THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 15

November

2018

DECISION

ZSOŚS.440.5.2018

Based on Article. 104 § 1 of the Act of June 14, 1960 - Code of Administrative Procedure (Journal of Laws of 2018, item 2096) and art. 12 point 2, art. 22 and art. 23 sec. 1 point 2 of the Act of August 29, 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922, as amended) in connection with Art. 160 sec. 1 and 2 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2018, item 1000, as amended), after conducting administrative proceedings regarding a complaint by R. W., residing in in O., irregularities in the processing of his personal data by the Police Commander in Chief, consisting in processing them in the National Police Information System (KSIP) in a situation where there has been a seizure of a conviction for a crime,

I refuse to accept the application

Justification

On [...] May 2018, the Office of the Inspector General for Personal Data Protection (currently: the Office for Personal Data Protection) received a complaint from Mr RW (hereinafter referred to as the "Complainant") about irregularities in the processing of his personal data by the Police Commander in Chief in Warsaw (hereinafter referred to as the "Commandant"), consisting in the processing of the complainant's personal data in the National Police Information System (KSIP) in a situation where the conviction for a committed crime has been seized. In the complaint, the complainant also included a request to order the Commander to remove his personal data from the KSIP in the scope of information obtained in the course of the conducted criminal proceedings.

Justifying his request, the complainant indicated that there were no grounds for which the Police authorities still store and process his personal data in the KSIP system, in a situation where the conviction was seized by operation of law on [...] June 2012. The applicant also submitted that the act the one committed by him is characterized by negligible social harmfulness, and since the time of committing the crime he has been observing the legal order. Considering the above, the Complainant

demands that the President of the Personal Data Protection Office undertakes actions aimed at protection of his personal data by deleting information about the commission of a prohibited act by him from the KSIP collection.

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 [...] September 2018, the President of the Office for Personal Data Protection informed the Complainant and the Commander about the initiation of the investigation procedure and asked the Commander to comment on the content of the complaint and provide written explanations. On [...] October 2018, the Office for Personal Data Protection received a letter from the Commander ([...]), in which he explained that on [...] February 2018, the General Police Headquarters received a request from the complainant to remove information about the him, on [...] April 2008, an offense under Art. 279 § 1 of the Act of 6 June 1997 - Penal Code (Journal of Laws of 2018, item 1600), hereinafter referred to as the CC, from the National Police Information System (copy of the application from the case files). The applicant also indicated in that application that on […] June 2012 his conviction was expunged and that he wanted to enjoy the full privileges of an unpunished person. In addition, he expressed regret and remorse for the act he had committed and indicated that he had committed the act himself and that no one's life or health had suffered as a result of committing it.

In a letter of [...] April 2018 - [...] (a copy of the letter in the case files) the Head of the Information Service Department of the Intelligence and Criminal Information Bureau of the National Police Headquarters, acting under the authority of the Police Commander in Chief, replied to the complainant, indicating that the Police processed personal data in accordance with joke. 20 of the Act of April 6, 1990 on the Police (Journal of Laws of 2017, item 2067, as amended), hereinafter referred to as the "Police Act". 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 2a, section 2ac, paragraph. 2b, section 17 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. It was emphasized that Art. 51 of the Constitution of the Republic of Poland allows for statutory limitations in the exercise of the right to information autonomy of an individual. Attention was also paid to the provisions of the Ordinance of the Minister of the Interior of July 21, 2016 on the processing of information by the Police (Journal of Laws of 2016, item 1091), in particular the grounds for assessing the usefulness of data specified in § 29 para. 1. The complainant was also informed about the different procedure and rules for processing information in the KSIP

and the National Criminal Register (hereinafter referred to as "KRK") and that, apart from the exceptions set out in the Acts, the KSIP collection was not available to employers. However, this does not apply to professions and functions that require an impeccable opinion under the provisions of statutes, because in this case both the criminal record of the person is subject to assessment, but also other behaviors of the person not constituting crimes within the meaning of the law, but creating doubts in the context of exercising a special social role assigned to a given professional group. be the position. It was also explained to the complainant that the fact that his personal data was processed at the KSIP did not stigmatize him in the light of the law, as he would remain an unpunished person in the event of an expungement of the conviction. In the above-mentioned In the letter, it was also noted that the Police process personal data only to the extent specified and in accordance with the provisions cited.

Then, in a letter of [...] April 2018, addressed to the Intelligence and Criminal Information Bureau of the Police Headquarters, the complainant appealed against the decision of [...] April 2018 ([...]) refusing to delete his personal data from the KSIP (copy letters in the case files). He emphasized that 10 years had elapsed since the commission of the prohibited act, the act was of a one-off nature and was characterized by low social harmfulness. He also indicated that he had repaired the damage caused to the aggrieved party.

In response to the complainant's "appeal", the Deputy Head of the Information Service Department of the Intelligence and Criminal Information Bureau of the National Police Headquarters, acting under the authority of the KSIP administrator, the Police Commander in Chief, in a letter of [...] April 2018 - [...] (a copy of the letter in the case files) upheld the arguments contained in the letter of [...] April 2018. Justifying his position, the Commandant indicated that on the basis of the premises arising from Art. 20 paragraph 17 and 17b of the Police Act and the methods of assessing data in terms of their usefulness in the conducted proceedings indicated in § 29 of the Regulation of the Minister of Internal Affairs of July 21, 2016 in the scope of information processing by the Police, as a result of a re-verification of information processed in the KSIP factual state and legal regulations have not changed with regard to the processed data since the submission of the previous request by the Complainant. At the same time, the Complainant was informed about the right to lodge a complaint with the Inspector General for Personal Data Protection pursuant to Art. 35 sec. 2 of the Act of August 29, 1997 on the Protection of Personal Data.

The President of the Office for Personal Data Protection informed the Complainant and the Police Commander in Chief in letters of [...] October 2018 about conducting administrative proceedings, as a result of which evidence was collected sufficient

to issue an administrative decision and about the possibility of expressing his opinion 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.

It should be noted here that on the date of entry into force of the Act of May 10, 2018 on the protection of personal data, i.e. May 25, 2018, the Office of the Inspector General for Personal Data Protection became the Office for Personal Data Protection. Pursuant to Art. 160 of this Act, the 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 in accordance with the principles set out in the Code of Civil Procedure. All activities undertaken by the Inspector General for Personal Data Protection before May 25, 2018 remain effective.

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

The above-mentioned Act on the Protection of Personal Data of August 29, 1997 provides legal grounds for applying state protection in situations of illegal processing of citizens' personal data by both public law entities and private law entities. In order to implement it, the personal data protection authority has been equipped with powers to sanction any irregularities found in the processing of personal data. This means that the personal data protection authority, 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. 23 sec. 1 above of the Act on the Protection of Personal Data and depending on the findings in the case - either issues an order or prohibition, 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.

Pursuant to Art. 1 of the aforementioned Act, everyone has the right to the protection of personal data concerning him, and the processing of such data, in the sense referred to in Art. 7 point 2 of this Act, it is allowed only for specific goods, i.e. the public good, the good of the data subject or the good of a third party, and only to the extent and in the manner specified by the act. Bearing the above in mind, therefore, when applying the provisions of this Act, it is necessary to weigh the underlying goods each time.

In the course of the proceedings, the President of the Office for Personal Data Protection established that in 2008 the

Complainant was subject to criminal proceedings concerning an offense under Art. 279 § 1 of the CC On the day the complaint was lodged with the Bureau of the Inspector General for Personal Data Protection, the conviction has already been seized. In the content of the complaint, the complainant argued that his personal data were still processed at the KSIP, despite the seizure of the conviction. Referring to the institution of exposing a conviction, it should be noted that it aims to enable the full social rehabilitation of the convict, which is associated with the recognition of the conviction as non-existent and the removal of the entry on the conviction from the National Criminal Code. A convicted person has the right to claim that he or she has not been punished, and that no institution may limit his / her rights on the basis of a criminal record. As rightly pointed out by subinsp. SD in a letter of [...] October 2018, this right is not prejudiced due to the further processing of data about the person committing the crime in the KSIP, because the information available to the National Police Information System is not a source of publicly available knowledge, as it is only used to implement the tasks of the Police referred to in Art. 1 clause 2 of the Police Act. While access to information on the criminal record of a person from KRK is universal, the information obtained and produced by the Police authorities at the KSIP is a closed, generally inaccessible set of information and data, used only by the Police authorities to carry out their statutory tasks related to ensuring safety and order. public.

In this case, the content of Art. 23 sec. 1 point 2 of the Act on the Protection of Personal Data, which states that the processing of data is permissible when it is necessary to exercise the right or fulfill the obligation resulting from the law. The legal basis for the processing of personal data of persons against whom the proceedings were conducted by the Police authorities is Art. 20 paragraph 1 of the Police Act, pursuant to which the Police, subject to the limitations resulting from Art. 19, can obtain information, including covertly, collect, check and process it. The police may download, obtain, collect, process and use, in order to carry out statutory tasks, information, including personal data - about persons suspected of committing crimes prosecuted by public prosecution - also without their knowledge and consent (section 2a). In the light of Art. 20 paragraph 2b of the Police Act, the collected information may include: personal data referred to in art. 27 sec. 1 of the Act on the Protection of Personal Data of August 29, 1997, except that the data on the genetic code includes only information about the non-coding part of DNA, and may include fingerprints, photos, sketches and descriptions of the image, features and special characters, pseudonyms, as well as information about: place of residence or stay, education, profession, place and position of work as well as the material situation and the condition of property, documents and objects they use, the method of the perpetrator's activities, his environment and contacts, the behavior of the perpetrators towards the aggrieved parties. The aforementioned

information is not collected when it is not useful for detection, evidence or identification in the conducted proceedings. The period of data storage is specified in Art. 20 paragraph 17 of the Police Act, pursuant to which personal data collected in order to detect a crime is stored for the period necessary to perform the statutory tasks of the Police. Police authorities verify these data after the end of the case, under which the data has been entered into the file, and also at least every 10 years from the date of obtaining or downloading the information, deleting redundant data. Pursuant to Art. 20 paragraph 17b, the personal data referred to in para. 17, shall be deleted if the Police authority has obtained credible information that: the act constituting the basis for entering the information into the file was not committed or there is no data sufficient to justify the suspicion of its commission; the event or circumstance in relation to which the information was entered into the collection does not bear the characteristics of a prohibited act; the data subject has been acquitted by a final court judgment. On the other hand, particularly sensitive personal data, e.g. revealing racial or ethnic origin, religious beliefs and data on the health, addictions or sexual life of persons suspected of committing crimes prosecuted by public prosecution, who have not been convicted of these crimes, are subject to commission and protocol destruction immediately after the relevant decision becomes final (section 18). Among the above-mentioned grounds for data deletion, there is no seizure of the conviction that would justify the removal of the Complainant's data from the KSIP. This means that the mere seizure of a conviction is not an independent and absolute condition for removing criminal information from the KSIP databases. In addition, attention should be paid to the issue of the data retention period; indefinite storage of personal data is unacceptable. The content of art. 20 paragraph 17 indicates that the Police authorities are obliged to systematically review and delete unnecessary data from the system, therefore there may not be a situation of indefinite processing of personal data in the KSIP by this entity. As a side note, it should be noted that the mentioned in Art. 20 paragraph 17 of the Police Act, the ten-year period for obtaining or downloading information in the case under consideration has not yet expired. Thus, this constitutes another argument in favor of the lawful processing of the Complainant's personal data by the Police authorities in the database. Moreover, as is clear from the letter of [...] October 2018, Podinsp. SD, acting under the authority of the Police Commander in Chief, the Police authorities properly verified the Complainant's data collected in the KSIP after the case was completed, i.e. in 2008, and additionally each time in connection with the complainant's requests to remove his personal data from the KSIP file, and also with a complaint submitted to the Inspector General for Personal Data Protection, and in the case of a request to delete personal data from the KSIP, the verification was made in particular in terms of the premises under Art. 51 sec. 4 of the Polish Constitution and the premises of

Art. 20 paragraph 17b and 18 of the Police Act.

In the case under consideration, one should also take into account the regulations, the ordinance of the Minister of Internal Affairs and Administration of 23 August 2018 on the processing of information by the Police (Journal of Laws, item 1636), in particular § 4 and § 10, which replaced the regulation Of the Minister of the Interior of July 21, 2016 regarding the processing of information by the Police, in force at the moment of initiating administrative proceedings before the Inspector General for Personal Data Protection.

In addition, Chapter 5 of the Regulation of 23 August 2018 indicates the criteria for verifying the storage of personal data in the system in terms of their further usefulness, which include, inter alia, the type and nature of the crime committed, the type and nature of the infringed good protected by law, the form of the perpetration, the form of the intention, the time that has elapsed since the data was entered into the filing system, the validity of the conditions of legality and the necessity of further data processing to perform statutory tasks, the occurrence of the circumstances specified in art. 20 paragraph 17b and 18 of the Police Act, and in the case of dactyloscopic data, the occurrence of the circumstances specified in art. 21 l of paragraph 2 and art. 21m of this act.

The above argumentation is justified in the judgment of the Supreme Administrative Court of April 21, 2017 (I OSK 2426/15) and in the judgment of the Constitutional Tribunal of December 12, 2005, file ref. K 32/04 (publ. OTK-A 2005/11/132), in which it was stated that the provision of Art. 20 paragraph 17 of the Police Act does not provide for the removal from the data files of persons suspected of committing crimes prosecuted by public prosecution, who have been legally acquitted or against whom the criminal proceedings have been legally and unconditionally discontinued, immediately after the relevant judgment becomes final. Final acquittal of a specific person or unconditional discontinuation of criminal proceedings against a specific person does not prejudge whether the collected data may contain information useful for the performance of statutory tasks of the Police towards other persons.

Moreover, the Constitutional Tribunal indicates that the reason for which the rights of an individual may be limited is the protection of the common good, and in particular - taking into account the needs of the country's security and defense. Therefore, the protection of state security is a special value against which the rights of the individual, even fundamental rights, may be - to the extent necessary - limited. The admissibility of restrictions dictated by such considerations is generally accepted in democratic countries (the judgment of the Constitutional Tribunal of February 16, 1999 in case SK 11/98, OTK of

1999, part I, item 5).

Bearing in mind the above, it should be stated that the manner of the Police's conduct in the discussed scope does not raise any doubts. The complainant's personal data were, in accordance with the provisions, subject to an assessment of their usefulness.

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 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.

2019-03-29