Summary Final Decision Art 60

Investigation

Compliance order

Background information

Date of final decision:	16 December 2019
LSA:	FR
CSAs:	BE, DE-Rhineland-Palatinate, DK, ES, IT, HU, LU, PL, PT, SE, SK
Legal Reference:	Transparency and Information (Articles 12, 13 and 14), Right to erasure (Article 17), Right to object (Article 21), Security of processing (Article 32)
Decision:	Order to comply
Key words:	Transparency and Information, Right to Erasure, Right to Object, Security of Processing, E-Commerce, Direct Marketing, Children, Consumers

Summary of the Decision

Origin of the case

The LSA conducted two on-site investigations at the controller's premises to audit the controller's compliance with the GDPR and tested the procedure set up by the controller to create an account.

Findings

The controller is a company offering subscription to educational magazines for children. On the basis of the investigation, the LSA found several GDPR infringements. First of all, several breaches of the obligation to inform data subjects, enshrined in articles 12 and 13 GDPR, were identified. No information relating to data protection nor link to the controller's Terms and Conditions was given to the data subjects upon registration or when placing an order. As a consequence, the information was considered to be not accessible enough. The Terms and Conditions did not include any information on the legal basis for processing, on the retention period and on the individual rights to restriction of processing, data portability, or to submit a claim to a supervisory authority. Although the target audience was French-speaking and the website is fully in French, the "unsubscribe" button in the newsletter and marketing emails was hyperlinked to a text in English, asking for confirmation. An additional hypertext link was included in the final page (titled "Clicking here"): this is misleading for the user, as clicking on such link actually resulted in a new subscription.

Secondly, a breach of the obligation to comply with the request to erase data was identified, as personal data was not erased systematically when requested by data subjects although there was no legal requirement to keep it and although users had been informed of the erasure of the data

Last, there was a breach of the obligation to ensure the security of data, concerning passwords, locking of workstations, and access to data. More specifically, the password requirements and methods for processing the passwords were found to be non-compliant with the obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, since authentication was based on insufficiently complex passwords and obsolete hash algorithms. Additionally, the computer used by one of the database's administrators was configured to never automatically lock or go on sleep mode. With regard to access to data, the absence of specific identification (i.e. the use of the same account by several people) made it impossible to ensure access traceability.

Decision

The LSA ordered the controller to comply, within two months of the notification of the decision, with several specific instructions.

First, the controller was ordered to provide full information to data subjects about the processing activities, in an easily accessible manner. Additionally, the LSA ordered the controller to set up a procedure for unsubscribing that is compliant with Articles 12 and 21 GDPR.

Secondly, the controller was ordered to ensure the effectiveness of all requests to exercise the right of erasure.

Last, the authority ordered the controller to take appropriate security measures to protect personal data and prevent access thereto by unauthorised third parties (by setting up a new password policy, avoiding the transmission of passwords in clear text, ensuring that workstations go on sleep mode, and setting up individual accounts).