ANDMEKAITSE INSPEKTSIOON

All SA-s

Our 20.12.2024 No. 2.1-12/24/851-1784-6

ARTICLE 60 FINAL ADOPTED DECISION
Termination of the proceedings

Circumstances

On 29 December 2023, the Estonian Data Protection Inspectorate (Estonian DPI) received a complaint from [redacted] (the Complainant) against [redacted] ([redacted], the Controller) for failure to respond to his request. As the complaint was submitted in English and unsigned, the Estonian DPI asked for the complaint to be submitted in Estonian and signed. The Estonian Administrative Procedure Act lays down substantive and formal requirements for complaints. On 5 January 2024, the Complainant lodged a complaint to the Estonian DPI in Estonian, but did not sign it. The Estonian DPI asked the Complainant to sign his complaint, since Paragraph 14(3) of the Administrative Procedure Act provides for an obligation to sign. However, the Estonian DPI drew the Complainant's attention to the fact that, in accordance with Article 77(1) of the GDPR, it is also possible for the Complainant to lodge a complaint with a supervisory authority, in particular in the Member State in which he has his habitual residence, place of work or place of the alleged infringement.

The Complainant did not remedy the deficiencies in the complaint within the prescribed period. Since the Estonian DPI is authorised under Article 58(1)(d) of the GDPR to notify the controller of an alleged infringement of the GDPR and the right of access is an essential part of the data protection system, the Estonian DPI informed the Controller on 5 February 2024 that, to the knowledge of the Estonian DPI, [redacted] had failed to respond to the Complainant's request. The Controller informed the Estonian DPI on 22 February 2024 that, unfortunately, the Complaint's request had not been answered on time, but the reply was sent on 19 February 2024.

Since the Complainant brought an action before the German DPI (SA Berlin), a complaint against [redacted] was subsequently transferred to the Estonian DPI in the same case.

According to the complaint, on 26 July 2023, the Complainant received an email to his personal email address from an employee of [redacted] concerning recruitment. On the same day (i.e. 26.07.2024), the Complainant sent an email to an employee of [redacted] asking him to explain how his personal data had entered [redacted]'s database.

As the Complainant did not receive a reply to his request, the Complainant sent a request for access to his data pursuant to Article 15 of the GDPR to [redacted] on 6 August 2023. [redacted] sent the Complainant a reply requesting to be informed of his location so that the relevant data protection officer could contact the Complainant. After informing [redacted] of his location, the Complainant was asked to send his request to [redacted]. The Complainant explained that he had already sent

his request to [redacted]. On 11 September 2023, the Complainant sent a reminder to [redacted], as he had not received a response to his request from the Controller. On 14 September 2023, the Complainant received confirmation from [redacted] that his request had been received, but the deadline for replying was extended until 6 November 2023 due to the complexity of the request. On 13 October 2023, 19 October 2023 and 25 October 2023, the Complainant received additional emails concerning recruitment from an employee of [redacted] to his personal email address. The Complainant did not receive a reply from [redacted] to his request.

Following a complaint lodged by the German DPI, the Estonian DPI initiated a supervisory procedure on the basis of Section 56(3)(8) of the Personal Data Protection Act. Considering that [redacted] is the controller[1] according to the published privacy policy on recruitment, the Estonian DPI sent an enquiry to [redacted] within the framework of the supervisory procedure.

Clarifications by the Controller

[redacted] reassured the Estonian DPI that it had replied to the Complainant's request on 19 February 2024 and enclosed a copy of the reply. No further correspondence has been exchanged between the Controller and the Complainant.

The Estonian DPI asked [redacted] to explain why, in order to respond to the data subject's request, it was necessary to collect additional data (in this case location information) from the Complainant in advance. The Controller explained to the Estonian DPI that [redacted] does not need to collect additional information on the location of the data subject in order to comply with the data subject's request. Under no circumstances do [redacted]'s internal rules require data subjects or legal entities to provide this type of information in connection with requests for access to personal data. In the present case, the customer support erroneously asked the Complainant to disclose his location, which is not in line with the procedure for processing data subject requests established by [redacted]. Instead, the request should have been identified at an early stage as a request for access to the data subject's personal data and referred to the Data Protection Team in accordance with [redacted]'s internal rules. [redacted] claims that the incident was due to human error rather than [redacted]'s usual practice.

In addition, the controller explained that despite the extensive training programme for [redacted]'s customer support (as well as external customer support agents), due to human error, the request may not be properly processed. The external customer support agent dealing with the Complainant's initial request had completed two training sessions on data protection in the last twelve months. These initiatives were specifically designed to improve the ability of trainees to recognise queries from users and authorities. These trainings are part of [redacted]'s compulsory onboarding program, which is mandatory for any new customer support agent.

The Controller explained that it has put in place the following remedial measures to prevent similar errors in the future:

- On 27 April 2024, [redacted] established a special customer support team dedicated to handling data protection requests in order to improve the handling of data subjects' requests and allocate additional resources for handling them. One of the goals of creating a team is to reduce the risk of similar incidents happening again. The team is responsible for guiding customer support agents, assisting in the identification and handling of data protection requests, and providing the data protection team with additional oversight in the handling of data subject requests.
- [redacted] has also contacted an external partner with whom a particular customer support agent worked, instructing him to be particularly attentive when dealing with data subject requests. In particular, the partner was asked to remind its agents that requesting the data subjects' location was contrary to the internal arrangements put in place by [redacted]. In

[1]Global Privacy Notice for Recruitment - [redacted]

addition, further instructions were given to the partner to strengthen the correct procedures for dealing with similar cases.

The position of the Estonian DPI

Pursuant to Article 15 GDPR, the data subject has the right to receive information about the processing of his or her personal data and to submit a request to the controller for this purpose. Pursuant to Article 12(3) GDPR, the controller shall respond to the data subject's request without undue delay, but no later than one month after receipt of the request.

When receiving a request for access to personal data, the controller must assess whether the request concerns personal data relating to the person making the request. In order to ensure the security of processing and minimise the risk of unauthorised disclosure of personal data, the controller must be able to identify which data refer to the data subject and identify that person. As a general rule, the controller cannot request more personal data than is necessary to enable authentication and that the use of such information should be strictly limited to the fulfilment of data subjects' requests. Where the controller requests or receives from the data subject additional information necessary to establish the identity of the data subject, the controller shall, on each occasion, assess what information it can use to establish the identity of the data subject and may ask the applicant additional questions or require the data subject to provide any additional element of identification, where proportionate.[2]

The Estonian DPI requested information from the Controller as to why the data subject was asked to provide information on his location when his request was received. [redacted] has confirmed that, in the present case, the customer support agent erroneously requested the location data of the data subject and that this is not in line with the procedure for processing data subject requests established by [redacted]. In the opinion of the Estonian DPI, asking the Complainant for location data was not proportionate and necessary (including for identification purposes) in order to resolve the request for access to personal data. Therefore, the Controller's request for additional data from the Complainant was not in line with the GDPR.

Under certain conditions, the controller may, if necessary, extend the period for responding to a request for access by an additional two months, taking into account the complexity and number of the requests.[3] The EDPB has underlined that this possibility is an exception to the general rule and should not be used excessively.[4] According to the complaint, the Controller informed the Complainant of the extension of the time limit for responding to the request only after receiving a reminder from the Complainant. However, the Complainant did not receive a reply to its request even after the expiry of the extended time limit. This indicates that the processes of the Controller in handling the data subject's request did not ensure compliance with the personal data protection regulation and did not work. Therefore, it is necessary for the Controller to improve its processes for handling the requests.

The Controller replied to the Complainant only after receiving the notification from the Estonian DPI that, to the knowledge of the Inspectorate, [redacted] had failed to respond to the Complainant's request. At the same time, the Estonian DPI takes into account that the Controller verified the facts and replied to the Complainant before initiating the supervisory procedure. At the time of the start of the supervisory procedure, the infringement had been remedied.

Since the Controller confirmed that the Complainant's request had been answered and that no further correspondence had been exchanged with the Complainant, the Estonian DPI asked the SA

[2]European Data Protection Board. Guidelines 01/2022 on data subject rights – Right of access, ver 2.1, adopted on 28 March 2023, p. 65, 67, page 26. - https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf
[3]Article 12(3) GDPR.
[4]Guidelines 01/2022, p. 162, page 51.

Berlin to contact the Complainant and ask him to confirm that [redacted] had replied to his request. The SA Berlin informed the Estonian DPI that the Complainant had been approached and asked to send confirmation by 31 October 2024 at the latest. As of 5 November 2024, the Estonian DPI did not receive any confirmation or other feedback from the Complainant.

The Controller has put in place organisational measures to improve the handling of the data subject's requests and has provided further guidance to the partner in the specific case to avoid similar cases. Since the Complainant's request has been answered before the commencement of the supervisory proceedings, the Estonian DPI **therefore terminates the present supervisory proceedings**. At the same time, we draw the Controller's attention to the following:

The fact that a large company receives a large number of applications cannot be a reason to extend the deadline for replying to a request. The controller, especially when processing large amounts of data, should have processes and mechanisms in place to be able to handle requests under normal circumstances within 30 days.[5]

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 the administrative court under the Code of Administrative Court Procedure[7] (in this case, the challenge in the same matter can no longer be reviewed).

Yours sincerely,

[redacted]
Lawyer
Under the authority of the Director-General

[5] Guidelines 01/2022, p. 164, p. 52.
[6] https://www.riigiteataja.ee/en/eli/527032019002/consolide
[7] https://www.riigiteataja.ee/en/eli/512122019007/consolide