REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Final decision article 60

Data controller [redacted]
Complainant [redacted]

Reprimand in the matter of personal data protection
Notice on the termination of proceedings

1. Complaint of [redacted]

1.1. The Estonian Data Protection Inspectorate received a complaint of [redacted], a citizen of Germany, through the IMI system that the complainant submitted on 2 January 2020 to the German data protection authority which added the complaint to the IMI system on 7 May 2020. The complaint states that when the user wished to register themselves as a user of [redacted] website, they had to give consent to direct marketing.

1.2. The complainant was unable to register as a user of [redacted] website without giving the consent. In addition, the complainant does not understand which third parties the contact data entered by them are transferred to, how the data are used, and how long the data are stored. According to the complaint, third parties have not been specifically indicated on the [redacted] website. The complainant also found that [redacted] had not appointed a data protection specialist and therefore they were unable to contact [redacted].

1.3. The Inspectorate forwarded a query to [redacted] on 8 April 2020. [redacted] responded on 20 April 2020 that it does not offer (incl. does not advertise) consumer credit to German citizens and therefore the supervision proceedings have been brought against the wrong person. [redacted] explained that [redacted] must be considered the actual data controller. The Inspectorate terminated proceedings taken against [redacted] and initiated proceedings against [redacted].

2. Explanations of the controller and the opinions of the Inspectorate sent to the data controller during the proceedings

2.1. Controller's response to the first query of the Inspectorate

[redacted], or the controller, explained that based on the query sent by the Data Protection Inspectorate, the solutions used for asking consent were analysed. *'We established that the current solution may lead to misunderstanding when using the service and therefore we have decided to change the procedure for asking consent following registration as a user and before allowing the user to make investments.* [redacted] *confirms that as at 20 April 2020, a person can register as a user and use their user account without any obligation to give consent to direct marketing, i.e. following*

registration, it is possible to use the respective user account after confirming of having become acquainted with the privacy policy and risk review. It is possible to skip giving consent to direct marketing and opting out of direct marketing does not restrict registering or using a user account.'

2.2. [redacted] explained that they ask a copy of the ID card and store the following personal data included therein: name, time of birth, origin, citizenship, place of birth, biometric data such as eye colour and height, bank account number, bank, user name, and contact data such as e-mail address, telephone number, and address.

2.3. [redacted] explained that they store contact data of clients in an archive with limited access for a term corresponding to the maximum limitation period of offences, which, pursuant to current legislation, is up to 15 years. In the opinion of [redacted], this term is not unreasonably long, as the widespread practice is to link the data storage period (10 years) to the limitation period (which in the case of civil transactions is up to 10 years). [redacted] confirmed that no other processing operations are undertaken with the contact data of users and the threat of harm to the rights and interests of users is minimal.

2.4. Controller's responses to the second inquery of the Inspectorate

The Inspectorate made a follow-up query on 21 April 2020 in which it asked how consent to direct marketing was obtained earlier, before 20 April 2020.

2.4.1. [redacted] answered on 4 May 2020 that as at 20 April 2020, a technical failure which prevented activating the 'Confirm' button (in Estonian 'Kinnita') if only the first two choices were marked has been fixed. *'Regrettably,* [redacted] *had failed to notice that there was a technical fault related to the activation of the 'Confirm' button and not one user of the portal, including the complainant, had drawn our attention to this fault before the current proceedings. We fixed the technical fault immediately after receiving the relevant inquiry from the Data Protection Inspectorate and we confirmed that as at 20 April 2020, the technical failure concerning the 'Confirm' button had been eliminated.'*

2.4.2. The controller gave the following explanation regarding biometrics:
The biometric data (eye colour and height) originate from the complainant's German ID card, which is different from the Estonian ID card in that it also includes a person's biometric data. [redacted] *asks the users to present their identity document for the purpose of identifying the person in accordance with law (subsection 20 (1) of the Money Laundering and Terrorist Financing Prevention Act). For* [redacted] *the biometric data of German clients exist only on the ID document submitted by the user and* [redacted] *does not in any way use them separately.*

2.4.3. In regard of data storage, the controller stated the following:
The referred storage period of 15 years is derived from the maximum limitation period of offences (subsection 18 (8) of the Penal Code). The offences, in connection with which [redacted] *may need to submit contact data to the competent supervision authority, include fraud (section 201 of the Penal Code) (separately computer-related fraud (section 213 of the Penal Code)), offences relating to money laundering (sections 394 and 394[1] of the Penal Code), or other offences that may be committed by misusing* [redacted]*'s service. The example of the 10-year term was given as a reference to market practice. As it is impossible to preclude situations where* [redacted]*'s service is also misused to commit offences in addition to a breach of obligations arising from civil law,* [redacted] *applies the maximum limitation period of offences.*

2.5. Inspectorate's consultation with the German data protection authority

2.5.1.The Inspectorate asked the opinion of Germany regarding biometrics on 7 May 2020. The German data protection authority explained that pursuant to the German Money Laundering Act (GwG) the controller has to establish the person's first name, family name, place of birth, nationality, address and document number when identifying a person. The controller does not have any legal grounds to process other data included in the ID document.

2.6. Forwarding the opinion of the German authority and Estonian Inspectorate to the controller

2.6.1.The Inspectorate forwarded a brief summary of the German authority's opinion to the controller on 3 November 2020, presented new questions to [redacted], and shared its opinions regarding storage periods. The Inspectorate also asked explanations concerning the appointment of a data protection specialist.

2.6.2.In relation to retention of data, the Inspectorate gave the controller the following explanations:
Section 47 of the Money Laundering and Terrorist Financing Prevention Act refers to retention of data for five years after termination of the business relationship. Pursuant to the Act, for the purpose of identification of persons and verification of submitted information, the obliged entity must retain the originals or copies of the documents specified in subsection 20 (2^1) and sections 21, 22, and 46 of the Act, information registered in accordance with section 46, and the documents serving as the basis for the establishment of a business relationship for five years after the termination of the business relationship.

2.6.3.Pursuant to subsection 12 (2) of the Accounting Act, accounting source documents shall be preserved for seven years after the expiry of their term of validity. This provision is solely concerned with accounting source documents, including invoices and other documents, not contact data and clients' eye colour.

2.6.4.Subsection 146 (1) of the General Part of the Civil Code Act enables retain data after termination of a contract for three years. Subsection 4 of the same section sets down that the limitation period for the claims specified in subsections (1)–(3) shall be ten years if the obligated person intentionally violated the person's obligations.

2.6.5.The Inspectorate pointed out that storage of data for 15 years is not reasonable and that the limitation period of ten years requires a special ground and therefore it is not possible to retain data of all persons for ten years as a general practice relaying on this ground. The controller can store data for ten years under subsection 146 (4) of the General Part of the Civil Code Act solely if it is proven that the person whose data are stored for this long has intentionally violated the person's obligations before the controller.

2.6.6.The Inspectorate explained that therefore, it must be assessed on a case by case basis whether a person has intentionally violated their obligations. If such situation has not emerged, data cannot be stored for ten years.

2.6.7.Based on the above, the Inspectorate found that the reasons given in support of the 15-year storage period in reference to the Penal Code are not sufficient or understandable and consequently, the Inspectorate did not agree to the data storage period of 15 years. The Inspectorate found that even 10 years is not a reasonable period for storing data in exceptional cases and is conditional on intentional violation. The Inspectorate also mentioned that the data storage period does not comply with the

principles set out in points (b) and (e) of Article 5 (1) of the General Data Protection Regulation.

2.7. Controller's third response to the Inspectorate

2.7.1.The controller answered the Inspectorate on 17 November 2020 as follows:
As at today, [redacted] has not yet appointed a data protection specialist; however, we plan to appoint a data protection specialist and currently negotiations are being held. As soon as [redacted] has appointed a data protection specialist, we will notify the Data Protection Inspectorate thereof through the Company Registration Portal (in Estonian 'Ettevõtjaportaal').

2.7.2.If the Data Protection Inspectorate is convinced that the storage period of 15 years regarding strictly contact data is unreasonable despite our explanations, we are ready to reduce the storage period of contact data to ten years based on the maximum limitation period of claims under civil law. Although the limitation period of ten years applies only in case the obligated person violated his or her obligations intentionally, we have no means to determine whether the person violated his or her obligations intentionally before the actual situation emerges. This could happen even after seven years.

2.7.3.In our field of activity, disputes are likely to arise and therefore we have a clearly understandable interest to be able to protect our rights. Besides, taking into account that a person's contact data are not deemed personal data of a special category or personal data that would be sensitive in any other way, we do not consider in this case the storage period of ten years to protect our rights and interest unreasonable. Thereby the principles of limitation of processing of personal data and retention of personal data have been complied with. In regard of storage of other data (taking into account the specific data category) that the Data Protection Inspectorate points out in their query of 3 November 2020, we will take into account the specified term limits as presented by the Data Protection Inspectorate and prescribed by law.

2.7.4.We note that the opinion of the German data protection authority is based on the German Money Laundering Act that does not apply in the current case because [redacted] as an Estonian company operates in compliance with Estonian legislation. Hence, we do not consider the opinion of the German data protection authority relevant.

2.7.5.Secondly, according to subsection 47 (1) of the Money Laundering and Terrorist Financing Prevention Act, retention of copies of the documents which serve as the basis for identification and verification of persons is mandatory, meaning that national law of Estonia has taken a different approach than Germany. Although all the data shown on a German ID card are not necessary for us, we do not consider covering up the specific data on an identification document possible as it makes impossible to verify document authenticity.

2.7.6.We maintain that we do not gather or process a person's eye colour shown on his or her German ID card in any other way or for any other purpose than as part of the copy of the ID card. We also assure that only a very limited number of persons have access to the copies of identification documents and they are used after they have been gathered.

2.8. The Inspectorate's explanations and questions of 28 January 2021 to the controller

2.8.1.The Inspectorate forwarded one additional query to [redacted] in relation to sharing information with third persons and explained the matter of storage

periods.

2.8.2.The Inspectorate stressed that the controller has to assess separately in respect of each person whether the person has intentionally violated his or her obligations. If such situation has not occurred, data cannot be stored for ten years. In addition, the Inspectorate explained that ten years is abstractly acceptable in case of claims under civil law; however, if a data subject submits an objection concerning storage of data for ten years, then the processor has to re-assess its legitimate interest according to Article 21 of the General Data Protection Regulation.

2.8.3.The Inspectorate found that for that purpose, a legitimate interest analysis in respect of the specific person must be conducted, or the interests of parties concerning the storage of data must be considered that should give an answer to the question whether there is a need to store data of the data subject for ten years. The Inspectorate compiled legitimate interest instructions providing an overview of and explanations on how the rights of both parties should be considered and how a legitimate interest analysis should be conducted in case of an objection. The instructions are made available here https://www.aki.ee/sites/default/files/dokumendid/oigustatud_huvi_juhend_aki_26.05.2020.pdf.

2.8.4. In addition, the complainant asked about sharing contact data with third persons. [redacted] wrote on 20 April 2020 that they do not transfer their clients' personal data to third persons. However, according to the privacy conditions of [redacted], contact data are transferred to third persons for different reasons (the chapter on data sharing and chapter 7.5), for example, upon assigning a claim, etc. Consequently, inconsistency between the answer given to the Inspectorate and the data protection conditions published on the home page is observed. The Inspectorate requested [redacted] to show in detail to which companies and based on which legal grounds clients' personal data/contact data are shared.

2.9. Controller's fourth response to the Inspectorate

2.91.The controller answered on 4 February 2021 as follows:

We agree that in our answer of 20 April 2020 it was mentioned that data are not transferred to third persons. We clarify and explain our response below. We share clients' personal data with third persons only:
1) if it is specified in the privacy notice; or
2) if it is required under applicable law (e.g. when we are obliged to share personal data with public authorities); or
3) upon the client's consent or under the client's order.

2.9.2.In our response of 20 April 2020 we meant the concrete complainant, i.e. the complainant had not given us a separate order to transfer data to third persons. We admit that the general wording of our answer may have given an erroneous impression. We apologise for ambiguity of the answer and provide additional information about transfer of data below. When processing clients' personal data we may transfer their personal data to [redacted]s processors or third persons. Such transfer takes place only under the following conditions:

2.9.3.Processors
We use carefully selected service providers (processors) for processing clients' personal data. Even so, we will remain completely responsible for clients' personal data. For example, we use following processors:
1) service providers that organise marketing and conduct surveys, and providers of

tools;
2) service providers that perform searches in order to manage money laundering and terrorist financing related risks;
3) identification of persons service providers;
4) customer support service providers;
5) accounting services providers;
6) server administration and server hosting service providers;
7) IT services providers;
8) other companies belonging to the same group as us that provide us services.

2.9.4. Third persons
As mentioned above, we share clients' personal data with third persons only if it is specified in the privacy notice, required under applicable law (e.g. we are obliged to share personal data with public authorities), or upon the client's consent or under the client's order.

2.9.5. We may share clients' personal data with the following third persons:
1) for making transactions chosen by the client with other users through the portal. In such case, the legal basis for transfer of personal data is the conclusion or performance of a contract (point (b) of Article 6 (1) of the GDPR);
2) for the performance of the contract with intermediary payment service. In such case, the legal basis for transfer of personal data is the performance of a contract concluded between us (point (b) of Article 6 (1) of the GDPR);
3) for the purposes of our internal administration with companies belonging to the same group as us. In such case, the legal basis for transfer of personal data is our legitimate interest to share data with companies belonging to the same group as us for the purpose of internal administration (point (f) of Article 6 (1) of the GDPR);
4) for the purpose of direct marketing with the companies belonging to the same group as us. In such case, the legal basis for transfer of personal data is the client's consent (point (a) of Article 6 (1) of the GDPR);
5) for the purpose of compliance with our legal obligations to which we are subject before public authorities and law enforcement authorities. In such case, the legal basis for transfer of personal data is compliance with our obligations arising from law (point (c) of Article 6 (1) of the GDPR);
6) for the purpose of protecting our rights and interests with debt collectors, lawyers, bailiffs, and other relevant persons. In such case, the legal basis for transfer of personal data is our legitimate interest to protect our rights and interests (point (f) of Article 6 (1) of the GDPR). We transfer clients' personal data only if we are convinced that our legitimate interest does not override the client's interest or fundamental rights and freedoms which require protection of personal data. As we generally transfer data only if it is actually necessary for the protection of our rights and interests (or a client is at fault or there is a suspicion of breach), it is legitimate in our opinion;
7) for the purpose of compliance with our obligations to which we are subject before auditors arising from law. In such case, the legal basis for transfer of personal data is compliance with our obligations arising from law (point (c) of Article 6 (1) of the GDPR and Auditors Activities Act);
8) for the purpose of compliance with our legal obligations or pursuing our or our transaction partner's legitimate interests if such transfer is necessary as a result of a transaction concerning the transfer of our activity or assets or in order to assess how perspective such transaction would be. In such case, the legal basis for transfer of personal data is compliance with our obligations arising from law (point (c) of Article 6 (1) of the GDPR and the Law of the Obligations Act) or pursuing our or our transaction partner's legitimate interest to make a transaction or assess how perspective

it would be (point (f) of Article 6 (1) of the GDPR). We transfer a client's personal data solely if we are convinced that our or our transaction partner's legitimate interest does not override the client's interests or fundamental rights and freedoms which require protection of personal data.

2.9.6.If the legal basis for processing of client's personal data is pursuing our or a third person's legitimate interest, the client has the right to receive additional information and at any time object such processing.

2.10. SA Poland's objection about the draft decision

2.10.1. Poland asked whether [redacted] has a money laundering law in terms of the entity, ie the institution with which [redacted] has money laundering and terrorism within the meaning of § 6 of the Prevention Act. The inspectorate asked the data controller on 09.08.2021 about the [redacted] entity, whether they apply the money laundering act or not.

2.10.2. [redacted] replied that *as of today,* [redacted] *is not yet an obligated person within the meaning of § 6 of the Money Laundering and Terrorist Financing Prevention Act. Nevertheless, there is money laundering the application of prevention measures is essential given the nature of our activities. Among other things, such need is based on § 15 (application of anti-money laundering measures within the Group) and § 24 (reliance on third party data). Not knowing exactly the question in the inquiry guarantees, we provide some explanations below that should help us understand our purposes for personal information*
anti-money laundering measures.

2.10.3. For the sake of clarity, we must first clarify the relationship between [redacted] *and* [redacted] *and the* [redacted]. [redacted] *is an obligated person within the meaning of § 6 (1) 2) of the Money Act and the Financial Supervision Authority a supervised creditor providing small loans to consumers.* [redacted] *is not the Financial Supervision Authority a supervised creditor (or other licensed entity) but acquires* [redacted] *Loan claims from AS. In addition,* [redacted] *and* [redacted] *belong to the same group.*

2.10.4. As an obligated person, [redacted] *must make sure that the assets used in the business relationship are legitimate § 20 (3) and (4). After concluding the loan agreement,* [redacted] *assigns the claim to* [redacted] *so that* [redacted] *remains to continue to administer the claims as a creditor, but the financial claim is transferred to* [redacted]. [redacted] *in turn assigns claims to its investors. In a very general way, therefore, the money to be borrowed also comes out at the end of the chain just from investors as follows:*
1) investors invest in [redacted] *products;*
2) [redacted] *transfers the money for the claim to* [redacted]*;*
3) [redacted] *becomes the owner of the money and transfers it to a specific consume as own funds. Because of this chain and business, it is extremely important that* [redacted] *can ensure that the business relationship is used the legitimacy of the origin of the assets and to be sure that they are not money laundering assets, so it is important that* [redacted] *would also apply the requirements arising from the Money Laundering Act.*

2.10.5. In addition to the above, [redacted] *has the right and obligation to apply the measures of RahaPTS pursuant to § 24 of Money Laundering Act acting as a third party on whose data the obligated person (eg the bank) relies. In practice, this is not possible* [redacted] *would be able to do business without anti-money laundering measures, as this would not be possible.* [redacted] *must also have a bank account through which investors*

can make financial transactions. The reason is that banks, as obligated entities, must also implement anti - money laundering measures; and In order for [redacted] to have a bank account for its business, the banks have imposed an obligation on us apply anti-money laundering measures in full, as they are based on the verification of transaction data including our data.

2.10.6. To this end, it grants banks the right, inter alia, § 20 (1) 4) and (6) of the Money Laundering Act and § 23 (2) of Money Laundering Act. In the application of due diligence measures, obligated parties have a wide discretion, including obligated persons customers (eg [redacted]) to provide information on their customers (ie [redacted] investors) so that the bank can assess the risks to your client and take other due diligence measures. The obligated person does not have to own collect data about customers themselves, but may rely on another person (ie their customer, in this case [redacted] collected in accordance with § 24 of the Money Laundering Act. If [redacted] does not submit to the bank within the required term information about its customers (ie [redacted] would not allow the bank to exercise due diligence), the bank would be entitled. To cancel the current account agreement entered into with [redacted] (§ 42 (4) of Money Laundering Act.

2.10.7. On a similar basis, [redacted] also requires [redacted] to control the activities of investors because of them. The assets originally arising from the transactions will be used by [redacted] to grant credit. Please also note EurLex-2 en In order to rely on the data collected by [redacted] pursuant to § 24 of the Money Laundering Act, [redacted] does not need to be in the sense of the Money Laundering Act obligated person. Pursuant to § 24 of the Money Laundering Act, measures may be taken to prevent money laundering and terrorist financing other persons to collect and process the data necessary for its application. Under that provision, collect data are also available, for example, to companies specializing in the application of due diligence (eg Veriff), which are not themselves.

2.10.8. Money under the Act for obligated persons, but who process data for obligated services to provide. This right and obligation has also been recognized by the FATF: "A third party usually has a client an existing business relationship that is separate from the relationship between the client and the relying institution, and apply its own rules of procedure when implementing due diligence measures." [redacted] operates by law on a prescribed basis and in accordance with official recommendations.

2.10.9. Pursuant to § 64 (1) of the Money Laundering Act, the State supervises the operation of Money Laundering Data Office. Please note that [redacted] has also reported on several occasions in the application of due diligence measures Money Laundering Data Offices and has not received any feedback or other instructions that [redacted] should not launder money prevent due diligence measures should perhaps not identify your customers in a business relationship unmonitored, without proving the origin of the assets used in the transaction, without checking the sanctions, etc.

2.10.10. In addition, we confirm that the application of [redacted]'s anti-money laundering measures is also monitored by sworn auditors. The last inspection was carried out by the audit firm [redacted] in May 2021, the results of which were positive, ie [redacted] has the right to apply anti-money laundering measures and they apply properly in accordance with the regulations in force.

2.10.11. As it seems from the above, [redacted] belongs to the same group [redacted] (registry code: [redacted]), which is an obligated person within the meaning of § 6 (1) 2) of the Money Laundering Act and a creditor operating under the supervision

of the Estonian Financial Supervision Authority, which provides small loans to consumers. [redacted] has also been issued a corresponding activity license by the Estonian Financial Supervision Authority. [redacted] is not a creditor (or other legal entity subject to an activity license obligation) under the supervision of the Financial Supervision Authority, but acquires loan claims from [redacted]

2.10.12. As an obligated person, [redacted] must make sure that the assets used in the business relationship are legitimate (§ 20 (3) and (4) of the Money Laundering Act). After concluding the loan agreement, [redacted] assigns the claim to [redacted] so that [redacted] will continue to administer the claims as a creditor, and the financial claim will be transferred to [redacted]. [redacted], in turn, assigns 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 Act.

2.10.13. Pursuant to § 47 (7) of the Money Laundering Act, the stored data must be deleted after the expiry of the term, unless otherwise provided by the legislation regulating the relevant field. Data relevant to the prevention, detection or investigation of money laundering or terrorist financing may be kept 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.

3. Breaches identified during supervision proceedings

3.1. In the course of the supervision proceedings, the Inspectorate found the following breaches of the General Data Protection Regulation: when opening an account the complainant could not refuse to give consent to electronic direct marketing, meaning that the complainant had to agree to direct marketing, although Article 7 (2) of the General Data Protection Regulation requires asking it clearly in a distinguishable manner.

3.2. The Inspectorate found that the controller breached point (e) of Article 5 of the General Data Protection Regulation by applying an unreasonably long data storage period of 15 years. Storing data for ten years abstractly for claims under civil law is acceptable; however, if the data subject objects to storage of data for ten years, according to Article 21 of the General Data Protection Regulation the controller has to re-assess its legitimate interest of retaining the data of the specific person based on the concrete circumstances related to the person (including also whether claims exist and whether the data subject violated his or her obligations intentionally). If it is determined that the need for defence of legal claims does not justify storage of the particular person's data, the data must be immediately deleted in accordance with point (c) of Article 17 (1).

3.3. The controller gave the Inspectorate unclear answers regarding transfer of data to third persons which caused us to request more details several times and determine the actual situation. The controller breached the principle of data transparency, i.e. it was not clear to whom and which third persons data are transferred.

3.4. The initial complaint related to the fact that the applicant did not have to agree to all the conditions for registering an account, including receiving direct marketing. This has been fixed by the data controller, where it was explained that it was a technical error.

3.5. The complaint stated that there was no retention period, as the complainant could not understand for how long the data will be restored. The data controller has explained

that different legal grounds must be used, which are also regulated by law. If there is consent, there are no retention periods, if the consent to send direct mail is revoked, then no more can be kept and sent.

3.6. The period of retention of data is regulated by § 47 of the Money Laundering Act. Act § 47 paragraph 1, 2, 3, 5, 6 states that the data controller must retain data for 5 years after after the termination of the business relationship. By order of the competent supervisory authority, the maximum retention period for personal data is 10 years.

3.7. Thus, it must be assessed separately for each person whether a particular person has intentionally breached his or her obligations. The inspectorate further explained that 10 years in the abstract for civil claims is acceptable, but if the data subject objects to 10 years of data retention, the data subject must be reassessed in accordance with Article 21 of the General Data Protection Regulation. The data controller did not argue further in this regard.

4. Reprimand and termination of proceedings

4.1. During the proceedings, the controller changed the procedure of asking consent to direct marketing and thereby eliminated the breach. The controller has been given explanations regarding data storage period that the controller has to take into account in future.

4.2. Based on the above, the Inspectorate terminates the supervision proceedings and issues a reprimand to [redacted] in accordance with point (b) of Article 58 (2) of the General Data Protection Regulation and draws attention to the requirements set out in the GDPR:

4.3. Article 7 (2): If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

4.4. Point (e) of Article 5 specifies storage limitation requirement: personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

4.5. Article 21 (1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6 (1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

4.6. Article 12 (1): The controller shall provide any information referred to in Articles 13 and 14 to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

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[1], or
- An appeal to an administrative court under the Code of Administrative Court Procedure[2] (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

[redacted]
Lawyer
Authorised by the Director General

[1] https://www.riigiteataja.ee/en/eli/527032019002/consolide
[2] https://www.riigiteataja.ee/en/eli/512122019007/consolide