



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

FOR INTERNAL USE

Information Holder: Data Protection Inspectorate

Note made: [REDACTED] 2025

Access restriction valid until: [REDACTED] 2030

Section 2 valid until the Decision enters into force

Basis: Section 35(1)(2), Section 35(1)(9)

Section 35(1)(18)(2) of the PIA

All SA's

[REDACTED] 2025 No. [REDACTED]

ARTICLE 60 FINAL ADOPTED DECISION**Reprimand and termination of supervisory proceedings**

The Estonian Data Protection Inspectorate (the Estonian DPI) has conducted proceedings¹ regarding a personal data breach by [REDACTED] ([REDACTED] in connection with the phoneless login feature.

Circumstances of the breach

[REDACTED] submitted a preliminary notification to the Estonian DPI on [REDACTED] 2024 and a final breach notification on [REDACTED] 2024, indicating that between [REDACTED] 2024, an attacker gained unauthorised access to user accounts.

[REDACTED] was in the process of introducing the 'phoneless login' feature, which enables users to login to [REDACTED] apps without a phone number (via Social Media Accounts). This process involves users being provided with [REDACTED]. During the development of the phoneless login feature, changes were made to the existing login process. The weakness was that [REDACTED] was not correctly [REDACTED] and, specifically not properly [REDACTED], resulting in a risk that unauthorised persons could access the [REDACTED] user authentication flow. To exploit the risk, the [REDACTED] had to take the following steps:

[REDACTED] became aware of the weakness from the user on [REDACTED] 2024 and took measures to eliminate the vulnerability on the same day as the notification.

The number of affected data subjects in the European Economic Area is 612. Among them, 64 users suffered financial loss, 120 users had their account deleted by unauthorised users, 64 users had their name, email address and/or phone number changed by unauthorised users. Additionally, a limited number of data subjects (managers and couriers) had their data accessed via order history in user accounts.

The personal data breach affected ordinary personal data, i.e. special categories of personal data

¹ The Inspectorate initiated proceedings pursuant to § 56(1) and (3) clause 8 of the Personal Data Protection Act. The legal basis for requesting explanations: §§ 57–58 of the Personal Data Protection Act, § 30(1) and (3) of the Law Enforcement Act, and Article 58(1)(a), (e), and (f) of the General Data Protection Regulation.

(Art. 9(1) GDPR) were not impacted by the breach.

Controller's explanations

█████ is developing a ‘phoneless login’ feature, which allows users to log into their █████ apps using social media accounts instead of a phone number.

[REDACTED] explained that the changes made to the existing login process during the development of the feature caused an unintended vulnerability. The cause of the incident was human error. It was a marginal occurrence where the [REDACTED], resulting in an unintended weakness. Consequently, an attacker was able to exploit the weakness to log into another user's account using [REDACTED] [REDACTED]

The dataset involved in this incident consists of ordinary, routinely shared, and non-sensitive personal data generated during regular use of the service. It does not include identity documents, health data, biometric data, or complete payment data. Although the volume of data may seem large and individuals may be easily identifiable, the overall risk level is low due to the low sensitivity of the data.

The weakness was eliminated [REDACTED]. Additional mitigation measures were implemented. The controller explained to the Estonian DPI the organisational measures in place, information security controls, specific security measures, and anti-phishing protections. Data subjects who suffered financial damage were compensated.

Apart from the aforementioned weakness and unauthorised access to accounts, [REDACTED]'s investigation did not identify other or additional personal data breaches or vulnerabilities in [REDACTED]'s systems or databases.

█ has established general principles of product security to be followed when developing new features and redesigning old applications. The controller outlined to the Estonian DPI the guidelines applied in the software development process.

For this feature, a product security risk assessment was initiated to identify and prioritise risks according to their likelihood and severity. The information security team conducted a risk assessment based on the planned implementation of the feature.

Additionally, [REDACTED] has established [REDACTED]
[REDACTED]
[REDACTED] These practices address security aspects to be evaluated during code review. Nevertheless, in this case, the vulnerability was not detected during code review.

As a general measure, [REDACTED] conducts [REDACTED] of [REDACTED] applications. Furthermore, [REDACTED] has a public vulnerability reporting programme through which freelance security researchers and volunteers can report any security issues.

Regarding notification of data subjects, [REDACTED] explained that, based on the assessment results, it was concluded that not all data subjects needed to be notified of the breach. The decision is based on the assessment, which found that the identified risks do not pose a significant threat to the rights and freedoms of all individuals, as for some individuals, the risk level has been reduced or eliminated through implemented measures. The controller provided the Estonian DPI with an analysis and assessment results conducted using the ENISA² methodology. [REDACTED] considers that the breach is unlikely to pose a significant risk to the rights and freedoms of those data subjects who

² European Union Agency for Cybersecurity. Recommendations for a methodology of the assessment of severity of personal data breaches, 2013. - <https://www.enisa.europa.eu/publications/dbn-severity>

did not suffer financial loss. This group of affected individuals does not require notification.

Position of the Estonian Data Protection Inspectorate

1. As the breach affected residents of various European Union and European Economic Area countries, the Estonian DPI initiated proceedings under General Data Protection Regulation (GDPR) Article 56(1) to determine the lead supervisory authority and forwarded information about the breach to relevant supervisory authorities in the cross-border procedure system. The Estonian DPI considers itself the lead supervisory authority in this matter, as [REDACTED] is an Estonian company with its main place of business and management located in Estonia.
2. Pursuant to Article 4(1) GDPR, personal data is any information relating to an identified or identifiable natural person (data subject). Through unauthorised access to [REDACTED] user accounts, the attacker gained access, depending on the application ([REDACTED], or [REDACTED]), to various data such as name, email, phone number, order/ride history, average rider rating, saved locations (where applicable), workplace data, payment methods, communication preferences (marketing consent), conversations with [REDACTED] customer support in the last 60 days, [REDACTED] amount (where applicable), campaign code (where applicable). Thus, there was unauthorised access to personal data.
3. Based on the principles of personal data processing, specifically GDPR Article 5(1)(f), personal data must be processed in a manner that ensures appropriate security and protects against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures (“integrity and confidentiality”). Compliance with the principle of integrity and confidentiality includes, among other things, preventing unauthorised access to personal data and the devices used for processing them, or their unauthorised use.³
4. The same obligation is further regulated in GDPR Articles 24, 25, and 32. Specifically, under Article 24(1), the controller implements appropriate technical and organisational measures to ensure and demonstrate that processing is performed in accordance with the GDPR, considering the nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. Additionally, the controller must consider the requirements for data protection by design and by default described in GDPR Articles 25(1) and (2).
5. Pursuant to Article 32(1) GDPR, the controller must 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 the systems and services processing personal data. Pursuant to Article 32(2) GDPR, the assessment of the necessary level of security shall in particular take into account the risks arising from the processing of personal data, in particular accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Therefore, controllers and processors must choose and implement measures that can ensure an appropriate level of security. This means that they must implement measures that are able to mitigate at least those risks that are most likely to materialise and that would have the most severe impact.⁴ The ability to ensure system resilience also entails minimising attack opportunities and improving system security, including learning from mistakes. Security measures must assume that systems can withstand attacks and recover from them, which in turn means that attack opportunities must be prevented and system security continuously improved.
6. To ensure security and prevent processing in violation of the GDPR, the controller should assess the risks associated with processing and implement measures to mitigate those risks.

³ GDPR recital 39.

⁴ Burton, in Kuner, Bygrave, Docksey, The EU General Data Protection Regulation (GDPR): A Commentary, Article 32 GDPR, p. 636 (Oxford University Press 2020).

The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined based on the nature, scope, context, and purposes of processing. The risk assessment should be carried out on the basis of an objective assessment which determines whether the processing operations present a risk or a high risk.⁵ Taking into account the latest scientific and technological developments and the costs of implementing the measures, those measures should ensure an appropriate level of security, including confidentiality, appropriate to the risks and the nature of the personal data to be protected. When assessing the data security risk, consideration should be given to the risks arising from the processing of personal data, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed, which may, in particular, result in physical, material or non-material damage.⁶

7. ■■■ has established general principles of product security to be followed when developing new features and redesigning old applications. Data protection by design and by default requires not only the establishment of rules, but also their actual implementation, starting from the design of data processing tools and throughout the lifecycle of data processing. The Estonian DPI considers that ■■■ has implemented organisational measures, but there was a deficiency in the implementation of technical measures, as in this incident the chosen technical solution allowed the attacker to access accounts, i.e. it was not reliable, and the vulnerability was not detected during the review of the solution.
8. The controller has explained to the Estonian DPI that the incident was caused by a human error. This was a case with a marginal frequency. At the same time, the Estonian DPI takes into account that the attacker obtained unauthorized access to accounts and thereby caused material damage to some data subjects. The risk thus materialised in respect of some of the data subjects.
9. No one is protected from a cyber-attack, but in order to prevent it, the 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 this case, ■■■ did assess the risks of changes to the login functionality, but the Estonian DPI considers that the risks were assessed too low and thus incorrectly. The Estonian DPI also takes into account that ■■■ learned of the breach from a user on ■■■.2024, i.e., ■■■ days after the start of the attack (■■■.2024).
10. Pursuant to Article 31 GDPR, the controller shall cooperate with the supervisory authority on request in the performance of its tasks. The Estonian DPI made enquiries to ■■■ during the proceedings, to which the controller replied and provided explanations on the circumstances of the breach.
11. Pursuant to Article 33 GDPR, the controller shall notify the personal data breach to the supervisory authority without undue delay and, where possible, within 72 hours of becoming aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. ■■■ submitted a preliminary notification of the breach to the Estonian DPI within 72 hours and therefore did not violate the requirements of Article 33 of the GDPR.
12. Pursuant to Article 34(1) GDPR, the controller shall, without undue delay, notify the data subject of a personal data breach where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The Estonian DPI takes into account that the controller has assessed, under Article 34 GDPR, the extent of the potential risk to data subjects arising from the breach. Based on the controller's risk assessment, data subjects were divided into two groups – for some, there was a high risk; for others, the risk was assessed as low. Data

⁵ GDPR recital 76.

⁶ GDPR recital 83.

subjects for whom there was a high risk were notified of the breach. Data subjects for whom the risk was assessed as low were not notified. The Estonian DPI agrees with the risk assessment carried out by the controller, i.e. not all data subjects affected by the breach are at high risk.

On the basis of the above, [REDACTED] did not implement appropriate security requirements for data processing, thereby violating, in particular, the obligations arising from GDPR Article 5(1)(f) and Articles 24, 25, and 32.

In addition to the above, the Estonian DPI takes into account that the controller cooperated with the Estonian DPI in the investigation of the breach, identified the reason for the breach and has taken measures to mitigate and prevent the adverse effects immediately after the breach. The controller has reviewed and adjusted its systems to ensure the use of technical and protective measures. Data subjects affected by the breach who are likely at high risk were notified. Data subjects who suffered financial loss were compensated.

Under Article 58(2)(b) of the GDPR, the Estonian Data Protection Inspectorate reprimands [REDACTED] and terminates the supervisory proceedings.

The addressee shall have 30 days to contest the reprimand and the notice of termination of the supervisory proceedings by submitting an appeal to the administrative court under the Code of Administrative Court Procedure.

Respectfully,

[REDACTED]

lawyer

authorized by the Director-General