), Article 9 (Processing of special categories of personal data), Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 13 (Information to be provided where personal data are collected from the data subject), Article 28 (Processor), Article 32 (Security of processing), Article 33 (Notification of a personal data breach to the supervisory authority).
Decision:	Administrative fine, Violation identified.
Key words:	Administrative fine, Data minimisation, Data retention, Data security, Transparency, Payment data, Lawfulness of processing, Clients, Data processing agreement, Sensitive data, Consent, Retention time

Summary of the Decision

Origin of the case

The controller is a company registered in France. It provides online clairvoyance readings to its customers through chat or on the phone. The LSA opened an investigation following a report in the press that the controller had been subject to a data breach. More specifically, the LSA carried out an online investigation, an onsite audit and also asked the controller to respond to specific questions and requests for information.

Findings

The LSA found that the controller breached many GDPR provisions.

First, the LSA found that the controller breached the data minimisation principle under **Article 5(1)(c) GDPR** because it collected excessive personal data for the applicable purposes. More specifically, the controller was systematically recording all the phone calls between on the one hand, its prospects and call agents, and on the other hand between its fortune-tellers and customers. The controller failed to justify the necessity to record all calls and the LSA considered that there were less intrusive means to achieve the different purposes identified by the controller. In addition, during the calls that were recorded, the customers shared their payment card details. The controller did not implement any specific measures to pause the recording of the phone calls during this data disclosure even though such data was not relevant for the purposes identified by the controller.

Secondly, the LSA found that the controller breached the storage limitation principle under **Article 5(1)(e) GDPR**, as it retained customer data for an excessive period after the end of the applicable contractual relationship. During the investigation, the controller's active database included personal data relating to customers who had not had a clairvoyance reading in more than three years (and sometimes in more than five years) without the controller justifying that customers still have credit.

In addition, the LSA found that the controller did not rely on a legal basis under **Article 6 GDPR**. The controller retained payment card information of its customers after the completion of transactions to facilitate the purchase of additional credit without their prior consent. According to the LSA, this processing activity cannot rely on the necessity to perform the contract.

Furthermore, the LSA found that the controller breached **Article 9 GDPR**. When providing clairvoyance services, the controller collected and processed customers' sensitive data (i.e. data concerning health and data about sexual orientation) without the data subjects' prior and explicit consent. The LSA rejected the controller's argument whereby spontaneously contacting a fortune-teller and disclosing special categories of personal data during the call with the latter amount to explicit consent on the part of the customers. To obtain "informed" consent, data subjects must first be provided with specific information regarding this processing activity, which was not the case in this context.

The LSA also found that the controller breached its transparency obligations under **Articles 12 and 13 GDPR**. The information provided by the controller was not easily accessible given that users had to actively search for it. More specifically, the information was not provided directly on the registration online page and it was included in a document not identified as such as relating to data protection, but in the standard terms and conditions. The LSA also considered that the information provided to users was incomplete as it did not include all the information required by Article 13 GDPR.

In addition, the LSA found that the controller breached **Article 28 GDPR** when contracting with processors. The data processing agreements in place were not all signed by the parties and did not include all the mandatory information set out under Article 28(3) GDPR. As a result, the LSA considered that the contractual safeguards were not sufficient.

Furthermore, the LSA found that the controller breached **Article 32 GDPR** for not having implemented basic security measures. The controller implemented insufficiently robust passwords for user accounts (for its customers as well as its employees) and did not secure access to its customer website using the http protocol instead of the https protocol. Lastly, the controller also used a bank data encryption mechanism that had vulnerabilities.

Lastly, the LSA found that the controller breached **Article 33 GDPR**. The controller was aware of the occurrence of a data breach and recorded the breach in its data breach internal register. However, it failed to notify the breach to the LSA. According to the LSA, at the date of the internal investigation, the controller had a reasonable degree of certainty that there was a data breach causing a risk to data subjects' rights and freedoms, especially given the duration of the breach (i.e., two months and four days) and the potential high number of data subjects. The obligation to notify the competent authority applies even if the breach was caused by an error that could be attributed to the processor.

Decision

The LSA imposed on the controller an administrative fine of 120,000 euros for the infringement of Articles 5(1)(c) and (e), 6, 9, 12, 13, 28, 32 and 33 GDPR. The LSA also decided to publish the final decision on its website and on the Légifrance website for two years, after which the controller will not be identifiable anymore.

To set the amount of the administrative fine, the LSA took into account the particularly high number of GDPR infringements, the fact that it involved special categories of personal data and the high number of data subjects. It also took into account the financial situation of the controller and the fact that it employed few employees.