



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

FOR INTERNAL USE

Controller of the information: Data Protection
Inspectorate

Entry made:: 08.07.2026

Access restriction valid until: 08.07.2026 -
08.07.2101

Legal basis: AvTS § 35 lg 1 p 12, AvTS § 35 lg
1 p 2

Ours: 08.07.2026 nr 2.1.-
1/20/960-1303-68

DS.523.7772.2021.PT.KF

Decision on the termination of the proceedings

Estonian Data Protection Authority (Estonian DPA) received a complaint from [REDACTED] (hereinafter also referred to as *the complainant*) against [REDACTED] (hereinafter also referred to as [REDACTED], *the controller*, or *the company*) concerning the processing of his personal data. Estonian DPA forwarded the complaint to the Polish supervisory authority, *Urząd Ochrony Danych Osobowych* (UODO), as the controller is established in Poland and UODO is therefore the lead supervisory authority.

UODO conducted a supervisory procedure and, on 28 May 2026, adopted a decision pursuant to Articles 5, 6(1), 12(4), 58(2)(b), 60(9), and 56(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter *the GDPR*), as well as the relevant provisions of the Polish Code of Administrative Procedure.

In its decision of 28 May 2026, UODO partially upheld the complaint and, pursuant to Article 58(2)(b) GDPR, issued a reprimand to the controller for infringing Articles 12(1), (2), (4), and (6) GDPR in conjunction with Article 5(1)(a) GDPR. The infringement consisted of the Company's failure to respond to the complainant's representative at the email address from which the request had been submitted.

Furthermore, pursuant to Article 58(2)(d) GDPR, UODO ordered the Company to bring its processing operations into compliance with Articles 12(1), (2), (4), and (6) GDPR by providing the complainant's representative with a response to the request for the erasure of the complainant's personal data and by informing UODO of the implementation of this decision within 30 days of its notification.

Pursuant to Article 60(9) GDPR, where the lead supervisory authority and the supervisory authorities concerned agree that part of a complaint should be dismissed or rejected and that another part of the complaint should be acted upon, separate decisions shall be adopted for each part. The lead supervisory authority shall adopt the decision concerning the part of the complaint related to actions with regard to the controller and shall notify it to the controller's or processor's main or single establishment in its Member State, while informing the complainant accordingly. The supervisory authority of the complainant's Member State shall adopt the

decision concerning the part of the complaint that has been dismissed or rejected, notify the complainant thereof, and inform the controller or processor accordingly.

Accordingly, the Estonian DPA hereby adopts its decision with respect to the part of the complaint that was dismissed.

Facts of the complaint

In the complaint of 09.04.2020 and the supplementary letter of 18.04.2022, the Complainant indicated that he had an employment relationship with the Company between 03.12.2018 and 23.03.2020. The employment contract was concluded on the basis of Estonian law. The Company terminated the extraordinary employment contract with the Complainant pursuant to Article 88(1)(5) of the Estonian Employment Contracts Act.

The Complainant claims that in the period from 23/03/2020 the Company used the Complainant's email address [REDACTED], even though the Complainant did not consent to this and was not informed in advance of the possibility for the Company to consult the correspondence kept by the Complainant using the email address [REDACTED]. The Complainant pointed out in this regard that on the date of filing the complaint, i.e. 09.04.2020 sending an e-mail to [REDACTED] resulted in an automatic reply, which incorrectly informed that the Complainant was on vacation and could not receive calls and did not have access to e-mail at that time. The Complainant points out that the above meant that his e-mail address was still used by the Company at the time when the complaint was lodged on 09.04.2020.

In addition, in the supplementary letter of 18.04.2022, the Complainant indicated that, after the termination of the employment relationship, [REDACTED] (then Vice-President of the Company) had obtained access to the Complainant's correspondence with [REDACTED] on 22.04.2020 and 16.04.2021 and had forwarded part of that correspondence to third parties.

On 30.03.2020, the Complainant's representative, [REDACTED], sent an email from the email address [REDACTED] to the following email addresses: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED] in which he requested the immediate closure and deletion of the Complainant's e-mail address [REDACTED] and the cessation of the processing of the Complainant's personal data. The Complainant's representative appointed one day to comply with the request. In the complaint, the Complainant indicated that, as at the date of lodging the complaint, the Company had not responded to the request of the Complainant's representative.

In the complaint of 09.04.2020 and the supplementary letter of 18.04.2022, the Complainant alleges that the Company processed the Complainant's personal data without a legal basis, as well as failed to reply and to comply with the request for deletion of data of 30.03.2020. The Complainant requests that the supervisory authority determine: (1) how the Company obtained access to the Complainant's (private) correspondence; (2) who personally uses the Complainant's e-mail address (including at whose request), whether the Complainant's private correspondence is read and recorded, and if so, who personally does so, including at whose request and to whom the data is transferred; (3) whether it is a one-off or a continuous activity; (4) for how long the e-mail correspondence is stored; (5) what data has been read and stored; (5) whether correspondence from other employees has been read; (6) analysis of the legitimate interest of the Company. The Complainant further requests that the supervisory authority order the Company to cease the disclosure and use of the Complainant's personal data, as well as to inform the Complainant of the breach concerning the storage and access to correspondence. In addition, the Complainant requests that the supervisory authority impose an administrative fine

on the Company.

In the course of the administrative proceedings, the President of the Personal Data Protection Office (hereinafter: PUODO) obtained explanations regarding the circumstances of the case and established the following facts:

1. The Complainant was employed by the Company from 03.12.2018 to 23.03.2020 (evidence: complaint of 09.04.2020).
2. On 23.03.2020, the Company terminated the employment contract with the Complainant pursuant to Article 88(1)(5) of the Estonian Employment Contracts Act. In the notice of termination of the employment contract, the Company indicated that the Complainant had committed theft, fraud or other act that caused the loss of the Company's trust in the Complainant, and therefore the termination of the employment relationship is justified by the following violations: participation in an organized group that charged Estonian entrepreneurs an unjustified fee for using the Company's platform (evidence: complaint of 09.04.2020).
3. The Company explained that the Complainant's personal data had been obtained in connection with his employment with the Company. The Company indicated that it had provided the Complainant with the e-mail address [REDACTED] in connection with the employment and that this address was to be used by the Complainant solely for business purposes for the purposes of the employment relationship (evidence: the Company's explanation of 15.11.2021).
4. The Company terminated the employment contract with the Complainant because it detected that the Complainant, in cooperation with other persons, including [REDACTED], used the Company's brand name and business email addresses in order to charge customers of the [REDACTED] capital group from Estonia an additional commission which was paid to the Estonian company established for that purpose ([REDACTED] translated as "[REDACTED]"). Due to the commission of the described acts in Estonia, the Company notified the Estonian law enforcement authorities. In particular, the Company provided the Estonian law enforcement authorities with evidence in the form of correspondence from the Complainant's business e-mail box, which allegedly showed that the Complainant, using his business e-mail address, had agreed on a course of action and confirmed the existence of an alleged additional commission to [REDACTED]'s customers. (evidence: the Company's explanation of 15.11.2021).
5. As at 15.11.2021, i.e. the date on which the Company submitted its first explanations in the case, criminal proceedings were ongoing in Estonia with the participation of the Complainant and [REDACTED] and separate court proceedings in the labour court with the participation of the Complainant. The complainant appealed to the labour court in Estonia in connection with the termination of the employment contract by the Company. The Estonian labour court at first instance agreed with the Company. The Complainant lodged an appeal against that judgment. (evidence: the Company's explanation of 15.11.2021)
6. Currently, criminal proceedings are still ongoing against [REDACTED] in respect of acting to the detriment of the Company. [REDACTED] has the status of wanted person and the emails containing the findings between the Complainant and [REDACTED] constitute evidence of the actions taken by the Complainant and [REDACTED] injuring the Company. (evidence:

explanations of the Company dated 28.03.2025)

7. Criminal proceedings against the Complainant were terminated by an order of the Economic and Corruption Crimes District Prosecutor's Office in Tallinn on 29.11.2024. They were terminated due to the absence of the elements of a criminal offence in the conduct of the Complainant. (evidence: Complainant's letter of 13.01.2026)
8. 22.04.2020, [REDACTED], from the email address [REDACTED], sent to: [REDACTED] and [REDACTED] the Complainant's correspondence with [REDACTED] and the Complainant's correspondence with a client (evidence: Complainant's supplementary letter of 18.04.2022)
9. On 22.04.2020, correspondence between the Complainant and [REDACTED] was forwarded from the email address [REDACTED] to the email address [REDACTED] (evidence: Complainant's supplementary letter of 18.04.2022)
10. 16.04.2021, the Complainant's correspondence with [REDACTED] of 15.01.2020 and 20 and 25.02.2020 was viewed (evidence: Complainant's supplementary letter of 18 April 2022)
11. [REDACTED] acted as the Company's legal representative in the proceedings in Estonia against the Complainant (evidence: the Company's explanation of 21.10.2025)
12. [REDACTED] acted as an independent proxy (pl. prokurent samoistny) of the Company. [REDACTED] was employed as the Company's Operations Director. [REDACTED] and [REDACTED] had authorisations, valid respectively from 30.09.2019 and 11.10.2018, to process personal data in accordance with the scope of professional or contractual duties performed for the position held in the Company (evidence: the Company's explanation of 21.10.2025)
13. Only [REDACTED] had access to the Complainant's mailbox. The Company explains that the Complainant's e-mails were verified only in view of the above-mentioned proceedings in Estonia and forwarded as evidence to the Estonian Police and courts. In this respect, the Company pointed to the need to determine the manner of operation of the Complainant and [REDACTED], as well as to identify the affected customers of the Company. This information served as evidence in the case. (evidence: explanations of the Company dated 28.03.2025)
14. The Company indicated that the Company's employee, by logging in to the e-mail, obtains information that the Company has access to the e-mail. On 11.09.2019, the Complainant signed a statement of acquaintance with the Company's Internal Regulations. (evidence: explanations of the Company dated 28.03.2025)
15. The Complainant's email address is currently deactivated. By sending an e-mail to the Complainant's address, the sender receives a return message that the address [REDACTED] does not exist. (evidence: explanations of the Company dated 28.03.2025)
16. The Company indicates that it is currently processing the Complainant's personal data in terms of name, surname and e-mail address pursuant to Article 17(3)(e)

GDPR in conjunction with Article 6(1)(f) GDPR (for the establishment, exercise or defence of claims). In addition, the Company indicated that it is processing the data contained in the Complainant's personal file on the basis of Article 6(1)(c) GDPR in conjunction with § 5 point 5 of the Estonian Employment Contracts Act, according to which the employer is obliged to store data for a period of 10 years, counting from the end of the calendar year in which the employment relationship was terminated or expired. (evidence: explanations of the Company dated 28.03.2025 and 21.10.2025)

17. On 30.03.2020, the Complainant's representative, [REDACTED] (hereinafter: Complainant's representative) sent an email from the email address [REDACTED] to the following email addresses: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED] in which he requested the immediate closure and deletion of the Complainant's e-mail address [REDACTED] and the cessation of the processing of the Complainant's personal data. The e-mail did not contain a power of attorney to represent the Complainant in exercising the right to delete the Complainant's personal data. The Complainant's representative asked for a reply to the request to be sent to [REDACTED] by 31.03.2020 (evidence: Complaint of 09.04.2020; the Company's explanation of 15.11.2021)
18. On 31.03.2020, the Company's attorney, [REDACTED], from the e-mail address [REDACTED], sent a message to the address [REDACTED] indicating that due to problems with identity verification, he asks for all correspondence to be sent in writing to the following address: [REDACTED]. The Company indicated that the Complainant's e-mail address and the domain [REDACTED] remain the property of the Company and will be deactivated in due time. (evidence: explanations of the Company dated 28.03.2025)

Legal reasoning of the decision

1. As regards the Complainant's allegation that the Company processes the Complainant's personal data without a legal basis and failed to comply with the request to delete his personal data, the PUODO considered the following.

The provision entitling controllers to process data of natural persons is Article 6(1) of the GDPR, according to which data processing is permissible only if one of the conditions set out in that provision is met. Catalogue of conditions listed in Article 6(1) GDPR, is closed. Each of the grounds for legalizing the processing of personal data is autonomous and independent. This means that those conditions are, in principle, equal, and therefore the fulfilment of at least one of them determines the lawful processing of personal data. Consequently, the consent of the data subject is not the only basis for the processing of personal data, since the data processing process will also comply with the GDPR if the controller demonstrates that another of the above-mentioned conditions is met. Irrespective of the consent of the data subject (Article 6(1)(a) GDPR), the processing of personal data is permissible, inter alia, when it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b) GDPR), for compliance with a legal obligation to which the controller is subject (Article 6(1)(c) GDPR) and the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the

data subject which require the protection of personal data, in particular where the data subject is a child (Article 6(1)(f) GDPR).

2. On the basis of the evidence gathered, it was established that the Complainant's email address was provided to him for work purposes. When logging into their email accounts, the Company's employees are informed that the Company has access to their emails, and the Complainant signed a declaration confirming that he had read the Company's Regulations. In light of the above, the Company had access to the Complainant's work email account during the course of the employment relationship pursuant to Article 6(1)(b) of the GDPR.

It should be emphasised, in particular, that the creation of an employment relationship generates a number of obligations on the part of the employer related to documenting the course of the employee's work, including, above all, keeping personal files. According to § 5 point 5 of the Estonian Employment Contracts Act, the employer is obliged to keep the data for a period of 10 years from the end of the calendar year in which the employment relationship was terminated or expired.

It stems from the above that the Company, as the Complainant's former employer, is obliged to keep employee documentation concerning the Complainant. Therefore, it is not possible for the authority to order the Company to cease processing the Complainant's personal data or to delete them from the documentation concerning him. In the light of the above, it must be concluded that the processing of the Complainant's personal data by the Company for this purpose and to the extent resulting, inter alia, from the above-mentioned provisions is necessary for the fulfilment of its legal obligation and is therefore based on the condition arising from Article 6(1)(c) GDPR.

3. In the course of the proceedings, it was established that the processing of the Complainant's personal data regarding the name, surname, e-mail address and correspondence kept by the Complainant available in the e-mail address [REDACTED] entrusted to the Complainant during the employment relationship, including maintaining access to this box, were made for the purpose of establishing, pursuing or defending claims. The Company pointed out that the data in the above-mentioned scope were made available only to Estonian law enforcement authorities and Estonian courts in connection with ongoing proceedings. The Company explained that it had provided the Estonian law enforcement authorities with evidence in the form of correspondence from the Complainant's business e-mail box, which allegedly showed that the Complainant, using his business e-mail address, had arranged a course of action and confirmed the existence of an alleged additional commission to [REDACTED]'s customers. In addition, the Company processed the Complainant's personal data in the above-mentioned scope in connection with the Complainant's appeal to the labour court in Estonia in connection with the Company's termination of the employment contract.
4. The decision on the merits of the claims brought by the Complainant and the Company falls within the jurisdiction of the relevant courts in Estonia. However, the Company's actions aimed at establishing, pursuing or defending claims, for which the processing of the Complainant's personal data in the above-mentioned scope is necessary, should be considered legal. The above has a legal basis in the condition resulting from Article 6(1)(f) GDPR. This applies to the processing of data by the Company's employees, i.e. [REDACTED] and [REDACTED], who had valid authorizations to process personal data in connection with their position and official duties. This also applies to the transfer of personal data to [REDACTED], who acted as a legal representative of the Company in proceedings conducted in

Estonia against the Complainant.

5. In the opinion of the President of the UODO, the processing of the Complainant's personal data consisting in making his personal data available by the Company in scope of name, surname, e-mail address and correspondence kept by the Complainant available in the e-mail address inbox [REDACTED] to the legal representative in order to represent the Company in the proceedings was a legal process and was based on the premise arising from Article 6(1)(f) GDPR.

In order to legitimise processing on the basis of Article 6(1)(f) of the GDPR, the first step requires the cumulative fulfilment of two conditions: namely, the existence of a legitimate interest on the part of the controller or a third party, and the necessity of the processing for the purposes arising from that interest. In the second stage, however, it is necessary to assess whether a negative condition is met, namely the existence, in the given circumstances, of the data subject's interests or fundamental rights and freedoms which override the legitimate interests of the controller or a third party (D. Lubasz, W. Chomiczewski [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, ed. E. Bielak-Jomaa, Warszawa 2018, art. 6.) In establishing this condition for the admissibility of data processing, the EU legislator used the vague term 'legitimate interest' without defining the concept. As accepted in legal doctrine, a legitimate interest should not be understood narrowly, merely as an interest directly arising from a legal provision (granting a specific right to a data subject); it should be interpreted more broadly as various types of interest that find their justification in the provisions (Fajgielski Paweł, Test ważenia interesów i praw przy stosowaniu klauzuli prawnie uzasadnionych interesów, LEX). It may therefore be a factual, economic or legal interest, but one that is lawful. In recitals 47 and 49, the EU legislator cited the following as examples of such interests: direct marketing, fraud prevention, and ensuring the security of services offered or made available via networks and systems. Furthermore, the controller must demonstrate that the processing is necessary for the purposes of legitimate interests. It is therefore not sufficient for these interests to exist; rather, their realisation must also require the processing of personal data. As is the case under Article 6(1)(b) of the GDPR, there must also be a direct link here between the pursuit of a legitimate interest and the need to process personal data (D. Lubasz, W. Chomiczewski [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, ed. E. Bielak-Jomaa, Warszawa 2018, art. 6.).

6. The protection of personal data is not an absolute right and its purpose is not to prevent actions in the course of proceedings before a common court. In the case at hand, the PUODO assessed that the right to the protection of the Complainant's personal data does not take precedence over the interests pursued by the controller of his data, in this case the Company. As indicated above, the Company processed the Complainant's personal data in connection with the ongoing proceedings, and the correspondence sent by the Complainant from the Company's domain served as evidence in those proceedings. It is not the role of the PUODO to conduct proceedings aimed at removing evidence in cases conducted before courts or other state authorities, even if they contain personal data. It should also be noted that the complainant's personal data was disclosed solely to the Estonian law enforcement authorities and the Estonian courts in connection with the proceedings referred to above.

In light of the circumstances outlined, in the opinion of the PUODO, the Company's legitimate interest in establishing, pursuing or defending claims—for which the processing of the Complainant's personal data was and remains necessary—takes

precedence over the Complainant's interests and rights.

7. It is irrelevant in the present case to invoke a request for deletion of the Complainant's data. In accordance with Article 17(1) GDPR the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the circumstances listed in that provision applies, in particular where the personal data have been processed unlawfully.

Having regard to the content of Article 17(3)(b) GDPR, paragraphs (1) and (2) shall not apply to the extent that the processing is necessary for compliance with a legal obligation requiring processing under Union or Member State law to which the controller is subject. As stated above, the Company processes the personal data contained in the Complainant's personal file on the basis of § 5 point 5 of the Estonian Employment Contracts Act, i.e. on the basis of a legal obligation, and therefore there are currently no grounds to order the Company to delete the Complainant's personal data with regard to the data contained in the personal file.

At the same time, taking into account the content of Article 17(3)(e) GDPR, paragraphs 1 and 2 shall not apply to the extent that the processing is necessary for the establishment, exercise or defence of legal claims. Despite the fact that the criminal proceedings against the Complainant have been terminated due to the absence of any criminal elements in the complainant's conduct, according to the information available to the PUODO, criminal proceedings are still ongoing against [REDACTED] in relation to acts detrimental to the Company, which took place in collaboration with the Complainant, and the emails exchanged between the Complainant and [REDACTED] constitute evidence in the proceedings, which are still ongoing. In view of the above, in the opinion of PUODO, access to the Complainant's correspondence constitutes a legitimate interest, it is not possible to order the Company to delete the Complainant's personal data as regards the name, surname and content of the Complainant's e-mail address box.

8. The administrative procedure conducted by the PUODO serves to control the compliance of data processing with the provisions on the protection of personal data and is aimed at issuing an administrative decision restoring the lawful state on the basis of Article 58(2) GDPR. The assessment carried out by the PUODO in each case serves to examine the legitimacy of an order addressed to a specific entity corresponding to the provisions of Article 58(2) GDPR to restore the lawful state in the data processing process - it is therefore justified and necessary only to the extent that irregularities in the processing of personal data exist. In the present case, the authority established that the Company had, and currently has, a legal basis for processing the Complainant's personal data, i.e. Article 6(1)(b) RODO as regards access to complainant's email account during the course of employment, Article 6(1)(c) GDPR as regards the Complainant's personal file and Article 6(1)(f) GDPR as regards the name, surname and contents of the Complainant's e-mail address.

In view of the above, the PUODO dismisses the complaint regarding the processing of the Complainant's personal data without a legal basis and failure to comply with the request to delete the Complainant's data.

With regard to the Complainant's requests for a determination by the supervisory authority: (1) how the Company obtained access to the Complainant's (private) correspondence; (2) who personally uses the Complainant's e-mail address

(including at whose request), whether the Complainant's private correspondence is read and recorded, and if so, who personally does so, including at whose request and to whom the data is transferred; (3) whether it is a one-off or a continuous activity; (4) for how long the e-mail correspondence is stored; (5) what data has been read and stored; (5) whether correspondence from other employees has been read; (6) analysis of the legitimate interest of the Company, it should be pointed out that the PUODO made the above findings in the course of the proceedings, which is reflected in the collected case file, as well as facts and legal justification indicated in this decision.

With regard to the request to impose an administrative fine on the Company, it should be pointed out that the PUODO may impose an administrative fine on the Controller (Article 58(2)(i) GDPR), however, does so ex officio and not at the request of the Complainant.

In light of the above, the DPA terminates the supervisory procedure.

The addressee of the decision may challenge the termination of the proceedings within 30 days by submitting either an objection under the Administrative Procedure Act to the Director General of the Data Protection Inspectorate, or a complaint under the Code of Administrative Court Procedure to the administrative court (in which case the objection can no longer be examined in the same matter).

Yours sincerely

/Digitally signed/



lawyer

authorized by Director General