Summary Final Decision Art 60

Complaint

EDPBI:FR:OSS:D:2023:762

Violation identified ; Administrative fine

Background information

Date of final decision:	11 May 2023
Date of broadcast:	22 May 2023
LSA:	FR
CSAs:	All SAs
Legal Reference(s):	Article 5 (Principles relating to processing of personal data) , Article 9 (Processing of special categories of personal data), Article 26 (Joint controllers), Article 32 (Security of processing)
Decision:	Violation identified, Administrative fine.
Key words:	Sensitive data, Health records Joint controllers Administrative fine, Anonymisation, Data retention, Data security

Summary of the Decision

Origin of the case

The controller is a website dedicated to health and wellness, established in France ("the company"). It mainly offers articles, tests, quizzes and discussion forums related to well-being and health. The company's website has visitors from all Member States of the European Union.

On 26 June 2020, the LSA received a complaint concerning all of the processing of personal data of users implemented by the controller on its website and, in particular, the legal ground for processing users' personal data when a user takes health-related tests; the provision of information to users of the website, as well as data security. The LSA carried out an online audit in September 2020, an on-site inspection in October 2020 and sent a request for information to the company.

Findings

Firstly, the LSA found that the controller has not sufficiently monitored the performance of the contractual instructions it gave to its processor and has not exercised satisfactory **control over the measures the processor implemented** to ensure GDPR compliance (in particular, the absence of collection of personal data or its anonymisation). The LSA considered that the retention of test data did not appear necessary after the communication of the test result to the user, finding a **breach of Article 5(1)(e) of the GDPR**. Until 11 October 2020, the responses to the tests and quizzes and the IP addresses of users were retained for 24 months from the time of completion of the tests. After 11 October 2020, the responses to the tests and quizzes were retained for a period of three months from the time of completion of the tests due to ineffective anonymisation, using the SHA256 function without a hash key. The LSA also found that the company retained user account's data for more than three years due to ineffective anonymisation as it retained the unique identifier ("id_user") of the user, associated with their pseudonymised username. According to the LSA, this process did not correspond to anonymisation but to a mere pseudonymisation. The LSA recalled that the pseudonymisation of personal data is a reversible operation and that it is possible to find a person's identity by having additional information. However, the LSA noted that the company complied during the procedure with the implementation of a new anonymisation procedure, so there was no need to send an injunction to the company on this point.

Secondly, as to the health-related tests, the LSA concluded that the data obtained when users take tests on the company's website amounts to personal data concerning health. In the absence of other lawful grounds that can be invoked to allow such processing under Article 9(2)(b) to (j) of the GDPR, the LSA considered that such processing can only be implemented based on the data subject's **explicit consent**. Consequently, the LSA considered that the company breached **Article 9 of the GDPR**. The LSA noted that the company brought this processing activity into compliance over the course of the procedure by introducing a consent checkbox.

Thirdly, regarding the **obligation to inform data subjects pursuant to Article 13 of the GDPR**, the LSA found no violation.

Fourthly, the LSA noted that the controller was jointly liable with an advertising company with regard to processing related to the marketing of advertising spaces on its website, and with another company for the processing using the technical tools and functional structures made available by the latter. The LSA concluded that the company **breached Article 26 of the GDPR** due to the absence of a joint processing agreement within the meaning of this article at the time of the LSA's audits.

Lastly, the LSA considered that the company **failed to implement the basic security measure** that constituted the use of the "HTTPS" protocol or another equivalent security measure. According to the LSA, this characterised a **breach of Article 32 of the GDPR**, as the security measures were not adequate to the risks to the protection of personal data (i.e. health data in this case). Similarly, the lack of security for the storing of users' passwords was also found to constitute a breach of this provision. The LSA noted the controller's subsequent compliance measures, nonetheless recalling that they cannot absolve the controller from its responsibility for past events.

Decision

The LSA noted all the infringements to Articles 5(1)(e), 9(2), 26 and 32 of the GDPR. Taking into account the company's liability, its financial capacity and the relevant criteria of Article 83 of the GDPR (e.g. the high number of people affected; the company's negligence, etc.), the LSA imposed an **administrative fine of 280,000 Euros** with regard to the GDPR breaches and an administrative fine of 100,000 euros (with regard to the breaches set out in Article 82 of the French Data Protection Act). The LSA also decided to publish the final decision on its website and on the Légifrance website for two years, after which the company will not be identifiable anymore.