Summary Final Decision Art 60

Legal obligation

No infringement

EDPBI:HU:OSS:D:2020:116

Background information

Date of final decision:	N/A
Date of broadcast:	23 June 2020
LSA:	HU
CSAs:	AT, DE, IT, SI, SK
Legal Reference:	Personal data breach (Articles 33 and 34)
Decision:	No infringement
Key words:	Data breach, Electronic communications, Employment, Identity theft, Spam

Summary of the Decision

Origin of the case

The controller informed the LSA of the personal data breach.

Findings

An attacker had gained access to an employee's email account, and therefore the contact information of approximately 800 colleagues. The attacker was able to log in via an online email application. In response, the controller's cyber defence centre initiated its standard investigation and response process to contain the incident and understand the scope of the event.

The controller's group network and system infrastructure was not compromised as the attack was limited to one email account. The forensic review conducted by the by the controller determined that the attacker viewed only a part of the contact list. It is understood that the attacker tried to send out numerous emails. This spam campaign had had very limited impact due to the fact that the controller's email infrastructure only permits a small number of emails to be sent during a given time period. Following the detection of the attack, an internal e-mail was sent by the controller, informing colleagues of the phishing campaign.

The compromised email account was disabled. A rollout of multifactor authentication is currently underway which will give an elevated level of security.

Decision

Based on the circumstances of the case and the measures adopted by the controller before and after the data breach occurred, the LSA concluded that the controller had fulfilled its obligations under the GDPR, and the procedure did not reveal any reasons to open administrative proceedings.