

**PRESIDENT  
OF THE PERSONAL DATA  
PROTECTION OFFICE**  
*Jan Nowak*

Warsaw, 8<sup>th</sup> June 2021

**Ref. No.: ZSPR.440.1114.2019.PT.BS**  
(previous Ref. No.: ZSPR.440.1114.2019.ZS.LS)

**DECISION**

On the basis of Article 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2021, item 735) and Article 6 para. 1, Article 12 para. 3 in connection with Article 15, Article 15 para. 1 and Article 58 para. 2 letter b) and c) of the 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 (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35), after having carried administrative proceedings in the case of [REDACTED], residing at [REDACTED] in Tallinn, relating to irregularities in the processing of his personal data and failure to respond to the request for access to data, within the time limit provided for in Article 12 para. 3 of the Regulation mentioned above, by [REDACTED] with its headquarters in Warsaw at [REDACTED], the President of the Personal Data Protection Office

- 1) issues a reprimand to [REDACTED] with its headquarters in Warsaw at 1 [REDACTED] for violation of Article 6 para. 1 of the 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 (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2, and OJ EU L 74 of 04/03/2021, p. 35), for the processing of [REDACTED], residing at [REDACTED] in Tallinn, personal data in the form of information about his citizenship, date of birth, number and expiry date of his identity card without legal basis;
- 2) issues a reprimand to [REDACTED] with its headquarters in Warsaw at [REDACTED] for violation of Article 12 para. 3 in connection with Article

**15 of the 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 (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35), consisting in failure to respond to the request of [REDACTED], residing at [REDACTED] in Tallinn, within the time limit prescribed in Article 12 para. 3 of the mentioned above Regulation;**

- 3) orders [REDACTED] with its headquarters in Warsaw at [REDACTED] to grant [REDACTED], residing at [REDACTED] in Tallinn, access to the scope of his personal data which it holds.**

### **JUSTIFICATION**

The Personal Data Protection Office received a complaint from [REDACTED], residing at [REDACTED] in Tallinn, hereinafter referred to as: the Complainant, about irregularities in the processing of his personal data and the failure to respond to the request for access to data within the time limit provided for in Article 12 para. 3 of the 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 (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35), hereinafter referred to as: Regulation 2016/679, by [REDACTED] with its headquarters in Warsaw at [REDACTED], hereinafter referred to as: the Company. The complaint was provided by the Estonian supervisory authority (Andmekaitse Inspektsioon) to the President of the Personal Data Protection Office as a lead supervisory authority pursuant to Article 56 para. 1 of Regulation 2016/679, through the Internal Market Information System established by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC (OJ EU L 316 of 04/11/2012, p. 1) in connection with the Commission Implementing Decision (EU) 2018/743 of 16 May 2018 on a pilot project to implement the administrative cooperation provisions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council by means of the Internal Market Information System (OJ EU L 123 of 18/05/2018, p. 115).

The Complainant pointed out that the Company did not respond to his request for access to data, which included information on the reasons why, before boarding the aircraft operated by the

Company, he had been asked to provide additional data (apart from those collected from him in the course of booking the flight) and information on the legal basis for processing and the recipients of this data. The Complainant also requested the presentation of a list of data the Company holds about him. The Complainant did not receive a response to the request from the Company and expressed doubts as to the legality of requesting him to provide the additional data and their further processing by the Company. The Complainant demanded to oblige the Company to answer his inquiries.

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

1. On 22 August 2018, the Complainant travelled from Tallinn via Warsaw to Brussels on a flight operated by the Company.
2. At the airport in Warsaw, before boarding the plane, the Complainant was asked to provide additional information that had been collected on behalf of the authorities of the airport in Brussels. Additional information included the Complainant's data on: his citizenship, date of birth, number and expiry date of his identity card.
3. On 22 August 2018, the Complainant sent a request to the Company by an e-mail to the address [REDACTED], in which he called the Company to indicate: the legal basis for processing additional data (including data related to the travel document), despite the fact that these data they are not required in order for the Company to operate; why such information was required; whether the data has been or is to be transferred to any third party. The Complainant expressed doubts as to the legitimacy of obtaining by the Company his passenger data (API data) for intra-EU flights, although they are not required for the Company's operations. Moreover, the Complainant also demanded a catalogue of data that the Company holds about him (quoted as 'an overview of data that [REDACTED] has of me').
4. The company indicated that it did not receive the Complainant's request of 22 August 2018 for technical reasons, because (quotation): 'the e-mail box to which the e-mail was sent was subject to a closing procedure and such incidents could have occurred in exceptional cases'.
5. On 24 October 2018, the Complainant sent a message to the Company at [REDACTED], reminding the Company that he had not received a reply to his request of 22 August 2018, and asked to respond to its content.
6. The Company pointed out that the Complainant's second request (quotation) 'was not recognized due to the human factor – a former [REDACTED] associate accidentally marked the message received from the Complainant as 'request resolved' and therefore it was not sent to the appropriate organizational unit of [REDACTED]'.

7. On 27 December 2018, the Complainant submitted a complaint to the Estonian supervisory authority. In the complaint, the Complainant indicated that he had not received a reply to his request for four months and that it was still not clear (and impossible to assess) why his data had been collected and whether the Company acted lawfully in collecting and processing his data. The Complainant also pointed out that the data of the travel document were not necessary in order for the Company to operate in the territory of the European Union and the Schengen area. The Complainant attached to the complaint a copy of the electronic correspondence, which he sent to the Company on 22 August 2018 and 24 October 2018. In the content of the complaint, the Complainant also indicated that he had received an automatic reply from the Company, in which the Company pointed out that his request was being examined and informed the Complainant that it was currently dealing with more requests than usual.
8. The complaint was transferred pursuant to Article 56 para. 1 of Regulation 2016/679 to the President of the Personal Data Protection Office, who took the case as the lead supervisory authority. The supervisory authorities that joined the proceeding as the supervisory authorities concerned are the Slovak, Dutch, French, Spanish, Danish, Norwegian and Italian supervisory authorities.
9. The Company in the explanations of 21 June 2019 indicated that this additional information was transferred to the authorities of the airport in Brussels pursuant to Article 3 para. 1 and 2 of Council Directive 2004/82/EC of 29 April 2004 and pursuant to the Belgian regulations implementing the above-mentioned directive, i.e. WET van 15 mei 2006 betreffende diverse maatregelen inzake vervoer in verband met Arrêté royal du 18 juillet 2015 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers oraz Loi du 25 décembre 2016 relative au traitement des données des passagers. In the Company's opinion, the data was collected in accordance with Article 6 para. 1 of the directive mentioned above and were removed within 24 hours from the moment of their transfer and arrival of the means of transport, of which the Complainant was informed on 18 June 2019. The company also pointed out that 'after careful verification of the above-mentioned legal basis, [REDACTED] has ceased the practice of transferring personal data of passengers traveling with [REDACTED] and at present these data are not processed'.
10. The Company attached to the above-mentioned explanations a copy of the reply sent to the Complainant on 18 June 2019. In addition to the legal basis for the transfer of data to the Belgian authorities, the reply also indicated the current legal basis for the processing of his personal data, which, in the Company's opinion, is the legitimate interest of the data controller related to the performance of the contract of carriage of flights on the Tallinn (TLL) – Warsaw

(WAW) route on 21 August 2018 and on the Warsaw (WAW) – Brussels (BRU) route on 21 August 2018 for the purpose of storing them for archival (evidence) purposes or possibility of establishing and pursuing of claims or defending against potential claims arising from the performance of the contract of carriage until the claims under this contract are expired. In addition, the Company indicated what data in connection with the requirements of Article 3 para. 1-2 of Directive 2004/82/EC may be transferred to the authorities responsible for carrying out border checks at the external borders. The data includes the number and type of travel document used, nationality, full names, the date of birth, the border crossing point of entry into the territory of the Member States, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport and the initial point of embarkation. In reply, which was addressed to the Complainant, the Company did not indicate that it had ceased to provide the above-mentioned data of passengers traveling with [REDACTED]. The Company pointed out that the Complainant will obtain further information on the data processing processes on the website [REDACTED] in the tab ‘Regulation/Information about personal data processing’ ([REDACTED]).

11. On 26 June 2019, the Complainant forwarded, by e-mail, to the Personal Data Protection Office the correspondence between him and the Company conducted in the period of 18-25 June 2019. In that correspondence on 18 June 2019, the Complainant indicated that, in his opinion, the Company incorrectly identified the legal basis for the transfer of his personal data to Belgium, because the Directive 2004/82/EC allows carriers to transfer passenger data to state authorities in order to carry out checks at the external borders of the European Union (as specified in the first sentence of Article 6 para. 1 of the directive). Therefore, in the opinion of the Complainant, this directive cannot constitute a legal basis for the transfer of his personal data to Belgium, as it does not apply to intra-EU flights, i.e. flights made by the Complainant on the Tallinn-Warsaw-Brussels route. The Complainant also indicated the limited purpose of the processing permitted by the directive, which in Article 6 para. 1 is limited to data processing for the purposes of border control and the fight against illegal immigration. Moreover, the obligation to collect passenger data (API data) has been imposed on carriers for the sole purpose of combating illegal immigration from third countries, and carriers do not need this data for purposes related to their business activities. Moreover, the Complainant pointed out that the Company, referring to Belgian legal acts, also referred to Directive 2016/681, the so-called PNR Directive, since, as the Complainant identified himself, Belgian law refers to the act of 25 December 2016. The Complainant pointed out that the PNR Directive does not impose an obligation to collect API data for intra-EU flights. Their

collection is possible only when API data are part of PNR data indicated in Annex I of the PNR Directive and as indicated in Article 8 may only be collected insofar as carriers already collect this data in the course of their normal activities. The Complainant indicated that on intra-EU flights the collection of API data is not part of the carrier's normal operations. In connection with this, the Complainant pointed out that so far he had not obtained information on the legal basis for the processing of his personal data. Moreover, the Complainant requested confirmation of deletion of his personal data within 24 hours from the carriers' databases, in the event that the Company relies (although incorrectly) on the provisions of Directive 2004/82.

12. On 25 June 2019, the Complainant received a reply by e-mail from the Company, indicating that the Company had verified communications with the Member States regarding the transfer of API data and suspended the transfer of data to countries that are not entitled to receive them. Taking into account that the requirements imposed by Directive 2004/82/EC concern only the external borders of the European Union, the Company has suspended the transmission of API data to the Belgian authorities. The company indicated that the Complainant's personal data had been collected only at the request of the Belgian authorities and not for commercial purposes. The Company pointed out that Belgian law implementing the PNR Directive (Directive 2016/681) and the API Directive (2004/82/EC) indicates that air carriers for intra-EU flights departing from, to and through Belgium are obliged to provide API data and PNR if they already collect them in the normal course of their business. Due to the fact that the re-analysis of the Company confirmed that the request of the Belgian authorities exceeded the scope of the above-mentioned directive, the Company on 26 November 2018, suspended the provision of this data. The Company confirmed that the Complainant's API data has been deleted and is no longer processed by the Company.
13. In the message of 26 June 2019, redirecting the correspondence between the Complainant and the Company from the period of 18-25 June 2019 to the President of the Personal Data Protection Office and to the Estonian supervisory authority, the Complainant indicated that the Company finally admitted that it had collected excessive data about passengers, however, it only ceased to provide them to the Belgian authorities in November 2018, and that this data has been deleted.

After reviewing the entirety of the evidence collected in the case, the President of the Personal Data Protection Office considered the following.

Referring first of all to the legal basis for collecting and then transferring the Complainant's data, which were not obtained in the course of the Company's normal operations, to the Belgian

authorities, it should be stated that the Complainant's data were processed in this respect without any legal basis.

Pursuant to Article 3 para. 1 of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ EU L 261 of 06/08/2014, p. 24), hereinafter referred to as: the API Directive, it should be stated that the obligation of carriers to 'transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State', is limited to information on passengers traveling from third countries to the territory of one of the Member States. In connection with the above, indicated by the Company in response to the request of the President of the Personal Data Protection Office for explanations of 3 June 2019 and in the response addressed to the Complainant on 18 June 2019, the legal basis for the processing of the Complainant's personal data that were not obtained in the course of normal operations by the Company and their transfer to the Belgian authorities, in the form of Article 3 para. 1 and 2 of the API Directive and the provisions of Belgian law implementing it, was incorrectly indicated and could not, on 21 August 2018, constitute the legal basis for the transfer of the Complainant's data in the form of information on his citizenship, date of birth, number and expiry date of the identity card to the Belgian authorities (API data).

These data could be collected and transferred to the relevant Belgian authorities on the basis of Article 8 para. 1 of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name records (PNR) for the prevention, detection, investigation and prosecution of terrorist offenses and serious crime (OJ EU L 119 of 04/05/2016, p. 132), hereinafter referred to as: the PNR Directive, only to the extent that carriers already collected such data as part of their normal activities.

The established facts of the case show that the Company, in order to obtain these data from the Complainant, had to ask him to provide them before boarding. This means that the Company was not in possession of these data and did not obtain them in the course of its activities (e.g. in the course of booking airline tickets). The Company itself indicated in the explanations that (quotation): 'after careful verification of the above-mentioned legal basis, [REDACTED] has ceased the practice of transferring personal data of passengers traveling with [REDACTED] and at present this data is not being processed'. The Company also, in the reply addressed to the Complainant, indicated that on 26 November 2018, it suspended the disclosure of this data. The above analysis and the Company's behavior indicate that it did not have, at the time of obtaining and transmitting, the Complainant's API data, in the form of information such as about his travel document, the legal basis for processing.

It should be stated that the violation of Article 6 para. 1 of Regulation 2016/679 in this case lasted from 22 August 2018 to 23 August 2018, because on 23 August 2018, in accordance with Article 6 para. 1 of Directive 2004/82, within 24 hours from the arrival of the means of transport, the data was removed from the Company's database and from the databases of authorities responsible for border control, which delete the data, within 24 hours from the moment of transferring, unless the data is later needed to fulfill the statutory functions of the bodies responsible for carrying out checks on persons at the external borders (...). It should be noted, however, that from the facts of the case it follows that from at least 22 August 2018 to 26 November 2018, i.e. for at least 3 months, it collected and transferred the data of passengers traveling on intra-EU routes from, to and through the territory Belgium to the Belgian authorities without a legal basis.

However, the legal status was finally restored by the Company with the removal of the Complainant's API data from the Company's databases and with the cessation of collecting and transferring API data of other passengers of intra-EU flights offered by the Company to unauthorized authorities.

Referring to the date of the exercise of the right to access the Complainant's data, it should be noted that the original request of the Complainant was sent to the Company on 22 August 2018 to the e-mail address [REDACTED], then a reminder message was sent to the Company on 24 October 2018. The Complainant received a partial reply to his request only on 25 June 2019, because it was only in this message that the Company responded to his request regarding the legal basis for collecting and transferring his data in the form of, inter alia, information about his travel document and indicated that it did not have a legal basis for transmitting these data to the Belgian authorities. However, the Company has not yet complied with his request regarding the right to access the data, which he is entitled to pursuant to Article 15 para. 1 of Regulation 2016/679.

Pursuant to Article 12 para. 3 of Regulation 2016/679 '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, however, the Company should have informed the Complainant about such an extension within one month of receiving his request, stating the reasons for the delay. While the Company itself indicated that the first e-mail of the Complainant addressed to the e-mail address [REDACTED] on 22 August 2018 was never received by the Company, because 'the e-mail message to which the e-mail was sent , was subject to the closing procedure (...)', the Complainant in the content of the complaint indicated that he had received an automatic reply from the Company, in which the Company indicated that his



request was being examined and informed the Complainant that it was currently dealing with more requests than usual.

The e-mail of 24 October 2018 sent by the Complainant to the same e-mail address ([REDACTED]) to which his original correspondence of 22 August 2018 was sent, was, as indicated by the Company, already received by it, but his request (quotation): ‘was not recognized due to the human factor – a former [REDACTED] associate accidentally marked the message received from the Complainant as ‘report terminated’ and therefore it was not sent to the appropriate organizational unit of [REDACTED]’. The Company’s argumentation as justifying the delay in responding to the Complainant’s request should be considered incorrect, as the indicated problems resulting from the liquidation of the electronic mailbox or the behavior of one of its employees would not have occurred if the Company had trained its employees in such a way that they would be able to identify requests of data subjects and redirecting them to the relevant organizational units of the Company and if the Company implements technical measures that would enable the redirection of e-mail messages to inactive e-mail addresses in such a way that the data subjects could exercise their rights.

Moreover, it should be noted that no technical problem or human factor limits the Company’s liability for the untimely response to the Complainant’s request for access to his data. According to Article 12 para. 3 of Regulation 2016/679, the maximum deadline for the Company to respond to the Complainant’s request of 22 August 2018 was one month. The Company did not provide evidence that it informed the Complainant about the reasons for the delay and extended the deadline for replying by another two months within one month of receiving the Complainant’s request. Although the Company indicated that it never reached the Complainant’s request of 22 August 2018, it clearly indicated that it had received the Complainant’s message, sent to the same e-mail address, reminding of his case on 24 October 2018. This means that in the case of both messages (dated on 22 August 2018 and 24 October 2018), the Company exceeded the permissible time frame and would not have responded to the Complainant’s request, if the President of the Personal Data Protection Office did not intervene, calling the Company for explanations in a letter of 3 June 2019. The Company, despite the fact that it was obliged to respond within one month, did not comply with this obligation.

The assessment by the President of the Personal Data Protection Office serves in each case the legitimacy of sending an order to a specific subject corresponding to the instruction of Article 58 para. 2 letter d) of the Regulation 2016/679 to restore the lawful state in the process of data processing or the disposition of Article 58 para. 2 letter c) of the above-mentioned Regulation to meet the request of the data subject – these instructions are justified and necessary only insofar as irregularities in the processing of personal data still exist.

In this case, it was established that the collection and transmission of the Complainant's API data took place without a legal basis, while as regards continuation of processing, it should be noted that the Company restored the legal status by removing these data from its databases and by resigning from the transfer of passenger data to the Belgian authorities. However, the processing of API data of the Complainant in the period from 22 August 2018 to 23 August 2018 and the processing of API data of other passengers on intra-EU flights in the period from at least 22 August 2018 to 26 November 2018 is a violation of Article 6 para. 1 of the Regulation 2016/679, therefore the President of the Personal Data Protection Office issued a reprimand to the Company.

Referring to the Complainant's request for the Company to indicate the legal basis for the processing of additional data (including data related to the travel document), despite the fact that these data are not required for the purposes of the Company's business, the reasons for which such information was required, information if these data have been transferred or are to be transferred to any third party and to grant him access to the content of data that the Company has about him, violation of Article 12 para. 3 of Regulation 2016/679, to the extent to which the Complainant received only a partial response from the Company to the request in question, therefore the President of the Personal Data Protection Office issued a reprimand to the Company.

Referring to the failure to meet the Complainant's request to provide the list of data that the Company holds about him, it should be considered that so far the Company has not exercised in this respect his right to access the content of the data, to access which he is entitled to pursuant to Article 15 para. 1 of Regulation 2016/679. In response to the Complainant's request, the Company's response was limited to provide the address of the website [REDACTED], where the Complainant can find information on data processing by the Company. The Company, therefore, failed to comply with the Complainant's request and did not grant him access to his data. Such activity of the Company is a violation of Article 15 para. 1 of the Regulation 2016/679, therefore the President of the Personal Data Protection Office, pursuant to Article 58 para. 2 letter c) of Regulation 2016/679 ordered the Company to grant the Complainant access to his personal data in the scope of the list of data that the Company has on him.

In this factual and legal background, the President of the Personal Data Protection Office adjudicated as in the operative part of this decision.

Under the authority of the President  
of the Personal Data Protection Office

[REDACTED]

[REDACTED]

This decision is a final decision. Based on Article 7 para. 2 of the Act of 10 May 2018 on the protection of personal data (consolidated text: Dz. U. [Journal of Laws] of 2019, item 1781 as amended) and in connection with Article 13 § 2, Article 53 § 1 and Article 54 of the Act of 30 August 2002 Law on proceedings before administrative courts (consolidated text: Dz. U. [Journal of Laws] of 2019, item 2325), the party has the right to bring a complaint to the Wojewódzki Sąd Administracyjny [Voivodship Court of Administration] in Warsaw against this decision, within 30 days from the date of delivery of this decision, through the President of the Personal Data Protection Office (address: Personal Data Protection Office, Stawki 2,00-193 Warsaw). The fee for the complaint is PLN 200. The party has the right to apply for the right of assistance, including exemption from court costs.