Summary Final Decision Art 60

Investigation

Administrative fine

EDPBI:LT:OSS:D:2021:298

Background information

Date of complaint:	N/A
Date of final decision:	29 November 2021
Date of broadcast:	29 November 2021
LSA:	LT
CSAs:	DE, IT, FR, NO, ES, DK, LV, SE, EE, NL, RO, BE, FI, PL, IE, HU, EL, LU, CZ, PT, SK, AT, CY, HR, MT, SI
Legal Reference(s):	Article 24 (Responsibility of the controller), Article 32 (Security of processing), Article 33 (Notification of a personal data breach to the supervisory authority), Article 34 (Communication of a personal data breach to the data subject).
Decision:	Administrative fine
Key words:	Data security, Personal data breach, Publicly available data

Summary of the Decision

Origin of the case

The LT SA started inspections on its own initiative upon receiving information that personal data of 110 302 customers of the controller (among which 433 residing in other EU countries), including personal identification numbers, had been made publicly available. The LSA subsequently received a data breach notification and additional information from the controller. The case was opened on the basis of a motion for imposition of an administrative fine sent by the LSA to the controller on 25 May 2021. The motion established that the personal data made public had been received from the backup copy of a database stored in the controller's online storage without protection. The unprotected database had been created on 27 February 2018, meaning that the breach had existed from this date until 16 February 2021 when the controller suspended external access to the database, hence the applicability of the GDPR to the case. The controller provided clarifications with regard to the motion, alleging procedural irregularities, including unreasonable extension of the investigation, improper definition of the GDPR applicability to the case, direct non-application of ISO/IEC 27002:2017 and factual errors, all of which the LSA considered and responded to in its final decision.

Findings

Analysis of the data stored in the database showed that personal data (name, address, telephone number, e-mail address, personal identification number, driving licence number, type of payment card and the last four digits of the card number, the date of expiration of the payment card and the user identifier (token) in Braintree) had been stored in open text without encryption, and the passwords in the database encrypted with SHA-1 had been weak and unsafe. The controller had failed to purchase additional log record services for the database which made it difficult to determine when and how many times customer data had been misappropriated. The LSA established that the controller had performed post-breach security analysis (audits of firewalls, access rights, testing systems etc.) in accordance with Article 33(3) GDPR, but had failed to comply with the requirements of Article 32(1)(a) and 32(1)(b) of the GDPR: the controller had failed to ensure proper access control and restrictions, thus enabling third parties to access the file containing personal data without authorisation, had failed to ensure confidentiality of data stored in such file, as well as to record and store log records of access to and actions with the file.

In addition, the controller had not ensured proper management and control of the security of personal data, had not appointed a competent person responsible for security and risk management, had failed to segregate the duties and limits of responsibilities in the area of IT creation and maintenance from those in the area of cyber security, and had not ensured recording, monitoring and assessment of access to and actions with the file. For these reasons, the LSA found that the controller had not complied with the requirements of Article 24(1) and Article 32(1)(d) of the GDPR. As a result, the personal data breach had created a risk to the rights and freedoms of natural persons, such as possible identity fraud, unlawful tracking, social engineering and others.

Decision

In light of the above, the LSA decided to impose on the controller an administrative fine of EUR 110,000.