REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

ASUTUSESISESEKS KASUTAMISEKS
Teabevaldaja: Andmekaitse Inspektsioon
Märge tehtud: 02.05.2022
Juurdepääsupiirang kehtib kuni: 02.05.2097
Alus: AvTS § 35 lg 1 p 2, AvTS § 35 lg 1 p 12

IMI - Berlin DPA

Yours: nr

Ours: {regDateTime} nr {regNumber}

Reprimand for failure to comply with the requirements of the General Data Protection Regulation & notice of termination of the proceeding in regard to the protection of personal data

RESOLUTION:

Reprimand in a personal data protection case in which [redacted] has violated the following norm arising from the General Data Protection Regulation (GDPR): article 17

Case

The Estonian Data Protection Inspectorate (Estonian DPA) received a complaint from [redacted] via Internal Market Information System.

According to the complaint the complainant was unable to exercise his right to have the data deleted. The complainant stated that, despite several appeals, the data was not deleted.

The Estonian DPA explained to the controller that processing of personal data is permitted only with the consent of the person or other legal basis abiding from law. In the absence of a legal basis, personal data may not be processed. If personal information processing is not permitted by law, a person has the right to ask for termination of data processing and additionally for deletion of data.

Based on the information contained in the complaint, the controller have repeatedly confirmed to the complainant that his personal information was deleted, so logically the controller had no further legal basis to process the complainant's data. Additionally the controller did not explain to the complainant the impossibility of deletion.

For above reasons the Estonian DPA started an investigation and asked questions listed with answers below.

1. On what date was the specific personal data of [redacted] data deleted?

On the 19th of November 2020, [redacted] requested that his user account in the [redacted] mobile application be deleted, along with all of his personal data. On the same date and in accordance with Article 38 of the [redacted] App Terms of Use, [redacted] immediately proceeded with deleting [redacted]' personal data and closing his user profile in the [redacted] application. In addition, [redacted]s compliance department encrypted and archived that data of [redacted] that is required to be retained for AML purposes.

2. Why was the data not deleted immediately at the request of the person?

As part of the standard account deletion procedure, once a [redacted] user requests to have his/her account deleted, they should manually log out of or delete the [redacted] App. [redacted] did not follow this step, which resulted in his login details (email address and account passcode) being kept in [redacted]'s database. We would like to emphasize that after the user account deletion, only [redacted] email and passcode were stored in [redacted]s database, due to the fact that [redacted] did not take the necessary technical steps to finalize his account closure. The remainder of his personal information was deleted and where applicable encrypted and archived, as per the information laid out in pt. 1 above. [redacted] contacted [redacted] on 11th January 2021 stating that according to him, his personal data was not deleted from [redacted]'s databases. After being made aware of the fact that [redacted] did not delete or log out of his [redacted] App, [redacted] immediately proceeded to force-logout [redacted] from the [redacted] App and the account closing procedure was finalized.

3. What measures will you take to deal with such situations in the future and to avoid that a person cannot exercise their right to have their data deleted?

To prevent the above-described situation from happening in the future, [redacted] implemented a force-logout from the [redacted] App as part of the user account deletion procedure. With this updated process, if a user wishes to delete their [redacted] account, they can make the account deletion request and they will be automatically logged out of the [redacted] App by the [redacted] ystem. The user no longer needs to click logout from their side. After the forced logout, the user login credentials will be disabled, and all user data will be deleted or archived as outlined in Article 38 of the [redacted] App Terms of Use.

As the data deletion part was still unclear, the Estonian Data Protection Inspectorate made on additional inquiry on 16th of March 2022. [redacted] replied on the 22nd of March 2022 as listed below.

4) Can you confirm that the complainants data (besides the data that is encrypted and archived) is now deleted and he has no access to his account?

"We hereby confirm that all data connected with the complaint of [redacted] has been deleted, notwithstanding that data which is subject to our record keeping obligations. The account is fully closed and the user no longer has the ability to access anything connected

with the account."

5) What is the legal basis for not deleting all the data and encrypting some of it? Please be precise – bring out the legal act, provision, section, reason.

[redacted]*s data retention obligations stem from § 47 of the Estonian Money Laundering and Terrorist Financing Prevention Act (the "AML Act"). Under this provisions,* [redacted] *is required to retain:*

- *Documents specified in §21, § 22 and §46 of the AML Act (which includes, but is not limited to documentation relating to proof of residence, date of birth, personal identification code), information registered in accordance with § 46 and the documents serving as the basis for identification and verification of persons, and the establishment of a business relationship for no less than five years after the termination of the business relationship;*
- *during the period specified in subsection 1 of § 47,* [redacted] *must also retain the entire correspondence relating to the performance of its duties and obligations arising from the* [redacted] *and all the data and documents gathered in the course of monitoring the business relationship or occasional transactions as well as data on suspicious or unusual transactions or circumstances which were not reported to the Financial Intelligence Unit.*
- [redacted] *must also retain the documents prepared with regard to a transaction on any data medium and the documents and data serving as the basis for the notification obligations specified in § 49 of the AML Act for no less than five years after making the transaction or performing the duty to report.*
- [redacted] *must retain the documents and data specified in subsections 1, 2 and 3 of § 47 in a manner that allows for exhaustively and without delay replying to the enquiries of the Financial Intelligence Unit or, in accordance with legislation, those of other supervisory authorities, investigative bodies or courts, inter alia, regarding whether* [redacted] *has or has had in the preceding five years a business relationship with the given person and what is or was the nature of the relationship.*
- *Lastly,* [redacted] *deletes the data retained on the basis of § 47 after the expiry of the time limits specified in subsections 1–6 of § 47, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a compliance notice issued by the competent supervisory authority, data of importance for prevention, detection or investigation of money laundering or terrorist financing may be retained for a longer period, but not for more than five years after the expiry of the first time limit."*

6) What exact data are you encrypting and archiving? Is it not possible to anonymize the data and then archive it?

[redacted]*'s compliance department encrypts and archives the data that is required to be retained for AML purposes (documentation relating to proof of residence, date of birth, personal identification code, transaction data), as per the requirements listed in § 47 of the AML Act.*

The reason why this data is not anonymized is that this data (documentation relating to proof of residence, date of birth, personal identification code, transaction data) has a specific function in relation to our obligations stemming from § 47 of the AML Act - this data is used to duly verify the identity/residence of our users and screen them against a variety of sanctions lists and lists pertaining to politically exposed persons. In turn, as per § 47, [redacted] should without delay reply to the enquiries of the Financial Intelligence Unit or, in accordance with legislation, those of other supervisory authorities, investigative bodies or courts, inter alia, regarding whether [redacted] has or has had in the preceding five years a business relationship with the given person and what is or was the nature of the relationship.

Anonymizing the above-described data (documentation relating to proof of residence, date of birth, personal identification code, transaction data) is irreversible and would render it impractical or even impossible for [redacted] to comply with its AML reporting obligations."

Taking into account the fact that the controller did not delete the data subjects data due to their own procedural mistakes the controller breached article 17 stipulated in the General Data Protection Regulation (GDPR).

Although the controller has now confirmed that the complainant's personal data is deleted (besides the data that they are obligated to retain by law), procedural mistakes are solved and the controller has improved its data processes (including deletion), we are closing the proceedings and reprimand [redacted] on the basis of Article 58 (2) (b) of the GDPR.

Best regards

[redacted]
lawyer
authorised by Director General