Summary Final Decision Art 60

Complaint

EDPBI:FR:OSS:D:2023:0753

Administrative fine

Background information

Date of final decision:	03 August 2022
LSA:	FR
CSAs:	AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, EL, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
Legal Reference(s):	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 15 (Right to access by the data subject), Article 21 (Right to object). Article 32 (Security of processing)
Decision:	Administrative fine
Key words:	Electronic communications, Data subject rights, Direct marketing

Summary of the Decision

Origin of the case

Between 2018 and 2019, five complaints were filed with the LSA against the controller, a company specialising in the hospitality sector established in the Member State of the LSA. The complaints concerned the failure to take into account the right to object to the marketing emails sent by the controller. An additional complaint concerned the difficulties encountered in exercising the right of access, in particular to bank data collected by the controller in connection with the reservation of a hotel room. Between 2019 and 2020, the LSA received five more complaints transferred by other SAs, regarding requests to object to the processing of personal data for the purpose of marketing by e-mail and the exercise of the right of access. Following this, the LSA sent a questionnaire to the controller and carried out an inspection. The LSA then submitted a draft decision to the concerned supervisory authorities (CSAs). Following the relevant and reasoned objections raised by a few CSAs, as well as new complaints

against the controller, the LSA resumed the investigation and carried out inspections on the controller's premises. At the end of the investigation, the LSA notified the controller of a report detailing the breaches of the provisions of Articles L. 34-5 of the French Post and Electronic Communications Code (CPCE) and Articles 12(1), 12(3), 13, 15(1), 21(2) and 32 GDPR. The report also proposed the imposition of an administrative fine. The controller presented written and oral observations. Following the adversarial procedure, the LSA send a new draft decision to the CSAs pursuant to Article 60(3) GDPR. The Polish SA raised relevant and reasoned objections which gave rise to a dispute resolution procedure under Article 65(1)(a) GDPR. On 15 June 2022, the EDPB adopted binding decision 01/2022.

Findings

The LSA found several violations of the obligation under French law to obtain data subjects' consent for direct marketing by email (Article L. 34-5 of the French Post and Electronic Communications Code or CPCE). Such obligation stemming from national law was not subject to the cooperation mechanism.

During the investigation, the LSA also established that the controller had violated its **transparency obligations**. More specifically, the forms for creating a customer account or joining the controller's loyalty programme did not contain all the information required by Article 13 GDPR, nor were users invited to take steps to access such information. In addition, when an account was created, access to the controller's "Personal Data Protection Charter" was only possible via a hyperlink available at the very bottom of the website's page, requiring the users to scroll-down and search for it, in disregard of the requirements under Article 12 GDPR. Finally, the controller had indicated that the processing of personal data for marketing purposes was based on "legitimate interest" and "performance of a contract" while marketing also related to the products and services of third parties, in which case consent was required. Thus, the LSA found that the controller breached Article 13 GDPR for not mentioning consent as a legal basis.

The LSA also found that the controller **failed to comply with the obligation to respect the right of access of individuals under Article 15 GDPR**. More specifically, the controller had failed to provide a complainant with a copy of her personal data requested within the time limit set by the GDPR.

The LSA established a **failure by the controller to comply with the obligation to respect the right to object of individuals under Article 21 GDPR** due to the existence of malfunctions in the unsubscribe link in the marketing emails, resulting from technical problems. Consequently, a complainant kept receiving marketing messages from the controller two months after making their request to unsubscribe, while another kept receiving the newsletter for a month despite the deletion of their data in the customer repository. The LSA considered that these anomalies were likely to have prevented a significant number of data subjects from effectively objecting to marketing messages and resulted in a breach of Article 21 GDPR.

Finally, during the LSA's on-site inspection, it became clear that the use of a password consisting of 8 characters containing only two types of characters was allowed to access the tool used to send messages to customers. In view of the volume of data processed by controller, the LSA found that the requirements put in place with regard to the robustness of passwords were insufficient and **did not**

guarantee the security of personal data. In addition, inspections showed that when a customer's account was suspended due to a suspected fraudulent login, the customer service department asked the data subject to provide a copy of his/her identity document in an email attachment. The LSA considered that the practice of transmitting unencrypted data by e-mail created a significant risk to the confidentiality of the data transmitted and established a breach of Article 32 GDPR.

Decision

The LSA found that the controller has violated Articles L. 34-5 of the French Post and Electronic Communications Code and Articles 12, 13, 15, 21 and 32 GDPR. The LSA took especially into account the number of alleged breaches by the controller, the fact that these breaches concerned several fundamental principles of personal data protection and that they constituted a substantial infringement of individuals' rights, the number of individuals concerned and the financial situation of the controller.

Consequently, the LSA imposed an administrative fine of €600,000 on the controller, broke down as follows: €100,000 for the controller's failure to comply with Article L. 34-5 of the French Post and Electronic Communications Code; €500,000 (five hundred thousand euros) for the controller's failure to comply with Articles 12(1), 12(3), 13, 15(1), 21(2) and 32 GDPR. The decision was made public on the LSA's website and on the Légifrance website.

The LSA took into account EDPB Decision 01/2022 instructing the LSA to reconsider the factors on the basis of which it calculated the amount of the fine, in order to ensure that the fine meets the criterion of dissuasiveness laid down in Article 83(1) of the GDPR.