REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Article 60 Final Decision

Ours: [redacted]2025

Reprimand and Notice of termination of the proceedings concerning the protection of personal data

Estonian Data Protection Inspectorate (DPI) received a notice from [redacted] (reg.nr [redacted], Data Controller, the Company) regarding a personal data leak on 24.07.2024. The report revealed that the company became the victim of a cyber attack, as a result of which the attacker was able to access the data of the company's [redacted] (in the course of the investigation it was established that the data of [redacted]persons were leaked), which were stored in the system of [redacted], Data Processor). The attacker was likely able to access the data [redacted] of the Data Controller.

According to the information available to DPI, some of the personal data leaked were for sale on the dark web. The Data Controller also submitted a criminal offence report on [redacted] 2024 to the Police and Border Guard Board, however the proceedings were not initiated.

Estonian Data Protection Inspectorate initiated supervisory proceedings on the basis of Section 56(3)(8) of the Personal Data Protection Act.

Data Controller´s and Data Processor´s explanations

The Data Controller [redacted] in cooperation with the [redacted]., In the course of this, personal data of [redacted] are collected and stored through the system of the service provider - the Lithuanian company [redacted] provided a video-based [redacted] for the Data Processor to meet regulatory requirements for [redacted]. When registering via the [redacted] domain, the [redacted] was redirected to [redacted]s website, where the camera recorded the person’s photo and captured the document.

The company was the victim of a hacker attack, as a result of which the attacker gained access to the data of [redacted] stored on the [redacted] system of the service provider. Access was gained using an email account [redacted] in the [redacted]’s web interface used the to gain access. According to the Data Processor's explanations, the malicious person [redacted]. The following data was stored in the database: name, surname, gender, date of birth, nationality, personal identification code, document number, date of issue of the document, date of expiry of the document, e-mail address, phone number, IP address, browser data, document photo, face photo. The Data Controller informed the persons concerned by the infringement by e-mail (citizens of

the European Union and third countries - Ukraine, South Africa, Israel and others).

Personal data processing contract was concluded between the Data Controller and the Data Processor. During the procedure, the Data Controller explained that the source of the data leak was a database under [redacted]'s (the Processor) administration, which was not managed by the Controller. The Data Controller had access to a web interface containing a list of forms and [redacted], including rotation and encryption, were not managed by the Controller, but were under [redacted]'s administration.

Since the Data Processor ([redacted])is a Lithuanian company, DPI approached the Lithuanian Data Protection Authority during the course of supervisory procedures in order to establish the liability of [redacted] in the infringement case. [redacted] explained that it was involved in the infringement only to the extent that the Data Controller decided to store the data in a [redacted] managed by the Data Processor. Ondato ensured the provision of secure solutions, including the [redacted] of the Controller, as well as the security of the data itself during the storage and transmission of information [redacted]. However, the Data Processor could not be responsible for the Data Controller disclosing [redacted] and thereby jeopardising the security of personal data - personal data became available to the intruder (as a result of a breach of personal data security).

The Data Processor explained that the attacker entered the [redacted] system using the Data Controller's account ([redacted]), for which the [redacted] had to have been obtained from the Controller, as only the Controller knew this information. With this data, [redacted] and used it to log into the Controller's account in the [redacted] system.

[redacted] noted that, in accordance with the requirements of the ISO 27001 standard (the information security management system of the authorised Data Processor is certified on the basis of ISO 27001) and as part of the continuous improvement of information security measures, [redacted] is constantly implementing new technical and organisational data security measures. Therefore, [redacted] informed all [redacted] (including the Data Controller) that as of [redacted], [redacted]. Previously, such functionality was only applied to [redacted] who integrated their [redacted] management system into the data controller's system and specifically requested the use of such a technical measure. Given the time of the data breach in question (a mass review of the data by a malicious person took place between [redacted]), it is expected that a malicious person who knew that [redacted] and who had [redacted]) that only the Data Controller knew, set up a [redacted] for [redacted], thereby impersonating the Controller.

According to [redacted], it could be reasonably assumed that the malicious actor realised that such actions would soon be detected by the Controller's employees or other authorised persons who have been granted access to that [redacted] account, since they would not be able to [redacted]. Consequently, the malicious person probably carried out a mass review of the personal data in order to scan or review as much data as possible. Thus, [redacted] established that the infringement was not caused by [redacted]'s actions, but by the disclosure of the Controller's [redacted] by the data controller, which enabled a malicious actor to access the personal data stored in the data controller's information system.

The Controller on the other hand explained that the company's technical specialists carried out an in-depth analysis on the basis of the materials provided and found that it was technically impossible to determine without [redacted]

[redacted]) was leaked through [redacted]'s account or through an email account on [redacted]'s [redacted]. The information provided was not conclusively sufficient to draw conclusions. According to the Data Controller's explanations, [redacted] are used in accordance with the applicable standards, including [redacted]. According to the Controller, it is not possible to determine with certainty whether and how [redacted] was added to [redacted]s account on the device of a malicious person.

The Data Controller is PCI DSS certified and the company has organised trainings for employees to prevent possible cyber attacks and prevent security vulnerabilities, which are carried out regularly [redacted]. In order to avoid similar incidents and reduce risks, the Controller has reduced the number of employees involved in the processing of personal data, and at the same time stopped cooperating with [redacted].

The position of Data Protection Inspectorate

According to the principles of personal data processing, it must be ensured that personal data are processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing (Art. 5 (1) (f) GDPR). The controller is responsible for this (Article 5(2) GDPR). Pursuant to Article 32 GDPR, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the nature, scope, context and purposes of the processing of personal data, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. According to GDPR recital 75, risks to the rights and freedoms of natural persons of varying likelihood and severity may arise, inter alia, from the processing of personal data revealing racial or ethnic origin where the processing involves a large amount of personal data and affects a large number of data subjects.

If a processor is used for processing, the controller shall only use processors who provide sufficient guarantees that the processing will meet the requirements of the GDPR and ensure the protection of the rights of data subjects (Art. 28 (1) GDPR).

On the basis of the information provided to the DPI by the Controller and Processor, it is not possible to determine with certainty whether the personal data leakage happened due to shortcomings in the activities of the Controller or Processor. The Controller has not been able to technically establish how the [redacted]) became possible through which the malicious person entered the system. The explanations provided by the Controller also showed that the Processor did not sufficiently cooperate with the Controller in the investigation of the case and the identification of its causes. However, on the basis of the explanations provided by the Processor, it cannot be concluded that the security measures implemented by the Processor were not sufficient to protect the systems from unauthorised access. The processor's information security management system has been certified on the basis of ISO 27001 and, as part of the continuous improvement of information security measures, [redacted] continuously implemented new technical and organisational data security measures, [redacted] 2024.

Although it is not possible to reach a final conclusion on whether the breach was caused by an error on the part of the Controller or Processor on the basis of the explanations provided by the Controller and Processor, the ultimate responsibility for ensuring the security of personal data rests with the Controller of personal data, i.e. [redacted] The Data Controller offers the service of [redacted] in the European Union and also outside the European Union, thus the Data Controller is in possession of a large number of [redacted]' personal data and is responsible for the security of this data. Since the breach was made possible by the [redacted] held by the Data Controller, it is clear that the measures applied were not sufficient to prevent large-scale personal data leakage.

Therefore, [redacted] breached the requirements of Article 5(1)(f) and Article 32 of the GDPR. The technical and organisational measures used to process personal data were not sufficient to ensure a level of security appropriate to the risk and resulted in individuals losing control over their data.

Taking into account that the Data Controller has cooperated with the DPI, notified the data subjects concerned of the breach, [redacted], the DPI **will terminate the supervisory procedures. Based on the above and based on Article 58(2)(b) GDPR, Estonian Data Protection Inspectorate issues a reprimand to [redacted] because the Data Controller has violated the requirements of the processing of personal data.**

Lugupidamisega

[redacted]
Lawyer