Summary Final Decision Art 60

Legal obligation, complaint

Administrative fine

EDPBI:FR:OSS:D:2021:181

Background information

Date of final decision:	06 January 2021
Date of broadcast:	12 February 2021
LSA:	FR
CSAs:	BE, DE-BE, DE-BY, DE-NI, DE-RP, ES, LU, UK
Legal Reference(s):	Transparency and Information (Article 12), Security of processing (Article 32)
Decision:	Compliance order, Administrative Fine
Key words:	Personal data breach, Data security, Password, Data subject rights

Summary of the Decision

Origin of the case

Following the notification of a personal data breach (intrusion attack on the controller's website affecting 210,692 European nationals), the LSA conducted both an on-site and online audits of the controller in order to verify its compliance with the GDPR, in particular with regard to the aforementioned data breach.

Thereafter, the LSA carried out a second on-site control of the controller in the context of the LSA's investigations regarding five complaints received from customers and prospects concerning the commercial prospecting by the controller they have been subject to, as well as the exercise of their rights.

Findings

The LSA found that the controller did not facilitate the exercise of data subject rights as the email address provided to them for this purpose was defective. In addition, the LSA pointed out the complexity of the right of access procedure implemented by the controller for prospects receiving

postal solicitations. Therefore, the LSA considered that the controller failed to comply with its obligations under Article 12(2) GDPR.

As a result of its investigations regarding the data breach notification, the LSA found that the controller had failed to ensure the security of the personal data it processed (Article 32 GDPR). Firstly, the LSA found that the controller did not ensure the effectiveness of the technical and organisational measures implemented by its processor. In this regard, the LSA concluded that the controller should had been more vigilant in complying with security standards considering that it had already been sanctioned by the LSA for security issues involving this same processor. Finally, the LSA considered that the controller's requirements regarding the robustness of passwords were insufficient to ensure the security of the personal data processed and to prevent third parties from accessing the personal data.

Decision

The LSA imposed an administrative fine of 250,000 euros to the controller.

In addition, the LSA imposed a compliance order on the controller to remedy its breaches of Articles 12 and 32 GDPR with a penalty payment of 500 euros per day of delay at the end of a period of 3 months following the notification of the decision.