REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Final Decision

Notice of reprimand and termination of the proceedings concerning the protection of personal data

The Estonian Data Protection Inspectorate (DPI) received [redacted]'s complaint concerning the data subject's right to rectification of personal data in accordance with Article 16 of the General Data Protection Regulation (GDPR). The complaint was forwarded to Estonian DPI by the IMI cross-border procedural system from SA Austria. The main establishment of [redacted] ([redacted]), the controller of personal data, is Tallinn, Estonia. In the context of this, Estonian DPI agreed to be the lead supervisory authority and initiated a supervision proceeding on the basis of clause 56 (3) (8) of the Personal Data Protection Act.

According to the complaint, the data subject wanted to change his phone number in the [redacted] app but did not find this option. The data subject then contacted [redacted] for clarification regarding the correction of the telephone number in the [redacted] application but did not receive a reply to his requests. It is apparent from the documents in the complaint that the data subject sent [redacted] an e-mail to [redacted] on 7 March 2021 at 9:17 and on 4 December 2021 at 5:14 p.m. The applicant used an e-mail address [redacted] to contact [redacted].

THE COURSE OF PROCEEDINGS

During the proceedings, the Estonian DPI has made several inquiries in order to get an overview of personal data processing activities in the [redacted] application. The Estonian DPI also met with the controller during these proceedings several times. According to [redacted]'s statements, it turned out that the phone number was assigned in the system as a user's unique ID, so it was not possible to change the phone number itself. The only solution was to delete an account and create a new one.

In addition, the Estonian DPI made an official proposal to [redacted] to change its system where users can change their phone number in the app. [redacted] agreed with the proposal but noted that due to the development being extensive, it will take time to be implement this solution globally. [redacted] confirmed that it complied with the Estonian DPI's proposal on August 15, 2023.

In addition, the second issue in the proceedings was fulfilment of requests made by the data subject, namely the complainant. In the course of the proceedings, the Estonian DPI proposed to [redacted], that the complainant be provided with answers on their data subject request. [redacted] responded

to the proposal: *"[redacted] contacted [redacted] on 7 March 2021 via a suspicious email domain – [redacted] Unfortunately, we cannot check if [redacted] has a [redacted] account because the information we currently have about the user is too limited.*

Before responding to a request from a data subject, we must confirm that the data subject is indeed a customer of [redacted] and has the right to exercise the data subject's right. We sent [redacted] an authentication request on November 30, 2023. We confirm that [redacted] successfully confirmed our authentication request on December 4, 2023, and received the requested information on December 28, 2023. Since then, we have not received any further questions from the data subject." Thus, [redacted] has fulfilled the Estonian DPI's proposal.

During the proceedings, the Estonian DPI also received information about cases in which a third party had unjustifiably accessed the data of another person when creating an account in the application. This case was related to the fact that the phone number was still linked to the previous account data in the app while [redacted] was using the phone number as a unique ID. All cases like these were met with immediate response from [redacted] and the infringement corrected.

Position of the Estonian Data Protection Inspectorate

According to Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), "personal data" means any information relating to an identified or identifiable natural person, in particular name, personal identification number, location information; the physical, physiological, and economic characteristics of the person, etc. The e-mail address and telephone number are also deemed to be personal data.

The GDPR also lays down the rights of data subjects to the processing of their personal data. Under Article 16 of the GDPR, the data subject has the right to request the controller to rectify inaccurate personal data concerning him or her. As the telephone number falls under the category of personal data, it must be possible to rectify it and the controller must enable the data subject to rectify the data at the request of the data subject.

[redacted], as the controller of the personal data, has to provide the data subject without undue delay, but no later than one month after receipt of the request, with information on the action taken in response to a request pursuant to Articles 15 to 22 of the GDPR. That period may, where appropriate, be extended by two months considering the complexity and amount of the application. The controller shall inform the data subject of any such extension and of the reasons for the delay within one month of receipt of the request (Article 12(3) GDPR).

If the controller fails to act on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not acting and explain the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy (Article 12(4) of the GDPR).

In the present case, [redacted] received several requests from the data subject in connection with Article 16, but [redacted] did not reply in due time and therefore the controller failed to comply with the obligation imposed in accordance with the GDPR. Although the data subject's request was completed only after the intervention of the Estonian DPI, the execution of the proposal was also severely delayed.

Pursuant to Article 24(1) of the GDPR, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the nature, scope, context and purposes of the processing of personal data, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. Pursuant to Article 32(1) of the GDPR, the controller must implement appropriate technical and organisational measures to ensure the level of security appropriate to the risk, including ensuring the continuing

confidentiality, integrity, availability and resilience of systems and services processing personal data.

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.

In the case of the [redacted] phone number solution, there was a problem where the transfer of the phone number to a new person gave that person the opportunity to obtain unjustifiably access to the data of another person when creating an account in the [redacted] application. Although the problem has been solved for affected persons to date, [redacted] still failed to implement appropriate organisational and technical measures beforehand to ensure the confidentiality of personal data.

I hereby terminate the proceedings as the data controller has complied with all the proposals made by the Data Protection Inspectorate. In addition, I am reprimanding on the basis of Article 58(2)(b) of the GDPR because the processing operations have infringed the requirements of the GDPR (Article 5(1)(d) and (f), Article 12(3) and (4), Article 16, Article 24(1), Article 32(1)).

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act[1], or
- An appeal to an administrative court under the Code of Administrative Court Procedure[2] (in this case, the challenge in the same matter can no longer be reviewed).

Best regards

[redacted]
Data security expert
authorized by Director General

[1] https://www.riigiteataja.ee/en/eli/527032019002/consolide
[2] https://www.riigiteataja.ee/en/eli/512122019007/consolide