

**PRESIDENT OF THE
PERSONAL DATA
PROTECTION OFFICE**

Mirosław Wróblewski

Warsaw, 28.04.2026

DS.523.7039.2024. [REDACTED]

DECISION

Pursuant to Article 105(1) of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2024, item 572), Article 60(8) of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 2016 No. 119, p. 1, as amended) (hereinafter: GDPR), following the administrative proceedings regarding the complaint filed by [REDACTED] (residing at [REDACTED] [REDACTED]) regarding irregularities in the processing of personal data by [REDACTED] (registered office: [REDACTED]) consisting in the disclosure of personal data contained in the Complainant's ID card, including her first name, last name, and residential address, to an unauthorized third party, the President of the Personal Data Protection Office

discontinues the proceedings

JUSTIFICATION

The Personal Data Protection Office received a complaint from [REDACTED] (residing at [REDACTED]) (hereinafter: the Complainant) regarding irregularities in the processing of her personal data by [REDACTED] (registered office: [REDACTED] [REDACTED]) (hereinafter: the Company) regarding the disclosure of personal data contained in the Complainant's ID card, including her first name, last name, and residential address, to an unauthorized third party.

In the complaint, the Complainant alleged that the Company disclosed her personal data to an unauthorized person and that it was used for criminal activities. The Complainant pointed to a breach of data confidentiality. Furthermore, the Complainant alleged a lack of transparency in the Company's actions following the report of the breach,

as well as a failure to take steps to restore compliance with the law and minimize the severe consequences of the breach.

In light of the foregoing, the Complainant requested that the President of the Personal Data Protection Office (hereinafter: the President of the Office) conduct an investigation into the violation of personal data protection regulations and take action against the Company to remedy the consequences of the unlawful disclosure of her personal data to an unauthorized person

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

- 1) User [REDACTED] (hereinafter: the User) sent a message to the Complainant via the Company's website stating that they possessed the Complainant's address information. The User indicated this, among other things, by using the following wording: "I received your information (...) I also have your address (...)". The User purchased a handbag from the Complainant, which was then shipped by the Complainant to the User as part of the transaction concluded via the Company's platform. (Evidence: Letter from the Complainant received by the the Office on November 11, 2024.)
- 2) On November 13, 2024, the President of the Office identified the case as having a cross-border character in accordance with Article 4(23) of the GDPR. Consequently, on November 28, 2024, the case was forwarded via notification No. A56 710868. 1 via the Internal Market Information System (hereinafter: IMI) to the Lithuanian supervisory authority (State Data Protection Inspectorate of the Republic of Lithuania) (hereinafter: Lithuania SA) for the purpose of having the case taken up by that authority as the lead supervisory authority within the meaning of Article 56(1) of the GDPR. (evidence: Memo from 13.11. 2024, Letter from the President of the Office 28.11.2024).
- 3) 19.02.2026, Lithuania SA sent the President of the Office a draft decision via the IMI System in notification No. A60DD 881294.1, the content of which is summarized below:

On 6 December 2024, the State Data Protection Inspectorate (hereinafter – the Inspectorate) received a complaint filed by the applicant [REDACTED] (hereinafter – the Complainant) forwarded by the Polish Supervisory Authority (Inspectorate reg. No. 1R-7911 (2.13 Mr)) (hereinafter – the Complaint).

In the Complaint, the Complainant stated that in October 2024, [REDACTED] (hereinafter – the Company) may have unlawfully disclosed the Complainant's personal data to another user under the name of [REDACTED] (hereinafter – the User). According to the Complainant, the User blackmailed and threatened her by claiming to have her personal data (name, surname and residential address).

The Inspectorate, being competent to act as the lead supervisory authority and to prepare a draft decision on the Complaint of the Complainant (Articles 56 and 60(3) of the GDPR)

has established that:

On 26 June 2025, the Inspectorate received a reply from the Company (Inspectorate reg. No. 1R-4178 (2.13 Mr)) (hereinafter – the Reply), stating that, during the investigation, the Company found that the Complainant has sold and sent a high value handbag to the User. After receiving the product, the User submitted a claim asserting that the handbag sold by the Complainant was counterfeit.

The Company points out that the investigation has not revealed any indications of unlawful disclosure or improper processing of the Complainant's personal data, as it has not been established that the Complainant's name, surname and / or address has been made public or disclosed to the User in the course of the communication with the Company's service specialists. The Company notes that no personal data breach, as defined in Article 4(12) of the GDPR, has been established.

In its Reply, the Company explains that in a transaction that requires physical delivery of the goods, the name, surname and address of the seller (the sender) are usually indicated on the parcel label, as this information is necessary to identify the parcels and to ensure their smooth delivery / return. The Company concludes that the Complainant's name, surname and city became known to the User possibly not due to any improper actions of the Company, but due to the fact that these data were legally and reasonably indicated on the label of the parcel sent by the Complainant to the User. It is also noted that the Company is not responsible for the content of the parcel labels, including the use of personal data contained therein, and that, where personal data are processed for purposes related to the delivery of parcels, the relevant delivery service provider chosen by the user is the independent controller.

The processing of personal data is governed by the GDPR and the LLPPD . Article 4(2) of the GDPR provides that 'processing' means any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Complainant complains about the possible unlawful disclosure of her name, surname and residential address, but has not provided evidence that the Company disclosed her data to the User. The correspondence between the User and the Complainant, in which the User mentions the name, surname and city of residence of the Complainant does not in itself allow to claim that the Company disclosed these data to the User. The Reply shows that the User could have found out the Complainant's data from the information on the label of the parcel. Furthermore, the Company explained that the investigation did not reveal that the Complainant's data had been made public. In the light of the above, there are no grounds to claim that the Company has disclosed the Complainant's data to the User.

In the light of the foregoing, and in accordance with Article 31(1)(2) of the LLPPD, the Inspectorate hereby decides as follows:

To reject the Complainant's Complaint.

The supervisory authority concerned with which the Complaint was lodged (in this case, the Polish supervisory authority) takes a final decision rejecting the Complaint (Article 60(8) of the GDPR).

(Evidence: Memo from 19.03.2026)

After reviewing all the evidence gathered in the case, the President of the Personal Data Protection Office has considered the following.

Pursuant to Article 56(1) of the GDPR, the supervisory authority of the main or single establishment of the controller or processor is competent to act as the lead supervisory authority—in accordance with the procedure set out in Article 60—with respect to cross-border processing carried out by that controller or processor. Pursuant to Article 60(3) of the GDPR, the lead supervisory authority shall without delay provide the other supervisory authorities concerned with relevant information regarding the matter. It shall without delay submit the draft decision to the other supervisory authorities concerned for their opinion and take due account of their comments. Pursuant to Article 60(6) of the GDPR, if, within the time limit referred to in paragraphs 4 and 5, no other supervisory authority concerned raises objections to the draft decision submitted by the lead supervisory authority, the lead supervisory authority and the supervisory authorities concerned shall be deemed to have reached an agreement on the draft decision and shall be bound by it.

In accordance with Article 60(7) of the GDPR, the lead supervisory authority shall adopt a decision and serve it on the main or single establishment of the controller or processor, as applicable, and shall inform the other supervisory authorities concerned and the European Data Protection Board of the decision, including a summary of the facts and the reasons for the decision. The supervisory authority to which the complaint was lodged shall inform the complainant of the decision. In turn, pursuant to Article 60(8) of the GDPR, by way of exception to paragraph 7, if the complaint is dismissed or rejected, the supervisory authority to which the complaint was lodged shall adopt a decision and serve it on the complainant and inform the controller thereof.

The provisions cited above were analyzed by the European Data Protection Board (hereinafter: EDPB), which states in paragraph 225 of Guidelines 02/2022 on the application of Article 60 of the GDPR that „ 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.”

In point 238 of the aforementioned Guidelines, EROD further notes 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).”

Lithuania SA, acting as the lead supervisory authority pursuant to Article 56(1) of the GDPR, submitted a draft decision pursuant to Article 60(3) of the GDPR, in which it indicated that the draft decision is being issued in accordance with Article 60(8) of the GDPR. The President of the Office did not raise any justified objections relevant to the case. In light of Article 60(6) of the GDPR, this means that the President of the Office has reached an agreement with Lithuania SA regarding the draft decision and is bound by it.

Pursuant to Article 60(8) of the GDPR, the President of the Office, as the authority to which the complaint was lodged, is competent to issue a final decision on the matter, serve it on the Complainant, and notify the controller thereof.

When issuing an administrative decision, the President of the Office is required to decide the case based on the facts existing at the time the decision is issued. As noted in legal doctrine, “a public administration body assesses the facts of the case as they stand at the time the administrative decision is issued. This rule also applies to the assessment of the legal situation of the case, which means that a public administration body issues an administrative decision based on the legal provisions in force at the time of its issuance (...). Decision-making in administrative proceedings consists of applying the applicable law to the established facts of the administrative case. In this way, the public administration body fulfills the purpose of administrative proceedings, which is to implement the applicable legal norm in the field of administrative-legal relations when such relations so require” (Commentary on the Act of June 14, 1960, Code of Administrative Procedure, M. Jaśkowska, A. Wróbel, Lex., el/2012). At the same time, this authority shares the position expressed by the Supreme Administrative Court in its resolution of November 25, 2013 (case no. I OPS 6/13), in which the aforementioned Court stated, quote: “In administrative proceedings governed by the provisions of the Code of Administrative Procedure, the rule is that a public administration authority resolves a matter by issuing a decision that settles the matter on its merits, in accordance with the legal and factual situation as of the date of the decision.”

In its judgment of May 7, 2008, in case no. I OSK 761/07, the Supreme Administrative Court stated that “when examining [...] the lawfulness of the processing of personal data, GIODO is required to determine whether, as of the date of the decision in the case, the data of a specific entity is being processed and whether such processing is carried out in a manner consistent with the law.”

The administrative proceedings conducted by the President of the Personal Data Protection Office are intended to verify compliance of data processing with personal data protection regulations and are aimed at restoring compliance with the law by issuing an administrative decision pursuant to Article 58(2) of GDPR.

In light of the foregoing, it should be noted that, in this case, an analysis of the evidence has not demonstrated unequivocally and beyond dispute that the Company disclosed the Complainant’s personal data, as alleged in the complaint. Of decisive importance for the resolution of the case is the fact that the evidence does not indicate that the personal data contained in the Complainant’s ID card, including her first name, last

name, and residential address, were made public or disclosed to the User during communication with the Company's customer service staff or as a result of a system error.

The Company denied the allegations, pointing out that in transactions requiring physical delivery of goods, it is customary to include the sender's first name, last name, and address on the label, which means that the Complainant's data could have been obtained by the User from a source other than direct disclosure by the Company. The Complainant did not submit any evidence that would refute the Company's explanation or indicate that the disclosure of her data to the User resulted from the Company's actions.

In light of the foregoing, the authority concludes that the evidence gathered in this case does not support the facts described in the complaint. Accordingly, the proceedings in this case are hereby dismissed.

Pursuant to Article 105(1) of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2024, Item 572, as amended), hereinafter referred to as the CAP, if proceedings have become irrelevant for any reason, the administrative authority shall issue a decision to discontinue the proceedings. The subject matter of the proceedings relates to the application by a public authority of the provisions of substantive administrative law. Legal doctrine indicates that, to quote: "the lack of subject matter in administrative proceedings, as provided for in Article 105 § 1 of the kpa, means that one of the elements of the substantive legal relationship is missing, and therefore a decision resolving the matter on its merits cannot be issued. The grounds for discontinuing proceedings may exist even before the proceedings are initiated, which will only become apparent during the pending proceedings, or they may arise during the course of the proceedings, i.e., in a case already pending before the administrative authority." (B. Adamiak, J. Borkowski, Code of Administrative Procedure. Commentary, C.H. Beck, Warsaw 2006, p. 489).

As emphasized in legal doctrine and case law, a public authority's determination that the condition referred to in Article 105 § 1 of the Code of Administrative Procedure has been met obliges it to dismiss the proceedings; for once this condition is met, there are no grounds for deciding the case on its merits, and continuing the proceedings in such a case would render them defective, with a significant impact on the outcome of the case. The proceedings may also become moot as a result of a change in the factual circumstances of the case.

In light of these factual and legal circumstances, the President of the Personal Data Protection Office ruled as stated 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 Signature]

This decision is final. Pursuant to Article 7(2) of the Act of May 10, 2018, on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and in connection with Article 13(2), Article 53(1), and Article 54 of the Act of August 30, 2002, on Proceedings before Administrative Courts (Journal of Laws of 2024, item 935), the party has the right to file a complaint against this decision with the Provincial Administrative Court in Warsaw within 30 days of the date of delivery of this decision, through the President of the Personal Data Protection Office (address: Office for Personal Data Protection, ul. Stanisława Moniuszki 1A, 00-014 Warsaw). The filing fee for the complaint is 200 zlotys. The party has the right to apply for legal aid, including exemption from court costs.