THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 13

March

2020

DECISION

ZKE.440.95.2019

Based on Article. 105 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2020, item 256), art. 160 sec. 1 and 2 of the Personal Data Protection Act of May 10, 2018 (Journal of Laws of 2019, item 1781), art. 12, art. 22 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) after conducting administrative proceedings regarding the complaint of Mr. GL, for failure to provide personal data by CSA, President of the Personal Data Protection Office

discontinues the proceedings.

JUSTIFICATION

The President of the Personal Data Protection Office (formerly the Inspector General for Personal Data Protection) received a complaint from Mr. G. L. (hereinafter referred to as: the Complainant) about the failure to disclose personal data by C. S.A. (hereinafter referred to as: the Company).

The complainant requested that the Company be ordered to disclose the personal data of the ip user who, in the complainant's opinion, breached his personal rights by publishing an offensive entry about him on the website [...] in the scope of his name, surname and address details. In the further part of the application, the complainant stated that the data was necessary for him to file a civil claim and to notify about the suspicion of a crime under Art. 212 and 216 of the Criminal Code.

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 complainant, by application of [...] February 2018, requested the Company to disclose the personal data of the subscriber using the IP address: [...] in the scope of: name and surname and address details (postal code, city, street and house / flat number / premises) and PESEL number, which on [...] January 2018 at: [...] posted an offensive post about him on the website forum [...]. The complainant justified his request with the intention to bring a lawsuit to the court for the protection of

personal rights. In addition, he indicated that he intended to submit a notification of suspected crime to law enforcement authorities under Art. 212 of the Criminal Code and Art. 216 of the Criminal Code.

2. By letter of [...] February 2018, the Company refused to disclose the requested data to the Complainant, referring to Art. 159 paragraph 1 point 1 of the Telecommunications Law (Journal of Laws of 2019, item 2460), hereinafter: the Telecommunications Law, according to which the personal data of the subscriber using the IP address: [...] are covered by telecommunications confidentiality. In addition, in the above-mentioned the letter indicated that under Art. 159 paragraph 2 of the Telecommunications Law, there is a general prohibition on the processing of data covered by telecommunications confidentiality, including their disclosure, from which exceptions are provided for in Art. 159 paragraph 4 of the Telecommunications Law. Pursuant to this provision, the processing of data covered by telecommunications confidentiality is prohibited, unless disclosed by a court decision issued in criminal proceedings, by an order of the prosecutor or on the basis of separate provisions.

3. The explanations of the Company also show that it is not currently processing data related to the merger as at [...] January 2018. The company referred in the letter to Art. 180 a sec. 1 point 1 of the Telecommunications Law, according to which "an operator of a public telecommunications network and a provider of publicly available telecommunications services are obliged, at their own expense: 1) to retain and store the data referred to in Art. 180 c, generated in the telecommunications network or processed by them, on the territory of the Republic of Poland, for a period of 12 months from the date of connection or unsuccessful connection attempt, and on the date of expiry of this period, destroy these data, except for those that have been secured, in accordance with with separate provisions ".

4. The company also explained that the IP address in question is the so-called IP address with NAT, which means that in order to clearly identify the end user of such an address, information on the source port is necessary, which the Company does not have.

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 2020, item 256), 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 the 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 “the public administration body assesses the actual state 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., El / 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 outset, it should be noted that the 1997 Act was in force at the time the event described by the applicants took place. The act required that each data processing (including sharing) be carried out on a legal basis. The provision of fundamental importance for the assessment of the legality of the processing of personal data was Art. 23 sec. 1 of the 1997 Act (Article 6 (1) of Regulation 2016/679 respectively). Pursuant to the aforementioned provision, 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 concerning him (Article 6 (1) (a) of Regulation 2016/679, respectively),

it is necessary to exercise an entitlement or fulfill an obligation resulting from a legal provision (Article 6 (1) (c) of Regulation 2016/679, respectively),

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 (Article 6 (1) (b) of the Regulation 2016/679, respectively) ,

it is necessary to perform tasks specified by law for the public good (Article 6 (1) (e) of Regulation 2016/679, respectively),

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 (Article 6 (1) (f) of the Regulation 2016/679, respectively).

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 processing process. These conditions apply to all forms of data processing listed in art. 4 point 2 of Regulation 2016/679, including in particular to make 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.

In the case at hand, the assessment stated whether the telecommunications operator reasonably refused to provide its subscriber's personal data, referring to Art. 159 of the Telecommunications Law. According to the rule expressed in Art. 5 of the "Act of 1997", the provisions providing for further protection of personal data apply. The provision of art. 159 of the Telecommunications Law is a special provision in relation to the general norm contained in Art. 23 (1) of the 1997 Act, which allowed for the disclosure of personal data in the event that the complainant's need for the data was substantiated. It is worth quoting here the thesis contained in the judgment of the Provincial Administrative Court in Warsaw of October 7, 2011, II SA / Wa 364/11, LEX No. 950577 "The applicants justified their request with the intention to bring a lawsuit to the court for the protection of personal rights. Pursuant to Art. 187 in connection with joke. 126 § 2 of the Code of Civil Procedure, the claim should indicate, inter alia, the place of residence of the defendant natural persons. However, in the opinion of the Court, to credibly justify the need to have the subscriber's personal data with assigned IP [...], the mere hypothetical intention to bring a civil action against him is not enough ”. Summing up, the provision of the personal data of the ip user requested by the Complainant is inadmissible due to the qualification of this data as a telecommunications secret. The above-mentioned

provisions of the Telecommunications Law exclude the application of Art. 23 sec. 1 on the basis of "lex specialis derogat legi generali".

Referring to the Complainant's request to order the Company to disclose the end user's personal data, it should be noted that the request was not legally justified in art. 23 sec. 1 clause 5 of the Act, and currently Art. 6 lit. f of the Regulation 2016/679 and could not be taken into account by the Company. In addition, the explanations of the Company show that the user's IP address provided by the Complainant in the application is the so-called IP address with NAT, which means that to clearly identify the person who violated his personal rights, information on the source port is also necessary. NAT it is in the "Network Address Translation" expansion, that is, the conversion of network addresses allows many devices, most often connected to each other via a local network, to use one address visible on the Internet. The complainant did not provide information on the source port in the application, hence it was impossible to establish the personal data of the end-user.

At the same time, it should be noted that pursuant to Art. 180 a sec. 1 point 1 of the Telecommunications Law, "an operator of a public telecommunications network and a provider of publicly available telecommunications services shall, at their own expense: 1) retain and store the data referred to in Art. 180 c, generated in the telecommunications network or processed by them, on the territory of the Republic of Poland, for a period of 12 months from the date of connection or unsuccessful connection attempt, and on the date of expiry of this period, destroy these data, except for those that have been secured, in accordance with with separate provisions ". The company does not currently process the personal data of the IP user for disclosure requested by the Complainant, and therefore conducting proceedings against this entity is pointless. Pursuant to the provisions of Art. 105 (1) of the Code of Civil Procedure, when the proceedings for any reason become redundant in whole or in part, the public administration authority issues a decision to discontinue the proceedings, respectively, in whole or in part. The irrelevance of the proceedings means that there is no element of the material legal relationship, and therefore a decision to settle the matter cannot be issued by resolving it on its merits (B. Adamiak, J. Borkowski "Code of Administrative Procedure. Comment" 7th edition Wydawnictwo CH Beck, Warsaw 2005, p. 485). The same position was taken by the Provincial Administrative Court in Kraków in its judgment of 27 February 2008, file ref. no. III SA / Kr 762/2007): "The procedure becomes pointless when any of the elements of the material-legal relationship is missing, which means that it is impossible to settle the matter by deciding on the merits".

The determination by the public authority of the existence of the condition referred to in Art. 105 § 1 of the Code of Civil

Procedure obliges him, as it is emphasized in the doctrine and jurisprudence, to discontinue the proceedings, because then there are no grounds for resolving the matter as to the substance, and continuing the proceedings in such a case would be defective, which would have a significant impact on the result of the case.

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 entry fee for the complaint is PLN 200. The party has the right to apply for the right to assistance, including exemption from court costs.

2021-05-24