



ANDMEKAITSE INSPEKTSIOON

Dear [REDACTED]
Member of the Management Board

Your: 18/01/2021

Our: 13/05/2021 No. 2.1.-1/20/2528

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

The Estonian Data Protection Inspectorate (the inspectorate) received a complaint from a Lithuanian citizen, according to which the number [REDACTED] had called his number, [REDACTED], on 3 June 2020. The call was made to advertise the services of [REDACTED]. According to the complaint, the complainant asked during the call why he had been called and where his number was obtained, but it was not answered and the call was disconnected.

Based on the above, we have initiated supervision proceedings on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

First, we would like to highlight that the inspectorate had also received a similar complaint in case no. 2.1.-1/20/4581, according to which [REDACTED] has also called an individual on 8 October 2020 and discontinued the call when asked for explanations in connection with the processing of personal data.

On 10 August 2020, [REDACTED] responded as follows in the course of the supervision proceedings: *After the quarantine was announced in Lithuania, the building used by [REDACTED] was closed. All employees of [REDACTED] were isolated and worked from home. Employees of [REDACTED] did not have access to customer service systems when working remotely, so they had to dial telephone numbers manually. The agent, who had repeatedly received a warning for improper work, dialled the wrong phone number and called the wrong person, and also conducted a conversation that did not comply with the quality requirements of [REDACTED]. To date, we have terminated the employment contract with this agent. [REDACTED]* [REDACTED] also confirmed that they does not have any personal data regarding the complainant's telephone number.

On 13 January 2021, the inspectorate submitted a further enquiry, which received the following response from [REDACTED] on 18 January 2021:

1. Have you implemented measures and which measures have you implemented to prevent similar situations in the future?

Incl.:

1.1. Do the employees of [REDACTED] still have no access to customer service systems when teleworking and must therefore dial telephone numbers manually?

We have been working towards acquiring more company computers which would enable those customer attendants who are working from home to access the customer service systems; unfortunately, we cannot claim today that this opportunity has been ensured for every employee who is teleworking, but we are working on achieving this goal.

1.1.1. If yes, then has [REDACTED] implemented measures to minimise errors in dialling telephone numbers when teleworking? Which measures?

In order to prevent such situations, we have provided further training for our employees on data protection and their positions at the company to ensure that they are aware of potential risks and know how to prevent these risks.

We have also drawn up work schedules to provide an opportunity to work in the office in shifts for those employees who are unable to access the customer service systems when working from their home office. The office is equipped with all the required tools, incl. access to the customer service systems. Based on the above, we have clearly understood the risk which may arise from working from home and are therefore constantly trying to remind our employees to perform their duties accurately and attentively, incl. train them, and we have also reminded them where the potential risks of making mistakes lie.

Furthermore, [REDACTED] has also responded to the inspectorate as follows in the supervision proceedings in case no. 2.1.-1/20/4581 on 22 February 2021:

When the quarantine was declared in Lithuania in the spring of 2020, the building which is being used by [REDACTED] was closed. All employees of [REDACTED] remained isolated and were working from home. The employees of [REDACTED] had no access to the customer service systems when teleworking. Therefore, instead of using the company's automated internal customer service system, they were required to dial telephone numbers manually. We were aware of the risk which could arise for the company from this situation and, assessing the risk from the perspective of the company's operations, we found that we had to accept the risk. In parallel, solutions were planned and implemented for minimising the risks, incl.:

- we have acquired more company computers which can be used by the customer attendants who are working from home to access the customer service systems.

Unfortunately, this situation is not available for all employees who are teleworking;

- we have also provided further training for our employees on data protection and their positions at the company to ensure that they are aware of potential risks and know how to prevent these risks;

- furthermore, we have drawn up work schedules to provide an opportunity to work in the office in shifts for those employees who are unable to access the customer service systems when working from their home office. The office is equipped with all the required tools, incl. access to the customer service systems.

In the autumn of 2020, people were strongly advised to work from home; in November 2020, however, another quarantine was established in the Republic of Lithuania, due to which office workers were again required to telework. Thus, we were again forced to accept the potential risk of making the wrong choice when it came to those employees who do not have company computers.

Unfortunately, we can see that our actions have not fully eliminated the negative situation, as a wrong person has been called again, as a result of a human error, without legal grounds for making the call.

Having learned about the complaint, we have conducted an internal investigation at the company to determine the potential further steps to minimise the risk of further similar situations. We are also continuing to implement the plan of acquiring company computers for all employees to minimise manual processing. The employee who made the call was again

reminded of their obligations in connection with the company's information assets, incl. personal data.

-

Even though [REDACTED] has implemented further measures to prevent calls being made to people without legal grounds, it is obvious that [REDACTED] has not been able to fully fix the situation. The latest response to the inspectorate also shows that it is admitted by [REDACTED] themselves that their actions have not been able to fully eliminate the negative situation, as a wrong person has again been called as a result of a human error, without any legal grounds for calling this individual. Thereat, the company is continuing to implement a plan of acquiring company computers for all employees to minimise manual dialling of telephone numbers. Further steps for minimising the risk of such situations are also being assessed.

However, we explain that it is obligation of a data controller to make sure that data is being processed in compliance with the General Data Protection Regulation (GDPR). Thereat, it is prohibited to process personal data (incl. call to an individual) if there are no legal grounds for the processing, i.e. if the processing is not compliant with Article 6 (1) of the GDPR. The complaint and [REDACTED]'s response indicate that personal data has been processed without legal grounds. We would also like to stress that individuals have the right to receive explanations from the data controller about the processing of their personal data (Articles 12–15 of the GDPR). Based on the materials of the complaint, however, the employee of [REDACTED] did not provide explanations to the individual who made the complaint about the processing of their personal data, but ended the call. Thereat, this is not one isolated case, this behaviour has occurred repeatedly.

As [REDACTED] has processed personal data (called to individuals) without legal grounds and failed to respond to the individual's inquiries about the processing of personal data, they have thereby violated the requirements of the General Data Protection Regulation.

Taking into consideration the following facts: 1) [REDACTED] only holds the telephone number of the individual who filed the complaint, as the employee dialled the number by mistake, 2) the employees of [REDACTED] have been mistakenly dialling incorrect telephone numbers, incl. the telephone number of the individual who filed the complaint, because the building which is being used by [REDACTED] was closed due to the quarantine in Lithuania, as a result of which the employees were required to work from home and therefore had no access to the customer service systems during teleworking, i.e. the employees were required to dial telephone numbers manually instead of using the automated internal customer service system, 3) [REDACTED] has implemented and is attempting to implement measures to prevent such situations in the future, we are hereby issuing a reprimand to [REDACTED] on the basis of Article 58 (2) of 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, the data controller must make sure that the processing is lawful, i.e. compliant with Article 6 (1) of the GDPR. The employees of [REDACTED] may not make telephone calls to individuals without lawful grounds. Processing of personal data must also be transparent and the data controller must respond to the individuals' inquiries about the processing of personal data (incl. those made over the telephone), taking into consideration Articles 12–15 of the General Data Protection Regulation. If an employee

of [REDACTED] who is making a sales call is not able to respond to questions which are related to the processing of personal data, they must forward the call to an individual who can respond to those questions. Ending the call and failing to respond are, however, not permissible, but is a breach of the requirements of the GDPR, which [REDACTED] is responsible for.

We would also like to stress that the complaints which have been submitted to the inspectorate show that [REDACTED] has been processing personal data (calling individuals) without lawful grounds and failed to respond to the individuals' questions in connection with processing personal data, i.e. the employee has ended those calls. This constitutes a violation for which we are issuing a reprimand to [REDACTED]. Taking into consideration the above, we would like to point out that in a situation in which such unlawful processing of data still continues, the inspectorate hereby issues a respective precept and a warning of being subjected to a penalty payment to [REDACTED]. The inspectorate may claim a penalty payment in the amount of up to 20,000,000 euros for each violation pursuant to section 60 of the Personal Data Protection Act or, in the case of a company, up to four per cent of its total global turnover in the previous financial year, depending on which amount is higher.

Based on the above, we are hereby closing the supervision proceedings.

This administrative act 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 the Director General

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

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