

# THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 21

November

2018

## DECISION

ZSOŚS.440.75.2018

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 the complaint of Mr. A. Ś., Residing in in L., on irregularities in the processing of his personal data by the Police Commander in Chief in Warsaw (Police Headquarters, ul. Puławska 148/150, 02-624 Warsaw), consisting in the processing of his personal data in the National Police Information System (KSIP) ),

I refuse to accept the application

### Justification

On [...] March 2017, Mr. A. Ś. (hereinafter referred to as the "Complainant") for irregularities in the processing of his personal data by the Police Commander in Chief in Warsaw (hereinafter referred to as the "Commander"), consisting in the processing of the complainant's personal data in the National Police Information System (KSIP). In the complaint, the complainant submitted 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 ongoing criminal proceedings in the case with the file number [...].

In justifying his request, the complainant argued that in his opinion 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 under the law. The applicant also pointed out that as soon as the conviction is seized, it is considered void. Not only is the conviction considered null and void, but also the commission of the crime itself, which introduces the legal fiction that no crime was committed at all. On the other hand, further processing of the complainant's personal data by the Police authorities distorts the purposefulness of the institution of seizure of the conviction and prevents the perpetrator from returning to full-fledged functioning in the

society. Moreover, the Complainant submitted that he still feels the consequences of the existence of his personal data at KSIP, and due to the fact that he had taken up studies in internal security and was afraid that further processing of his personal data at KSIP would prevent him from working in uniformed services. The applicant further argues that there are no reasons for the usefulness of this type of information for the statutory activities of the Police, in particular for activities of a detective nature and aimed at preventing future crime. Considering the above, in the content of the complaint, the Complainant demands that the President take action to protect his personal data by removing information about the commission of a prohibited act from the KSIP database.

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 2017, the Inspector General for Personal Data Protection informed the Complainant and the Commander of the initiation of explanatory proceedings and asked the Commander to comment on the contents of the complaint and to provide written explanations. On [...] May 2017, the Office of the Inspector General for Personal Data Protection received a letter from the Commander ([...]) explaining that the Complainant with a request of [...] January 2017 (a copy of the request from the case file) addressed to the Commander Of the Chief of Police, and then transferred to the Intelligence and Criminal Information Bureau of the General Police Headquarters, asked for the removal of his personal data from the KSIP as part of the proceedings conducted by the District Court in B. in the case with file number [...]. As the basis for his claim, the Complainant indicated that pursuant to Art. 107 § 4a of the CC there was a seizure of the conviction, and also pointed out that he no longer appears on the National Criminal Register. Moreover, the complainant indicated that he was currently studying internal security at the University of Higher Education [...] and that he would like to associate his work with the uniformed service, therefore he would like to enjoy an impeccable reputation in the eyes of the law. In a letter of [...] January 2017 - [...] (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 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 and Art. 51 sec. 5 of the Constitution of the Republic of Poland, which refers to specific regulations in terms of the principles and procedure for collecting and disclosing information about a person. In addition, the letter in question clearly indicated that the legal act specifying the principles and procedure for collecting and sharing information, including personal data, is the Police Act, in particular Art. 20 paragraph 2a. The complainant was also informed about the different procedure and rules for processing information in the KSIP and KRK and that, apart from the exceptions set out in the Acts, the KSIP collection is 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. The letter also referred to the provisions of the Regulation of the Minister of the Interior and Administration of July 21, 2016 on the processing of information by the Police, including, in particular, the premises for assessing the usefulness of data specified in § 29 para. 1 of this Regulation. It was also explained to the complainant that the fact that his personal data was processed by 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 pointed out that the Police processed the complainant's personal data necessary for the performance of its statutory tasks on the basis, to the extent and for the purpose specified in the provisions cited above. At the same time, the Commandant indicated that after [...] January 2017 the complainant did not submit any further requests to remove personal data from the KSIP.

The President of the Office for Personal Data Protection informed the Complainant and the Police Commander in Chief in letters of [...] September 2018 about conducting 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.

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, on 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 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 in the District Court in B., under file number [...], criminal proceedings were conducted in the case of an act pursuant to Art. 178a § 1 of the CC against the Complainant ended with a conviction. On the day the complaint was lodged with the Bureau of the Inspector General for Personal Data Protection, the conviction was already seized. In the content of the complaint, the complainant argued that despite a request to the Police Commander in Chief of the Police on [...] January 2017 to remove his personal data from the KSIP, this request was not accepted, therefore his data are still processed in the indicated filing system, and therefore The applicant cannot fully exercise his right to seize a 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 Register. 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 [...] May 2017, this right is not prejudiced due to the further processing of the data about the person committing the crime in the KSIP, because the information at the disposal of 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 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. 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 [...] May 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 case, i.e. in 2012, and additionally in connection with the Complainant's request to remove his personal data from the KSIP file, as well as in connection with the application submitted to the Inspector General for Personal Data Protection regarding the deletion of data from the KSIP.

In the case under examination, one should also take into account the provisions of the Regulation 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), which replaced the Regulation of the Minister of the Interior of July 21, 2016. on the processing of information by the Police, in force at the time of initiation of administrative proceedings before the Inspector General for Personal Data Protection. § 4 of the

ordinance of 23 August 2018 defines the procedure for collecting information, including personal data, as well as procedures ensuring the collection, collection, obtaining of information and organization of the files in a way that allows for the control of access to the files and supervision over the processing of information. At the same time, according to § 27 sec. 1 of the Regulation, access to the indicated data is strictly regulated, which means that it is limited to the authorized persons indicated in this provision. Moreover, in accordance with para. 2 of this provision, information, including personal data, collected in data files is made available only to authorized persons, which at the same time proves, as mentioned above, the non-widespread nature of this collection, which is used to perform the statutory tasks of the Police.

Pursuant to § 10 of the above-mentioned regulation to perform activities in the field of downloading, obtaining, collecting, checking, processing and using information, including personal data, referred to in art. 20 paragraph 2a points 1-6, sec. 2ac and paragraph. 2b of the Police Act, the National Police Information System (KSIP) is maintained in the Police, which is a set of data files processed in ICT systems (section 1). 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 and protecting human life and health (paragraph 2). 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 prejudice 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).

Considering the above, it should be stated that the Complainant's personal data was obtained by the Police authorities in a legal manner and is also processed by them in the KSIP. The Police authorities assess the usefulness of the collected data, which implies that the complainant's data will be kept in the National Police Register. On the other hand, if the data about a person contained in the file becomes useless for preventive, evidence or detection purposes, the Police authority may decide to remove them as a result of the assessment referred to in § 29 of the Regulation of the Minister of Internal Affairs and Administration of 23 August 2018. on the processing of information by the Police. In view of the above, it should be stated that the manner of the Police's conduct in the discussed scope does not raise any doubts, and the applicant's request does not deserve to be granted.

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 CAP, the party has the right to submit an application for reconsideration of the case within 14 days from the date of delivery of the decision to the party. If a party does not want to exercise the right to submit an application for reconsideration of the case, he has the right to lodge a complaint against the decision with the Provincial Administrative Court in Warsaw within 30 days from the date of its delivery to the party. The complaint is submitted through the Inspector General for Personal Data Protection. 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.

2019-03-29