REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

INTERNAL INFORMATION
Information holder: Estonian Data Protection Inspectorate
Date: 27.11.2023
Valid until: 27.11.2098
Legal ground: Public Information Act § 35 (1) p.2, p.12, p. 17.

Ours: 27.11.2023 nr 2.1.-1/23/760-1906-9

Final decision

Reprimand and notice of termination of the proceedings concerning the protection of personal data

Estonian Data Protection Authority received a complaint from [redacted] via the cross-border procedural system IMI which was forwarded by Berlin SA. The controller – [redacted] ([redacted]) has its main establishment in Tallinn, Estonia. Estonian DPI has accepted the case as LSA.

Based on the information contained in the complaint, the controller has 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.

Estonian DPI closed the proceedings and reprimanded [redacted] on the basis of Article 58 (2) (b) of the GDPR in March 2022. **After the final decision complainant still received direct marketing emails from [redacted] in January 2023 even though [redacted] confirmed before that the complainants' data was deleted.**

THE COURSE OF PROCEEDINGS

Estonian DPI initiated a supervision proceeding on the basis of clause 56 (3) 8) of the Personal Data Protection Act due to the fact that complainant still received direct marketing emails even though [redacted] confirmed complainants' data was deleted. Firstly, Estonian DPI contacted the Controller to clarify if which company is the controller since on [redacted] website there are two different privacy notices.

[redacted] answered the first inquiry 17.08.2023 and explained:
Question of deletion of user's personal data

As explained in detail in Part II of our reply of 22 March 2022, the Company has a strict data retention obligation arising from Section 47 of the Estonian Money Laundering and Terrorist Financing Prevention Act ("Money Laundering and Terrorist Financing Prevention Act") because we are a regulated company, i.e. we hold an activity licence to provide a virtual currency service (for more information see Section 1 of Part I below), which is why we are an obligated entity under the RahaPTS. Based on these obligations, we are obliged to retain

certain personal data, including email addresses, for at least five (5) years. In the case of [redacted], this period started from 19.
November 2020, from the date on which he applied for the closure of his [redacted] account.

In the present case, direct marketing emails continued to be sent to [redacted] even after he had asked for his account to be closed because, at that time, our standard account closure procedure required users to log out of the [redacted] mobile application themselves or delete a mobile application that [redacted] did not do. However, when the potential problem was highlighted, we implemented an automatic forced-out log-out to all users.

We confirm here, as mentioned above, that [redacted]'s data was deleted wherever possible – he was removed from, among other things, all email lists used by our automated marketing software HubSpot. Data subject to our data retention obligation was archived and encrypted.

We have conducted a thorough internal investigation into the emails sent to [redacted] on 24 January 2023, 22 February 2023 and 24 February 2023, and our position is as follows:

On 11 January 2023, [redacted]'s email address was erroneously added to the email list used by HubSpot because of a technical error in our back-office software at the time. For marketing campaigns, our marketing and data processing departments sometimes separate user lists from relevant databases and use these lists to create an email audience. Such extracts should, as a rule, cover only active users, not archived users, but in this case our backoffice software did not block [redacted]'s email address.

We would like to point out that the above mentioned error was corrected in May 2023. As part of the wider back-office reorganisation, we improved our systems so that each account closure/closure request involves automatic deletion of users' email addresses from all third-party marketing platforms. In addition, such email addresses are blacklisted (based on an encrypted version of the email address) and all manual interventions are automatically blocked. Technically, it should not be possible for this situation to happen again in the case of [redacted] or any other user. To confirm this, we are ready to provide you with an appropriate statement.

We fully understand that this case is frustrating for all parties involved, including us, because we always strive to ensure the highest level of data handling vis-à-vis our customers, in full compliance with applicable laws and regulations. However, we currently have over half a million (500,000) active users on a daily basis, including many complex in-house systems that we use to support our daily activities. As can be inferred from the timing of our recent improvements (May 23), we strive to continuously improve our data processing systems, regardless of whether we are faced with specific complaints or not. Finally, we would like to stress that the case of [redacted] is exceptional and that we know that other users have not experienced similar problems.

II. Company information

1. Which entity takes decisions on the processing of personal data?

Decisions concerning the processing of personal data of [redacted] mobile app users residing in the European Economic Area, Switzerland and the United Kingdom are made by [redacted]. We would like to draw attention to the fact that after a strict renewal process, [redacted] is one of the few virtual currency service providers whose activity licence was recently renewed by the Estonian Financial Intelligence Unit. This, in turn, demonstrates our excellent performance in terms of compliance and compliance with the highest possible standards in terms of anti-money laundering, countering the financing of

terrorism and risk management. Please refer to the extract from our licence in Annex 1.

The [redacted] mobile application is owned and developed by [redacted] with its registered office at [redacted]. [redacted] has an application licensed for commercial use to [redacted], a wholly owned subsidiary of [redacted]. Please refer to Annex 2 below for an extract from the notarised shareholder register of [redacted].

In addition, [redacted] is a sister company of [redacted] and serves only Swiss residents.

2. If the decisions related to the processing of personal data are taken independently by [redacted], in which country the management board of the company is located? Please provide the exact address of the Management Board.

The composition of the Management Board of [redacted] is as follows:

a. [redacted] – [redacted], Chairman of the Estonian Management Board

b. [redacted], Member of the Estonian Management Board

c. [redacted]
Member of the Board

d. [redacted]
Member of the Board

3. Please explain in more detail who is the controller of personal data when personal data is collected from both the website and the application?

a. Website

For visitors to the website [redacted] (the "Website"), the data controller is [redacted], as detailed in the website's privacy statement, which is included in Annex 3 below.

The data collected from visitors to the website is described in detail in Article 5 of the website's privacy notice and is as follows:

i. Details of visitors. [redacted] automatically:
- *collects your cookies;*
- *use Google Analytics;*
- *uses Facebook pixels;*
- *uses Hotspot;*
- *use Intercom;*
- *uses Hotjar; and*
- *uses Twitter connect.*

ii. User data. [redacted] collects
- *users' Ethereum addresses; and*
- *the user's email addresses;*

iii. Details of the referendum. If users participate in a referendum, [redacted] will collect:

- *the user's IP address; and*
- *user-Agent of the user browser.*

iv. Details of the newsletter subscriber. When a visitor or user subscribes to our newsletter, [redacted] *collects them:*
- *IP address;*
- *first name and surname;*
- *country of residence; and — e-mail address.*

Users and/or visitors have the right to unsubscribe from our newsletter at any time by contacting us in accordance with point 19 of this notice.

B. [redacted] *mobile app*

For users of the [redacted] *mobile application residing in the European Economic Area, Switzerland and the United Kingdom, the data controller is* [redacted]*, as detailed in the Privacy Notice of the Application, which is included in Annex 4 below.*

The Application Privacy Notice applies to all personal data obtained as a result of downloading and using the app when the user has registered as a user of the mobile application. The data collected from users of the [redacted] *application is described in detail in Article 5 of the Privacy Notice of the application and is as follows:*

i. KYC and AML data. Such data is used and stored to enable the company to fulfil its legal obligations towards any regulatory authority. Our Services are subject to laws and regulations that require the Company to collect and use some personal information in a certain way, including, but not limited to, User Personal Data, official identification data, financial information, transaction data, business information, web identifiers and/or usage data.

ii. User suitability data. User fitness data is used and stored to enable us to comply with our legal obligations by ensuring that we can provide users with more relevant information, better understand their preferences, and verify whether they are entitled to use our Services and have sufficient knowledge to use our Services.

iii. Financial data. The Company processes personal data when users make contributions or withdrawals, including, but not limited to, the following sources:
- *The origin of the Fiat currency account;*
- *the overall balance of the user account at any point in time;*
- *the balance of virtual currency assets in the user account at any point in time;*

IV. Transaction data. The Company collects the following personal data depending on when the User performs a transaction and/or uses Company Support Services, including, but not limited to:
- *Transaction details;*
- *user account audit logs;*
- *user account communication protocols;*
- *the level of the user account;*
- *the displayed currency;*
- *the external wallet address of the user;*
- *details of the User's International Bank Account Number (IBAN);*
- *virtual currency assets, existing balance and all data available at the user's external wallet.*

Transaction data is used and stored in order to comply with our legal obligations and to ensure

that transactions made through the use of the application can be coordinated and settled. Transaction data is also used to compare transactions in our accounting records with financial data in order to obtain a clear and accurate overview of user orders and user account balances.

4. **Please provide your explanations and the opinion you consider necessary.**

Here we refer to Part I above, which explains in detail [redacted]'s circumstances and measures taken to ensure better data handling.[1]

Since in the first supervisory proceeding [redacted] also had confirmed that the data was deleted but that turned out not to be the case, Estonian DPI requested proof of deletion and made two additional inquiries. [redacted] explained that they made improvements to their back office and sent an overview how it is conducted in their systems.[2] They also provided evidence that the complainants' data was in fact deleted from the direct marketing system.

In terms of Hubspot and Mixpanel, we are not able to produce a similar extract, due to technical constraints. However, we would be more than happy to organize a call and walk you through these systems, in order to demonstrate that [redacted]'s email is not stored therein and that it is impossible for his email to be re-added or processed.[3]

Considering the fact that the controller did not delete the data subject's data due to their own procedural mistakes again 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] based on Article 58 (2) (b) of the GDPR.

As we are required to provide both draft and final decisions, if SA Berlin does not have any comments, final decision will be issued on 27.11.2023.

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[4], or
- An appeal to an administrative court under the Code of Administrative Court Procedure[5] (in this case, the challenge in the same matter can no longer be reviewed).

[redacted]
lawyer
authorized by Director General

[1] Full answer in Estonian will be added to relevant documents.
[2] Since their overview of what changes they made and how they make sure that such incidents won't take place in the future, are ca 10 pages, the full answers to inquiries will be added to relevant documents.
[3] Full answers to the inquiries will be added to relevant documents.
[4] https://www riigiteataja.ee/en/eli/527032019002/consolide
[5] https://www riigiteataja.ee/en/eli/512122019007/consolide