REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

[redacted]
[redacted];
[redacted]

Ours: June 20, 2023, nr 2.1.-1/20/7242

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

The Data Protection Inspectorate (the 'Inspectorate') received a complaint from Polish citizen [redacted] ([redacted]) (the 'complainant') concerning the fact that the complainant did not understand on what legal basis and for what purpose it was necessary for [redacted] (the controller) to process (including collect and store) copies of identity documents (ID-card), including why a selfie was necessary with the document. In addition, the complainant wanted to know which data the controller needed to collect and a description of the technical and organisational security measures for the data processing. The complainant also asked for information on whether the data would also be processed automatically (for example, if profile analyses would be created). Although the complainant has approached the controller several times and also received answers, these answers have not been clear and comprehensible enough. Some questions have also been left unanswered.

Based on the submitted complaint, we initiated supervision proceedings on the basis of clause 56 (3) 8) of the Personal Data Protection Act. The supervision proceedings were carried out in cooperation with the other supervisory authorities concerned.

In the following, we present the questions submitted by the Inspectorate, the answers of [redacted], and, if necessary, additional explanations of the Inspectorate.

1. Inspectorate: ***List all the information (e.g. name, e-mail address, ID card copy, a selfie) that you collect as part of your service(s).***

1.1. [redacted]:
[redacted] *processes the following personal data in the framework of our services at* [redacted] *exchange:*
user data *- e-mail address, login, full name, safety code, citizenship, residency, country of birth, login history, telephone number, PESEL number, date of birth, data from their personal ID card/passport/residency card (series and number, expiry date, place of issue, state of issue), image (photo or video), residence address (street name, street number, apartment number, postal code, town, country), data from utility bills, information about business activity, purpose of creating an account, source of funds transferred into the exchange, source of funds available to the user, information about any political positions held (status of a Politically Exposed Person ("PEP") or a PEP's family member or close collaborator); image (service link via a third party tool, e.g. Facebook, Google or Weibo), details of orders (amount spent, date, time, vouchers or offers used), data for fraud prevention, data required by anti-money laundering ("AML") provisions, payment data (including verification data); data from user data messages concerning the Services (e.g. chat logs and support requests) or feedback about user data experience with the controller; <u>additionally for corporate users</u>: form of legal organisation, company name/business alias, Tax ID (NIP), KRS (Polish National Court Register) or some*

other company register, REGON (statistical number), country of business, date of formation, website, information about partners/shareholders (equity structure, how many shares held);

2. Inspectorate: ***Is it necessary for [redacted] to make a copy of the customer's identity document (e.g. ID-card) and in which cases?***

If it is not necessary, confirm it;
if it is necessary:

- ***on what legal basis are copies of identity documents made? If the obligation arises from a specific piece of legislation, refer to a specific clause in that legislation.***
- ***If the obligation does not arise directly from the legislation, then thoroughly and comprehensibly explain the necessity (purposefulness) of a copy of the identity document, including why it is not possible to use measures that are less infringing on people's rights to fulfil a specific purpose.***
- ***Whether and in which cases it is necessary to take a selfie in addition to the copy of the ID-card. Indicate the specific legal basis and purpose.***

2.1. [redacted]:

[redacted] *has a legal obligation to process of identity documents of customers.* [redacted] *is an obliged entity in the meaning of Money Laundering and Terrorist Financing Prevention Act from 26.10.2017 (hereinafter the "AML Act" (§ 3 par. 1 sec. 3), therefore as such entity it is obliged to apply due diligence measures (§ 19). In accordance with § 20 par. 1-6 "basic" due diligence measures consist of:*

- ***identification of a customer*** *or a person participating in an occasional transaction and* ***verification of the submitted information*** *based on information obtained from a reliable and independent source, including using means of electronic identification and of trust services for electronics transactions;*
- *identification and verification of a customer or a person participating in an occasional transaction and their right of representation;*
- *identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the obliged entity to make certain that it knows who the beneficial owner is, and understands the ownership and control structure of the customer or of the person participating in an occasional transaction;*
- *understanding of business relationships, an occasional transaction or act and, where relevant, gathering information thereon;*
- *gathering information on whether a person is a politically exposed person, their family member or a person known to be close associate;*
- *monitoring of a business relationship.*

All of the above corresponds with requirements of European Union Directives:

a) *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance);*
b) *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance).*

For the purposes of the response, the focus was solely on the first due diligence

measure mentioned above: identification and verification of the information.

It is said in the § 21 par. 3 sec. 2) of the AML act, that identification of a client may be made basing a valid travel document issued in a foreign country. In accordance with § 21 par. 2 of the AML act, verification of the identity may be made basing on the previously mentioned document. Due to the fact that all [redacted] *customer´s are acquired remotely via the internet therefore, there is no possibility to process verification of identity in a "face to face" way, like it happens in bank branches. Therefore to process verification requirement* [redacted] *asks customer for the copy of an ID as a base of identity verification. Additionally, the customer is being asked to send a selfie photo with the document to compare his or her effigy with the one on the ID, this part is crucial to complete liveness check – according to recommendation of FATF[1]-especially in the case where business relation is being established without physical presence of a customer. What´s more this is a measure which is being established without physical presence of a customer. What´s more this is a measure which is being describer § 21 sec. 4 of the AML act (verification on the basis of other information originating from a credible and independent source, including means of electronic identification – in our case Jumio).*

One of the next obligation arising from the AML act is a preservation of a data (§ 47), on basis which the obliged institution must retain the originals or copies of the documents specified in § 21 (...) of the AML Act, which serve as the basis for identification and verification of persons, and the documents serving as the basis for the establishment of a business relationship no less than five years after termination of the business relationship. Therefore, It is an obligation to store the copy of ID.

Under these circumstances one should conclude that it is exist a legal basis of processing personal data of customer like the copies of the identity of documents and "selfies" – processing is necessary for compliance with a legal obligation to which the controller is subject (art. 6 sec. point. C of GDPR).

2.2. Inspectorate:

[redacted] provides virtual currency services to which the Money Laundering and Terrorist Financing Prevention Act[2] applies (see clause 2 (1) 10). [redacted] has a valid activity license for offering the virtual currency service issued by the Estonian Police and Border Guard Board.

Regarding making a copy of the customer's identity document and taking a selfie, the Inspectorate agrees with the explanations of [redacted]. In the opinion of the Inspectorate, [redacted] has correctly indicated if it has pointed out the following: "*Due to the fact that all* [redacted] *customer´s are acquired remotely via the internet therefore, there is no possibility to process the verification of identity in a "face to face" way, like it happens in bank branches. Therefore to process the verification requirement* [redacted] *asks customer for the copy of an ID as a base of identity verification. Additionally, the customer is being asked to send a selfie photo with the document to compare his or her effigy with the one on the ID, this part is crucial to complete liveness check – according to recommendation of FATF[3]-especially in the case where business relation is being established without physical presence of a customer. What´s more this is a measure which is being describer in § 21 sec. 4 of the AML act (verification on the basis of other information originating from a credible and independent source, including means of electronic identification – in our case Jumio).*".

The Estonian Financial Supervision Authority has also prepared a guide[4] in Estonian to clarify the legislation regulating the activities of the financial sector. The guide explains to obligated

[1] *http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf*
[2] https://www riigiteataja.ee/en/eli/511082020003/consolide
[3] http://www fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf
[4] https://www fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf

persons the content and fulfilment of the requirements provided for in the Money Laundering and Terrorist Financing Prevention Act and directly related legislative acts (European Union directives and regulations transposed into Estonian law by the Money Laundering and Terrorist Financing Prevention Act, as well as Financial Action Task Force recommendations and other instructions that have been the basis for establishing the relevant European Union directives and regulations), as well as the risks involved in the provision of the service, and guides obligated persons in the construction and operation of an organisational solution for preventing money laundering and terrorist financing. It follows from clause 4.3.1.14 of that guide that:

Verification of information collected in the course of identification:

i. must take place in the same place where the person is located (i.e. face-to-face) or by means of an information technology device (i.e. video identification) if the total amount of outgoing payments in one calendar month exceeds 15,000 euros for natural persons and 25,000 euros for legal persons, regardless of origin or their place of residence or domicile;
ii. does not therefore have to take place in the same place as the person (i.e. face-to-face) or by means of an information technology device (i.e. video identification) and can thus benefit from the option set out in clause 4.3.1.18 (**so-called two sources**) if (i) the total amount of outgoing payments to a natural person less than 15,000 euros per calendar month and less than 25,000 euros in the case of a legal person, and (ii) the person originates in a Contracting State of the European Economic Area or their place of residence or domicile is there.

Clause 4.3.1.22 of the guide states that one source is always:

i. **an identity document with the image provided for in clause 4.3.1.11 of this guide, i.e. a colour and legible copy/image of this document**[5]; or
ii. personal data and an image of the same document obtained from reliable and independent sources (for example, an image of a document obtained from the Police and Border Guard Board); or
iii. in the case of a lower than usual risk of money laundering and terrorist financing associated with both the customer and the business relationship, information obtained during strong authentication with a digital identification device (minimum: name and personal identification code or, in the absence of a personal identification code, date and place of birth) and audit trail certifying the performance thereof.

Pursuant to clause 4.3.1.23 of the guide, the following information may be the other source:

I. another document meeting the conditions of sub-clauses 1 or 2 of clause 4.3.1.22 of the guide (a copy thereof or the data and image obtained therefrom); or
II. information obtained in the course of strong authentication performed with a digital personal identification device (minimum: name and personal identification code or, in the absence of a personal identification code, date and place of birth) and an audit trail certifying the performance thereof; or
III. verification of data directly related to the person through the population register or other equivalent register, provided that it is a reliable and independent source within the meaning of clause 4.3.1.18 of the guide; or
IV. information received from the control payment; or
V. **other biometric data (fingerprint, facial image) or similar information;** or
VI. information to verify data directly related to the person (for example, place of work, residence, or study).

[5] For example, an ID-card

Thus, based on the reasons of [redacted] and taking into account the obligations of financial institutions (including explanations provided in the guide of the Estonian Financial Supervision Authority), [redacted] has the right and obligation to collect copies of personal ID-cards and selfies within its financial service. Therefore, the Inspectorate did not find any violation in this matter.

3. Inspectorate: ***Describe in as much detail as possible what <u>technical and organisational</u> measures [redacted] uses to ensure the appropriate security of personal data. Among other things, indicate where the data is stored and how access to the data is regulated (how many people have access, their job position, how the obligation of confidentiality of the personal data of employees is regulated, etc.). If the information provided to the Inspectorate also contains information which may not be provided to the complainant, this part must be clearly indicated.***

3.1. [redacted]:

[redacted] has only a one employee – [redacted] who works for [redacted] under a civil agreement. Moreover, [redacted] is a board member of [redacted] since 13.02.2020.

List of appropriate technical and organisational measures describes using the measures by [redacted] and entities which are related by capital or personally to [redacted]., [redacted], [redacted], [redacted] (Polish companies and Czech Company).

The list of employees refers to employee of [redacted] and as to employees of the abovementioned entities. The employees´ entitlements are vary depending on their official duties related to data processing.

3.2. Inspectorate:

The Inspectorate reviewed the documents submitted and found that [redacted] has sufficiently justified to the Inspectorate the use of appropriate technical and organisational measures. In addition, the Inspectorate agrees that the provision of these documents to the complainant may adversely affect the rights of [redacted] and that the provision of a description of the security measures may jeopardise the effectiveness of the security measures.

4. Inspectorate: ***Does [redacted] also use the collected data to make automated decisions (including to perform profile analysis)?***

If so, please provide substantive information on the logic used, the purpose for which the data is processed in this way, and the foreseeable consequences for the data subject.

4.1. [redacted]:

Personal data of users are subject to an automated processing decision based when verification of user´s account on the site [redacted] using the Jumio Corporation program. Decision based in an automated processing is used to use the services of the Data Administrator of services rendered for the service [redacted] in accordance with art. 22 sec. 2 p. of GDPR. The Jumio program automatically suggest whether the user account verification is approved, rejected or sent for manual checking by the Data Administrator.

However, due to some error and incompatibilities, that sometimes happens, Jumio Corporation Program rejects the user verification process, which prevents the user from going through the verification process and using [redacted] services. The user verification process is not fully and solely automated. The final decision to pass user verification is up to the security officer.

5. Inspectorate: ***Have you deleted all the data you have about complainant?***
If yes, on what date?
If no:
- ***point out all the information that you still have about him (e.g. name, personal identification code, e-mail address);***
- ***indicate the legal basis and retention period for all data to be retained.***

5.1. [redacted]:
The data controller have not deleted data of [redacted] *because there is still legal basis to process (storage) his personal data – in accordance with the art. 6 sec. 1 point. C of GDPR – processing is necessary for compliance with a legal obligation to which the controller is subject i.e. § 47 section 1 of AML Act – the data controller as „obliged entity must retain of the originals or copies of the documents specified in §§ 21, 22 and 46 of this act, which serve as the basis for identification and verification of persons, and the documents serving as the basis for the establishment of a business relationship* ***no less than five years after termination of the business relationship****". Moreover, in connection with § 48 section 2 of AML Act, The obliged entity (data controller) is allowed to process personal data gathered upon implementation of this Act only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.*

[redacted] *as the data controller still process the following personal data of the Complainant:*
name, surname, telephone number, e-mail address, logs (IP), place and address of residence, number of bank account, scan of ID, the date of issue of the document and date arising from e-mail correspondence.

Additionally explanation

The Complainant has created an account on the platform on 20.12.2017. There was the time when the sole owner of the platform was a Polish company – [redacted] *The Complainant has passed the account verification correctly and has actively carried out transactions on the exchange.*

Meanwhile, in connection with the new anti-money laundering regulations, the platform introduced a new KYC.

On 4 July 2019, the Complainant sent a verification form in accordance with the new requirements – to obtain access to all functionalities of the exchange.
The same day the verification was rejected. The reason for this rejection was: "In order to go through the verification process correctly, you need to resend the photos/scans of your ID card, visible in its entirety and in a better quality to read data from the document. Please send a self-made photo with a visible identity document in hand. The quality of the identity document sent should be better to read the data from the document held."

[redacted] *corresponded via e-mail for several months in 2019 with Complainant.* [redacted] *did not agree with our term of providing services, especially regarding the* [redacted]*'s request for a copy of an ID card without any changes, marks, cover in any way. Finally after several months, Based on art. 12 sec. 5 point (b), the data controller refused to act on the request because of the request from the Complainant was manifestly unfounded or excessive, in particular because of their repetitive character.*

Therefore, [redacted] *hopes that this letter has explained all doubts, misunderstanding of Complainant. In the future,* [redacted] *undertakes to responding to user request in more accessible, clearly and understandable way. On behalf of the company, I apologize for the situation. The company did not want to violate any user rights. Compliance with the provisions of the GDPR is our priority.*

5.2. Inspectorate:
The Inspectorate agrees that the complainant's personal data cannot be deleted within five years after termination of the business relationship in accordance with clause 6 (1) c) of the GDPR and the Money Laundering and Terrorist Financing Prevention Act.

However, with regard to the reply to the complainant, we note that the complainant has repeatedly asked questions to which no clear answers have been given, and no reasons have been given for the refusal to reply.

Among other things, on 14 August 2019, the complainant requested clarifications regarding the processing of personal data (including the processing of an identity document).
On 4 September 2019 [redacted] sent a notification to the complainant in response to a further enquiry, stating that the enquiry had been forwarded to the Data Protection Officer, and that the complainant would be contacted as soon as a reply was received.
On 11 September 2019, [redacted] sent a notification to the complainant in response to a further enquiry, stating again that the enquiry had been forwarded to the Data Protection Officer, and that the complainant would be contacted as soon as a reply was received.
On 11 September 2019, the complainant sent a further letter requesting to know the exact time when they would be answered.
On 12 September 2019, the complainant was informed as follows: *Due to the large number of cases, we are forced to extend the deadline for responding. Our Data Protection Officer will review the case and provide an appropriate response as soon as possible*.
On 7 October 2019, a letter was sent from the address [redacted] to the complainant stating the following: *I have received information about the prolonged resolution of your request (enclosed correspondence). Please kindly specify all your questions and possible requests to* [redacted] *and I will try to answer them immediately*.

In view of the above, it can be seen that the enquiry sent by the complainant on 14 August 2019 has not been answered. Although the reply submitted to the Inspectorate states that [redacted] refused to deal with the complainant's application because the complainant's application was clearly unfounded or excessive, no such explanations were provided to the complainant. In addition, the Inspectorate does not find that the submitted application is clearly unfounded or excessive. However, if paragraph 12 (5) of the GDPR is invoked, it must be demonstrated very clearly to both the complainant and, where appropriate, the Inspectorate that the application is clearly unfounded or excessive. As this has not been done, and it does not appear to the Inspectorate that the request was unfounded or excessive, the failure to reply to the complainant has not been lawful.

In doing so, [redacted] has stated the following: "*In the future,* [redacted] *undertakes to responding to user request in more accessible, clearly and understandable way.*". Looking at the submitted correspondence, it can be seen that the complainant has not been answered clearly and intelligibly, which is acknowledged by the representative of [redacted]. There is also no substantive reply to some of the complainant's questions, no explanation is given for the refusal to reply, and the possibility to lodge a complaint with the supervisory authority and to seek redress is not explained. Thus, in the opinion of the Inspectorate, the requirements provided for in paragraphs 12 (1), (3), and (4) of the GDPR have been violated.

However, with regard to the complainant's right of access, this is governed by Article 15 of the GDPR. In addition, the controller must have in place data protection clauses in accordance with Articles 12 to 14 of the GDPR.

However, with regard to the questions sent by the complainant to [redacted] on 14 August 2019, [redacted] has, firstly, no obligation under the GDPR to provide the

complainant with a certificate concerning the implementation of ISO/BS standards and, secondly, there is no obligation to provide a risk analysis (which [redacted] is not required to have) concerning the processing of identity documents in accordance with the Money Laundering and Terrorist Financing Prevention Act. Nevertheless, as mentioned above, [redacted] should have either provided the data or clearly justified the refusal itself. However, as the complainant does not have the right to request the above data under the GDPR, the Inspectorate does not oblige [redacted] to send an additional answer either.

However, with regard to the second question, information on this point is available in the privacy policy of [redacted] ([redacted]), and explanations on the technical and organisational security measures and the automated processing can also be found in this notice of termination of proceedings. Nevertheless, we note that the controller has a duty to answer the questions clearly and intelligibly (simply referring to the data protection conditions is not enough), and this must be taken into account in the future.

In addition, the Inspectorate asked the SA Poland on February 6, 2023 to send the answers from the controller to the complainant. The SA Poland informed the Estonian SA that they have sent the specified documents, along with translations of them, to the complainant on February 10, 2023. The documents include the answers that the Inspectorate had gotten from the controller regarding the complainant's queries.

6. In addition, at the time of initiating the supervision proceedings, [redacted] did not have a Data Protection Officer appointed (there was no relevant information in the Estonian Commercial Register). However, in the opinion of the Inspectorate, [redacted] meets three criteria for the mandatory appointment of a Data Protection Officer – main activity, extensive data processing, and regular and systematic monitoring (clause 37 (1) (b) of the GDPR). [redacted] also agreed with the Inspectorate: "*Taking into consideration interpretation of the Office in the context of necessity of appointing by the* [redacted] *exchange an appropriate person for the position of DPO we agree with arguments presented by you*", and appointed a Data Protection Officer ([redacted], [redacted]).

Reprimand and notice of termination of proceedings

Although [redacted] had a legal basis for processing the personal data of the complainant, we would like to clarify that the controller is also obliged to comply with the requirements set out in the GDPR when responding to the individual. However, [redacted] has failed to reply the complainant's questions, has not explained the reasons for its failure to reply, and has not explained the possibility to lodge a complaint with the supervisory authority and seeking a judicial remedy.

Based on the above, [redacted] has violated the requirements of the General Personal Data Protection Regulation. Given that:
1) [redacted] had a legal basis for the processing of personal data (including for the collection of identity documents and selfies);
2) [redacted] has confirmed that in the future people will be answered clearly and intelligibly;
3) in the opinion of the Inspectorate, the complainant received the answers to the questions raised in the complaint (the Poland SA has sent the answers on February 10, 2023);

we reprimand [redacted] on the basis of the General Data Protection Regulation, and draw attention to the following:

1. **The controller shall take appropriate measures to inform the data subject of the processing of personal data in accordance with Article 15 in a concise, transparent, intelligible, and easily accessible form, using clear and plain language (article 12 (1) of the GDPR).** In the future, [redacted] shall answer people's questions clearly and intelligibly.
2. **The controller shall provide the data subject with a report on the action taken on the application in accordance with Articles 15 to 22 without undue delay, but no later than one month after receipt of the application. That period may be extended by two months, if necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension and the reasons for the delay within one month of receiving the application (article 12 (3) of the GDPR).** In this case, [redacted] extended the deadline for answering, but did not specify the date by which the answer would be submitted and then failed to reply to the questions asked.
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).** Although [redacted] failed to reply to the complainant, the reasons for the failure to reply were not explained, nor was the possibility to lodge a complaint with the supervisory authority and to seek redress explained.

In view of the above, 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 Act[6], or
- An appeal to an administrative court under the Code of Administrative Court Procedure[7] (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

[redacted]
Lawyer
Authorised by the Director General

[6] https://www riigiteataja.ee/en/eli/527032019002/consolide
[7] https://www riigiteataja.ee/en/eli/512122019007/consolide