THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 29

of August

2019

DECISION

ZSOŚS.440.38.2019

Based on Article. 105 § 1 of the Act of June 14, 1960 - Code of Administrative Procedure (Journal of Laws of 2018, item 2096, as amended), art. 5 sec. 1 point 6 in connection with Art. 12 and art. 13, art. 14 of the Act of December 14, 2018 on the protection of personal data processed in connection with the prevention and combating of crime (Journal of Laws of 2019, item 125, hereinafter: the Act of December 14, 2018) after administrative proceedings in on the complaint of Mr. RB (residing at ul. [...]) against the refusal to provide him with personal data by the Police Commander in Chief in Warsaw (address: Police Headquarters, ul. Puławska 148/150, 02-624 Warsaw) processed in the National Police Information System (KSIP),

I discontinue the proceedings

Justification

The Office for Personal Data Protection received a complaint from Mr RB (hereinafter referred to as the "Complainant") about irregularities in the processing of the Complainant's personal data by the Police Commander in Chief in Warsaw (hereinafter referred to as the "Commander"), consisting in a refusal to provide him with information about the personal data being processed in The National Police Information System (hereinafter: "KSIP"). In justifying the request, the Complainant also submitted a request to order the Commander to disclose personal data processed at the KSIP.

In the course of the proceedings initiated by the complaint, the President of the Personal Data Protection Office obtained explanations regarding the circumstances of the case, read the evidence and made the following findings.

By letters of [...] May 2019, the President of the Personal Data Protection Office informed the Complainant and the Commander of the initiation of the investigation procedure and asked the Commander to comment on the content of the complaint and submit written explanations.

On [...] June 2019, the Office for Personal Data Protection received a letter from the Head of the Information Service Department of the Intelligence and Criminal Information Bureau of KGP ([...]), in which he explained that the complainant in a

letter of [...] February 2019 (a copy of the application from the case files) addressed to the Police Commander in Chief, asked for access to all processed personal data at the KSIP, referring to the content of Art. 23 sec. 1 of the Act of December 14, 2018 on the protection of personal data processed in connection with the prevention and combating of crime. He further explained that in a letter of [...] March 2019 - [...] (a copy of the letter in the case file) the Head of the Information Service Department of the Intelligence and Criminal Information Bureau of the National Police Headquarters replied to the complainant, indicating that the Police processed data personal in accordance with art. 21nb in connection with joke. 20 of the Act of April 6, 1990 on the Police (Journal of Laws of 2019, items 161 and 125). In the justification of the position, the Complainant was indicated the legal grounds for the processing of personal data by the Police, in particular art. 20 paragraph 1-1d, paragraph 2b-2c and art. 20 paragraph 2ad and paragraph 2ba of the Police Act, their scope and purpose of processing, paying attention to the particularity of these standards (lex specialis) in relation to general provisions, such as the provisions of the Act on the Protection of Personal Data and Art. 51 sec. 5 of the Constitution of the Republic of Poland (Journal of Laws of 1997, No. 78, item 483, as amended), which refers to specific regulations in terms of the rules and procedure for collecting and disclosing information about a person. In addition, the letter in question clearly indicated that the legal act specifying the rules and procedure for collecting and sharing information, including personal data, is the Police Act, in particular Art. 20 paragraph 1d, which allows the processing of personal data without the knowledge and consent of the data subject. In addition, it was pointed out that the access to data is subject to limitations for applicants under Art. 26 of the Act of December 14, 2018 on the protection of personal data processed in connection with the prevention and combating of crime. Therefore, the Police are not obliged to inform the person whose personal data they process about the fact and the scope of the processing of such data. Moreover, the Complainant was informed that in this legal state the Police were not obliged to disclose personal data to him. Considering the above, the Deputy Head of Department informed the Complainant about the lack of legal grounds for disclosing the requested information.

The President of the Office for Personal Data Protection informed the Complainant and the Commander in letters of [...] July 2019 about the conduct of administrative proceedings, as a result of which evidence was collected sufficient to issue an administrative decision and about the possibility to comment on the collected evidence and materials and reported requests in accordance with the content of art. 10 § 1 of the Act of June 14, 1960, Code of Administrative Procedure, within 7 days from the date of receipt of the above-mentioned writings.

In such a factual and legal state, the President of the Personal Data Protection Office considered the following:

The complainant alleged that the Police Commander in Chief did not disclose information about his personal data processed at the KSIP.

First of all, it should be noted that the provisions of the Act of December 14, 2018 on the protection of personal data processed in connection with the prevention and combating of crime (Journal of Laws of 2018, item 125), hereinafter referred to as : "By the Act of December 14, 2018". The aforementioned act creates legal grounds for the application of state protection in situations of unlawful processing of citizens' personal data, by defining the principles and conditions for the protection of data processed by competent authorities that process personal data for the purpose specified in art. 1 section 1 of the Act of December 14, 2018, i.e. for the purpose of identifying, preventing, detecting and combating prohibited acts, including threats to public safety and order, as well as performing pre-trial detention, penalties, order penalties and coercive measures resulting in deprivation of liberty. Pursuant to Art. 21nb paragraph 1 of the Police Act, the Police Commander in Chief runs the National Police Information System, which is a set of data sets in which information, including personal data, is processed in connection with the performance of statutory tasks. For the statutory tasks of the police, pursuant to Art. 1 clause 2 should be i.a. detecting crimes and offenses and prosecuting their perpetrators. In view of the above, it should be noted that the operation of the above-mentioned of the register by the Commandant is an obligation performed as part of the implementation of the statutory tasks of the Police, which falls within the scope of the application of the Act of December 14, 2018. For these reasons, the Act of December 14, 2018 is competent to consider the case in question.

Pursuant to Art. 23 point 1 of the Act of December 14, 2018, the data subject may request the administrator to disclose his personal data from a given data set. The processing and exchange of information, including personal data, may concern the data referred to in art. 14 sec. 1 of the Act of December 14, 2018, processed in connection with the prevention and combating of crime, i.e. sensitive data including personal data revealing racial and ethnic origin, political views, religious beliefs, philosophical beliefs, trade union membership and genetic data, biometric data in order to unambiguously identification of a natural person, data concerning health, data concerning a natural person's sexuality and sexual orientation. Pursuant to Art. 20 paragraph 2b of the Police Act, the information processed by the Police authorities may include the above-mentioned sensitive data, where the data on the genetic code includes only information about the non-coding part of DNA, fingerprints, photos, sketches and descriptions of the image, features and special signs, pseudonyms, as well as information about the place of

residence or stay, education, profession, place and the workplace and the material situation and condition of the property, documents and objects used by the perpetrator, the perpetrator's method of action, his environment and contacts, the perpetrator's behavior towards the aggrieved parties. It should be noted, however, that pursuant to Art. 20 (2c) of the Personal Data Act referred to in Art. 14 sec. 1 of the Act of December 14, 2018, shall not be collected in the event that they are not useful for detection, evidence or identification.

The personal data protection authority, in order to implement the state protection of citizens in situations of unlawful processing of personal data, has been equipped with powers to sanction any irregularities found in the processing of personal data. This means that the personal data protection authority, when assessing the status of the case and subsuming, determines whether the questioned processing of personal data is based on at least one of the premises legalizing the processing of personal data indicated in art. 13 of the Act of December 14, 2018, according to which the competent authorities process personal data only to the extent necessary to exercise the right or fulfill the obligation resulting from the law and in the case of processing sensitive data in the grounds for legalizing the processing specified in art. 14 sec. 2 of the above-mentioned Act. Depending on the findings in the case, the data protection authority issues an order to restore the lawful state or refuses to accept the request, or discontinues the proceedings. The issuing of an order to remedy deficiencies in the processing of personal data takes place when the personal data protection authority states that there has been a violation of legal norms in the field of personal data processing. On the other hand, the occurrence of the above-mentioned premises legalizing the processing determines the recognition of the questioned processing activities as lawful. For these reasons, in the case at hand, it had to be determined whether the Police authorities had an appropriate legal basis legalizing the processing of the Complainant's personal data, fulfilling the provisions of Art. 13 and 14 of the Act of December 14, 2018.

In the field of processing various types of information, including personal data, the function of the Police is special, as it collects information that is subject to a special regime and protection. This is reflected in Art. 20 paragraph 1 and sec. 2a of the Police Act (Journal of Laws of 2019, item 161, as amended), on the basis of which the Police, subject to the limitations resulting from Art. 19, may obtain information, including classified information, collect, check and process it (section 1). The police may download, obtain, collect, process and use, in order to perform statutory tasks, information, including personal data, about the following persons, also without their knowledge and consent: about persons suspected of committing crimes prosecuted under public indictment, by the Act as crimes prosecuted by public indictment, about persons with undetermined identity or trying to

conceal their identity, about persons posing a threat, referred to in the Act of 22 November 2013 on proceedings against persons with mental disorders posing a threat to life, health or sexual freedom of other persons, on wanted persons, missing persons and persons against whom protection and assistance measures, provided for in the Act of 28 November 2014 on protection and assistance, provided for in the Act of 28 November 2014 on the protection of and help for the victim and the witness (Journal of Laws of 2015, item 2 1) (Art. 20 paragraph 2a of the Police Act).

Detailed rules for the processing of personal data of persons mentioned in art. 20 paragraph 2a of the Police Act is specified in the regulation of the Minister of Internal Affairs and Administration of 24 August 2018 on the processing of information by the Police (Journal of Laws, item 1636, hereinafter: "the Regulation"). Pursuant to § 10 of the regulation in question, the Police operates the National Police Information System (KSIP), which is a set of data sets in which information is collected, checked, processed and used, including personal data referred to in art. 20 paragraph 2a points 1-6 and par. 2b of the Police Act. The KSIP may also process information, including personal data, to which the Police is entitled to collect, obtain and process on the basis of separate acts, if this contributes to the coordination of information and more effective organization and implementation of the statutory tasks of the Police in the field of detecting and prosecuting perpetrators of crimes. and preventing and combating crime, as well as protecting human life and health (§ 10 (2) of the Regulation). It should be emphasized that the criterion of the necessity to process personal data in the KSIP must always be related to the statutory tasks of the Police, the implementation of which is to be achieved by the provisions of Art. 20 paragraph 1, sec. 2b-2c of the Police Act. In addition, in Chapter 5 of the above-mentioned Regulation, the criteria for the verification of the storage of personal data in the system in terms of their further usefulness, which are, among others, the type and nature of the crime committed, the type and nature of the infringed good protected by law, the forms of the perpetration, the form of the intention, the time that has elapsed since the data was entered into the filing system.

In the course of the proceedings in question, the President of the Personal Data Protection Office established that the Complainant requested the Police Commander in Chief to provide information on whether his personal data were processed in the KSIP database, in particular including: the content of trial registrations, searches, detention, records, and preventive measures applied. , prohibitions, orders, legitimate ect.

In response to the above request, the Police Commander in Chief refused to provide the Complainant with the requested information, pointing to Art. 20 paragraph 1d of the Police Act and Art. 26 of the Act of December 14, 2018 Pursuant to Art. 23

sec. 3 of the Act of December 14, 2018, the controller is obliged to inform the data subject about the reasons for refusing or limiting access and about the possibility of submitting a complaint to the President of the Personal Data Protection Office in the event of violation of a person's rights as a result of the processing of their personal data.

Against the background of the case under examination, it should be stated that the Commandant complied with the above-mentioned statutory obligation indicating the purposes and scope of the personal data being processed, legal grounds and limitations that make it impossible to provide the personal data requested by the Complainant, and at the same time indicated a further legal path enabling the pursuit of his rights related to the protection of personal data (a copy of the letter in the case files). At this point, with regard to the issue of the unavailability of data from the KSIP database, it is also impossible to ignore the wording of recital 44 of Directive (EU) 2016/680 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 by competent authorities for the purposes of crime prevention, investigation, detection and prosecution of offenses and the execution of penalties, on the free movement of such data and repealing Council Framework Decision 2008/977 / JHA (Journal of Laws EU L of 4 May 2016, ., hereinafter: "Directive 2016/680"). It states that "Member States should be able to adopt legal acts allowing to delay, limit or omit the information of data subjects, or to limit, in whole or in part, the access of data subjects to their own personal data to this extent and for as long as the measure in question is necessary and proportionate in a democratic society, with due regard to the fundamental rights and legitimate interests of the natural person concerned, so as to prevent the interference with official or judicial inquiries, investigations or procedural steps, so as not to interfere with crime prevention , investigation, detection and prosecution of criminal offenses and the execution of penalties in order to protect public or national security or to protect the rights and freedoms of others. The controller should assess - by examining each case on a specific and individual basis - whether the right of access should be partially or completely restricted. ' The above recital is reflected in the content of Art. 15 of Directive 2016/680. Pursuant to Art. 15 sec. 1 of Directive 2016/680, Member States may adopt legal acts allowing the restriction of the data subject's right of access in whole or in part to the extent and for as long as such a partial or total restriction is necessary and proportionate in a democratic society , with due regard to the fundamental rights and legitimate interests of the natural person concerned, to: (a) prevent obstruction of official or legal inquiries, investigations or procedures; b) prevent the interference with the prevention of crime, the investigation, detection and prosecution of criminal offenses or the execution of penalties; c) protect public safety; d) protect national security; e) protect the rights and freedoms of others. The

indicated art. 15 of Directive 2016/680 has been implemented in Art. 26 of the Act of 14 December 2018, and as the Commander rightly pointed out, given the status of police data files different from the official files - information, including personal data, is processed in order to perform the tasks of the Police referred to in the earlier part of this argument, in a discretionary manner. And the mere disclosure of information from police data files is possible only and exclusively to public authorities, services and other institutions on the basis of applicable laws and within the limits of their powers in the field of personal data processing. Therefore, contrary to the complainant's claims, access to the collections stored in the KSIP is not universal. The occurrence of at least one of the negative premises referred to in Art. 26 sec. 1 - 6 of the Act of 14 December 2018 restricts access to personal data to the extent and for the period in which the relevant measure is necessary and proportionate in a democratic society - with due regard to the fundamental rights and legitimate interests of a given natural person - so as to prevent the interference with the activities of official and court proceedings, or to prevent the interference with the prevention of crime, detection and prosecution of prohibited acts, so as to protect public or national security. It should also be emphasized that in the realities of the present case there is no premise resulting from par. 2 Art. 26 of the Act of December 14, 2018, namely, there is no situation where disclosure of data by the controller (Police Commander in Chief) would be necessary to protect human life or health. The Complainant's request was limited to information purposes only, and not higher, justifying the disclosure of such personal data by the administrator. For these reasons, the position presented by the Commander in this case was adequate. Considering that the controller of the data processed in the KSIP is the Police Commander in Chief and the statutory tasks of the Police, in this case, the disclosure of information about the processed data in the internal Police system, which is the KSIP, may undoubtedly result in the fulfillment of the conditions referred to in the above provision.

For the above reasons, the proceedings are redundant and therefore had to be discontinued pursuant to Art. 105 § 1 of the Code of Civil Procedure Pursuant to the aforementioned provision, when the proceedings for any reason have become redundant in whole or in part, the public administration authority issues a decision to discontinue the proceedings, in whole or in part, respectively. At the same time, the literature on the subject indicates that the pointlessness of the administrative procedure, as provided for in Art. 105 § 1 of the Code of Civil Procedure means that there is no element of the material legal relationship, and therefore it is not possible to issue a decision settling the matter by deciding on its substance (B. Adamiak, J. Borkowski "Code of Administrative Procedure. Comment" 7th edition Wydawnictwo CH Beck, Warsaw 2005 r., p. 485). The

same position was taken by the Provincial Administrative Court in Kraków in its judgment of 27 February 2008 in the case no. act III SA / Kr 762/2007, in which he stated that "the procedure becomes pointless when any of the elements of the substantive 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 there are no grounds to decide the merits of the case, and the continuation of the proceedings in such a case would be defective, which would have a significant impact on the result of the case.

As a result of the above findings and considerations, the personal data protection authority concluded that there was no breach of the provisions on the protection of personal data in this case. The Police authorities, fulfilling the legal obligation resulting from the provisions of the Act of 6 April 1990 on the Police, collected and processed the complainant's personal data in a proper and adequate manner, which rendered the entire proceedings redundant.

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

The decision is final. Based on Article. 9 sec. 2 of the Act of December 14, 2018 on the protection of personal data processed in connection with the prevention and combating of crime (Journal of Laws of 2019, item 125), the party has the right to lodge a complaint with the Provincial Administrative Court against this decision, 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.

2019-09-04