



**REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE**

FOR INTERNAL USE

Holder of information: Data Protection Inspectorate

Notation made: [REDACTED] 2026

The access restriction shall be valid until: [REDACTED] 2031, with regard to point 2, until the decision enters into force,

Legal ground: Public Information Act § 35(1)(18)(2), Public Information Act § 35(1)(2).

SA Latvia
SA Lithuania
SA Poland

Ours: [REDACTED]

All CSA-s

Article 60 Final Decision

Admonition and Termination of Supervisory Proceedings

The Estonian Data Protection Inspectorate (hereinafter the Inspectorate) received on [REDACTED] 2025 (registered in the Inspectorate's document register on [REDACTED] 2025) a personal data breach notification, according to which [REDACTED] (hereinafter [REDACTED]) was using copies of production environment data in its test environments. These copies contained personal data of employees of the [REDACTED] and their relatives, including special categories of personal data.

On the basis of § 56(3)(8) of the Personal Data Protection Act, the Inspectorate initiated supervisory proceedings.

In order to clarify the circumstances of the breach and the corrective measures taken, the Inspectorate submitted inquiries to [REDACTED] on [REDACTED] 2025 and [REDACTED] 2025. The controller responded on [REDACTED] 2025 and [REDACTED] 2025, respectively.

Explanations Provided by the Data Controller

According to the controller's explanations, the breach was discovered through an audit in which the [REDACTED]'s IT auditor also participated. Within the framework of an identity and access management audit, it was identified that the test environments of the applications [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED] had (likely for an extended period) been using copies of production environment data containing personal data of both current and former employees of the [REDACTED] and their relatives, including special categories of employee personal data (health examination information).

The personal data in the test environment had not been anonymised or pseudonymised.

The breach affects:

- In Estonia: 27,500 employees (current and former), 17,800 employees' children, and 8,800 employees' contact persons;
- In Latvia: 180 employees, 160 children, and 50 contact persons;
- In Lithuania: 160 employees, 80 children, and 90 contact persons;
- In Poland: 70 employees, 50 children, and 30 contact persons.

The personal data processed in the test environment included employee names, personal identification codes, gender, employee numbers, identity document details, photographs, education data, and health examination information (including clinic name and conclusions such

as fitness for work or need for glasses). Contact details included personal addresses, work and personal email addresses, and telephone numbers. Employment-related information included organisational unit, job title, workplace address, cost centre code, bank account number, and salary calculation basis.

For children, the processed data included name and personal identification code or date of birth. For contact persons, the processed data included name and type of contact person (spouse, parent, other).

Regarding notification of data subjects, ██████████ explained that the Data Protection Officer informed the organisation of the need to notify data subjects. Information about the incident was communicated through the ██████████'s weekly management information circulation and published in the intranet under the "██████████ Weekly Overview" section, accessible to employees in all countries in Estonian, English, and Russian.

Corrective Measures

██████████ outlined the planned measures intended to be implemented in order to prevent the occurrence of similar incidents in the future. The initial actions, consisting of the deletion and anonymisation of data, were carried out within the first two weeks. The further plan is to develop a test environment framework to be applied across the entire organisation. This framework also includes the development of policies governing the use of data in test environments, specifically addressing the principles of personal data processing within such environments. In addition, a data anonymisation tool will be introduced in order to enable testing to be conducted using anonymised data in test environments. The entire framework, together with the tool, is planned to be implemented no later than by the end of the third quarter of 2025. As of the date of this decision, ██████████ has developed a framework/regulation establishing the principles for handling data in test environments, including the applicable roles and responsible persons, methods, and standards across the organisation. According to input provided by the Head of the IT Development Department of ██████████, the principles and requirements set out in the regulation have already been followed by all development teams since the incident occurred, and guidance on data obfuscation has been issued across all teams. The development teams have reviewed and analysed the principles of data obfuscation and, where necessary, have identified case-specific solutions for generating test datasets.

According to ██████████'s explanation, access to the test data was granted to two IT developers, as well as to ██████████ employees who held similar access rights in the production database. In order to mitigate potential adverse effects on data subjects, the ██████████ is prospectively modifying its testing practices and has communicated a clear message to all parties involved in testing regarding the prohibition of using personal data for testing purposes. Given that personal data in the test environments were deleted or anonymised, and that other improvement practices are being implemented, the ██████████ is thereby reducing the associated risks through the aforementioned measures. The use of the test environment was suspended immediately upon discovery of the breach. Thereafter, the personal data were deleted or anonymised, and the breach has ended. In addition to the measures described above, a root cause analysis of the incident is currently ongoing within the ██████████, with the aim of clarifying the underlying circumstances of the event and preventing the recurrence of similar situations in the future.

According to ██████████'s explanations dated ██████████ 2025, a new regulation on data handling in test environments has been prepared, harmonising the principles, roles, responsibilities, and standards across the entire ██████████. The Management Board will approve the regulation on ██████████ 2025. The Head of IT Development confirmed that the requirements set out in the regulation have already been applied by the development teams following the incident, and that guidance on data obfuscation has been provided to all teams.

Position of the Data Protection Inspectorate

1. The requirements applicable to the processing of personal data are governed by the General Data Protection Regulation (hereinafter the GDPR)¹. The fundamental principles of the GDPR include lawful, fair and transparent processing of data, purpose limitation, data minimisation, accuracy, storage limitation, and the security of processing (GDPR Article 5(1)). The data controller is obliged to comply with these principles at every stage of personal data processing. The controller is responsible for ensuring the lawfulness of processing and must be able to demonstrate compliance with these principles (GDPR Article 5(2)).
2. Pursuant to Article 4(1) of the GDPR, personal data means any information relating to an identified or identifiable natural person. According to Article 4(15) of the GDPR, data concerning health constitutes personal data related to the physical or mental health of a natural person, including data concerning the provision of health care services to that person, which reveal information about his or her health status.
3. In accordance with Article 5(1)(a) of the GDPR, the processing of personal data must be lawful, fair and transparent to the data subject. Processing is lawful only where at least one of the legal bases set out in Article 6(1) of the GDPR applies. The processing of special categories of personal data is generally prohibited under Article 9(1) of the Regulation, unless one of the exceptions provided for in Article 9(2) applies. Consequently, the processing of health data may take place only on the basis of Article 6 in conjunction with one of the derogations set out in Article 9(2) of the GDPR.
4. The data controller acknowledged that no legal basis existed for the processing of the data; however, we consider it necessary to provide the following additional clarifications. As a general rule, the use of real personal data for the development or testing of information systems is prohibited. For instance, under the Estonian Information Security Standard (E-ITS)², testing is carried out in development and test environments that are segregated from the operational (production) environment. One of the risks identified by E-ITS in connection with testing using operational data is that individuals involved in software testing may thereby gain access to confidential work-related or personal data. Therefore, E-ITS recommends, as a safeguard, the anonymisation of test data relating to natural persons, meaning that it is no longer directly or indirectly possible to link specific data to a particular data subject, or at a minimum the pseudonymisation of such data (OPS.1.1.6.M11).
5. Nevertheless, in exceptional cases and where an appropriate legal basis exists, it may be permissible to use original data for testing purposes. However, E-ITS identifies as a risk that if operational (production) environment data are used for testing, rather than copies of such data, the data may be inadvertently altered or deleted. Where operational data are used in the integration testing of IT systems, the processing of test data may unintentionally affect operations involving real data in other systems. Therefore, software must be tested only in designated test and pre-live environments that are separated from and clearly distinguishable from the operational environment (OPS.1.1.6.M11).
6. In the present case, a potential legal basis for using employees' data as test data could have been either the employees' consent (GDPR Article 6(1)(a)) or the legitimate interests of

¹ Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

² <https://eits.ria.ee/>

the company (GDPR Article 6(1)(f)). However, since special categories of personal data (health data) were also processed in this case, it must be taken into account that the processing of such data cannot be based on legitimate interest. Instead, only the exceptions provided for in Article 9(2) of the GDPR may apply, one of which is the explicit consent of the data subject.

Article 4(11) of the GDPR defines consent as follows: “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.” Accordingly, based on the principles set out in Article 4, consent must always be freely given, specific, informed and constitute an unambiguous expression of the data subject’s will, whereby the data subject, through a statement or clear confirmation, agrees to the processing of personal data relating to him or her. Consent must be given in such a manner that there is no doubt that all of the conditions are fulfilled simultaneously (freely given, informed, specific and unambiguous).

It must also be taken into account that, in the context of employment relationships, reliance on consent as a legal basis is rather exceptional due to the imbalance of power between employer and employee. Where an employee feels that refusal to provide consent may result in negative consequences, such consent cannot be regarded as freely given. In the present case, this was not a situation in which employees had provided consent for the processing of their personal data; therefore, a lawful basis for the processing of special categories of personal data was lacking.

Legitimate interest may serve as a legal basis for processing provided that the interests or fundamental rights and freedoms of the data subject (the company’s employees) do not override such interest, taking into account the data subject’s reasonable expectations based on his or her relationship with the controller. In any event, the existence of a legitimate interest must be carefully assessed, including whether the data subject may reasonably expect, at the time and in the context of the collection of the data, that personal data may be processed for that purpose.³

The controller’s interest in processing certain personal data does not automatically mean that it may rely on the legal basis of legitimate interest. First, the controller must have a legitimate interest; second, the processing of personal data must be necessary for the purposes of pursuing that legitimate interest; and third, the interests or fundamental rights and freedoms of the data subject must not override the controller’s legitimate interest. In addition, it must be assessed whether the legitimate interest pursued through the processing could reasonably be achieved just as effectively by other means that interfere less with the fundamental rights and freedoms of data subjects.⁴ In the present case, [REDACTED] did not rely on the legal basis of legitimate interest.

7. With regard to testing using original data, the Data Protection Inspectorate has previously taken the position that, prior to carrying out such testing, a data protection impact assessment must be conducted and prepared in order to assess the risks associated with the planned activity for data subjects. Furthermore, where personal data collected for one purpose are intended to be used for another purpose, the assessment must also take into account the requirements set out in Article 6(4) of the GDPR.

Since, in the present case, no legal basis existed for the processing of personal data, the use of personal data in the test environment therefore constituted an infringement

³ GDPR Recital 47

⁴ Judgment of the Court of Justice of the European Union in Meta Platforms and Others, [Case C-252/21](#), paragraphs 106 and 108.

of the requirement of lawful processing arising from Article 5(1)(a), as well as Articles 6 and 9 of the GDPR.

8. Furthermore, we clarify that where personal data are intended to be used as test data and a legal basis for such processing exists, the processing must also comply with the data processing principles set out in the GDPR, including, inter alia, the principles of purpose limitation and data minimisation (GDPR Article 5(1)(b) and (c)). The processing of personal data must be carried out for specified and legitimate purposes. The principle of data minimisation requires that personal data be processed only to the extent strictly necessary for the achievement of the specific purpose and as little as possible. This means that the controller must always consider, when disclosing or using personal data, whether the processing of such data is necessary at all for the fulfilment of the intended purpose and, if so, that it is carried out using the minimum amount of data required.

Pursuant to Article 5(1)(e) of the GDPR, personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (the principle of storage limitation). Accordingly, as stated in Recital 39 of the GDPR, the controller must ensure that the period for which personal data are stored is strictly limited to the minimum necessary. In order to ensure that personal data are not retained longer than required, the controller must establish time limits for erasure or for periodic review of the data.

According to [REDACTED]'s explanations, personal data of former employees, as well as, for example, employees' children, were used in the test environment. Consequently, the processing also infringed the principles arising from Article 5(1)(b), (c) and (e) of the GDPR.

9. Article 5(1)(f) of the GDPR provides that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical or organisational measures ("integrity and confidentiality"). Compliance with the principle of integrity and confidentiality includes, inter alia, preventing unauthorised access to personal data and to the equipment used for their processing, as well as preventing unauthorised use thereof (GDPR Recital 39).
10. Article 24(1) of the GDPR imposes an obligation on the controller to implement appropriate technical and organisational measures in order to ensure that the processing of personal data is carried out in compliance with the requirements of personal data protection law. When implementing such measures, the controller must, inter alia, take 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.
11. Article 32(1) of the GDPR obliges both the controller and the processor to ensure the security of processing. The technical and organisational measures implemented must be proportionate to the risks posed to the rights and freedoms of natural persons arising from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It is particularly important to ensure that unauthorised third parties do not gain access to personal data. Article 32(2) further requires that, when assessing the appropriate level of security, account shall be taken in particular of the risks presented by processing, such as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may result, in particular, in physical, material or non-material damage.
12. The controller must, inter alia, take into account the requirements of data protection by design and by default as set out in Article 25 of the GDPR. Data protection by design

requires that the protection of privacy be embedded into organisational and technological measures, and that the more sensitive the data being processed, the stronger the level of protection that must be ensured⁵. Data protection by default, in turn, means, among other things, that the controller must restrict access to personal data, including the categories of personal data accessible, based on an assessment of necessity. The controller must also ensure that personal data are actually available to those who require access to them when necessary. Accordingly, it must be clearly regulated internally (for example, in job descriptions, internal rules of procedure, or other internal policies governing persons authorised by the controller to process data) who processes data within the organisation, how such processing is carried out, and to what extent. Therefore, in a situation where the company's rules did not foresee personal data being transferred into the test environment, and unauthorised persons thereby gained access to such data, the requirements laid down in Article 25(2) of the GDPR have been infringed.

In the present case, the controller had failed to exercise the necessary duty of care in the processing of personal data under its control, with the result that employees' and their relatives' data were used as test data without a lawful basis. The fact that the breach was revealed in the course of an audit, that it persisted over an extended period of time, and that the individuals affected by the incident did not immediately notify the company's Data Protection Officer, indicates deficiencies in compliance with the above-mentioned requirements for secure processing of personal data. This includes, inter alia, insufficient data protection awareness within the organisation. Accordingly, measures to remedy the situation are necessary, including raising information security standards and providing training to employees. The incident described could have been prevented had the controller implemented the relevant measures outlined above, including, for example, employee training and awareness-raising activities.

Accordingly, the principle of integrity and confidentiality arising from Article 5(1)(f) of the GDPR has been infringed in the processing of personal data. More specifically, this consists of:

- 1) a breach of the requirements relating to the security of personal data processing (GDPR Article 32 in conjunction with Article 24(1)); and**
- 2) a breach of the obligation to implement data protection by design and by default (GDPR Article 25(1) and (2)).**

In summary, personal data were processed as test data without a lawful basis, and in the Inspectorate's assessment, ██████████ could have prevented such an infringement by implementing appropriate security measures and data protection principles. ██████████ is a large-scale controller, and therefore the expectations regarding the organisational and information technology security measures applied by such a controller are higher than average. The Inspectorate acknowledges that the incident occurred as a result of human error; however, it could nevertheless likely have been prevented. Personal data were processed over an extended period of time, and the test data contained a substantial amount of personal data, including data of former employees as well as special categories of data and children's personal data, which merit particular protection.

At the same time, the Inspectorate takes into account that, in light of the incident, the controller has immediately implemented the necessary changes to improve the security of personal data processing. ██████████ promptly submitted a personal data breach notification to the supervisory authority upon becoming aware of the infringement, in which the company acknowledged its error in the processing of personal data. Furthermore, the company has

⁵ Estonian Data Protection Inspectorate, [General Guidance for Personal Data Controllers](#), p. 11; [European Data Protection Board, Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default, Version 2.0](#), adopted on 20 October 2020, paragraphs 55 and 56.

cooperated fully with the supervisory authority, and the breach has ended. The data was accessible only to a limited number of employees within the [REDACTED] and, as a mitigating measure, the employees affected by the breach have also been informed of the incident.

In light of the above, I hereby terminate the present supervisory proceedings; however, pursuant to Article 58(2)(b) of the GDPR, I issue an admonition to [REDACTED], as the processing operations infringed the requirements arising from Article 5(1)(a), (c), (e) and (f), Article 6(1), Article 9, Article 24(1), Article 25(2), and Article 32(1) of the GDPR.

Respectfully,

[REDACTED]

lawyer
authorized by Director General