

# THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 23

of December

2019

## DECISION

ZKE.440.46.2019

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2018, item 2096, as amended), art. 160 sec. 1 and 2 of the Personal Data Protection Act of May 10, 2018 (Journal of Laws of 2019, item 1781) and art. 12 point 2, art. 22, art. 23 sec. 1 of the Act of August 29, 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922, as amended, and of 2018, item 138), in connection with Art. 6 sec. lit. c of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (Journal EU L 119 of 04/05/2016, p. 1 and EU Official Journal L 127 of 23/05/2018, p. 2), after conducting administrative proceedings regarding the complaint of Mr. RB about the processing of his personal data by ESA (formerly E. Sp. z o.o.), President of the Personal Data Protection Office

refuses to accept the request.

## JUSTIFICATION

The President of the Personal Data Protection Office (formerly the Inspector General for Personal Data Protection) received a complaint from Mr. R. B. (hereinafter: the Complainant) about the processing of his personal data by E. S.A. (hereinafter referred to as: the Company).

In the content of the complaint, the complainant indicated that the quotation "the website publishes information about orders, which contain customer data (name and surname, address) and information about the ordered goods on its websites". In addition, "access to these pages is in no way secured or limited. They can be read by third parties. (...). The data contained on the website (including the name and address) are sent via the http protocol over the Internet without security. "

The complainant requested "immediate deletion (...) of the entire Customer account, including all data" from the website [...] (hereinafter referred to as: the website).

In the course of the administrative procedure conducted in this case, the President of the Personal Data Protection Office (hereinafter: "the President of the Personal Data Protection Office") determined the following.

1. The explanations of the Company show that it obtained the complainant's personal data during registration on the website [...] in the scope of: name, surname, e-mail address and order specification from the e-mail address: [...] in 2007 and from the address e-mail: [...] in 2014. The complainant also subscribed to the newsletter from the first address by giving additional consent and withdrew his consent on the same day.
2. From the e-mail address: [...] On [...] September 2015, the complainant purchased the product on the website of the service. The Complainant received a link to the e-mail address containing a security token, unique and appropriate for one user. After clicking on the link sent to the e-mail address, the complainant was connected to the main page of the website, entered the "Your order" tab, and was not logged in to the website. The redirect link was unencrypted.
3. On [...] December 2015, the complainant "requested to delete the entire Client's account" by sending a request to the Company's e-mail address: [...]. The account was deleted by the administrator the next day. On [...] February 2016, the Complainant lodged a complaint with the Office of the Inspector General for Personal Data, requesting "immediate deletion (...) of the entire Client's account". However, on [...] March 2016, the Complainant re-registered on the website.
4. The company explained that in connection with the implementation of the above-mentioned the order was not published on the website (or any other) of the complainant's personal data. These data were visible only to the Complainant as a person having access to the e-mail account. Currently, the complainant's personal data has been anonymised, which means that when he tries to log in to the account, he will receive a message that the account with the given e-mail address does not exist. The complainant cannot generate an email to remind the password. The company removed the Complainant's consent to send the newsletter and commercial information is no longer sent to his e-mail. A cryptographic mechanism has been implemented on user accounts through the use of an SSL certificate. When placing an order by a customer and editing it on the website, the section is secured with an encryption protocol.
5. The company explained that it is currently processing the complainant's personal data pursuant to Art. 86 § 1 of the Tax Ordinance (hereinafter referred to as: "Ordinance") in connection with Art. 70 of the Ordinance, according to which the Company, as a taxpayer, is obliged to keep tax books, store books and documents related to them until the tax liability expires, i.e. after 5 years from the end of the calendar year in which the tax payment deadline expired.

In these facts, the President of the Personal Data Protection Office considered the following.

On May 25, 2018, the provisions of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws 2019, item 1781), hereinafter referred to as "u.o.d.o.", entered into force.

Pursuant to Art. 160 sec. 1-3 of the Act, proceedings conducted by the Inspector General for Personal Data Protection, initiated and not completed before the date of entry into force of this Act, are conducted by the President of the Personal Data Protection Office on the basis of the Act, in accordance with the principles set out in the Act of June 14, 1960. Code of Administrative Procedure (Journal of Laws of 2018, item 2096, as amended), hereinafter referred to as "the Code of Administrative Procedure". At the same time, the activities performed in the proceedings initiated and not completed before the effective date of the provisions of the Act on

From May 25, 2018, also Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95 / 46 / WE (Journal of Laws UE L 119 of 04.05.2016, p. 1 as amended), hereinafter referred to as "Regulation 2016/679".

Taking into account the above, it should be stated that the present proceedings, initiated and not completed before May 25, 2018, are conducted on the basis of the Act of August 29, 1997 on the Protection of Personal Data, hereinafter referred to as: "the Act of 1997" (with regard to regulating the administrative procedure) and on the basis of Regulation 2016/679 (in the scope determining the legality of the processing of personal data). The method of conducting proceedings in cases initiated and not completed before the date of entry into force of new regulations on the protection of personal data, resulting from the provisions of law, correlates with the well-established position of the doctrine, according to which "a public administration body assesses the facts of the case according to the moment of issuing the administrative decision. This rule also applies to the assessment of the legal status of the case, which means that the public administration authority issues an administrative decision on the basis of the provisions of law in force at the time of its issuance "(Commentary to the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws No. 00.98.1071) M. Jaśkowska, A. Wróbel, Lex., EI / 2012).

In the judgment of May 7, 2008 in the case file ref. Act I OSK 761/07 The Supreme Administrative Court stated that "when examining [...] the legality of the processing of personal data, GIODO is obliged to determine whether the data of a specific entity are processed on the date of issuing the decision on the matter and whether it is done in a lawful manner" .

At the time the event described by the applicants took place, the 1997 Act was in force. The provision of fundamental importance for the assessment of the legality of the processing of personal data was Art. 23 sec. 1 of the Act of 1997, according to which the processing of personal data is lawful when the data controller meets one of the conditions listed in this article, i.e. when:

the data subject has consented to it, unless it concerns the deletion of data relating to him,

it is necessary to exercise an entitlement or fulfill an obligation resulting from a legal provision,

it is necessary for the performance of the contract when the data subject is a party to it or when it is necessary to take action before concluding the contract at the request of the data subject,

it is necessary to perform tasks specified by law for the public good,

it is necessary to fulfill legally justified purposes pursued by data controllers or data recipients, and the processing does not violate the rights and freedoms of the data subject.

It should be added that these conditions apply to all forms of data processing listed in art. 7 sec. 2 of the 1997 Act, including making them available. These conditions are also equal to each other, which means that for the legality of the data processing process, it is sufficient to meet one of them.

Currently, in the light of the provisions of Regulation 2016/679, the processing of personal data is authorized when any of the conditions listed in art. 6 sec. 1 of the Regulation 2016/679.

Referring to the legality of the processing of the Complainant's personal data by the Company in view of the necessity to perform the contract, the President of the Office for Personal Data Protection did not find any irregularities, as the processing of the Complainant's personal data was justified by the provisions of law. The legal basis which legalized the processing of the Complainant's personal data by the Company was art. 23 sec. 1 point 3 of the Act of 1997, which authorized the administrator to process personal data of a person when it is necessary to perform the contract and art. 23 sec. 1 point 1 of the Act of 1997, i.e. consent to the sending of the newsletter. The processing of the complainant's personal data is currently carried out on the basis of art. 6 (1) (a) c of Regulation 2016/679, according to which "processing is necessary to fulfill the legal obligation incumbent on the administrator". The company indicated that pursuant to Art. 86 sec. 1 of the Ordinance, the Complainant's personal data included in the sales invoice constitute an accounting document, and the company as a taxpayer is obliged to keep books and related documents until the tax liability expires, i.e. after 5 years from the end of the calendar year in which the

tax payment deadline. This period will end in 2020.

Regardless of the above, it should be noted that the proceedings conducted by the President of the Office are aimed at issuing an administrative decision pursuant to Art. 18 sec. 1 of the 1997 Act. According to this provision, in the event of a breach of the provisions on the protection of personal data, the President of the Office ex officio or at the request of the person concerned, by way of an administrative decision, orders the restoration of the legal status, in particular: 1) removal of the deficiencies, 2) supplementing, updating, rectifying, or failure to provide personal data, 3) application of additional security measures for the collected personal data, 4) suspension of the transfer of personal data to a third country, 5) data protection or transfer to other entities, 6) deletion of personal data.

In these administrative proceedings, the allegation of the publication by the Company of the Complainant's personal data on the website or other pages of the Complainant's personal data in the order information, which was to contain the customer's data (name and surname, address) and information about the ordered goods, has not been confirmed. These data were visible only to the Complainant as a person having access to the e-mail account to which a link containing a unique, security token was sent. The company explained that it had implemented a cryptographic mechanism through the use of an SSL certificate. When placing an order by a customer and editing it on the website, the section is secured with an encryption protocol. The Complainant's account was removed by the Company from the website.

Taking into account the above, it should be concluded that there was no basis for issuing a decision ordering the restoration of legal status by the President of the Personal Data Protection Office, referred to in Art. 18 of the 1997 Act. It is justified to issue a decision refusing to meet the data subject's request.

In this factual and legal state, the President of the Personal Data Protection Office resolved as in the sentence.

Based on Article. 127 § 3 of the Code of Administrative Procedure, the party has the right to submit an application for reconsideration of the case within 14 days from the date of delivery of the decision to the party. If a party does not want to exercise the right to submit an application for reconsideration of the case, he has the right to lodge a complaint against the decision with the Provincial Administrative Court in Warsaw within 30 days from the date of its delivery to the party. The complaint is lodged through the President of the Personal Data Protection Office (address: ul. Stawki 2, 00-193 Warsaw). The fee for the complaint is PLN 200. The party has the right to apply for the right to assistance, including exemption from court costs.

