

**PRESIDENT
PERSONAL DATA
PROTECTION OFFICE**

Mirosław Wróblewski

Warsaw, 28.05.2026

DS.523.7772.2021. [REDACTED]

DECISION

On the basis of Art. 104(1) of the Code of Administrative Procedure of 14 June 1960 (consolidated text: Journal of Laws 2024, item 572) (hereinafter: CAP), Art. 7 (1) and (2) of the of the Personal Data Protection Act of 10 May 2018 (Journal of Laws 2019, item 1781) and Art. 5, 6(1), 12 (1)-(4), 12(6), 58(2) (b) and (d) and Article 60(9) 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: GDPR) following the investigation of [REDACTED] complaint (address: [REDACTED] [REDACTED]) (hereinafter: Complainant), represented by [REDACTED] [REDACTED]), forwarded to the President of the Personal Data Protection Office via the Estonian Supervisory Authority (Andmekaitse Inspektsioon, seat: Tatari tn 39 / 10134 Tallinn, Estonia), concerning irregularities in the processing of the Complainant's personal data by [REDACTED] (address: [REDACTED]) (hereinafter: The Company) consisting in the processing of personal data without a legal basis and failure to respond and comply with the request to delete personal data, the President of the Personal Data Protection Office acting as a leading supervisory authority within the meaning of Article 56(1) GDPR:

- 1. orders the Company to bring processing operation into compliance with Article 12 (1),(2), (4) and (6) of the GDPR, by providing the Complainant with information in connection with the request to delete the Complainant's data pursuant to Article 17 of the GDPR;**
- 2. issues a reprimand to the Company for violation of Article 12 (1),(2), (4) and (6) GDPR in connection with Article 5(1)(a) GDPR, consisting in the failure to respond to the request for deletion of the Complainant's personal data pursuant to Article 17 of the GDPR;**
- 3. dismisses the complaint in the remaining scope.**

Justification

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 [REDACTED]) 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] 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] 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)

After examining all the evidence gathered in the case, the President of the Personal Data Protection Office weighed the following.

The GDPR sets out obligations of the controller, which include the processing of personal data in compliance with the prerequisites set out in that regulation. The provision authorising the controller to process the data of natural persons is Art. 6(1) GDPR, according to which, the processing of data is only allowed if one of the prerequisites indicated in this provision is fulfilled. The catalogue of legal grounds listed in Art. 6(1) GDPR is closed. Each of conditions legalising the processing of personal data is autonomous and independent in nature. This means that these prerequisites are, as a rule, equal, and therefore the fulfilment of at least one of them constitutes lawful processing of personal data.

Art. 12 GDPR refers to transparent information, communication and modalities for the exercise of the rights of the data subject. In accordance with Art. 12(1) GDPR, the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. Art. 12(2) GDPR provides that the controller shall facilitate the exercise of data subject rights under Articles 15 to 22 GDPR. In the cases referred to in Art. 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22 GDPR, unless the controller demonstrates that it is not in a position to identify the data subject. In accordance with Art. 12(3) GDPR, the controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. Art. 12(4) GDPR provides that if the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. In accordance with Art. 12(6) GDPR, without prejudice to Art. 11 GDPR, where the controller has reasonable doubts concerning the identity of the

natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

In the present case, the Complainant raised two main complaints against the Company, the first concerning the failure to respond to the Complainant's request for erasure of personal data, and the second concerning the processing of the Complainant's personal data without a legal basis and the failure to comply with the request for erasure of his personal data.

Firstly, as regards the Complainant's allegation that the Company did not respond to the request for erasure of the Complainant's personal data, the PUODO considered the following.

On 30.03.2020, the Complainant's representative sent an email from the email address [REDACTED] to the following email addresses: [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. By e-mail, the Complainant's representative asked for a reply to the request to be sent to [REDACTED] by 31.03.2020.

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.

In this regard, it should be noted that, in accordance with Recital 59 GDPR, procedures should be provided to facilitate the exercise of the data subject's rights under this Regulation, including mechanisms to request and, where applicable, obtain free of charge, in particular access and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

In accordance with Art. 5(1)(a) GDPR, personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). The principle of fairness of processing requires controllers of personal data to be accurate, diligent and to duly comply with their obligations, as well as to behave honestly and in good faith. "The duty of fairness requires that the controller should not mislead the data subject, deceive it, take advantage of its vulnerability, constraints or coercive position, exploit its superior position by imposing restrictive conditions on the

processing, and should respect the will and interests and the legitimate expectations of the data subject” (see: P. Fajgielski [in:] Commentary to Regulation 2016/679 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 (General Data Protection Regulation) [in:] General Data Protection Regulation. Personal Data Protection Act. Commentary, Warsaw 2018, Article 5).

Art. 5(2) GDPR makes the controller responsible for complying with the provisions set out in Art. 5(1) GDPR and requires the controller to be able to demonstrate compliance (principle of accountability).

The Complainant's representative approached the Company on 30.03.2020 and indicated that he represented a specific person, the Complainant. This message was effectively delivered, as evidenced by the content of the reply of 31.03.2020 sent from [REDACTED] to the e-mail address [REDACTED]. The company was therefore aware that it had received a specific letter containing a specific request. The response to the request was provided from the e-mail address [REDACTED] to the e-mail address [REDACTED], i.e. an address different from the address from which the request was received. It is worth noting that 23.03.2020 the Company terminated the employment contract with the Complainant pursuant to Article 88(1)(5) of the Estonian Employment Contracts Act, therefore at the time that the response to the request was sent to the Complainant's work e-mail address, he was no longer employed in the Company.

It should be stressed here that every individual should be able to easily exercise their rights under the GDPR. The GDPR does not prohibit data subjects from exercising their rights through a proxy and does not require requests to be made only directly by the data subjects in order to be effective. Therefore, the ability to easily exercise rights under the GDPR also implies the ability to exercise the rights by a proxy. Where certain third parties are authorised to exercise their rights under the GDPR or to act on behalf of data subjects, situations may arise where the controller has doubts as to the effectiveness of such representation. In such situations, as a general rule, the controller, taking into account the principle of proportionality, may carry out a verification of the representation, for example by requesting a copy of the authorisation document or by making the authorisation available for inspection.

The PUODO notes that where the controller has doubts as to the identity of the natural person making the request or his or her entitlement to make such a request, it is necessary for him or her to make use of the solution provided for in Article 12(6) GDPR, i.e. requesting additional information in order to carry out appropriate verification. Similarly, the Voivodship Administrative Court in Warsaw stated in its judgment of 23 May 2022 (II SA/Wa 3550/21) that '[...] despite the unconditional right of an individual to obtain information as to whether the controller processes his or her personal data, the bank is not entitled to make data covered by banking secrecy available to any person without first verifying whether this is the person entitled to receive such data. Any doubt by the bank as a controller of personal data in this regard requires the taking of verification measures as provided, inter alia, in Article 12(6) of Regulation 2016/679.'

The controller also has a general obligation to take appropriate measures to communicate with the data subject under Articles 15-22 and 34 of the GDPR on the processing (Article 12(1) of the GDPR). Therefore, where the controller receives a request in respect of which the controller has doubts as to whether it originates from the data subject or a person representing him or her, the controller is obliged to take appropriate measures to communicate with the requester, including to communicate to him or her doubts as to his or her identity or authority to act. The Controller cannot ignore the request from what it believes to be a questionable source and request that the communication be made to the Company's traditional mail address, at the same time forwarding this response to an address different from the one from the one from which the request was made. Here, the PUODO observes that the request made by the Complainant's representative could not be regarded as manifestly unfounded and not requiring any response, since it was possible to identify the person making the request, as well as the person likely to represent him, and the request itself and the actual addressee of that request. Knowing the contact details of the Complainant's representative, the Company was able to easily contact the Complainant's representative in order to clarify its doubts and make up for any shortcomings or ambiguities in the request, but did not do so.

Moreover, it should be noted that, in accordance with Art.12(2) GDPR, the controller shall facilitate the exercise of data subject rights under Articles 15 to 22 GDPR. In the cases referred to in Article 11(2) GDPR, the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22 GDPR, unless the controller demonstrates that it is not in a position to identify the data subject. Therefore, even when a request is received and the controller has doubts as to whether it originates from a data subject, the controller is still obliged to facilitate the exercise of the data subject's rights provided for in the relevant provisions of GDPR. Thus, the controller should facilitate the exercise of the rights of the requester whose identity it doubts by verifying the identity of the requester or by verifying the authorization to act on behalf of another data subject. Failure to respond to the email address of the Complainant's representative from whom the request originated made it difficult to exercise the Complainant's rights. If doubts were raised as to the identity of the person making the request by the Company directly, the Complainant's representative would have a chance to prove the existence of a legal authority, and thus the Complainant would have a chance to actually exercise his rights under the GDPR.

The PUODO also points out that, in accordance with Art. 12(3) GDPR, the controller is required to provide the data subject with information on the action taken on the request pursuant to Articles 15 to 22 without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. In accordance with Art. 12(4) GDPR, if the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. The Company did not provide

any reply in the present case, which could meet the requirements of the above-mentioned Art. 12(3)-(4) GDPR.

Thus, the PUODO therefore concludes that, the controller, in a case of receiving a request from a person in respect of whom it has doubts as to whether it has the appropriate authority to act on behalf of the data subject, is still obliged to carry out the relevant communication (Art. 12(1) GDPR), facilitating the exercise of the data subject's rights (Art.12(2) GDPR) and should, in such a situation, verify the identity and authority to act of the person making the request (Art. 12(6) GDPR). Transmission by the Company of the response to the request of the Complainant's representative only to the e-mail address [REDACTED], and thus leaving the request without a response to the Complainant's representative (as provided for in Article 12(3) or (4) of the GDPR), constitutes a clear breach of the rules governing transparent information and communication and the procedure for exercising the rights of the data subject in relation to the principle of fair and transparent processing. The PUODO notes that ensuring compliance with Article 12 of the GDPR, i.e. providing a response and determining the existence of appropriate powers of attorney or indicating the shortcomings and ambiguities of the letter submitted to the Company, does not require it to take disproportionate actions or significant financial outlays.

The administrative proceedings conducted by the PUODO on the basis of the GDPR are aimed at controlling the compliance of data processing with the rules on the protection of personal data and are aimed at issuing an administrative decision restoring a lawful state on the basis of Art. 58(2) GDPR. The assessment carried out by the PUODO in each case shall be used to examine whether it is appropriate to address the corrective measure referred to in Art. 58(2) GDPR to a specific entity, intended to restore the state of lawfulness of data processing.

In the light of the above, the PUODO considers it reasonable to issue a reprimand in accordance with Article 58(2)(b) GDPR, for violation Art. 12.(1), (2), (4), and (6) GDPR in conjunction with Art. 5(1)(a) GDPR, consisting in the Company's failure to respond to the request of the Complainant's representative to the address from which this request originated.

In addition, the PUODO, acting on the basis of Article 58(2)(d) GDPR, orders the Company to orders the Company to bring its processing operations into compliance with the provisions of Art. 12 (1),(2),(4),(6) GDPR, by providing information to the Complainant's representative in connection with the request to delete the Complainant's personal data and notifying the PUODO within 30 days of delivery of this decision on its implementation.

Secondly, 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).

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.**

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

██████████ 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] 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.

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. 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.).

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.

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.

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 those factual and legal circumstances, the PUODO ruled as in the operative part.

Under the authority of the President
of the Personal Data Protection Office
Head of the Cross-border Proceedings Unit
International Cooperation Department

██████████

INSTRUCTIONS

In accordance with Article 60(9) GDPR, where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

The decision adopted by the PUODO as the lead supervisory authority therefore concerns the part concerning actions in relation to the Company, i.e.:

- 1. ordering the Company to bring processing operation into compliance with Article 12 (1),(2), (4) and (6) of the GDPR, by providing the Complainant with information in connection with the request to delete the Complainant's data pursuant to Article 17 of the GDPR;*
- 2. issuing a reprimand to the Company for violation of Article 12 (1),(2), (4) and (6) GDPR in connection with Article 5(1)(a) GDPR, consisting in the failure to respond to the request for deletion of the Complainant's personal data pursuant to Article 17 of the GDPR.*

In the above-mentioned scope, pursuant to Article 7(2) of the Act of 10 May 2018 on the protection of personal data (Journal of Laws 2019, item 1781) in conjunction with Articles 13(2), 53(1) and 54 of the Proceedings before Administrative Courts Act of 30 August 2002 (Journal of Laws 2024, item 935), a party dissatisfied with this decision shall have the right to lodge a complaint with the Voivodship Administrative Court in Warsaw within 30 days from the date of service on that party. The complaint is submitted via the President of the Personal Data Protection Office (address: Personal Data Protection Office, ul. Moniuszki 1A, 00-014 Warsaw). The entry for the complaint is 200 zlotys. A party has the right to apply for exemption from court costs or the right to assistance.

For the remainder of the case, i.e. part concerning dismissal of the complaint, the final decision on the case will be adopted by the Estonian Supervisory Authority (Andmekaitse Inspektsioon, seat: Tatari tn 39 / 10134 Tallinn, Estonia) as the authority with which the complaint was lodged. An appeal against this part of the case shall be lodged in accordance with the relevant provisions of Estonian law.