ANDMEKAITSE INSPEKTSIOON

Unofficial translation

Ours: [redacted].2024 nr [redacted]

ARTICLE 60 FINAL ADOPTED DECISION

Notice of termination of proceedings in the case of personal data protection

On [redacted] (registry code [redacted]) submitted a personal data breach notification to the Estonian Data Protection Inspectorate (DPI), [redacted].

According to the data breach notification, the Estonian DPI received a final notification, but it was noted that [redacted] was investigating the incident and its scope further. Therefore, on the basis of Section 56(3)(8) of the Personal Data Protection Act, the Estonian DPI initiated a supervision proceedings.

The persons affected by the infringement, broken down by country, are: [redacted]. The Estonian DPI initiated the procedure for the designation of the lead supervisory authority under Article 56 of the GDPR. Since [redacted] is a company operating in Estonia, the leading supervisory authority in the supervision proceedings is the Estonian DPI.

According to the breach notification, [redacted] received on [redacted] an [redacted]

Tatari 39, 10134 Tallinn
Registry code 70004235
Telephone 627 4135
E-mail info@aki.ee
www.aki.ee

[redacted] informed all data subjects (in total [redacted]) of the breach. The notification was sent on [redacted] The violation was also reported to the Estonian Financial Supervision Authority.

[redacted] explained that the investigation of the incident led to the conclusion that the incident occurred [redacted]. The investigation did not establish that the attack was directly directed against the software and security systems implemented by [redacted]. In addition, [redacted] developed a plan of measures to prevent potential personal data breaches in the future:

- [redacted] has started moving [redacted] The final transition is planned for the first quarter of 2024 at the latest. [redacted]
- [redacted] by customers to automatically inform customers of changes in their current [redacted] practices so that they can prevent malicious use of personal data if necessary.

[redacted] also explained that all persons affected by the incident used [redacted] to access the [redacted] platform, [redacted]. By using the personal information obtained during the attack [redacted], the attacker managed to obtain access to the personal data of the client of [redacted] This was confirmed by the analysis of the system logs and the investigation carried out. However, it is not known how the attacker got access [redacted]. During the investigation of the incident, [redacted] asked for this information from its customers, but did not receive any relevant answers.

Estonian DPI's opinion

According to Article 24(1) of the General Data Protection Regulation (GDPR), the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate the processing of personal data in accordance with the GDPR, taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. Article 32(1) of the GDPR requires the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including ensuring the continued confidentiality, integrity, availability and resilience of systems and services processing personal data. According to Article 32(2) of the GDPR, the assessment of the necessary level of security shall take into account, in particular, the risks arising from the processing of personal data, in particular the accidental or unlawful destruction, loss, alteration and unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

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.

Under Article 4(12) of the GDPR, 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In accordance with Article 31 of the GDPR, the controller shall cooperate, on request, with the supervisory authority in the performance of its tasks.

[redacted] has cooperated with the Estonian DPI in responding to inquiries and conducting an investigation to identify a potential weakness of the software and security systems implemented by [redacted], which has not been confirmed. Thus, it has not been confirmed in the course of the supervision proceedings that personal data processing operations of [redacted] have violated the requirements of the GDPR (in particular Article 5(1)(f), Article 32 of the GDPR). This means that there has not been identified security breach by [redacted], which would have resulted in a personal data breach. In addition, [redacted] has proposed additional measures to make its systems safer and to prevent personal data breaches.

Based on above, Estonian DPI will terminate the proceedings.

With respect

[redacted]
lawyer
authorized by Director General