Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:ES:OSS:D:2021:239

Background information

Date of final decision:	18 February 2021
Date of broadcast:	23 June 2021
LSA:	ES
CSAs:	All SAs
Legal Reference:	Article 32 (Security of processing), Article 33 (Notification of a personal data breach), Article 34 (Communication of a personal data breach to the data subject).
Decision:	Administrative fine
Key words:	Personal data breach, Hacker-attack, Data security

Summary of the Decision

Origin of the case

The controller, a company owning a web platform, was hit by several cyber-attacks from an unidentified third-party who accessed to its database hosted on the platform of a cloud service provider. On 29 June 2018, the controller notified the LSA of a first cyber-attack, which occurred on 27 June 2018 and resulted in the unauthorized access to the personal data of 232,766 customers residing in more than 170 countries (comprising almost all EU countries). On 27 July 2018, the controller notified to the LSA a second data breach, which occurred on 25 July 2018, and resulted in the unauthorized access of the usernames and email addresses of 2,892,786 account holders. In response to these data breaches, the controller implemented several technical and organisational corrective measures.

Findings

Following the notification of the two data breaches, the LSA initiated investigations into a possible breach of Articles 32, 33 and 34 GDPR by the controller.

As a result of these investigations, it was found that the controller failed to implement up-to-date technical and organisational security measures taking into account the degree of risk of the processing activities carried out. Considering that these security deficiencies were to a large extent responsible for the occurrence of the above-mentioned incidents, the LSA ruled that the company infringed Article 32(1) GDPR (Security of processing).

Nonetheless, the LSA pointed out that the company notified the breaches in accordance with its obligation under Article 33 GDPR (Notification of a personal data breach).

Finally, in light of the studies provided to it regarding these incidents, the LSA concluded that there was no high risk to the rights and freedoms of natural persons that would require informing data subjects in accordance with Article 34 GDPR (Communication of a personal data breach to the data subject).

Decision

The LSA imposed an administrative fine of 100,000 euros on the controller for having infringed Article 32(1) GDPR.