



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Management board member

Our: 03.03.2021 no 2.1.-1/18/3275

Reprimand for failure to comply with the requirements of the General Data Protection Regulation

Notice of termination of the proceeding

The proceeding of the Estonian Data Protection Inspectorate (Inspectorate) concerned the claim of a Polish citizen (complainant) in regard to the fact that the person was unable to realise his right for deletion of data. The Supervision proceeding was conducted in cooperation with the concerned data protection authorities.

The claim states that despite several enquiries, personal data (incl. e-mail address, telephone number, payment card data) has not been deleted. You were first contacted on 23 May 2018 and requested to delete data. Your reply to the enquiry stated that the data would be deleted within 72 hours. On 5 June 2018, the complainant checked whether his data has been deleted, but it was not. The complainant then contacted the technical support service and requested once more for the data to be deleted. The person received a reply along with an apology and assurance that the account was forwarded for deletion. On 23 June 2018, the complainant checked once more whether his data has been deleted, but it was still not done.

Given the above, we initiated a supervision proceeding on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

-

During the proceeding, stated the following: *"We anonymised all personal data related to the account No. on 12 July 2018. We fulfilled the data subject's application of 23 May 2018 only on 12 July, forwarded misleading information about the data deletion and did not forward information about the legal basis for data processing as a result of the employee's violation. We have compiled guidelines for the customer service representatives for responding to such data subject applications, but unfortunately, the aforementioned application was processed by an employee who ignored the guidelines given to them. We terminated the employment contract with that employee on October 2018.*

has not deleted personal data related to the account No. insofar as we blocked the account on 23 March 2018 because of a suspicion of fraud that arose in the process of routine checks. We explain that the data subject had more than one account on the platform, meaning that the client used several devices and phone numbers which is in accordance with the requirements and allowed. shares promo codes to its clients that can be used to invite another person to be a user, which results in a one-time

discount when using [REDACTED] services. The data subject did not share the promo code given to them with another person, but rather between their own two devices (the violation took place on 2018-02-11 05:41:55), meaning that they invited themselves to (re)join the platform with a purpose of getting the aforementioned personal benefit, which conflicts with the established rules of [REDACTED] (reference: [REDACTED]) and which led to the user's account being blocked. After having detected that access to the account was blocked, the data subject requested that the account be reopened. In these cases, the [REDACTED]'s standard procedure is to verify the identity of the customer using additional methods, i.e. we ask a copy of the data subject's identity document from the data subject. In a situation where an account is blocked and the data subject has submitted an application for reopening the account, we do not routinely delete the personal data related to the blocked account according to the aforementioned guidelines given to customer service representatives, we instead store them pursuant to clause 6 (1) f) of the General Data Protection Regulation with a purpose of protecting our rights in the case of disputes arising from the contract concluded with the data subject within three years after the last ride was made using the account.

Considering what we learned from this case, we will improve our internal guidelines within this calendar month, including in such a way that the employees answering to and fulfilling the applications of data subjects will clearly understand which actions are necessary to realise the rights of the data subject. In addition, within this year and the first quarter of the following year, we will train our employees in addition to routine training in order to avoid situations where the data subject cannot use the right of deleting the data related to them or where people are given information that their personal data is being deleted, although it is not.“.

-

Given the above, we asked information from [REDACTED] in regard to whether and why it is necessary to retain the personal data of the complainant under Article 6 (1) f) of the GDPR.

[REDACTED] responded as follows: “We have conducted an assessment of legitimate interests in regard to this case, consisting of three stages: first, we identify the specific legitimate interest; next we implement a necessity test; finally, we compose an impact assessment in which we consider the impact on the interests and the rights and freedoms of individuals, and assess whether it exceeds our legitimate interests or not.”

1) Stage 1: identification of legitimate interest(s)

[REDACTED] is performing the identification and prevention of fraud on the basis of legitimate interest. These operations are important and serve a wider purpose, as it is not only necessary for [REDACTED] but also protects the interests of the persons whose credit card (or credit card data) has been stolen. These interests and benefits are significant for [REDACTED] as a company, as without appropriate anti-fraud measures, our clients would become subject to financial fraud and that could jeopardise the entire existence of our company, as the company is responsible for fair billing and must provide compensation to the person suffering direct damages, if necessary. In this case, we have identified an abuse of the friend code where the given client has invited themselves to join the [REDACTED] platform, thus acting directly in self-serving interests, and the client has been aware of their fraudulent activity or at least their unethical behaviour.

2) Stage 2: implementation of the necessity test

We retain the data described in our letter of 31 July 2019 for the purpose of detecting fraud. The retention of this data helps us identify fraud and, in particular, networks of fraudsters, which have the biggest impact of all. If we did not have these data, each fraudulent user could simply log into the platform again by using the same e-mail address, telephone number, device and/or credit card. The retention period of 10 years helps to identify and map the schemes and devices of fraudsters. Replacement of devices and telephone numbers is also costly for fraudsters, thus it serves a restrictive effect, as the changing of single elements (only credit card data, e-mail address) still prevents access to the platform. The impact of networks multiply the impact of frauds in comparison with individual fraud cases. Less interfering and less intrusive methods have not been determined for achieving these objectives. The resolution of individual fraud cases is also time- and energy-consuming, which is not proportionate to the amounts subject to fraud, especially given that such cases occur in several jurisdictions on different continents. The networks of fraudsters are considered the most significant and harmful of the legitimate interests described in first stage. Therefore, our operations include identification of fraud, including networks, and blocking thereof.

3) Stage 3: consideration of the impact assessment and decision-making

None of the data we collect are considered special data in terms of the GDPR. Our services are not aimed at children or other categories of vulnerable persons and all data have been collected directly from the data subjects. We do not share these data with other parties and only use it internally, meaning that it does not prevent the individual from using the services of any other service provider in any way, whether in regard to the service areas provided by us or other. As explained above, we take reasonable preventive measures regarding access, while not rendering re-registering as a user impossible, if another e-mail address, telephone number, device and/or credit card is used. This is illustrated by the fact that the user filing the complaint has rejoined the platform by using the same name, but a different e-mail address, telephone number, device and/or payment method. [REDACTED] mentions in its privacy policy that the data shall be retained for ten years in the context of detecting frauds (Article 7). We understand that in this case it could not be excluded that the message did not come off clearly enough in the privacy regulation, as it was only conveyed in English. This description is intentionally general in the current Polish version in order not offer any tips to possible fraudsters. Although it can be presumed that some people may dispute the data processing, we can also safely assume that the people who file a dispute are most likely the ones who have actually committed fraud. Customer support is available in local languages. If the suspicion of fraud is incorrect (false positive), it can be determined via customer support. If it becomes apparent that there is no reason for (further) suspicion, these data shall not be retained for ten years and shall be deleted in accordance with the retention term of the account data or deleted on the basis of a deletion request. In this case, the customer service addressed the questions of the data subject in Polish. In light of the information arising from all three stages mentioned above, [REDACTED] is of the opinion that the personal data of Polish citizen [REDACTED] may be retained on the basis of legitimate interest under Article 6 (1) f) of the GDPR.”

Based on the above reply, the supervisory authorities were not convinced that the 10-year retention of the complainant’s data complies with the requirements provided for in the GDPR.

Therefore, the Inspectorate made a further enquiry on 30 October 2020, in which we requested: *To provide very detailed and comprehensive explanations regarding the 10-year retention period, based specifically on the complainant and taking into account the requirements provided in articles 17 (3) and 21 (1) of the GDPR.*

██████████ justified the data processing as follows: ██████████ retains ██████████'s personal data for 10 years because it adheres to our internal rules of procedure in the event fraud is detected. In the case of ██████████, fraud was confirmed, and therefore we have to further process the personal data. The most important factor for a 10-year period for the retention of personal data of persons who have committed fraud is ██████████'s legal protection. There is a high probability that this case may escalate into a civil or criminal case; therefore, we must keep records to prove what happened. As mentioned earlier, the 10-year retention period is provided for by Estonian legislation.

In this situation, ██████████ protects itself from a person who committed a violation, violated our terms and conditions, and caused damage to the company (the team had to deal with the detection of fraud, etc.).

We also believe that a person must be prepared to take responsibility for intentional fraud and anticipate that the legal person against whom fraud is being committed wishes to protect itself.

Therefore, the person's right to erasure of data is also restricted, as ██████████ may wish to use the data for the establishment, exercise, or defence of legal claims. With regard to the right of objection, ██████████ believes that we process personal data for a valid and legitimate reason that outweighs the interests, rights, and freedoms of the data subject, i.e. for the purpose of preventing further fraud and ensuring ██████████ is able to file a legal claim or defend itself.

On the basis of this response, the Estonian Data Protection Inspectorate was unable to ascertain whether the retention of data complies with the requirements set out in the GDPR, which is why we explained the following in the repeated enquiry sent to ██████████ on 20 November 2020:

1.1. First of all, we clarify that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed (see point a) of article 17 (1) of the GDPR). Given that the complainant's account has been blocked and the service can no longer be used with that account, the purpose for which the data was collected no longer exists.

1.2. Article 17 (3) of the GDPR provides as follows: paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- a) for exercising the right of freedom of expression and information;*
- b) for compliance with a legal obligation which requires processing by a Union or Member State law to which the data controller is subject;*
- c) for reasons of public interest in the area of public health;*
- d) for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes;*
- e) for the establishment, exercise, or defence of legal claims.*

1.2.1. *In the specific case, points a), c), and d) are not relevant.*

1.2.2. *With regard to point b), we note that the processing of personal data (incl. the retention of data) on the basis of this point is permitted if the obligation to process personal data arises from a specific law (e.g. subsection 12 (1) of the Accounting Act). In doing so, we emphasise that data may also be processed in such a case only for the purposes provided by a specific law (e.g. for retention purposes only).*

However, with regard to section 146 of the General Part of the Civil Code Act, this section gives rise to a claim limitation period and does not give rise to a direct obligation (statutory obligation) to retain data. Moreover, [REDACTED] has not referred to any other specific law that would give [REDACTED] a statutory obligation to process data for 10 years, including which would give the right/obligation to retain data for 10 years for the purpose of detecting or preventing fraud. Nor is such a specific law known to the Inspectorate. In view of the above, in the specific case, point b) is also irrelevant for the processing of data for the purpose of fraud prevention, which would presuppose that there is a legal obligation to process the data.

Based on the above, [REDACTED] does not have the right/obligation to process (including to retain, use) data for 10 years for the purpose of detecting, preventing, and/or avoiding fraud.

1.2.3. *With regard to point e), however, we note that this clause only applies if the processing of personal data is necessary for the establishment, exercise, or defence of legal claims.*

In order for the supervisory authorities to assess whether the retention of the complainant's personal data in this specific case is necessary for the establishment, exercise, or defence of legal claims, [REDACTED] must prove to the supervisory authorities that the processing of the complainant's data is necessary and that the data processing also complies with the requirements provided for in articles 5 and 6 of the GDPR.

First of all, we emphasise that the processing of personal data is lawful only if at least one of the conditions set out in article 6 (1) of the GDPR is met. Only point f) of article 6 (1) of the GDPR (legitimate interest) is relevant in the specific case. We also note here that [REDACTED] has sent an analysis of legitimate interest to the Inspectorate on 20 December 2019, but it is based on the detection and prevention of fraud. For this purpose, however, it is not justified to retain personal data for 10 years. Thus, the Inspectorate also does not have an analysis of legitimate interests that would justify the retention of data for 10 years. The Inspectorate also doubts that the retention of data for 10 years is necessary and legitimate in the case of this specific violation.

1.2.3.1. *If [REDACTED] maintains that the retention of personal data for a period of 10 years is necessary in this specific case for the establishment, exercise, or defence of legal claims, and that the processing of data complies with point f) of article 6 (1) of the GDPR, [REDACTED] must also provide the supervisory authorities with a thorough analysis of the legitimate interest, on the basis of which the supervisory authorities can assess the need for data processing.*

On 8 December 2020, [REDACTED] sent a confirmation that the personal data of the complainant had been deleted. It was also confirmed during the supervision proceedings that they still retain only the documents retained on the basis of the Accounting Act, i.e. invoices with basic invoice data (transactions performed on the platform) with a term of 7 years. Invoices shall be retained for seven years in accordance with Article 6 (1) c) of the GDPR and subsection 12 (1) of the Accounting Act. Polish clients receive invoices at the end of each trip that include the following data: invoice number, invoice sent by: [REDACTED] ([REDACTED]), invoice received by: first name, start address, end address, amount for trip, 4 last digits of payment card used. The invoice is sent to the email address specified by the client.

In addition, we identified that [REDACTED] has not translated the data protection terms and conditions of all EU countries into the local language. In this regard, [REDACTED] noted the following on 22 May 2020: *“The data protection terms and conditions of all passengers of EU Member States have been respectively translated into the local language or into English, if the use of the latter is common in the relevant country (e.g. Malta). The data protection terms and conditions of passengers of third countries and the translations thereof (if these have been translated into the local language due to the recommendations of our local team) are available on the website [REDACTED]. In the case of many third countries, the local team of [REDACTED] has not submitted an order/proposal for local translations, as the English translation is considered sufficient.”*

Reprimand and notice on the termination of proceedings

Based on the above, [REDACTED] has deleted all the personal data of the complainant, except for the data which is required to be retained for seven years pursuant to the Accounting Act.

However, we shall clarify that the controller is obligated to ensure that data processing occurs in accordance with the General Data Protection Regulation. Yet, [REDACTED] has provided the complainant untrue information in regard to the deletion of data. It has been noted in the response to the complainant that the data have been deleted, although not all data have been deleted. First, no personal data which are required to be retained pursuant to the Accounting Act have been deleted, and secondly, the remaining data were deleted only during the supervisory procedure. In addition, not all data protection terms and conditions of EU countries are available in the local language.

As not all data protection terms and conditions of EU countries have been translated into the local language on the network site of [REDACTED] and the complainant was provided untrue information regarding the deletion of data, the requirements of the General Data Protection Act were violated. Considering that: 1) the personal data for the processing of which there is no legal basis have been deleted, 2) [REDACTED] has taken and is taking measures to avoid similar situations in the future, and 3) the data protection terms and conditions have been translated into local languages, we are issuing a reprimand to [REDACTED] under the General Data Protection Regulation and draw attention to the following:

- 1. The data controller shall ensure during the processing of personal data that said data is processed lawfully, fairly and in a transparent manner in relation to the data subject (article 5 (1) a) of the General Data Protection Regulation).** In this regard, it is important that data processing is clear and understandable and that people are not provided misleading information in regard to the processing of personal data (including deletion of data).

2. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, provided there is no legal basis for further data processing (article 17 of the General Data Protection Regulation).
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 General Data Protection Regulation).

On the basis of the aforementioned and the fact that the personal data of [REDACTED], for the processing of which there is no legal basis, has been deleted, we shall terminate the supervisory proceeding.

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 Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

/signed digitally/

[REDACTED]

lawyer

authorised by Director General

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolide>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolide>