REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

FINAL ADOPTED DECISION
IMI case nr 376841/428420

Our: 09.09.2022 nr 3.1.-3/22/1190

Data controller
Complainants **and**

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

1. Complaint of

1.1. On 14.08.2019 Estonian Data Inspectorate received a complaint through IMI system concerning data controller formerly known as The complainant stated that unlawfully processed his personal data. The complainant received direct marketing by phone.

1.2. The director of provided that is not a data controller found that data contoller is address: Estonia, and therefore supervisory authority of data controller is Estonia Data Protection Inspectorate (Estonian DPI). Estonian DPI accepted the case as a lead supervisory authority.

2. The response of the data controller) in regards to ´ complaint

2.1. Estonian DPI started a supervision procedure and inquired information from the data controller concerning ´ complaint. On 03.09.2019 the data controller stated *that (customer riders:) is our contractual customer who has not provided consent to direct marketing within the meaning of Article 7 of the General Data Protection Regulation. sent the SMS in question to the applicant on the basis of § 103.1 (3) of the Electronic Communications Act (ESS), the so-called soft opt-in. When you join the platform, the platform performs a soft opt-in to the newsletter. The customer has the opportunity to perform an opt-out operation in the application at any time.*

2.2. forwarded this campaign notice pursuant to § 103.1 (3) of the ESS. The customer has free authority always to refuse newsletters in the application or in response to a message sent by sending a notice to the customer service. provided the customer with a campaign notification, i.e. direct sales of the same service which the applicant had already used.

2.3. The messaging service provider's platform did not have a technical solution to perform the opt-out solution which was issued in March 2019. Opt-out rights could be exercised in the application by disabling the newsletter and contacting support, which this customer did.

2.4. Upon the customer's request, his data was provided and notifications were disabled. The ability of the messaging platform to perform opt-out operations has been resolved, and the messages sent by [redacted] contain information on how to opt-out of newsletters from the STOP command.

2.5. 26.09.2019 the data controller specified that *the agreement between [redacted] and the user is governed by Estonian law (see [redacted]), including the Estonian Electronic Communications Act, and the service is provided from the Republic of Estonia.*

2.6. [redacted] sent the campaign notification on the basis of § 103.1 (3) of the ESS. For the purposes of the GDPR, the corresponding data processing takes place on the basis of Art 6, (1) (f), i.e. on the basis of a legitimate interest.

2.7. The term "soft opt-in" here means a pre-filled selection, where the customer can make the opposite choice to the pre-filled one. We do not use the term soft opt-out.

2.8. Soft opt-in takes place within the application upon customer registration. The customer can opt-out both internally and externally through the respective communication channel that [redacted] used to transmit the information, eg in the case of an SMS, by sending a STOP order to the number at the end of the message.

2.9. In response to the second inquiry on 07.10.2019 the data controller specified:

2.10. [redacted] has given the buyer during the initial collection of his electronic contact information a clear and understandable opportunity to prohibit such use of his contact information in a free and simple way. When you join the platform, a check mark appears in the terms of user and privacy policy. Chapter 10 from [redacted] Privacy Policy contains the right to opt out of direct marketing communications. The app is two taps away from giving up direct marketing.

2.11. [redacted] specifies its previous position regarding the legal basis on which newsletters and direct marketing notifications are sent to customers. When concluding a contract with a customer, [redacted] proceeds with § 103.1 (3) of the ESS that allows to send direct marketing messages of its similar products, and based on Estonian DPA´s instructions, the use of electronic contact information for direct marketing is permitted either with the person's prior consent or in the presence of a previous customer relationship. Customers are always guaranteed an easy way to opt out of direct marketing messages.

2.12. [redacted] will review and specify its privacy policy to increase transparency in direct marketing within the next 30 days.

2.13. In response to the third inquiry on 11.11.2019 the data controller specified that *in our letter sent on 23.08.2019, we explained that the consent to send electronic direct sales messages within the meaning of Article 7 (1) of the General Regulation has not been taken from this customer. [redacted] sent the SMS in question to the applicant under § 103.1 (3) of the Electronic Communications Act.*

2.14. When creating an account, consent to direct marketing will not be asked. After customer's first connection with the platform, a contract is entered into and on the basis of § 103.1 (3) of the Electronic Communications Act, so-called soft opt-in is sent for direct marketing within the limits permitted by the same law.

2.15. [redacted] *is reviewing its privacy policy. We would like to get some clarification on the interaction between the General Regulation and the ESS, where the ESS allows direct marketing of similar products or services if customers are allowed to simply opt-out of direct marketing notifications in-app and through the channel through which the customer was contacted (so-called unsubscribe).*

3. Position of the Estonian Data Protection Inspectorate

3.1. Estonian DPI met [redacted] data specialist in December 2020 and agreement was made that data controller will review the privacy policy on direct marketing. Data controller said that they apply Estonian national law which is Electronic Communications Act.

3.2. On April 9, 2021, the Estonian DPI asked for feedback from concerned supervisory authorities regarding the implementation of the provisions on direct marketing. Estonian DPI requested the following information:

1. In the opinion of the concerned authorities, should the national law of each complainant country be applied to electronic direct marketing, considering that the controller is located in Estonia and it has been agreed that the applicable law is Estonian law in accordance with the conditions of use (both taxi drivers and passengers)?
2. Is the Lithuanian Data Protection Authority of the opinion that the data controller has infringed the GDPR in conjunction with the national law of Lithuania when sending direct marketing messages and, if so, which provision has been infringed and how has it been infringed and what should the data controller do in the future to lawfully provide the service in your country?
3. In French SA´s view, should the national law be applied in electronic direct marketing complaints if the complaint is submitted by a French data subject? If so, which national provision has been infringed?

3.3. Hungary SA´s opinion:

A 1 and 3. The complaint is partly related to consumer protection law in the case of unsubscribing from DM messages, so its evaluation is not within the competence of the Hungarian SA, but the National Media and Info-communications Authority is the competent organ, pursuant to the Sec. 16/B of the Act CVIII of 2001 on Electronic Commerce and Information Society Services. During investigating that legal issue, we recommend the LSA to apply its national law implementing the Directive 2002/58/EC on Privacy and Electronic Communications.

3.4. A 2. After examining the case, we suggest to state the breaches of the following GDPR provisions:

- Art. 5 (1) (a) transparency and (2) accountability principles,
- Art. 12 the transparent information and modalities for the exercise of the rights of the data subject,
- Art. 15 the right to access of the data subject

3.5. In order to ensure the data subjects' rights, the data controller must comply with the sections of the GDPR described above. It can be concluded from the case that the complainant objected to the general practice of the data controller, so the LSA must carefully investigate in its procedure the extent to which the objected data controller complied with the above provisions.

3.6. Danish SA´s opinion:

The Danish SA found that the question does not fall inside the scope of the competence of the Danish SA since it is related to consumer protection law. The Danish Consumer Ombudsman is the competent authority in Denmark as it pertains to consumer protection law (The Marketing Practices Act).

3.7. French SA´s opinion:

3.8 According to paragraph 91 of the EDPB's opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR adopted on 12 March 2019 : « The cooperation and consistency mechanisms available to data protection authorities under Chapter VII of the GDPR, concern the monitoring of the application of GDPR provisions. The GDPR mechanisms do not apply to the enforcement of the national implementation of the ePrivacy Directive. The cooperation and consistency mechanism remains fully applicable, however, insofar as the processing is subject to the general provisions of the GDPR (and not to a "special rule" contained in the ePrivacy Directive) ».

3.9. Therefore, if a complaint was submitted to the French Supervisory Authority regarding the lack of consent for electronic direct marketing, the French provisions under the eprivacy Directive would apply. As a result, the CNIL would not share this complaint with other Supervisory Authorities as the One stop shop mechanism does not apply.

3.10. However, if the complaint, as Mr [redacted] is about the reception of electronic direct marketing despite the objection of the data subject, the provision applicable is Article 21.2 of the GDPR, regardless of the national provisions about electronic direct marketing. Therefore, we believe that the Estonian Supervisory Authority is competent to address [redacted]'s complaint.

3.11. Berlin SA

The sending of advertising per se is subject to Section 7 of the German Unfair Competition Act (UWG) or the corresponding national provisions of other Member States. The processing of personal data required for this (insofar as natural persons are affected) is subject to the GDPR. If the sending of the advertising is not lawful, there is no legitimate interest in processing the personal data for advertising purposes or there is a violation of Article 6 (1) of the GDPR. There is already case law on this in Germany.

3.12. Estonian DPI has taken into account all the comments and observations of the concerned supervisory authorities. Lithuanian Data Protection Authority did not give any feedback on these questions. However, based on the responses of the other concerned supervisory authorities, the national provisions on electronic direct marketing apply in each country or in some cases e-privacy directive.

3.13. E-privacy directive does not contain such one-stop-shop mechanism as GDPR. Thus, in case of violation of e-privacy directive and national laws on direct marketing, each EU member state has to handle such violations by themselves. Estonian DPI can handle only those complaints where there is a violation of GDPR.

3.14. Estonian DPI received an objection against the Draft Decision from Berlin Commissioner for Data Protection and Freedom of Information (Berlin DPA). According to Berlin DPA all customer data that have been collected by [redacted] before the changes in [redacted]´s enrolment processes (e.g March 2019) must not be used for marketing purposes and must therefore be deleted. The reason for that according to Berlin DPA is a question whether the prerequisites of such data collection were met in regards to GDPR Art. 6(1)(f) and Electronic

Communication Act § 103[1] (3). It was argued that [redacted] did not give customers an opportunity to refuse in an easy manner from direct marketing before March 2019. Estonian DPI finds that although [redacted]´s messaging service provider´s platform did not have a technical solution to perform the opt-out before March 2019, customers were offered a possibility to refuse the marketing messages through [redacted] application by disabling the newsletter (clicking the app twice) and also by contacting [redacted] support.

According to Estonian Electronic Communications Act[1] § 103[1] (3) - *If a person obtains the electronic contact details of a buyer, who is a natural or legal person, in connection with selling a product or providing a service, such contact details may still be used, regardless of the provisions of subsection 1 of this section, for direct marketing of its similar products to the buyer if:*
1) the buyer is given, upon the initial collection of electronic contact details, a clear and distinct opportunity to refuse such use of its contact details free of charge and in an easy manner.

During the investigation process [redacted] confirmed to Estonian DPI that when a person joined their platform, he was presented terms of use and privacy policy in which the opportunity to refuse the use of his contact details was presented under Section 10. Customer had to tick the box to confirm that he agrees with and has read the conditions. There was an option to refuse from direct marketing in [redacted]´s app by opening Settings -> Open Profile -> disabling the newsletter.
In Estonian DPI`s opinion clicking an app twice can be considered a clear and distinct refusing opportunity, that is free of charge and is presented in an easy manner. Since the prerequisites of Estonian Electronic Communications Act[1] § 103[1] (3) p. 1 were met, we cannot consider the collection of customer data before March 2019 unlawful. The complainant ([redacted] received the marketing message from [redacted] only once (13.03.2019) according to the original complain, so Estonian Electronic Communications Act[1] § 103[1] (3) p 2 does not apply.
[redacted] changed its processes - they added STOP command option to the direct sales messages sent to customers. Estonian DPI must also note that it is not possible to impose a fine on a data controller in administrative proceedings pursuant to Estonian Data Protection Act, as Berlin DPA suggested.

3.15. In this case [redacted] did not ask for consent regarding direct marketing. This is possible according to Estonian § 103[1] (3) of the Electronic Communications Act. Lithuanian DPA did not answer whether consent is always needed for direct marketing. In case consent (in the meaning of GDPR) should have been asked, but was not, it would also be a violation of GDPR. As Lithuania has not given any information about their local law, Estonian Data Protection Authority has also not identified a breach of the GDPR art 7.

3.16. However, based on the GDPR art 21, the natural person must be able to object to the processing of the data, which must be assessed and answered by the data controller. It is therefore appropriate to reprimand the controller.

4. Decision of the inspectorate in the complaint of [redacted]

4.1. The Estonian Data Protection Inspectorate issues a reprimand to the data controller [redacted] under Article 58 (2) b) of the General Data Protection Regulation and draws attention to the following:

4.2. When processing personal data, the controller shall ensure that the 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). It is also important that persons are not provided misleading information concerning the processing of data (including the deletion of data).

In view of the above, we shall terminate the supervisory proceeding in this matter.

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).

5. Complaint of [redacted]

5.1. [redacted] complaint was also added to the [redacted] proceedings because French Data Inspectorate linked it from IMI system. Silvestre complains that he received electronic direct marketing from [redacted] by e-mail.

6. The response of the data controller ([redacted] in regards to [redacted] s complaint

6.1. Estonian DPI sent an inquiry to the controller on 18.05.2020 about the complainant [redacted] *Data controller confirms that* [redacted] *will no longer receive electronic direct marketing from us until he creates a new user account where privacy settings allow direct marketing.*

6.2. The results of our internal investigation confirm [redacted] *version:* [redacted] ***promised 05.02.2020 to stop sending e-mails, but despite this,*** [redacted] ***received an e-mail from*** [redacted] ***again on 27.02.2020.***

6.3. The results of the internal investigation show that the transmission of the e-mail to Mr. [redacted] *was caused by the following: Mr.* [redacted] *request to unsubscribe ("unsubscribe") was correctly registered in* [redacted] *respective internal information system, but was nevertheless not "properly transferred" to the external marketing email delivery platform CleverTap, from which the email was sent.*

6.4. The logs of the relevant internal information systems and external platforms do not unambiguously indicate in which specific system or process the error occurred, but by now we have all reasonable grounds to claim that it occurred in the perimeter of [redacted] *s liability. We sincerely apologize for the inconvenience.*

6.5. In addition, [redacted] *undertakes to conduct an in-depth analysis of the systems and processes involved in order to identify and eliminate the error by 2020 at the latest. By October, 1 any deficiencies that could result in similar e-mails being sent to users who have duly requested an opt-out. In the meantime,* [redacted] *shall take all reasonable precautions and measures to prevent the transmission of e-mails and other marketing communications to users who have opted out of such communications.*

7. Position of the Estonian DPI

7.1. The Estonian DPI finds that the data controller has responded to the complainants and cooperated with the inspectorate. Therefore, it would be reasonable to reprimand the data controller in accordance with the GDPR and terminate proceedings regarding the complaint.

7.2. The data controller has made changes in its privacy policy concerning direct marketing.

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

In response to the intervention by the inspectorate, the data controller provided detailed and specific answers to the complainants. Therefore, there is not much left to accuse the data controller of, which is why a reprimand is appropriate as a result of the proceeding.

7.3. The Supervisory Authority finds that [redacted] violated Article 21 (2) and (3) of the General Regulation on the Protection of Personal Data. [redacted] forbid the data processing, but still received direct sales after that. There is therefore an infringement of Article 21 (2) and (3) which entails a reprimand to the data controller.

7.4. The Inspectorate has taken into account the comments and observations of all the concerned supervisory authorities. Estonian DPI would like to thank the Portuguese SA, who found that the data controller should be reprimanded. The Estonian DPI agrees. The Inspectorate also agrees with Portugal SA that the data subject has the right to object to the processing of the data in accordance with Article 21.

8. Decision of Estonian DPI in the complaint of [redacted]

8.1. The Estonian Data Protection Inspectorate issues a reprimand to the data controller [redacted] under Article 58 (2) b) of the General Data Protection Regulation and draws attention to the following:

8.2. When processing personal data, the controller shall ensure that the data processing is lawful, fair and transparent to the data subject (Article 5 (1) a) of the General Data Protection Regulation). It is also important that persons are not provided misleading information concerning the processing of data (including deletion of data).

8.3. The Lead Supervisory Authority finds that the data controller violated Article 21 (2) and (3) of the General Regulation on the Protection of Personal Data. Article 21 (2) states that where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Article 21 (3) states that where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

In the view of 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[3], or
- An appeal to an administrative court under the Code of Administrative Court Procedure[4] (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

[redacted]
Lawyer
authorized by Director General

[3] https://www riigiteataja.ee/en/eli/527032019002/consolide
[4] https://www riigiteataja.ee/en/eli/512122019007/consolide