REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

FOR INTERNAL USE
Holder of information: Data Protection Inspectorate
Notation made: [redacted].2023 The access restriction shall be valid until [redacted] 2028 p 2 until the entry into force of the decision Base: AvTS § 35 lg 1 p 18(2), AvTS § 35 lg 1 p 2

Unofficial translation

Our: [redacted] 2023 nr [redacted]

[redacted]

Final decision

Reprimand and notice of termination of proceedings in the case of personal data protection

[redacted] (hereinafter [redacted]) submitted a pre-notification to the Data Protection Inspectorate on [redacted], according to which on [redacted] it became known that there is a security weakness in [redacted], which allows to [redacted]. [redacted] immediately contacted its IT support partner [redacted] (hereinafter [redacted]) and asked for [redacted] to be checked. It was discovered that the [redacted] It follows from the data collected that someone made an automated solution that [redacted]. [redacted] detected that the same user has tried to change [redacted]. For example, [redacted] has tried to [redacted] and tried to [redacted]. Nothing happened because the necessary security measures have been put in place.

On [redacted], [redacted] submitted a final infringement notification in which it was further explained that it follows from the facts of the infringement that an automated solution was made to [redacted].

[redacted] immediately made changes to the [redacted] on the same day ([redacted]) following the detection of a security weakness, as a result of which it is no longer possible to see [redacted] (including by [redacted]). As a result of the update, only [redacted] will be stored on the server and only [redacted] can be viewed.

[redacted] has explained that the [redacted]. The [redacted] shall be presented only in a [redacted]. The [redacted] in detail.

The third party had access to [redacted] from [redacted] and [redacted].

With regard to leaked data, [redacted] is both a controller and a processor.

[redacted] has informed all data subjects of the breach. Notifications were sent on [redacted] and [redacted].

[redacted] has explained on [redacted] that the data became available to the person as a result of his or her own active attack and search for security weakness, including the automated solution for [redacted]. [redacted] also submitted an [redacted] in connection with the incident.

On [redacted], [redacted] has stated that it will develop the following additional technical security measures:
(a) ID-based identification of [redacted] – when [redacted], the person must first identify himself/herself using an ID-card, Smart-ID or Mobile-ID.
(B) [redacted]

On [redacted], [redacted] has confirmed that additional security measures have been implemented. All [redacted] have been replaced by [redacted]. The [redacted] has been chosen on the basis that it is [redacted], and it is [redacted]. An [redacted]

[redacted] has explained that these measures have a higher level of security than the [redacted] and that, at the same time, ID-based authentication tools with the highest level of security are currently not equally available to all [redacted]. In choosing the security measures to be implemented, [redacted] proceeded on the basis that they would be as universal and unambiguous as possible for users at different levels and locations, without significantly reducing the availability of services to customers to whom [redacted] has obligations arising from previously concluded contracts.

Position of the Data Protection Inspectorate

According to Article 24(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), the controller implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, considering the nature, scope, context and purposes of the processing of personal data, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. Pursuant to Article 32(1) of the GDPR, the controller must implement appropriate technical and organisational measures to ensure the level of security appropriate to the risk, including ensuring the continuing confidentiality, integrity, availability and resilience of systems and services processing personal data.

The same obligation arises from the principles governing the processing of personal data, namely Article 5(1)(f) of the GDPR, according to which personal data must be processed in a manner that ensures their appropriate security and protects against unauthorised or unlawful processing.

[redacted] had not put in place adequate safeguards for the protection of personal data for [redacted], as an unauthorised person had the possibility to access [redacted].

In order to ensure security and prevent processing in breach of the GDPR, the controller must assess the risks associated with the processing and implement measures to mitigate those risks, such as encryption. Considering the latest scientific and technological developments and the costs of implementing the measures, those measures should ensure an appropriate level of security, including confidentiality, commensurate with the risks and the nature of the personal data to be protected. When assessing the risk of data security, consideration should be given to the risks arising from the processing of personal data, such as accidental or unlawful destruction, loss, alteration and unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, which may, in particular, result in physical, material or intangible damage.[1]

No one is protected from cyberattacks, but in order to prevent it, the data controller must ensure the security of the information systems and the systems must be regularly monitored to identify any risks that may have arisen. In the case of this incident, a data leak would have been avoided if additional security measures had already been applied to access to [redacted] in the past.

The Data Protection Inspectorate makes a reprimand to [redacted] on the basis of Article 58(2)(b) of the GDPR, because the processing operations of personal data have violated the requirements of the General Data Protection Regulation (Article 5(1)(f), Article 32 of the GDPR).

Since [redacted] has taken additional measures to ensure the requirements for the protection of personal data set out in the GDPR, the Data Protection Inspectorate terminates the supervision proceedings.

Best regards

[redacted]
Lawyer
authorized by Director General

[1] GDPR recital 83