Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:NL:OSS:D:2020:173

Background information

Date of final decision:	10 December 2020
Date of broadcast:	11 December 2020
LSA:	NL
CSAs:	All SAs
Legal Reference:	Notification of a personal data breach to the supervisory authority (Article 33)
Decision:	Administrative fine
Key words:	Personal data breach, Administrative fine

Summary of the Decision

Origin of the case

On 7 February 2019, the service provider of an online platform notified to the LSA a personal data breach that it had discovered on 10 January 2019. The controller indicated in its notification that an unknown third party had gained access to personal data in the controller's reservation system which are used by the platform's partners to manage the reservations. As a result, the personal data of various data subjects who had made reservations via the controller's platform were compromised.

The LSA commenced an investigation on the controller's compliance with Article 33(1) GDPR.

Findings

During its investigations, the LSA found that the controller had been informed on 8 January 2019 by one of its partners that, following a possible personal data breach in the reservation system, an unknown third party had contacted customers and pretended to be affiliated with the controller, once as employee of the controller and other times as an employee of one of the partner organisations on the platform. The LSA noted that the controller received two similar complaints from the same

provider on 13 January 2019 and 20 January 2019; and that on 20 January 2019, a second partner reported the same type of incident.

The LSA noted that, despite the reports about these several incidents, the controller's entity in charge of the receipt of these incidents did not notify the controller's security team until 31 January 2019. After having conducted investigations, the controller's security team informed the controller's privacy team on 4 February 2019.

In view of the circumstances in which the incidents were reported to the controller by the partners, the LSA found that the controller was deemed to have knowledge of the personal data breach at least on 13 January 2019, as the information given by the partner indicated with a reasonable degree of certainty that personal data had been compromised. As a result, the LSA pointed out that the controller should have notified the LSA of the personal data breach by 16 January 2019 at the latest. It is an established fact that the controller only made this notification on 7 February 2019, i.e. 22 days too late. The same applies if 20 January 2019 should be adopted as the starting date, then the notification was done 15 days too late compared to the deadline of 72-hour set out by Article 33(1) GDPR.

In response to the arguments put forward by the controller, the LSA recalled that the fact, that the delay in notifying the data breach was due to a failure by a single part of the controller's organization to report the incident to the security team in accordance with the controller's internal procedure, is without effect. The LSA also stressed that, by choosing to carry out in-depth investigation instead of a notification in phases, the controller did not comply with the rules laid down in Article 33(3) GDPR.

The controller had informed and advised the data subjects about taking measures to reduce the potential damage. The controller had also declared itself willing to compensate any damages (suffered or to be suffered) by the data subjects. The controller also immediately informed its affected partners and placed warnings on the website.

Decision

According to the 2019 Fining Policy Rules adopted by the LSA, the basic fine for the infringement of Article 33(1) of the GDPR was set at € 525,000. In view of the actions taken by the controller to mitigate the damage of the data subjects resulting from the breach, the LSA decided to reduce the basic amount of the fine by € 50,000 in accordance with Article 7(c) of the 2019 Fining Policy Rules adopted by the LSA. The LSA did not find any reason to increase or decrease the basic amount of the fine on the basis of other circumstances.

In the view of the above, the LSA imposed on the controller an administrative fine of € 475,000 for the infringement of Article 33(1) GDPR.