THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 18

of December

2018

DECISION

ZSOŚS.440.69.2018

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2018, item 2096), art. 12 point 2, art. 27 sec. 1 and 2, point 2, 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 Art. 20 of the Act of April 6, 1990 on the Police (Journal of Laws of 2017, item 2067, as amended), in connection with art. 160 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2018, item 1000, as amended) after administrative proceedings regarding the complaint of Mr. K. H., residing in in R., for the processing of his personal data in the National Police Information System (KSIP) by the Police Commander in Chief (Warsaw, ul. Puławska 148/150),

I refuse to accept the application

Justification

The Office of the Inspector General for Personal Data Protection (currently: the Office for Personal Data Protection) received a complaint from Mr. K. H. in R. (hereinafter: "the Complainant"), for the processing of his personal data in the National Police Information System (hereinafter: "KSIP") by the Police Commander in Chief (Warsaw, ul. Puławska 148/150), (hereinafter: " KGP ").

In the complaint, the complainant indicated that KGP processed his personal data in the KSIP system without any legal basis. The applicant also requested a decision ordering KGP to delete his personal data stored in the KSIP system.

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.

In 2013, criminal proceedings were pending against the Complainant for an offense under Art. 178a § 1 of the Act of 6 June 1997 Penal Code (Journal of Laws of 2018, item 1600). On the terms set out in Art. 20 paragraph 2a of the Act of 6 April 1990 on the Police (Journal of Laws of 2017, item 2067, as amended), in connection with the presentation of the above-mentioned

charges, the competent Police authority made the so-called trial registration, i.e. entered the complainant's personal data into the KSIP data set as a person suspected of committing an offense prosecuted by public indictment. By letter of [...] October 2016, the applicant requested the Police Commander in Chief to remove from the police database information about the act he had committed on [...] .01.2013. Then, in a letter of [...] November 2016, the Deputy Head of the Information Service Department of the Intelligence and Criminal Information Bureau of the KGP replied to the above-mentioned the complainant's request, informing that, as it results from art. 20 paragraph 2a, section 2ac and 2b of the Police Act, the Police may download, obtain, collect, process and use, in order to perform statutory tasks, information, including personal data, on persons suspected of committing crimes prosecuted by public indictment, minors committing acts prohibited by the Act as offenses prosecuted by public prosecution, persons with undetermined identity or trying to conceal their identity, persons posing a threat, referred to in the Act of 22 November 2013 on proceedings against persons with mental disorders, posing a threat to the life, health or sexual freedom of others persons, wanted persons, missing persons, persons against whom protection and assistance measures have been applied, provided for in the Act of 28 November 2014 on the protection and assistance for the victim and the witness (Journal of Laws of 2015, item 21) and about the persons referred to in art. 10 sec. 1 of the Act of 10 June 2016 on anti-terrorist activities, also without the knowledge and consent of these people. The letter explained that the information may include: personal data referred to in art. 27 sec. 1 of the Act of August 29, 1997 on the Protection of Personal Data. Additionally, the said letter explained to the Complainant that the provision of Art. 20 paragraph 2a in fine of the Police Act is a lex specialis in relation to the norms specified in Art. 51 of the Polish Constitution and Art. 25, 32 and 33 of the Act on the Protection of Personal Data, which seems to be understandable and reasonable in all respects, in view of the statutory tasks assigned to the Police (including preventing and combating crime). Therefore, the Police is not obliged to inform the person whose personal data is being processed about the processing of such data, as well as about the scope of processing or sharing personal data. Considering the above, KGP refused the Complainant to grant the request. On [...] January 2017, Mr. K. H. again applied to the Intelligence and Criminal Information Bureau of KGP with a request to remove his personal data from the KSIP system. In response to the letter of Mr. K. H., Deputy Head of the Information Service Department of the Intelligence and Criminal Information Bureau of the KGP, he informed the complainant that, on the basis of the grounds for deleting personal data from the KSIP system indicated in Art. 20 section 17 and 17b of the Act of 6 April 1990 on the Police (Journal of Laws of 2016, item 1782 as amended) and the methods of assessing personal data in terms of their usefulness in

the proceedings indicated in §29 Regulation of the Minister of Internal Affairs and Administration of 21 July 2016 on information processing by the Police (Journal of Laws of 2016, item 1091) - the data concerning the Complainant processed with the KSIP was re-verified. At the same time, the complainant was informed that the factual and legal status had not changed and that the position presented in the letter [...] of [...] November 2016 was maintained. applied again (after [...] January 2017) to delete data from the KSIP. In addition, in connection with the implementation of the standards set out in the Act on the Police, the Police authorities, after the end of the case in 2013, verified the collected personal data of the Complainant in the scope of acts under Art. 178a § 1 of the Penal Code. The police also carried out the above-mentioned verification in connection with the Complainant's complaint to the Inspector General regarding the processing of his data at the KSIP and each time in connection with requests for the deletion of personal data. Authorized by the Police Headquarters, the Head of the Information Service Department of the Criminal Service Bureau of the General Police Headquarters, explained that, according to the norms specified in Art. 20 paragraph 17 - The police are obliged to verify the data after the end of the case under which the data was entered into the file (here: KSIP), and also at least every 10 years from the date of obtaining or downloading the information, deleting redundant data. Above The head stated that the verifications required by the act were made in particular in terms of the premises under Art. 51 sec. 4 of the Polish Constitution and in terms of legality, including the premises of Art. 20 paragraph 17 b and 18 of the Police Act. When carrying out the above data verifications (assessments in terms of their usefulness), the Police did not have any information indicating the existence of the premises under Art. 20 paragraph 17b and 18 of the Police Act. Moreover, the Head of the Information Service Department of the Criminal Service Office of the Police Headquarters explained that the 10-year period of compulsory verification of the collected data has not yet expired, therefore, in the opinion of KGP, there are no statutory grounds for removing the complainant's data from the KSIP. The type of crimes committed by the applicant is also not without significance (apart from the failure to meet the above-mentioned criterion of time).

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 issuance 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 Personal Data Protection Office established that criminal proceedings were pending in the case of an offense under Art. 178 and § 1 of the CC. against the applicant. 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 the Police Commander in Chief refused to request the removal of his personal data from the KSIP, despite the fact that the information was not useful in the proceedings conducted by the Police and was not necessary for the performance of the statutory tasks of the Police.

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, according to which the Police, subject to the limitations resulting from Art. 19, can obtain information, including classified information, collect it, 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 also include personal data referred to in art. 27 sec. 1 of the Act on the Protection of Personal Data of August 29, 1997. 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 in which the data was entered

into the file, and moreover, 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. 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 void 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 the letter of [...] November 2017, this right is not prejudiced due to the further processing of the data about the person committing the crime in the National Police Act, 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 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 remove 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 apparent from the letter of [...] November 2017, 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 end of the case, i.e. in 2013, 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 examination, one should also take into account the regulations of the regulation of the Minister of the Interior 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 Internal Affairs 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 fee for the complaint is PLN 200. The party has the right to apply for the right to assistance, including exemption from court costs.

2019-04-08