THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 01

July

2021

DECISION

DKE.523.29.2021

Based on Article. 104 § 1 and art. 105 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2018, item 2096, as amended) and pursuant to Art. 160 sec. 1 and 2 of the Act of 10 May 2018 on the protection of personal data (Journal of Laws of 2018, item 1000, as amended) in connection with joke. 12 point 2, art. 18 sec. 1 point 2) and 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 with Art. 57 sec. 1 lit. a and f in connection with joke. 58 sec. 2 lit. c of the Regulation of the European Parliament and the EU Council 2016/679 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 (Journal of Laws UE L 119 of 04/05/2016, page 1) and Journal of Laws UE L 127 of 23/05/2018, p. 1, as amended), after conducting administrative proceedings regarding the complaint of Mr. GW, represented by the attorney MM from the Law Office in W., against the website administrator [.. .] - Mr. MS, President of the Personal Data Protection Office

1. orders Mr MS to provide Mr GW, represented by the attorney MM from Kancelaria Adwokacka in W., with the personal data of the author of the article posted on the website at [...] in the scope of: the date of the article and the computer's IP address.2 . in the remaining scope, it discontinues the proceedings.

Justification

The Office of the Inspector General for Personal Data Protection (currently the Office for Personal Data Protection) received a complaint from Mr. GW (hereinafter referred to as: "Complainants"), represented by MM attorney from the Law Firm in W., against the website administrator [...] - Mr. MS hereinafter referred to as the "administrator", regarding the failure to provide the Complainant with the personal data of the author of the offensive article posted on [...] January 2017 on the website at the address entitled: [...], in terms of the date of writing this article, the computer's IP address and the port from which the article was created.

The Complainant's attorney, in the content of his application, in a more detailed letter of [...] October 2017, requested a

decision ordering the website administrator [...] to disclose the personal data of the author of the article posted on the website at the date of the article, address IP of the computer and the port from which this article was created. The plenipotentiary emphasized that as a result of the creation of the article and its publication on Facebook, the complainant, as a person holding the public position of the President of the Management Board [...] of the Housing Cooperative, was exposed to the risk of loss of trust, dignity, honor, image and good name. For this reason, the applicant decided to refer the case to civil and criminal proceedings. Currently, proceedings for the protection of personal rights and payment are pending before the District Court in G., under the reference number [...] against the person who published the offensive article on Facebook. The plenipotentiary, specifying the justification of his request, indicated that the data of the author of the article regarding the IP number of the computer and the port from which the article was created are necessary for the effective bringing of both civil and criminal claims. He explained that in order to file a lawsuit or a private indictment against the author of the article, it is necessary to establish the details of the person who wrote the article. This cannot be done against an anonymous person who would subsequently be established in a civil or criminal trial. ' He added that the proceedings are initiated by a complaint against a specific person, which requires prior identification of the perpetrator, and that any evidence may be secured by a law enforcement authority only after the complaint has been lodged, i.e. only after the identity of the author of the article has been established. Similarly, the case also applies to civil proceedings, where the formal requirement of the statement of claim is to identify the defendant.

In the course of the investigation conducted in this case, the President of the Personal Data Protection Office established the following facts:

On [...] January 2017, without the complainant's consent and knowledge, an article was published on the website [...] that, in his opinion, was against his personal rights and fulfilled the criteria of an act under Art. 212 of the Act of 6 June 1997 Penal Code (Journal of Laws of 2020, item 1444, as amended), hereinafter referred to as "the Penal Code", entitled: [...]. This article was published on Facebook on a profile belonging to [...]. The information contained in the created article was untrue, and the event indicated there was fictitious.

The regulations of using the website [...] show that this website is the so-called a news generator used to create imaginary press stories, the main characters of which may be ourselves or our friends. This is done by substituting the data for the empty spaces in the article template. The regulations prohibit using the website in bad faith and also prohibit sharing the article with

another person without their consent. Personal data is saved in article links, and messages are generated dynamically by downloading encoded data stored in the address (proof: terms of use of the website [...]). The website's privacy policy indicates that by using the form, each user may voluntarily provide the website with personal data, including first name, surname and age in years, in order to create a fictitious article using this information. This data is not saved on the server, but only processed for the purpose of encoding it in the web address of the article. The user is the sole holder of this address and is responsible for the privacy of this data. The administrator does not collect data provided by the form. However, they appear in encrypted form as part of the internet address, and these will be saved in the server logs and in the website counting tools used by the website. Server logs include the user's IP address and port, the date and time of registration, as well as information about the user's web browser and operating system. The data stored in the server logs are not associated with specific people using the Website and are not used by the administrator to identify users. The server logs are auxiliary, used to administer the website, and their content is not disclosed to anyone except those authorized to administer the server. Contact with the administrator is possible at [...] (proof: website privacy policy [...]).

In an e-mail of [...] April 2017, addressed to the administrator's e-mail address, i.e. [...], the Complainant's attorney asked for information whether it was possible to establish the computer's IP number or created the article using the website [...] (proof: e-mail of the attorney from [...] April 2017).

In response, the administrator indicated that it was possible to determine the computer's IP address, port and the date of the creation of such an article, however, so that it could provide the above-mentioned the data requires a decision of the Inspector General for Personal Data Protection in this respect and the full address of this article (proof: e-mail M. S. of [...] April 2017).

In an e-mail of [...] May 2017, the Complainant's attorney indicated that he wanted to disclose the above-mentioned personal data, therefore, proceedings will be initiated to issue a relevant decision by the Inspector General for Personal Data Protection (proof: e-mail of the attorney from [...] April 2017).

In the explanations of [...] February 2020, Mr. M. S. stated that he is the administrator of the website [...], which processes the data contained in the address of the article on the fly without saving these data on the server. The data saved are server logs that contain the date and IP address of each person creating the article. The administrator also stated that he was in possession of the date of the article in question and the IP address of the computer, but did not have data on the protocol port from which the article was created. The protocol port was not registered for the article referred to in the complaint. The

administrator informed that he had informed the Complainant's attorney that, in order to be able to provide the above-mentioned the data needs a decision of the Inspector General for the Protection of Personal Data exempting him from the obligation to protect personal data, which, due to an unclear legal interpretation, may be considered the computer's IP address. He added that after the Complainant had received the address for the offensive article, the data had been secured (evidence: explanations of [...] February 2020).

In this factual state, the President of the Personal Data Protection Office considered the following.

On May 25, 2018, with the entry into force of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), the Office of the Inspector General for Personal Data Protection became the Office of Personal Data Protection Personal Data. Proceedings conducted by the Inspector General for Personal Data Protection, initiated and not completed before May 25, 2018, are conducted by the President of the Personal Data Protection Office, pursuant to the Act of August 29, 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922, as amended) in accordance with the rules set out in the Code of Administrative Procedure (Journal of Laws of 2018, item 2096, as amended). All actions taken by the Inspector General for Personal Data Protection before May 25, 2018 remain effective (Article 160 (1) and (2) of the Act of May 10, 2018 on the protection of personal data).

On May 25, 2018, the provisions of 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 began to be applied in the national legal order and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 04/05/2016, page I and Journal of Laws of the EU 1, 127 of 02/05/2018, page 2), hereinafter: Regulation 2016/679, the provisions of which regulate issues related to the processing of personal data of natural persons. From that date, the President of the Office is obliged to apply the provisions of the above-mentioned of Regulation 2016/679 to all administrative proceedings that it conducts. When issuing a decision in a given case, the President of the Office takes into account the legal status in force at the time of issuing the decision.

At the time when the event described by the Complainant took place, the Act of August 29, 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922, as amended), hereinafter referred to as the Act, was in force. The provision of fundamental importance for the assessment of the legality of the processing of personal data was Art. 23 of the Act. Pursuant to Art. 23 sec. 1 point 5 of the Act, data processing was allowed when it was necessary to fulfill legally justified purposes

carried out by data administrators or data recipients, and the processing does not violate the rights and freedoms of the data subject.

Currently, the premise legalizing the processing of personal data is Art. 6 sec. 1 of Regulation 2016/679. Pursuant to Art. 6 sec. 1 letter f of the above-mentioned of the regulation, processing is lawful only in cases where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where these interests are overridden by the interests or fundamental rights and freedoms of the person whose data concern, requiring the protection of personal data, in particular when the data subject is a child. As demonstrated by the conducted administrative proceedings, the Complainant has grounds to obtain data as to the date of the article posted on the website at [...] and the IP address of the computer from which the article was created.

The attorney justified his complaint with the intention to take legal action against the author of the article and the necessity of the requested data from the point of view of the possibility of pursuing claims against this person in court for defamation. Pursuant to Art. 212 § 1 of the Act of June 6, 1997 of the Penal Code - whoever slanders another person, group of persons, institution, legal person or organizational unit without legal personality for such conduct or properties that may degrade it in the public opinion or expose it to the loss of trust needed for a given position, profession or type of activity, shall be subject to a fine or penalty of restriction of liberty. Pursuant to § 2 of the above-mentioned Art. 212 of the CC, if the perpetrator commits the act specified in § 1 by means of mass communication, he or she is subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year. Individualizing the author of the questioned entry is a necessary condition for pursuing a private indictment against him. According to Art. 332 § 2 point 1 of the Act of 6 June 1997 - Code of Criminal Procedure (Journal of Laws 2021, item 534, as amended), hereinafter referred to as "the Code of Criminal Procedure": "The indictment should contain: 1) the name and surname of the accused, other data about his person, data on the application of a preventive measure and property security ". Moreover, the complainant's attorney indicated that the possible regulation on the ground in which the complainant seeks legal protection and pursues his claims is the Civil Code of 23 April 1964 (Journal of Laws of 2020, item 1740, as amended), hereinafter referred to as "the Civil Code". Moreover, the applicant had already taken legal steps to exercise his rights, as he had filed a lawsuit with the District Court in G. for the protection of personal rights and payment against the person who published the offensive article on Facebook, i.e. Mr AM (ref. [...]) . According to the content of Art. 23 of the Civil Code Regardless of the protection provided for in other regulations, personal rights of a person, including

the right to privacy, remain under the protection of civil law. The provision of Art. 24 of the Civil Code guarantees the person whose personal rights has been endangered with the right to request to refrain from acting violating the personal rights, and in the event of an already committed violation of the request, that the person who committed the infringement will complete the actions necessary to remove its effects. At the same time, pursuant to Art. 448 of the Civil Code, in the event of infringement of a personal interest, the court may award an appropriate amount to the person whose interest has been infringed as compensation for the harm suffered, or, upon his request, order an appropriate amount of money for the social purpose indicated by it, regardless of other measures needed to remove the effects of the infringement. Moreover, pursuant to Art. 187 § 1 of the Act of November 17, 1964 - Code of Civil Procedure (Journal of Laws of 2020, item 1740, as amended), hereinafter referred to as the "Code of Civil Procedure", the claim should satisfy the conditions of the pleading. According to Art. 126 § 1 of the Code of Civil Procedure each pleading should therefore contain, inter alia, first and last names or names of the parties, their statutory representatives and proxies. When the pleading is the first letter in the case, it should contain the designation, inter alia, place of residence or seat and addresses of the parties or, if the party is an entrepreneur entered in the Central Register and Information on Economic Activity - correspondence address entered in the Central Register and Information on Economic Activity, or the place of residence or seat and addresses of statutory representatives and proxies pages (Article 126 § 2).

Referring to the data controller's doubts as to whether the IP address constitutes personal data, it should be stated that, pursuant to art. 4 pts 1 of Regulation 2016/679 "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be directly or indirectly identified, in particular on the basis of an identifier such as name and surname, identification number, location data, internet identifier or one or more specific physical, physiological, genetic, mental factors, the economic, cultural or social identity of a natural person.

Information that is associated with a specific person - even indirectly - carries a certain message about him. Therefore, information about a person is both information relating directly to him, and one that relates directly to objects or devices, but due to the possibility of linking these objects or devices with a specific person, it also indirectly constitutes information about himself. An IP address (Internet Protocol Address) is a unique number assigned to devices in computer networks. It is therefore information about a computer and not a specific natural person, especially when it is possible to share one IP

address by many users within a local network. Therefore, the IP address may not always be treated as personal data within the meaning of Regulation 2016/679. However, where the IP address is for a longer period of time or permanently assigned to a specific device, and the device is assigned to a specific user, it should be considered that it constitutes personal data, because it is information that allows the identification of a specific natural person [judgment of the Supreme Administrative Court of on May 19, 2011, file ref. no. I OSK 1079/10].

Considering the above, there is no doubt that the Complainant must have information identifying the person against whom he intends to bring a private bill of indictment. In a situation where the Complainant has essentially no information about the person who posted on the website [...] the article considered by the Complainant to be defamatory, except only those that resulted from their publication (i.e. apart from the date, time, content of the publication) used by this person to conceal his identity, it is reasonable to assume that the actions taken by the Complainant serve to establish the identity of that person, in order to bring him to criminal liability in relation to the content of the publication and fall within the concept of a legally justified purpose. It is obvious that the acquisition (processing) of personal data in the above-mentioned purpose, in each case, will be considered by the data subject to be contrary to his or her interests. This circumstance - especially taking into account the legal guarantees of defense against the claims of the opposing party - does not, however, prove that its rights and freedoms have been violated. Adopting the opposite position would result in unjustified protection of those who may have unlawfully interfered with the sphere of legally protected interests of another person (especially those convinced of the anonymity guaranteed by the Internet) against possible liability for their actions.

In the opinion of the President of the Personal Data Protection Office, the controller unjustifiably refused to disclose the requested data to the Complainant until an administrative decision in this matter was issued. Thus, he prevented the applicant from pursuing his rights in court. To confirm the correctness of the position presented in this case, it is worth reiterating the judgment of the Provincial Administrative Court in Warsaw of February 3, 2010 (file reference number II SA / Wa 1598/09), in which in particular the quotation was indicated: "(.. .) the right to free, anonymous expression cannot protect people who infringe the rights of others from responsibility for the words they say. Nobody is and cannot be anonymous on the web. Although it may be difficult to determine the identity of a given person, due to the fact that every computer leaves a trace on the Internet - the IP address by means of which the computer from which the alert was made can be determined, it makes it possible to indirectly establish the identity of the person who made the alert (...) a participant in the proceedings has

information about the login date, nicknames of persons performing this activity and the content of entries. In the opinion of the Court, the above information, combined with the IP numbers, makes it possible to unequivocally identify the persons who violated the personal rights of the participant in the proceedings. (...) the IP addresses requested by the participant in the proceedings constitute personal data in this case within the meaning of Art. 6 sec. 1 of the Act on the Protection of Personal Data, and ordering them to be made available constitutes the implementation of the instructions of para. 2 of this provision, i.e. it will enable the identification of a person or persons whose identity can be indirectly determined. (...) the computer's IP address alone is not enough to indicate the person who used it, but in combination with other information it allows to assume that its identity can be established. In the opinion of the Court, the identification of this person does not have to be associated with excessive costs, time or activities (...) ". Moreover, the Supreme Administrative Court in the judgment of 21 August 2013 emphasized that "(...) the person committing these violations must be aware that he cannot abuse his rights by violating the rights of others. This has nothing to do with restricting the principle of freedom of speech. The freedom to express one's views is related to taking responsibility for those views. Anyone who speaks in public, outside the Internet, is aware of the possible consequences of statements that violate the fundamental, statutorily protected rights of others. However, it is unjustified to say that someone speaking anonymously, in a way that violates the interests of other entities, is to be subject to special protection and that his personal data is a good that the legislator intended to protect in the first place ".

The circumstances of the case suggest that disclosure of the personal data of the person creating the article to the Complainant is necessary in order to file a bill of indictment with a private court pursuant to Art. 212 of the Penal Code as well as a civil lawsuit. To this end, the Complainant took a number of steps, including asking the administrator to disclose his personal data to the above-mentioned persons who, however, failed to meet the applicant's demands.

To sum up, the President of the Personal Data Protection Office is of the opinion that the controller unjustifiably refused to provide the Complain with the IP number and the publication date of the author of the article, thus preventing the Complainant from taking further actions that would allow for the effective initiation of court proceedings against this person.

In the case at hand, the administrator confirmed that he has the above-mentioned data. In addition, he made this personal data available to the supervisory body, which is the President of the Office for Personal Data Protection.

Referring the above to the circumstances of the case at hand, it should be noted that, in the opinion of the President of the Personal Data Protection Office, the Complainant's request for disclosure of the user's personal data in the scope of the date

of creating the article, the IP address of his computer and the port from which the article was created was legally justified in art. 23 sec. 1 point 5 of the Act, and is currently justified in Art. 6 lit. f of Regulation 2016/679, and as such should be taken into account by the administrator at the stage of its submission by the Complainant.

Pursuant to Art. 18 sec. 1 point 2 of the Act, in the event of violation of the provisions on the protection of personal data, the President of the Personal Data Protection Office ex officio or at the request of the person concerned, by way of an administrative decision, orders the disclosure of the requested personal data. Taking into account the circumstances of the case, the President of the Personal Data Protection Office is authorized to order the controller to disclose to the Complainant the personal data of the author of the questioned article to the extent that the entity has these data, i.e. information about the IP number of the device from which the person created the questioned article. the article and the date of writing the article. However, referring to the complainant's request for the administrator of the personal data of the author of the article to be made available to him by the administrator of the report, it should be noted that the above-mentioned the entity does not process these data, therefore the ordering by the President of the Personal Data Protection Office to disclose them should be considered as pointless. Pursuant to the provisions of Art. 105 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2021, item 735), hereinafter referred to as the CCP, when the proceedings for any reason became redundant, the administrative authority issues a decision to discontinue the proceedings. The subject of the proceedings is related to the application by the public authority of the provisions of substantive administrative law. The doctrine indicates that the quotation: "the objectivity of the administrative procedure, as provided for in Art. 105 § 1 of the Code of Civil Procedure, it means that there is no element of a material legal relationship, and therefore it is not possible to issue a decision settling the matter by resolving its substance. The prerequisite for discontinuation of the proceedings may exist before the initiation of the proceedings, which will be revealed only in the pending proceedings, and it may also 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.II. Beck, Warszawa 2006, p. 4891. Determining by the public authority the existence of the condition referred to in Art. 105 § 1 of the Code of Administrative Procedure, obliges it, as it is emphasized in the doctrine and jurisprudence, to discontinue the proceedings, because in the event of this premise there are no grounds for resolving the matter on the merits, and continuing the proceedings in such a case would constitute its defectiveness, significantly impact on the outcome 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 file an application for reconsideration of the case within 14 days from the date of its delivery to the party. The party has the right to waive the right to request a retrial. The waiver of the right to submit an application for reconsideration makes the decision final and binding. 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 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.

2021-09-10