Summary Final Decision Art 60

Legal obligation

Reprimand to controller

EDPBI:DEBE:OSS:D:2020:114

Background information

Date of final decision:	10 June 2020
Date of broadcast:	16 June 2020
LSA:	DEBE
CSAs:	All SAs
Controller:	EyeEm Mobile GmbH
Legal Reference:	Personal data breach (Articles 33 and 34)
Decision:	Reprimand to controller
Key words:	Consumers, Data breach, E-commerce

Summary of the Decision

Origin of the case

The case originated from a data breach notification. The controller was made aware of the breach through a media report that there had been a cyberattack on their platform. According to the media report, user's personal data was obtained without authorisation and was being sold on the dark net. The personal data included names, email addresses, user account data and encrypted passwords.

Findings

As part of the measures taken to address the data breach as reported to the LSA, an external security auditor identified two possible security vulnerabilities. The vulnerabilities included an outdated OpenVPN server version and open SSH ports, which probably enabled the attack that caused the data breach.

Decision

The reprimand is based on Art 58(2)(b) GDPR. According to Art. 32 GDPR, a controller must implement appropriate technical and organisational measures to ensure a level of protection appropriate to the risk. By using insufficiently updated software and an insufficiently secured configuration of IT systems, these requirements were not met.

Taking the specific circumstances of the facts determined into account, a reprimand was considered appropriate following the completion of the investigation. This is the controller's first Art 32 GDPR violation and it has now resolved the security vulnerabilities.