Gregor Eesmaa
E-mail: gregoreesmaa1@gmail.com

20-06-2025
No LE-OU-110

ANSWER
To the Notice

On May 31, 2025 UAB "Kesko Senukai Digital" (the "**Company**") got the notice from the data subject (the "**Data Subject**") regarding the processing of his personal data while using the website of the Company https://www.k-rauta.ee/ (the "**Notice**"). The Data Subject informed the Company that he tested the login form, password reset form and account registration form of https://www.k-rauta.ee/ (the "**Website**") and identified security issues on the login form and account registration form, which have been described in the annex ("vulnerability-reassessment-report") attached to the Notice (the "**Annex**"). Accordingly, the Data Subject requested the Company to respond to the questions set out in the Notice.

Firstly, we are grateful that the comments indicated in the Annex were brought to the Company's attention. We appreciate your initiative and diligence in identifying and reporting potential data protection concerns. Observations and feedback from our users are highly valued, as they contribute significantly to the continued improvement and security of the services provided. Therefore, an immediate internal review was conducted. As a result, we have taken the corrective actions, and the reported issue potentially affecting the login and registration forms has been fully resolved. The system has been updated to ensure that no indication is provided as to whether a specific email address is registered, in accordance with data protection and privacy principles.

Secondly, with regard to the formal request submitted, we want to note that the processing of user credentials during login and registration is primarily based on Article 6(1)(b) of the EU General Data Protection Regulation (the "**GDPR**"), as it is necessary for the performance of a contract — specifically, to provide users with access to account-based services. Additional security-related processing may be supported by the Company's legitimate interest under Article 6(1)(f), in ensuring the integrity and protection of user accounts. It is acknowledged, however, that the previous implementation may have inadvertently allowed certain responses that could be interpreted as confirmation of account existence. This has now been addressed.

Regarding the request pursuant to Article 18 of the GDPR, the Company confirms that as the previously reported issue has been rectified and the vulnerability removed, the processing in question no longer occurs. Moreover, regarding the objection pursuant to Article 21 of the GDPR, we want to note that the objection has been noted and respected. The current system no longer includes any processing that would result in disclosure of account existence to unauthorized parties.

Finally, the Company once again confirms its commitment to upholding the highest standards of personal data protection, in full alignment with the GDPR. Considering what has been said, the contribution made by the Data Subject in identifying and reporting the possibly existing vulnerability is highly appreciated.

Should any further questions arise, the Company remains fully available to provide the assistance in accordance with applicable legal obligations.

Sincerely,
Director for Baltic states

Ana Parafinaitė