TRANSLATION

PRESIDENT
OF THE PERSONAL DATA
PROTECTION OFFICE
Mirosław Wróblewski

Warsaw, 19.12.2025

DS.523.746.2024.[redacted]

DECISION

Pursuant to Article 105(1) of the Code of Administrative Procedure of 14 June 1960 (Dz. Journal of Laws 2024, item 572) and Art. 60(6)(9) 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 (General Data Protection Regulation) (OJ EU L 119, 2016, p. 1, as amended), following the administrative procedure concerning [redacted] complaint (address: [redacted]) concerning irregularities in the processing of the Complainant's personal data by [redacted] (registered office: [redacted]) by unlawfully processing the Complainant's personal data, including his e-mail address for marketing purposes, making the Complainant's personal data available to unauthorised entities and failing to comply with the information obligation towards the Complainant, President of the Personal Data Protection Office

discontinues the proceedings.

JUSTIFICATION

The Personal Data Protection Office received a complaint from [redacted] (address: [redacted] (hereinafter: Complainant) concerning the processing of his personal data by [redacted] (registered office: [redacted]) (hereinafter: The Company) consisting in the unlawful processing of the Complainant's personal data, including his e-mail address for marketing purposes, making the Complainant's personal data available to unauthorized entities and failing to comply with the information obligation towards the Complainant.

In the complaint, the Complainant indicated that on 2 June 2017 he received a marketing e-mail from [redacted] to his email address [redacted], even though [redacted] was unknown to him and never had any relationship with him. The Complainant stressed that he did not consent either to the processing of his personal data or to receiving marketing content.

The Complainant indicated that on 4 June 2017 he asked [redacted] about the reason for using his e-mail-address and informed that he did not have an account with [redacted] and treated the message as spam. In its reply of 5 June 2017, the Company assured that the Complainant would not receive newsletters. The Complainant was convinced that his data had been erased from that date.

Subsequently, the Complainant stated that, on 1 February 2024, after purchasing an additional service from the long-standing antivirus software provider [redacted], a scan of historical data was carried out in order to determine the sources of unauthorised access to his personal data. As a result of this scan, a data leak from the Company of 22 April 2019 was identified. In the Complainant's opinion, this confirms that, despite the Company's assurances, his data was still stored and processed until at least 2019, without a legal basis and without his consent.

The complainant argued that the consequence of the leak is a prolonged exposure to malicious e-mails-addressed to his e-mail address. The complainant indicated that, as of 25 May 2019, he receives an average of 36 messages per day containing potential threats, including attempts to extort data and funds and content that could compromise the security of the IT system. According to the calculations presented, in the period of 912 days he received a total of 68 832 such messages, and the time spent on blocking, reporting and filtering them amounted to 286 hours, which, at the Complainant's average work rate of PLN 187 per hour, gives a total cost of PLN 53 482. The complainant pointed out that the e-mail-box was his main working tool and that the described activities were a significant and long-lasting nuisance for him.

In the Complainant's opinion, the Company, as the controller of personal data, was obliged to ensure the security of processing and transparency in the scope of information obligations. The complainant indicated that in his February 2024 correspondence to [redacted], he was not given the opportunity to lodge a complaint with the Data Protection Officer, and the employees informed that there was no account assigned to his e-mail-address in the system. According to the Complainant, this does not preclude a finding that the Company acquired, processed, did not delete and subsequently allowed the disclosure of its data to third parties.

The Complainant referred to the provisions 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 (General Data Protection Regulation) (OJ EU L 119, 2016, p. 1, as amended) (hereinafter: GDPR) in particular recital 40, according to which the processing of data should be based on the consent of the data subject or on another legal basis, Article 13(1)(d) GDPR, which imposes an obligation to inform the data subject about legitimate interests, if they constitute the basis for processing, as well as on Art.17(1) GDPR,

guaranteeing the right to erasure (‘right to be forgotten’). The complainant stressed that he never received from the controller the information required by Article 13 of the GDPR, he did not consent to the processing of his data, and yet his data was processed and they were not provided with adequate security, which results from the disclosure of data by the Company on 22 April 2019.

In connection with the above, the Complainant asked the President of the Personal Data Protection Office to verify the legality of the processing of his personal data by the Company, including determining the legal basis for their acquisition, the scope and period of processing and the source of the data, to order the immediate deletion of all his data and to cease further processing without a legal basis, as well as to oblige the controller to fully implement the information obligations and provide effective contact channels, including data of the Data Protection Officer. The complainant also requested that the information on the leak of 22 April 2019 be taken into account in the assessment of the breach and that he be informed of the outcome of the proceedings, including the determined data of the Company’s controller and Data Protection Officer.

In the course of the administrative proceedings, the President of the Personal Data Protection Office established the following facts:

1) On 4 June 2017, the Complainant asked [redacted] for the reason for using his email address and stated that he did not have an account with [redacted] and treated the message as spam. In its reply of 5 June 2017, the Company assured that the Complainant would not receive newsletters. (evidence: Complainant’s letter of 5 February 2024)
2) On 1 February 2024, through an additional service provided by the long-standing antivirus software provider [redacted], the Complainant conducted a scan of historical data in order to establish the sources of unauthorised access to his personal data. As a result of this scan, he identified a data leak from the Company on 22 April 2019 (evidence: Complainant’s letter of 5 February 2024)
3) On 1 February 2024, the Complainant sent an e-mail to the Company to [redacted], under which he informed the Company of the identified leak and submitted to the Company a proposal for a settlement regarding the payment by the Company to the Complainant of compensation in the amount of PLN 25,000 in exchange for failure to submit a complaint to the President of the Personal Data Protection Office and to process a claim for compensation. At the same time, the Complainant requested confirmation that no personal data of the Complainant are currently processed by the Company and that these data have been deleted. In further correspondence of 2 February 2024, the Complainant requested to be contacted by the Company’s Personal Data Officer (evidence: Complainant’s letter of 5 February 2024)
4) In its correspondence of 5 February 2024, the Company confirmed that there is no account linked to the Complainant’s email address [redacted] in the database (evidence: Complainant’s letter of 5 February 2024)

5) The President of the Personal Data Protection Office identified the case as being of a cross-border nature in accordance with Article 4(23) of the GDPR. Accordingly, the case was referred through the IMI Internal Market Information System (hereinafter: IMI) to the French Supervisory Authority (Commission nationale de l'informatique et des libertés (hereinafter: CNIL) to be considered as lead supervisory authority in accordance with Art. 56(1) GDPR (evidence: letter of 16 February 2024 from the President of the Personal Data Protection Office)
6) On 26 March 2024, the President of the Personal Data Protection Office informed the Complainant that the CNIL had recognised itself as the lead supervisory authority pursuant to Article 56(1) GDPR (evidence: letter of 12 March 2024 from the President of the Personal Data Protection Office)
7) On 7 October 2024, notification No 60IC 691401 was received via the Internal Market Information System (IMI), under which the CNIL submitted a 'State of Play' document, providing updated information on the conduct vis-à-vis the Company. In that document, the CNIL stated that, on 8 November 2022, the Company had stated that a file containing, according to its reseller, the email addresses of more than 200 million users of its services was intended for sale on the 'Breached' pirate forum. This security incident was reported in the press on 2 January 2023 and reported to users. Subsequently, a number of complaints were lodged with the CNIL and the Irish, German, Spanish, Norwegian and Polish supervisory authorities concerning that infringement. (evidence: Memo of 10 October 2024)
8) In the 'State of play' document concerning the Complainant's complaint, the CNIL stated that the Complainant had indicated that it had received unsolicited marketing correspondence from the Company on 2 June 2017. Subsequently, the Complainant stated that his antivirus software had signalled that his data had been the subject of a data breach incident. The activities carried out by the CNIL based on the verification of the Company's databases confirmed that the Complainant's data had been deleted by the data controller as of March 2024. Consequently, the Company no longer had the Complainant's contact details and was therefore unable to provide him with information relating to the data breach. It is therefore apparent from those findings that, once the data had been deleted, it was not possible for the Company to inform the Complainant directly of the leak. (evidence: Memo of 10 October 2024)
9) On 2 April 2025, the CNIL sent the President of the Personal Data Protection Office a draft decision on the case under the IMI system in notification 60DD number 755437. In its draft decision, the CNIL stated, first of all, that the CNIL had carried out an investigation on 25 April 2023 at the Company's registered office and, on 26 April 2023, an online inspection of the website available at the URL [redacted]. The purpose of these investigations was to verify the compliance of the processing carried out by the Company with the provisions of the GDPR. In particular, the purpose of those investigations was to address complaints submitted to the CNIL and its European counterparts regarding the data breach that

led to the online availability of the data of the users of the Company's service in November 2022.

The company informed the CNIL that it had established, on 8 November 2022, a file containing, according to its reseller, the email addresses of more than 257.8 million users of the Company's services that were on sale on the [redacted]. The CNIL noted that the file offered for sale on the [redacted] website contained user names, surnames, first names, email addresses, gender, dates of birth, cities and country of residence.

The investigation carried out by the Company indicates that one of its former subcontractors, [redacted], was responsible for this infringement. Under Israeli law, this company operated commercially under the name [redacted] and acted on behalf of the Company's user groups for the purpose of commercial segmentation.

On 10 November 2022, the Company notified the CNIL of a data protection breach. In addition, on 31 January 2023, the Company started sending data breach emails to all persons registered before 1 July 2019 residing in the territory of the European Union whose email address it still had.

Following the investigation, the CNIL found that the Company had infringed: Article 5(1)(c) GDPR – the Company has provided its processor [redacted] with personal data that were not necessary for the processing; Article 5(1)(e) GDPR – the Company indicated that it deactivates user accounts at their request or after three years from the date of the last action, whereby the CNIL has determined that personal data from deactivated accounts are still in the Company's databases, but do not serve a specific purpose; Articles 12 and 13 of the GDPR – the Company has not provided complete information to data subjects regarding the retention periods of personal data; Article 15 of the GDPR, by failing to provide information on requests for access to the data of two complainants; Article 12(3) of the GDPR, by infringing the time-limit for replying to the applicants' requests; Article 12(4) GDPR – by failing to respond to a request for access to the data of the complainant's representative; Article 32 GDPR – by violating data security; Article L.34-5 of the French Postal and Electronic Communications Code.

As part of the draft decision, the CNIL proposed to exercise the following corrective powers in respect of the Company. First, a reminder in accordance with the provisions of Art. 20(2) of the French Law of 6 January 1978 for infringement: (i) the obligation to process data that are adequate, relevant and limited to what is necessary for the purposes for which they are processed; (ii) the obligation to reply to data subjects within one month of their request, in accordance with Art.12(3) GDPR; (iii) the obligation to respond to a request for access made by a data subject's representative in accordance with Art.12(4) GDPR; (iv) the obligation to respond to the applicants' request for access, in accordance with Article 15 of the GDPR. Secondly, an order to adapt the processing operations, in accordance with the provisions of Article 20.II of the French Law of 6 January 1978, within three (3)

months of notification of this Decision and subject to the measures which the Company may have already taken, by: (i) defining and implementing retention periods for personal data processed that are proportionate to the purposes for which they are processed, in particular by deleting data that are no longer relevant; (ii) defining and implementing a password complexity policy for the user accounts of the website [redacted], which is sufficiently robust to ensure the security of those accounts in accordance with the provisions of Article 32 of the GDPR; (iii) supplement the privacy policy of the Company's website, available on the website [redacted], in order to provide, in accordance with the provisions of Articles 12 and 13 of the GDPR, complete, concise, transparent, intelligible and easily accessible information to data subjects, in particular with regard to data retained for the purpose of pursuing claims; (iv) to allow data subjects, in accordance with the provisions of Article L34-5 of the French Law of 6 January 1978, to object to receiving commercial surveys by electronic means at the time of collection of their personal data. (evidence: Memo of 17.04.2025)

10) As part of the draft decision, the CNIL also indicated that, inter alia, with regard to [redacted] complaint (complaint No 24003302 6), the Company had responded to the request within a period exceeding the time limit referred to in Article 12(3) GDPR. On 17 April 2025, the President of the Personal Data Protection Office, acting through IMI, sent a letter to the CNIL containing comments on the draft decision and asking for it to be supplemented and clarified. In the opinion of the President of the Personal Data Protection Office, the draft decision did not comprehensively address the Complainant’s allegation regarding the collection of his personal data without his knowledge and consent, as well as their subsequent storage and processing by the data controller. The President of the Personal Data Protection Office stressed that both in the complaint and in the Complainant’s supplementary letter he unequivocally pointed to the lack of a legal basis for the processing of his data, indicating that, despite the confirmation by the controller in June 2017 of the deletion of the data, in 2019 they were still stored and processed. In the light of the above, the President of the Personal Data Protection Office requested that the allegation be clearly identified and its substantive resolution as well as an indication of the specific time-limited deficiencies found in the course of the proceedings, as it does not follow from the evidence that the Company infringed Article 12(3) of the GDPR when responding to the Complainant's correspondence. In addition, the President of the Personal Data Protection Office challenged the legal basis adopted in the draft decision. The CNIL referred to Article 60(9) of the GDPR as the legal basis, while in the situation of exercising corrective powers against the data controller, Article 60(7) of GDPR. Therefore, the President of the Personal Data Protection Office asked for clarification of the reasons for the reference to Article 60(9)of GDPR. (evidence: IMI Notification No 755437.1 and Memo of 17 April 2025)

11) In response to a letter from the President of the Personal Data Protection Office sent to the CNIL by means of IMI notification No 755437, on 25 April 2025, the

French supervisory authority indicated as part of the same notification: *The complainant claims that, on 2 June 2017, he received unsolicited marketing correspondence from* [redacted] *and indicated that he did not have a* [redacted] *account, with the result that his personal data were processed without a legal basis. In addition, he declares that he received confirmation of the deletion of his data by* [redacted] *in 2017, but despite this, his data was still stored by the data controller, as on 4 February 2024 he received a notification from his antivirus software provider that his data was in a data leak. First, the investigation team formally confirmed that the complainant's data were no longer included in the* [redacted] *database, as they had been deleted by the data controller before the complainant lodged its complaint in 2024. Therefore, the team was not able to determine the source of the data and, consequently, could not decide whether the complainant's allegations concerning the processing of his data without a legal basis were well founded. In the absence of the possibility for the investigation team to substantiate these allegations and thus the absence of an infringement subject to corrective measures, we do not take them into account in this Decision. As regards the subsequent storage and processing of the data by the controller, it is apparent from the correspondence between the applicant and the controller that the applicant did not submit a formal request for erasure in 2017 and that the company merely confirmed that it would no longer receive marketing communications. Therefore, the company considered that the complainant had objected to receiving marketing communications and not to requesting the deletion of data, as the complainant claims. His data was probably stored in accordance with the retention periods in force at* [redacted]*, which corresponds to the date on which the data processed by* [redacted] *was leaked. Consequently, the French investigating authority did not find an infringement on the basis of the material collected. Secondly, as the Polish authority pointed out in its commentary, the draft decision erroneously refers to the breach of the deadline for replying to the complainant's request. This point will be corrected in the final decision. Finally, as regards the requests made by the applicant in 2024, the procedure showed that the data controller had provided several answers to the applicant, in particular with a view to identifying him for the purposes of dealing with requests, mainly relating to a claim for damages. The company replied on 5 February 2024 that no account was linked to the complainant's email address. The investigation team confirmed in the* [redacted] *database that no data is linked to the complainant's email address, in line with the data controller's reply. In the light of the foregoing, the French investigating authority did not find an infringement on the basis of the pleas put forward by the applicant*. (evidence: Memo of 30.04.2025)

12) On 28 May 2025, the President of the Personal Data Protection Office received the final decision as part of notification A60FD 777020 prepared by the CNIL. As part of the final decision, the CNIL upheld the decision set out in draft decision 60DD No 755437 and took into account the comments of the President of the Personal Data Protection Office in so far as there was no breach of the deadline for replying to the Complainant's request referred to in Article 12(3) of the GDPR by removing this

finding from the content of the final decision. In the context of notification A60FD 777020, the CNIL stated that the complainants' supervisory authorities could inform the complainants of the outcome of the investigation, the nature of the infringements found and the type of decision taken; However, a copy of the decision cannot be sent to the complainants in its current form, as it is a non-public decision. (evidence: Memo of 30 May 2025)

After examining all the evidence gathered in the case, the President of the Personal Data Protection Office considered as follows:

In accordance with Article 56(1) of the GDPR, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60. Pursuant to Article 60(3) of the GDPR, the lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views. . In accordance with Article 60(6) of the GDPR where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

In accordance with Article 60(7) of the GDPR the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision. However, pursuant to Article 60(8) of the GDPR, by derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof. .

The above-mentioned provisions have been analyzed by the European Data Protection Board (hereinafter: the EDPB), which states in paragraph 225 of Guidelines 02/2022 on the application of Article 60 GDPR, "Thus, a decision dismissing or rejecting a complaint (or parts of it) should be construed as a situation where the LSA has found, in handling the complaint, that there is no cause of action regarding the complainant's claim, and no action is taken in relation to the controller. In such case, the complaint has to be dismissed or rejected via the decision adopted by the complaint receiving SA, as the case may be."

EDPB in the above mentioned guidelines further states in point 238 that "The CSA, when issuing a decision, must give full effect to the draft decision, which is binding

on LSA and other CSAs under Article 60(6) and/or the EDPB binding decision following Article 65(1)(a).”

On the basis of Art. 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 EDPB further clarifies in Guidelines 02/2022 the function and timing of the application of Article 60 para. 9 GDPR, indicating that: ‘Article 60(9) is mainly a procedural step of the Article 60 procedure, which applies once the involved SAs have agreed on, and are bound by, a draft decision that contains both parts that were acted upon, and parts that were rejected/dismissed.” In addition, the EDPB underlines the practical effect of this step of the procedure: “In practice, this means that, at this point of the procedure, the decision on partial dismissal/rejection will have already been taken, and the parts in the draft decision that relate to the dismissal/rejection and those that refer to further action by the LSA have been clearly marked in the draft decision. SAs now only need to formalise it through the necessary adoption procedures described in Article 60(9)”

The CNIL, acting as the lead supervisory authority pursuant to Art. 56(1) GDPR, submitted on 2 April 2025 on the basis of Art. 60(3) GDPR draft decision as part of notification 60DD with the number 755437.1, indicating that the draft decision is issued in accordance with Art. 60(9) of GDPR. The President of the Personal Data Protection Office did not express a reasoned and relevant objection to it. Having regard to the content of Art. 60(6) GDPR means that the President of the Personal Data Protection Office has agreed with the CNIL on the draft decision and is bound by it.

The CNIL’s application of Article 60(9) of the GDPR in the draft decision in this case stems from the fact that the draft decision includes determinations relating to all relevant complaints transmitted by the supervisory authorities of multiple Member States, including the Complainant’s complaint at issue. In the draft decision, the CNIL took action against the Company in relation to some of those complaints and some of the allegations raised therein, while proposing to dismiss the remaining complaints and the remaining allegations arising therefrom. Consequently—pursuant to Article 60(9) of the GDPR—the lead supervisory authority adopts a decision with respect to the part concerning action taken against the controller, whereas the supervisory authorities of the complainants adopt separate decisions with respect to the parts concerning the dismissal of complaints or parts thereof, serve them on the complainants, and inform the controller thereof,

while at the same time giving full effect to the draft decision agreed in accordance with Article 60(6) of the GDPR.

This is confirmed by the explanation provided by the CNIL, according to which: "With regard specifically to the selection for this case of Article 60(9), the latter results from the fact that the outcomes of our investigations contain both parts of the complaints that were acted upon, and parts for which no breach has been identified by our investigation department." As is apparent from the evidence gathered in the case, the CNIL found an infringement and decided to take action, i.e. to apply corrective powers to the Company in respect of the identified disclosure of the complainants' personal data in the Company, including the Complainant's personal data. The substance of the CNIL's decision as regards the infringements identified in the course of the proceedings, including the infringement consisting in the disclosure of the complainants' personal data, is set out in point 9 of the factual background of this decision. However, with regard to the part of the Complainant's complaint alleging the processing of the Complainant's data without a legal basis including the processing of the Complainant's email address for marketing purposes and the failure to fulfil the information obligation towards the Complainant the CNIL found no infringement concerning the Complainant's data.

The GDPR lays down the obligations of the Controller, which include the processing of personal data under the conditions laid down in that regulation. In accordance with the principle of objective truth, as expressed in Article 7 of the Code of Administrative Procedure, in the course of proceedings, public administration bodies shall uphold the rule of law and take all necessary steps to clarify the facts accurately and to settle the matter, having regard to the public interest and the legitimate interest of citizens. This is ensured in particular by the guarantees contained in the rules governing the taking of evidence. The Supreme Administrative Court in its judgment of 26 October 1984 (ref. II SA 1205/84, ONSA 1984, No 2, item 98) has ruled: 'It follows from Articles 7 and 77(1) of the Code of Administrative Procedure that it is for the authority conducting the administrative procedure to conduct a comprehensive examination and examination of all evidence. This does not mean that a party is exempt from complicity in the fulfilment of that obligation, especially since failure to prove a specific fact may lead to results unfavourable to the party.' Having exhausted the possibility of making the necessary findings of fact, the authority conducting the proceedings is entitled, or even obliged, to adopt a version of events that logically corresponds to the remaining evidence.

As regards the allegation that the Complainant's data were processed without a legal basis, including the processing of the Complainant's email address for marketing purposes and failure to comply with the Complainant's obligation to provide information, it should be noted that the evidence gathered in the present case did not unequivocally confirm that the Complainant's data had been infringed. The Complainant claimed that he had received unsolicited marketing materials from the Company on 2 June 2017, despite the fact that he did not have an account on

that website and that his personal data were to be processed without a legal basis. The complainant also claimed that he had obtained confirmation of the deletion of his data by the Company in 2017, however, his data would still be stored by the controller, as evidenced by the communication from the antivirus software provider of 4 February 2024 informing about the data leak. In the course of the proceedings, the CNIL investigation team formally confirmed that the Complainant's data were no longer in the Company's database, as they had been deleted by the Controller before the Complainant lodged its complaint in 2024. Therefore, it was not possible to determine the source of the data and thus verify whether the Complainant's allegations regarding the processing of his data without a legal basis were well founded. Nor did the Complainant provide evidence that the Controller had breached its obligation to provide information. In addition, it follows from the findings made during the proceedings that the Complainant did not submit a formal request for deletion of data in 2017, and the Company only confirmed the cessation of sending marketing communications, treating the Complainant's notification as an objection to receiving commercial information, and not a request to delete data. The Complainant's data were therefore stored in accordance with the retention periods in force at the Company, which corresponds to the date on which the data was leaked at the Company.

In the light of the above, there are no grounds to consider that, in the present case, the Company processed the Complainant's personal data, including the Complainant's email address for marketing purposes without a legal basis, and that it infringed its obligation to provide information to the Complainant.

It is necessary to share the view indicated in the doctrine that the following quotes: 'the devoid of purpose of the administrative procedure provided for in Article 105(1) of the Code of Administrative Procedure means that one of the elements of the substantive legal relationship is missing and, therefore, a decision dealing with the case cannot be adopted by ruling on the merits of the case. The condition of discontinuance of proceedings may exist even before the initiation of proceedings, which will be disclosed only in the pending proceedings, and it may also arise during the proceedings, i.e. in a case already pending before an administrative authority.' (B. Adamiak, J. Borkowski, Code of Administrative Procedure. Commentary, C.H.Beck, Warsaw 2006, p. 489). The determination by a public authority of the existence of the condition referred to in Article 105(1) of the Code of Administrative Procedure obliges it, as is emphasised in legal literature, to discontinue the proceedings, since there are no grounds for resolving the case on the merits in the event of that condition, and the continuation of the proceedings in such a case would constitute its defectiveness, having a significant impact on the outcome of the case. The devoid of purpose of proceedings may also be the result of a change in the facts of the case, because according to the wording of Article 105(1) of the Code, when proceedings have become devoid of purpose in whole or in part for any reason, the public administration authority issues a decision to discontinue proceedings in whole or in part, respectively. As indicated by the

Voivodeship Administrative Court in Warsaw, cited above: 'the devoid of purpose of the administrative procedure is the absence of the subject-matter of the procedure. This subject is a specific case in which a state administration body is competent and, at the same time, obliged to decide on the basis of substantive law on the rights or obligations of an individual entity' (rulling of 5 October 2017, ref. VI SA/Wa 1093/17). In addition, the position expressed by the Wojewódzki Sąd Administracyjny w Łodzi (Regional Administrative Court, Łódź) of 29 May 2019 in case II SA/Łd 202/19, in which that court indicated that (quoted) 'the devoid of purpose of proceedings may result from the existence of a subjective condition or a subjective condition in the proceedings conducted. In particular, if, in the legal sense, the subject-matter of the proceedings is missing, it can be said that there is no subject-matter condition for a substantive decision. The same applies where there is no subjective condition, that is to say, where there is no party to the proceedings having an interest in obtaining a decision.' In the present case, and in line with the view expressed in the court judgment cited above, it must be held that there is a condition that the proceedings be devoid of purpose and that the proceedings be discontinued on the basis of Article 105(1) of the Code of Administrative Procedure. The assessment carried out by the President of the Personal Data Protection Office in each case serves to examine whether it is justified to address to a given entity an order corresponding to Article 58(2) of GDPR, aimed at restoring compliance with the law in the course of data processing. Therefore, such an assessment is justified and necessary only to the extent that the contested personal data processing has occurred. In these factual and legal circumstances, the President of the Personal Data Protection Office decided as set out 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
[redacted]

The decision is final. On the basis of 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 Article 13(2), Article 53(1) and Article 54 of the Act of 30 August 2002 - Proceedings before Administrative Courts (Journal of Laws 2024, item 935, as amended), a party dissatisfied with this decision has the right to lodge a complaint with the Voivodship Administrative Court in Warsaw within 30 days from the date of its delivery to the party. The complaint is submitted via the President of the Personal Data Protection Office (address: Personal Data Protection Office, ul. Stanisława Moniuszki 1a, 00-014 Warsaw). The entry from the complaint is 200 PLN. A party has the right to apply for exemption from court costs or the right to assistance.