



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Dear [REDACTED]

Your: 28.10.2021

Our: 19.01.2022 no 2.1.-1/21/2877

Reprimand and notice of termination of proceedings in a case concerning personal data protection

I FACTUAL CIRCUMSTANCES

1. On 8 February 2021, [REDACTED] sent its updated privacy policy and general terms and conditions to [REDACTED] ('Appellant'), who lives in Germany.
2. On 14 February 2021, the Appellant replied to [REDACTED] that he did not agree with the updated privacy policy and general terms and conditions and therefore wished to stop using the services of [REDACTED]. The Appellant asked [REDACTED] to close his user account and to transfer the amount in the account to the current account he had specified.
3. On 18 February 2021, the Appellant wrote to [REDACTED] to withdraw his consent to the processing of his personal data, requesting the erasure of the personal data collected about him and asking [REDACTED] to notify the other data processors to whom the data had been submitted of the deletion of his data. The Appellant asked [REDACTED] to confirm that his personal data had been erased and that a corresponding notification had been sent to the other data processors. The Appellant asked [REDACTED] to give reasons and to specify the legal basis for the possible refusal to erase the personal data.
4. On 18 February 2021, [REDACTED] confirmed that it had closed the user account of the Appellant on 15 February 2021. [REDACTED] explained that the terms and conditions for the protection of personal data were available to the Appellant on the website of [REDACTED]. [REDACTED] further explained that pursuant to the Money Laundering and Terrorist Financing Prevention Act, the controller is obliged to retain the personal data used for identification for five years after the closure of the user account. [REDACTED] also added a web link to the relevant national legislation (<https://www.riigiteataja.ee/en/eli/ee/530062021005/consolide>).
5. On 16 March 2021, the Appellant turned to [REDACTED] for information on whether [REDACTED] had stored his personal data and, if so, what data, referring to Article 15 (1) of the General Data Protection Regulation (GDPR). The Appellant also requested information as to whether [REDACTED] had transferred his personal data to a third country or to an international organisation and what safeguards would be applied in such a case, referring to Article 15 (2) of the GDPR. The Appellant also requested that a copy of the

personal data collected about him be sent electronically. In addition, the Appellant requested that the personal data collected about him be erased. █████ sent a reply to the Appellant on the same day, reiterating its letter of 18 February 2021 and adding that █████ had to act in accordance with Estonian law and not German law (including referring to the Money Laundering and Terrorist Financing Prevention Act). The Appellant had agreed to these conditions when registering as a customer of █████. The Appellant considered that since Estonia is a member state of the European Union, the GDPR should be applied. █████ explained to the Appellant that the legal basis for the storage of personal data comes from section 47 (1) of the Money Laundering and Terrorist Financing Prevention Act. **In the following letter, the Appellant agreed that personal data should be retained**, but requested a copy of the personal data collected, referring to Article 5 (1) and (2) of the GDPR. █████ explained that it retained the data of the Appellant which the Appellant had provided to █████ when registering as its customer and that this data was known to the Appellant. The Appellant replied that he would contact the relevant supervisory authority if █████ did not provide him with the requested information and a copy of the personal data within the deadline.

6. On 20 April 2021, the Appellant lodged a complaint with the Hamburg Commissioner for Data Protection and Freedom of Information. The Appellant requested the erasure of his personal data and the provision of information on the personal data collected about him by █████.
7. A complaint was submitted to the Data Protection Inspectorate for processing through the Internal Market Information System (IMI) of the European Commission.
8. On the basis of the correspondence attached to the complaint by the Appellant, the Data Protection Inspectorate established that the controller had provided the Appellant with a link to the website of █████, from which it was possible to read its privacy policy. █████ did not issue a copy of the personal data processed to the Appellant. In its replies, █████ referred to the legislation (including web links to the legislation) on the basis of which the personal data is processed.
9. On 22 October 2021, the Data Protection Inspectorate initiated supervision proceedings on the basis of clause 56 (3) 8) of the Personal Data Protection Act and requested the controller to answer the following questions in its inquiry:
 1. Has █████¹ issued to the Appellant:
 - a. a copy of the personal data of the Appellant processed by █████ (Article 15 (3) of the GDPR);
 - b. information on the processing of the personal data of the Appellant pursuant to Article 15 (1) and (2) of the GDPR?
 2. If █████ has provided the Appellant with the information mentioned in the previous clause, please provide the Data Protection Inspectorate with the relevant proof (including a letter to the Appellant, information sent to the Appellant about the processing of personal data, a copy of the personal data processed sent to the Appellant).
 3. If █████ has not provided the Appellant with the above, I propose to comply with the request of the Appellant and send the Appellant information under Article 15 (1)

¹ In its inquiry, the Data Protection Inspectorate used the short name █████.

and (2) of the GDPR and a copy of personal data under Article 15 (3) of the GDPR, or, if ██████████ considers that there is a legal basis for refusal, provide the Appellant and the Data Protection Inspectorate with a legally motivated justification for not sending the information.

II EXPLANATIONS FROM THE PERSONAL DATA PROCESSOR

██████████ submitted its explanations on 28 October 2021:

On 14 February 2021, ██████████ (the Appellant) sent an e-mail to ██████████ stating that he did not agree with the updates to the general terms and conditions and privacy policy of ██████████ and therefore wished to stop using the services of ██████████ and close his user account. In the same e-mail, the Appellant requested that ██████████ close his account and requested that the investments be transferred to the bank account referred to (Annex 1). On 18 February 2021, the Appellant sent ██████████ a request to delete all his personal data after the account had been closed. ██████████ explained to the Appellant that, in accordance with the applicable regulations, it was not possible to do so immediately (Annex 2). The correspondence between ██████████ and the Appellant on the same subject continued in March 2021, when the Appellant asked for confirmation if we were still keeping his data after the account was closed. In addition, the Appellant again requested information on Article 15 (1) and (2) of the GDPR. The information referred to in Article 15 (1) and (2) of the GDPR is available in the privacy policy of ██████████

References to such information were sent Appellant separately on 18 February 2021 (Annex 2) and 16 March 2021 (Annex 3). We additionally provided this information to the Appellant on 28 October 2021 (Annex 4).

As regards the submission of a copy of the personal data, we have requested additional information and explanations from the customer service employee who was in contact with the Appellant and regrettably, they misunderstood (especially in the light of previous communication) that it was merely a request to confirm that his data had been deleted immediately after the account was closed. Therefore, the employee had only provided general information on the processing. We forwarded to the Appellant a copy of the personal data directly in encrypted form on 28 October 2021 (Annex 4). We have contacted the relevant customer service employee and given instructions for the future.

We hope that the answers and documents provided are sufficient and that you consider it possible to close the proceedings against ██████████. Please let us know if you have any further questions and we will be happy to answer

In its reply, ██████████ had attached the e-mail of the Appellant of 14 February 2021, the correspondence between the Appellant and ██████████ on 18 February 2021 and 16 March 2021, the e-mail of ██████████ of 28 October 2021 to ██████████ Appellant, and a copy of the personal data of the Appellant

III JUSTIFICATIONS OF THE DATA PROTECTION INSPECTORATE

(a) REQUEST FOR ERASURE OF PERSONAL DATA

1. Pursuant to Article 17 (1) (b) of the GDPR, the data subject has the right to request that the controller delete personal data concerning them without undue delay if the data subject withdraws consent on which the processing is based in accordance with Article 6 (1) (a) and where there is no other legal ground for the processing.
2. However, the right to the erasure of data (the ‘right to be forgotten’) is not absolute. Article 17 (3) (b) of the GDPR provides that paragraphs 1 and 2 shall not apply to the

extent that the processing of personal data is necessary for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest. These legal bases for the processing of personal data are set out in Article 6 (1) (c) and (e) of the GDPR. Pursuant to recital 42 of Directive (EU) 2015/849 of the European Parliament and of the Council² on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, all Member States consider the fight against money laundering and terrorist financing to be an important public interest and the processing of personal data on the basis of the directive for the purposes of the prevention of money laundering and terrorist financing shall be considered to be a matter of public interest under the GDPR (Article 43). Article 6 (3) of the GDPR specifies that the basis for the processing of personal data referred to in paragraphs 1 (c) and (e) shall be established by Union law or by the law of the Member State applicable to the controller. The Estonian legislator has established the corresponding rules in the Money Laundering and Terrorist Financing Prevention Act. Namely, pursuant to subsection 48 (2) of the Money Laundering and Terrorist Financing Prevention Act, the obliged entity is allowed to process personal data gathered upon implementation of the Money Laundering and Terrorist Financing Prevention Act only for the purpose of preventing money laundering and terrorist financing, which is considered a matter of public interest for the purposes of the GDPR, and such data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

3. The retention period of data is regulated by section 47 of the Money Laundering and Terrorist Financing Prevention Act. Pursuant to subsections (1), (2), (3), (5), and (6) of this section, the obliged entity must retain the data for **five years** after the termination of the business relationship, making of the transaction, or performance of the reporting obligation. In its replies, ██████ referred to the same legal basis for the retention of the personal data of the Appellant.
4. It remains to be clarified whether ██████ is an obliged entity within the meaning of Money Laundering and Terrorist Financing Prevention Act. Although ██████ is not an institution within the meaning of section 6 of the Money Laundering and Terrorist Financing Prevention Act and therefore ██████ is not an obliged entity within the meaning of section 2 of the Money Laundering and Terrorist Financing Prevention Act, I find, based on the explanations given by ██████ to the Data Protection Inspectorate on 12 August 2021 that the obligation to retain personal data arises for ██████ from the combined effect of sections 47, 15, 20, and 24 of the Money Laundering and Terrorist Financing Prevention Act for the following reasons:
 - 4.1. given the nature of the activities of ██████, the application of measures to prevent money laundering is essential. Among other things, the basis for such a need is section 15 (application of measures to prevent money laundering within the group) and section 24 (reliance on third party data) of the Money Laundering and Terrorist Financing Prevention Act.
 - 4.2. ██████ belongs to the same group as ██████ who is an obliged entity within the meaning of clause 6 (1) 2) of the Money Laundering and

² <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A32015L0849>

Terrorist Financing Prevention Act and a creditor operating under the supervision of the Estonian Financial Supervision Authority who provides small loans to consumers. [REDACTED] has also been issued a corresponding activity license by the Estonian Financial Supervision Authority on 21 March 2016.³ [REDACTED] is not a creditor (or other legal entity subject to an activity license) under the supervision of the Financial Supervision Authority, but acquires loan claims from [REDACTED].

- 4.3. As an obliged entity, [REDACTED] must make sure that the assets used in the business relationship are legitimate (sections 20 (3) and (4) of the Money Laundering and Terrorist Financing Prevention Act). After concluding the loan agreement, [REDACTED] assigns the claim to [REDACTED] so that [REDACTED] will continue to administer the claims as a creditor, but the financial claim will be transferred to [REDACTED], in turn, assigns the claims to its investors. Due to this chain and business activities, it is extremely important that [REDACTED] can ensure the legitimacy of the origin of the assets used in the business relationship and be sure that they are not money laundering assets. Therefore, it is important that [REDACTED] also applies the requirements arising from the Money Laundering and Terrorist Financing Prevention Act.
- 4.4. Under the guidance of the Financial Action Task Force (FATF), the Estonian Financial Intelligence Unit, and related legislation, financial groups should be required to implement group-wide measures to prevent money laundering and terrorist financing, including principles and codes of practice for the exchange of group-wide information in relation to the prevention of money laundering and terrorist financing.⁴
- 4.5. In addition to the above, [REDACTED] has the right and obligation to apply the measures of the Money Laundering and Terrorist Financing Prevention Act when acting on the basis of section 24 of the Money Laundering and Terrorist Financing Prevention Act as a third party on whose data the obliged entity (e.g. a bank) relies. In practice, it would not be possible for [REDACTED] to do business without measures to prevent money laundering, as in that case, it would not be possible for [REDACTED] to have a bank account through which investors could make financial transactions. The reason is that banks, as obliged entities, must also implement measures to prevent money laundering and, in order for [REDACTED] to have a bank account for its business, banks have required [REDACTED] to apply measures to prevent money laundering in full, because they rely, inter alia, on [REDACTED] data to verify transaction data.
- 4.6. Banks are granted this right, inter alia, by clauses 20 (1) 4) and 6) of the Money Laundering and Terrorist Financing Prevention Act and subsection 23 (2) of the Money Laundering and Terrorist Financing Prevention Act. In applying these due diligence measures, banks have a wide discretion. According to these provisions banks may require [REDACTED] to provide information about its customers (i.e. [REDACTED] investors) so that the bank can assess the risks associated with [REDACTED] and apply other due diligence measures. The bank does not have to collect data about their own customers, but may rely on the data collected by another person (i.e. its customer, in this case [REDACTED]) in accordance with section 24 of the Money Laundering and Terrorist Financing Prevention Act. If [REDACTED] did not provide the bank with data on its customers within the required deadline (i.e. [REDACTED] would not allow the bank to perform due diligence

³ [REDACTED]

⁴ <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>, clause 18, pp. 18–19.

measures), the bank would have the right to cancel the current account agreement entered into with [REDACTED] (subsection 42 (4) of the Money Laundering and Terrorist Financing Prevention Act).

- 4.7. On a similar basis, [REDACTED] requires [REDACTED] to control the activities of investors, as the assets originally arising from these transactions will be used by [REDACTED] to grant credit in the future. I further note that in order to rely on the data collected by [REDACTED] pursuant to section 24 of the Money Laundering and Terrorist Financing Prevention Act, [REDACTED] need not be an obliged entity within the meaning of the Money Laundering and Terrorist Financing Prevention Act. Pursuant to section 24 of the Money Laundering and Terrorist Financing Prevention Act, other persons may also collect and process data necessary for the application of measures to prevent money laundering and terrorist financing. Under that provision, data are also collected, for example, by undertakings specialising in the application of due diligence measures, which are not themselves obliged entities under the Money Laundering and Terrorist Financing Prevention Act, but which process the data in order to provide services to obliged entities.
5. Pursuant to subsection 47 (7) of the Money Laundering and Terrorist Financing Prevention Act, the retained data must be erased after the expiry of the term, unless the legislation regulating the relevant field establishes a different procedure. Data relevant to the prevention, detection, or investigation of money laundering or terrorist financing may be retained for a longer period, but not more than five years after the expiry of the initial period, by order of the competent supervisory authority. Thus, the maximum retention period for personal data is 10 years.
6. If the controller does not satisfy the request of the data subject (e.g. the data is not erased), then in accordance with Article 12 (4) of the GDPR, the controller must also clearly justify the rejection of the request. It appears from the correspondence between the Appellant and [REDACTED] that the account of the Appellant was closed on 15 February 2021 and that the Appellant also requested that his personal data be erased. [REDACTED] explained to the Appellant that, in accordance with the applicable regulations, his personal data could not be erased immediately and [REDACTED] was obliged to retain them for five years. The correspondence on the same topic continued on 16 March 2021 and [REDACTED] again referred to the obligation to retain data arising from the Money Laundering and Terrorist Financing Prevention Act. [REDACTED] therefore informed the Appellant twice of its obligation to retain his personal data. **The information that the personal data of the Appellant could not be erased immediately was noted by the Appellant in the e-mail to [REDACTED] on the same date.**
7. Based on the above, since [REDACTED] is fulfilling its legal obligation and performing a task of public interest in collecting personal data (Article 6 (1) (c) and (e) of the GDPR) and has a legal obligation to retain personal data (sections 15, 20, 24, and 47 of the Money Laundering and Terrorist Financing Prevention Act), [REDACTED] cannot fulfil the request of the Appellant for the deletion of his personal data (Article 17 (3) (b) of the GDPR). **The Appellant himself has already taken note of this information on 16 March 2021, i.e. before submitting his complaint on 20 April 2021.**

(b) REQUEST OF THE DATA SUBJECT FOR ACCESS TO PERSONAL DATA PROCESSED**i. Information on the terms and conditions for the processing of personal data (Article 15 (1) and (2) of the GDPR)**

8. The data subject has the right under Article 15 of the GDPR to inspect the personal data collected about them and to receive explanations regarding the circumstances of the processing. In the present case, the Appellant requested [REDACTED] to provide that information on the basis of Article 15 (1) (b) to (h) and (2) of the GDPR.
9. [REDACTED] has published the privacy policy of the company on its website [REDACTED] and provided the Appellant with the relevant information in its e-mails of 18 February 2021 and 16 March 2021. In addition, [REDACTED] clarified its privacy policy in an e-mail sent to the Appellant on 28 October 2021.
10. **In view of the above, the request of the Appellant has been met and [REDACTED] has provided the Appellant with the information requested under the complaint concerning the terms and conditions for the processing of the personal data of the Appellant.**

II Provision of a copy of personal data (Article 15 (3) of the GDPR)

11. The data subject has the right of access to personal data collected about them under Article 15 of the GDPR. Article 15 (3) of the GDPR entitles the Appellant to request a copy of the personal data processed about him. In this case, the controller must issue the information within one month (Article 12 (3) of the GDPR).
12. According to the explanations provided by [REDACTED] during the supervision procedure, the customer service employee of [REDACTED] misunderstood the Appellant and therefore did not provide the copy of his personal data requested by the Appellant. **The Data Protection Inspectorate cannot accept this, as the e-mail of the Appellant of 16 March 2021 contains an explicit request to provide a copy of his personal data** (*Please provide me with a copy of the personal data I have stored about you free of charge. If I submit this application electronically and do not note otherwise, the information must be made available to me in a common electronic format*), from which there can be no misunderstanding or questions as to whether or not the person wants to receive a copy. Even if such a request remained unclear to the customer service employee, as [REDACTED] claims, considering the dispute which lasted for almost a month, the customer service employee should have carefully read the e-mails of the Appellant and the requests contained therein, and talk through any misunderstandings with the Appellant. However, [REDACTED] did not do that. **Thus, [REDACTED] violated the obligation arising from Article 15 (3) of the GDPR.**
13. According to the explanations given during the supervision procedure, [REDACTED] issued a copy of his personal data to the Appellant on 28 October 2021 (the corresponding e-mail is attached to the reply sent to the Data Protection Inspectorate). **Thus, [REDACTED] has fulfilled its obligation under Article 15 (3) of the GDPR.**

IV REPRIMAND AND NOTICE OF TERMINATION OF PROCEEDINGS

However, I would like to explain that it is obligation of the controller to make sure that data is being processed in compliance with the GDPR. [REDACTED] disregarded the explicit request of the Appellant to provide him with a copy of the personal data collected about him. In view of the above, [REDACTED] violated the requirements set out in the GDPR. However, in view of the fact that [REDACTED] w provided [REDACTED] with all his personal data and confirmed that the customer service employee has also been given the relevant instructions for the future, **I reprimand [REDACTED] pursuant to Article 58 (2) (b) of the GDPR and draw attention to the following:**

- 1. the controller has the obligation to submit a copy of the personal data concerning the data subject at the request of the data subject (Article 15 (3) of the GDPR).**

If the data subject wants data about themselves, [REDACTED] must do everything in its power to ensure that all data is provided. If personal data are not provided, it must be made very clear which type of data and for what reason cannot be provided.

- 2. The controller provides information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. This period may be extended by two months, if necessary, taking into account the complexity and volume of the request. The controller informs the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay (Article 12 (3) of the GDPR).**

Thus, if a person requests a copy of personal data concerning them, the copy must be provided within one month or, if justified, the deadline for replying may be extended within that month. In accordance with the GDPR, the maximum legal term for providing data can be three months.

- 3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (Article 12 (4) of the GDPR).**

Thus, if [REDACTED] considers that it has reasonable grounds for not providing data, this must be justified to the data subject within one month.


In view of the above and the fact that [REDACTED] has now provided [REDACTED] with his personal data, I terminate the supervision proceedings.

I further note that in a situation where the improper practice of processing personal data in this way continues, the Data Protection Inspectorate has the right to issue a precept to [REDACTED] (and, if necessary, impose a penalty payment) or hold the controller liable in a misdemeanour. A legal person may be fined up to 20,000,000 euros or up to 4% of its total annual worldwide turnover for the previous financial year, whichever is greater.

This decision can be disputed within 30 days by:

- submitting a challenge to the Director General of the Data Protection Inspectorate pursuant to the Administrative Procedure Act⁵ or
- filing a petition with an administrative court pursuant to the Code of Administrative Court Procedure⁶ (in this case, any challenges submitted in the same case can no longer be processed).

Yours sincerely

/signed digitally/


Authorised by the Director General