Summary Final Decision Art 60

Complaint

Administrative fine

EDPBI:FR:OSS:D:2023:475

Background information

Date of complaint:	12 December 2020
Draft decision:	19 July 2022
Revised draft decision:	N/A
Date of final decision:	08 September 2022
Processor:	N/A
LSA:	FR
CSAs:	All SAs
Legal Reference(s):	Article 5 (Principles relating to processing of personal data), Article 32 (Security of processing)
Decision:	Administrative fine
Key words:	Password, Data retention, Data security, Anonymisation, User account

Summary of the Decision

Origin of the case

On 12 December 2020, the LSA received a complaint concerning a website operated by the controller, which allows its users to get specific legal information on companies and/or to order certain types of documents. The complainant claimed that the controller's website stored users' passwords in clear text and that it was able to obtain its own password over the telephone by simply giving its name to the helpline operator. Following this complaint, the LSA launched an investigation to verify the compliance with the GDPR of any processing accessible from that domain, or concerning personal data collected from the latter.

Findings

During its investigation the LSA found that the controller retained the personal data of 946,023 members and 17,558 subscribers whose last order, formality or invoice was dated of more than 36 months ago, contrary to the retention period indicated in the controller's confidentiality charter. In

addition, the LSA found that no procedure for automatic deletion of these data was put in place by the controller. In its defence, the controller argued that although its confidentiality charter indicates a retention period of 36 months, it would be justified for some data to be kept for a longer period and pointed out that only about 25% of the accounts were kept for more than 36 months without being anonymised.
In this respect, while the LSA acknowledged that the retention of certain data for compliance with legal obligations or for pre-litigation or litigation purposes is possible, it noted however that the controller had not identified these purposes in its confidentiality charter, and that the retention of such data for these purposes could not in theory concern members who pay immediately in exchange for the receipt of a certain type of document. In addition, the LSA recalled that the data kept for these purposes must be placed in intermediate storage, for a period not exceeding that necessary for the purposes for which they are retained. Finally, the LSA pointed out that these data should be placed in interim storage, either in a dedicated archive database or by making a logical separation within the active database, allowing only authorised persons to access it. However, the LSA noted that none of these actions had been implemented by the controller on the day of the audit. Secondly, the LSA noted that only manual anonymisation was implemented by the controller for the deletion of accounts whose deletion was specifically requested by the users and that no automatic anonymisation procedure was in place for the other accounts. The LSA therefore concluded that the controller breached its obligation to store data for a period proportionate to the purpose of the processing pursuant to **Article 5 (1)(e) GDPR**.

Furthermore, the LSA found that the methods of transmitting and storing passwords implemented by the controller were not appropriate in view of the risk that the data subjects would be exposed to if a third party were to capture their username and password. In particular, the LSA observed that the criteria imposed by the controller for the creation of passwords to log in to the controller's website were not sufficiently robust, as they are limited to eight characters, without any complexity criteria, and are not associated with any additional security measures. The LSA also found that the controller sent non-temporary passwords for accessing accounts in clear text via e-mail. Finally, the LSA noted that the controller kept passwords, secret questions and answers used by users in clear text and did not notify them of a (possibly unauthorised) change of these passwords. In view of the risks incurred by the data subjects and the volume and nature of personal data that may be contained in more than 3.7 million accounts (including, inter alia, bank details of the subscriber accounts, last name, first name, postal and email address, landline and mobile telephone numbers, secret question and its answer of all of the accounts), the LSA considered that the controller failed to fulfil its obligations under **Article 32 GDPR.**

Decision

The LSA found that an administrative fine of €250,000 would be dissuasive, proportionate and justified in the case at stake. Additionally, the LSA decided to make its decision public, identifying the company by name, for a period of two years.