



ANDMEKAITSE INSPEKTSIOON

FOR INTERNAL USE ONLY

Information holder: Data Protection Inspectorate

Entry made: [REDACTED].2026

Access restriction valid until: [REDACTED].2031,

in part 2 until the decision enters into force

Basis: Public Information Act § 35 (1) p 2, § 35 (1) p 18 (2)

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED].2026 no [REDACTED]

Reprimand and termination of supervisory proceedings

The Estonian Data Protection Inspectorate (AKI) conducted supervisory proceedings in relation to a personal data breach notification stating that an intrusion had occurred into the database of [REDACTED], which contained data of approximately 1800 patients, including around 250 foreigners. The affected data categories included: name, personal identification code, contact details, and health data.

According to the breach notification and additional information received through AKI's inquiries, the breach was discovered on [REDACTED].2025, when the company's information system [REDACTED] could no longer be used. This was a ransomware attack during which the data and backups of the [REDACTED] database on the server were encrypted. The encrypted data were not downloaded.

The processor immediately notified the relevant state authorities, including CERT-EE and the police, who initiated criminal proceedings. CERT-EE managed to partially restore the encrypted data, but a large portion of the data remains inaccessible.

Explanations of the data processor

"The server has now been shut down and we are using [REDACTED]'s server service, to which data from previous backups and data collected from other healthcare databases have been transferred."

"/.../"

"There are no log entries indicating that data was downloaded, and therefore there is no reason to believe the data have leaked. The data are also not present on the server in a human-readable format, but rather as database tables. Even if some data were theoretically copied, they could not be used

without the database engine, which would require copying the entire computer contents—something for which there would not have been time between the occurrence and discovery of the incident.”

“/.../”

“At present, not all individuals have been notified because the police have initiated proceedings to investigate the matter. It is also not known that the attack poses a risk to the rights and freedoms of data subjects. At this stage of the investigation, there is no indication that the data have leaked or become accessible to third parties. Patients are informed during appointments if missing data impede their treatment.”

“/.../”

“We now store the database on [REDACTED]’s server, which is no longer located on the premises of the [REDACTED], and [REDACTED] will henceforth be responsible for its security and backups. External access to the company’s internal network has been closed. An agreement has been made with a company that will additionally assess the security of the information system.”

Position of the Data Protection Inspectorate

1. The central requirements and principles of personal data processing derive from Article 5 of the General Data Protection Regulation (GDPR), which provides, among other things, that personal data must be processed lawfully, for specific purposes, minimally, and transparently.
2. In addition, fulfilling the GDPR’s fundamental principles requires that personal data be processed in a manner ensuring their appropriate security—protection against unauthorised or unlawful processing and accidental loss, destruction, or damage.
3. In this case, the incident constituted primarily a threat to the confidentiality and availability of personal data, which created a risk that individuals (patients) could have had their health data accessed by persons with no legal basis. Additionally, the risk materialised that the data would no longer be available to the data subjects or the processor, which could hinder the provision of healthcare services and affect service quality. Although healthcare providers are obliged to document services in the national health information system, meaning most data also exists there, this only partially mitigates the availability issue. Additional data stored in the processor’s database may not be included there, meaning that their loss or temporary inaccessibility may still negatively affect patients.
4. Therefore, protecting individuals’ rights and freedoms in personal data processing requires the implementation of appropriate technical and organisational measures to ensure compliance with the GDPR. When planning and implementing security measures, the state of technological development, implementation costs, the nature and scope of processing, and the risks that may arise from data processing must be taken into account. Relevant risks include accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to transmitted, stored, or

otherwise processed personal data—a situation that may result in harm to individuals (GDPR Art. 32).

5. Furthermore, health data processing carries a higher privacy risk and increases the potential threat to individuals' rights and freedoms. Misuse of such data may have serious consequences, such as extortion.
6. The GDPR does not prescribe exact security measures but requires each controller to determine appropriate measures. Basic IT security measures include keeping software updated, using antivirus protection and firewalls, managing access rights, applying password policies, and maintaining logs and monitoring. More specific cybersecurity requirements are provided in the Cybersecurity Act, which also applies to [REDACTED]. Compliance is supervised by the Information System Authority.
7. At this point, the processor has established that the data have not leaked and has eliminated the possibility of later access by the attacker (the server has been disconnected). The processor has also implemented measures to prevent similar incidents and plans to commission an information security audit. We strongly recommend reviewing and updating all data protection and information security procedures in light of the incident.
8. Additionally, we note that under GDPR Art. 34, data subjects must be notified of an incident if it is likely to pose a high risk to their rights and freedoms. The processor has stated that patients are informed during appointments if missing data impede their treatment.
9. We agree that immediate general notification to all data subjects is not proportionate, as the risk does not materialise uniformly for all. However, notification must be provided if it becomes apparent that specific health data of a patient cannot be used and this affects or may affect the quality of care.
10. When notifying data subjects, a short and clear explanation must be provided of what happened, what categories of data were affected, and what the potential consequences may be for their rights and freedoms. The notification should describe the measures implemented to contain the incident and prevent further risks, what the data subject can do if they have questions or wish to provide additional information, and whom to contact for further details. The notification must also remind individuals of their rights, including the right to request additional information or lodge a complaint with the supervisory authority.

Based on the above, [REDACTED] violated the GDPR by processing health data in a manner that did not ensure their confidentiality and availability. In particular, the

requirement of confidentiality under GDPR Art. 5(1)(f) was not met—the security of personal data processing was not ensured.

The Data Protection Inspectorate also takes into account that the processor has cooperated fully and taken measures to prevent recurrence.

Pursuant to GDPR Art. 58(2)(b), the Data Protection Inspectorate issues a reprimand to [REDACTED] and terminates the supervisory proceedings.

The recipient may challenge the reprimand and termination notice within 30 days by submitting an appeal under the Code of Administrative Court Procedure to an administrative court.

Respectfully,
Digitally signed

[REDACTED]

Lawyer
Authorised by the Director General