

THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 19

May

2020

DECISION

ZKE.440.53.2019

Based on Article. 104 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended) and pursuant to Art. 160 sec. 1 and 2 of the Personal Data Protection Act of May 10, 2018 (Journal of Laws of 2019, item 1781) and art. 12 point 2, art. 22, 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. 6 sec. 1 lit. c) Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46 / EC (Journal UE L 119 of 04/05/2016, p. 1 and EU Official Journal L 127 of 23/05/2018, p. 2), in connection with Art. 105 paragraph. 4 and art. 105a paragraph. 1, 3, 4 and 5 of the Banking Law of August 29, 1997 (Journal of Laws of 2019, item 2357, as amended), following administrative proceedings regarding the complaint of Mr. WM, against the processing of his personal data by MSA , President of the Personal Data Protection Office,

refuses to accept the request

Justification

The President of the Personal Data Protection Office (formerly the Inspector General for Personal Data Protection) received a complaint from Mr. W. M. (hereinafter also referred to as the "Complainant") about the processing of his personal data by M. S.A. (hereinafter also referred to as "the Bank"), in particular making them available to unauthorized persons.

In the content of the complaint, the complainant informed about the possibility of leakage of his personal data concerning the balance of his bank account and incoming bank transfers and the high probability that the Bank's employee informed the "former" colleague of the complainant and partner, Mr. M. Ž. about receiving a transfer important for the Complainant. The complainant indicated that he did not know the Bank's employee who had provided his personal data, but that he was acquainted with Mr. M. Ž. Acquiring by Mr. M. Ž. data on the transfer resulted in a change in business decisions, which

exposed the Complainant to a loss of approx. PLN [...].

The complainant requested that the employee be found guilty of unauthorized disclosure of his personal data.

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

The Bank obtained the complainant's personal data on [...] October 2011 in connection with the conclusion of the agreement with the Complainant on maintaining bank savings and checking accounts No. [...].

The scope of personal data processed by the Bank includes: name and surname, date and place of birth, parents' names, mother's maiden name, sex, marital status, registered address, PESEL number, series and number of ID document, customer number, bank contract number, postal address electronic, mobile phone number, turnover on the bank account.

The bank explained that pursuant to Art. 104 sec. 1 of the Act of August 29, 1997 Banking Law (Journal of Laws of 2019, item 2357, as amended), the obligation to maintain banking secrecy applies not only to banks but also to their employees and persons through whom banks perform banking activities. This means that a bank secret is a kind of professional secret and anyone who comes into its possession is obliged not to disclose it. All employees of the Bank are obliged to maintain banking secrecy and inform them of their criminal liability in the event of its disclosure.

According to the Bank's explanations, on the basis of the Bank's analysis of the possibility of disclosing bank secret personal data concerning the Complainant, no employee of the Bank was identified who would disclose the data on the applicant's bank accounts to Mr. M. Ž. The analysis also showed that the Complainant's data had not been disclosed by the Bank's employee to any other unauthorized person.

The complainant on [...] August 2016 reported to the Bank unauthorized access to his account and disclosure of information about the account balance to an unauthorized person by submitting a complaint No. [...] to the Bank. The Bank replied to the Complainant to the above-mentioned the complaint explaining that Ban did not find any unauthorized access to his account, nor did he find disclosure of information about the status of this account to an unauthorized person. Moreover, the Bank informed the Complainant that the Bank's employee was not acting on his own behalf, but as a representative of the Bank. The Bank also informed the Complainant about the right to appeal against the above-mentioned Bank decision. Such an appeal was not received by the Bank.

After analyzing the evidence collected in the case, the President of the Office for Personal Data Protection states as follows.

On May 25, 2018, the provisions of the Act of May 10, 2018 on the protection of personal data entered into force (Journal of Laws of 2019, item 1781), hereinafter also: "Act on the Protection of Personal Data of 2018 r. "

Pursuant to Art. 160 sec. 1-3 of the Act on the Protection of Personal Data of 2018, proceedings conducted by the Inspector General for Personal Data Protection, initiated and not completed before the date of entry into force of this Act, are conducted by the President of the Office for Personal Data Protection on the basis of the Act of August 29, 1997 on protection of personal data (Journal of Laws of 2016, item 922, as amended), hereinafter also referred to as "the Personal Data Protection Act of 1997", in accordance with the principles set out in the Act of June 14, 1960, Code administrative proceedings (Journal of Laws of 2020, item 256, as amended). At the same time, the activities performed in the proceedings initiated and not completed before the date of entry into force of the provisions of the Act on the Protection of Personal Data of 2018 remain effective.

From May 25, 2018, also 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, and repealing Directive 95 / 46 / EC (general regulation on the protection of personal data) (Journal of Laws UE L 119 of 04.05.2016, p. 1 and Journal of Laws UE L 127 of 23.05.2018, p. 2), hereinafter referred to as the "Regulation 2016/679 ".

Pursuant to Art. 57 sec. 1 of Regulation 2016/679, without prejudice to other tasks specified under this regulation, each supervisory authority on its territory monitors and enforces the application of this regulation (point a) and considers complaints submitted by the data subject or by - in accordance with Art. 80 by Regulation 2016/679 - the entity, organization or association, to the extent appropriate, conducts proceedings on these complaints and informs the complainant about the progress and results of these proceedings within a reasonable time (point f).

It should be noted here that the President of the Personal Data Protection Office, when issuing an administrative decision, is obliged to decide on the basis of the actual state of affairs at the time of issuing this decision. As the doctrine points out, "the public administration body assesses the facts of the case according to the moment of issuing the administrative decision. This rule also applies to the assessment of the legal status of the case, which means that a public administration authority issues an administrative decision based on the provisions of law in force at the time of its issuance (...). Settlement in administrative proceedings consists in applying the applicable law to the established factual state of an administrative case. In this way, the public administration body implements the goal of administrative proceedings, which is the implementation of the applicable legal norm in the field of administrative and legal relations, when such relations require it "(Commentary to the Act of June 14,

1960, Code of Administrative Procedure, M. Jaśkowska, A . Wróbel, Lex., El / 2012). Also the Supreme Administrative Court - in the judgment of May 7, 2008 in case no. Act I OSK 761/07 stated that: "when examining the legality of the processing of personal data, GIODO is obliged to determine whether the data of a specific entity are processed as at the date of issuing the decision on the matter and whether it is done in a legal manner".

Regulation 2016/679 constitutes provisions on the protection of natural persons with regard to the processing of personal data and provisions on the free movement of personal data, and protects the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data (Article 1 (1) and (2) of Regulation 2016 / 679). This issue was adequately regulated by Art. 2 clause 1 of the Act on the Protection of Personal Data of 1997. In the light of the provisions of the above-mentioned legal act, the processing of personal data is authorized when any of the conditions listed in Art. 6 sec. 1 of Regulation 2016/679 (previously Article 23 (1) of the Personal Data Protection Act of 1997). These conditions apply to all forms of data processing listed in art. 4 point 2 of Regulation 2016/679 (formerly Article 7 point 2 of the Personal Data Protection Act of 1997), including, in particular, their disclosure. These conditions are also equal to each other, which means that for the legality of the data processing process, it is sufficient to meet one of them.

The legal act regulating in detail the processing of personal data of bank customers is primarily the Banking Law. Therefore, the assessment of the processing of the Complainant's personal data in connection with the contract between him and the Bank should be made in conjunction with the provisions of this Act.

Pursuant to Art. 104 sec. 1 of the Banking Law, the Bank, its employees and persons through whom the bank performs banking activities, are obliged to maintain banking secrecy, which includes all information regarding banking activities obtained during negotiations, during the conclusion and performance of the contract, on the basis of which bank performs this activity. It should be emphasized here that the responsibility of the personal data controller for improper processing of personal data extends not only to his personal behavior towards this information, but also to the behavior of his employees. The Supreme Administrative Court in its judgment of April 4, 2003 (file number II SA 2935/02) stated that "the controller is responsible (...) for the actions of its employees in breach of the Act on the Protection of Personal Data. At the same time, he cannot exculpate himself, pursuant to Art. 26, that he exercised special care to protect these data".

Therefore, referring to the Complainant's demand regarding the legality of the currently conducted processing of his personal data by the Bank, it should be noted that the Complainant's personal data are processed by the Bank in the scope of

information constituting banking secrecy in accordance with Art. 105 paragraph. 4 of the Banking Law. Pursuant to this provision, banks may, together with banking chambers of commerce, establish institutions authorized to collect, process and make available to: banks - information constituting banking secrecy to the extent that this information is needed in connection with the performance of banking activities and in connection with the application of internal methods and other methods and models referred to in Part Three of Regulation No 575/2013; other institutions legally authorized to grant loans - information constituting banking secrecy to the extent to which such information is necessary in connection with granting loans, cash advances, bank guarantees and sureties; credit institutions - information constituting banking secrecy to the extent necessary to assess the consumer's creditworthiness, as referred to in art. 9 of the Act of 12 May 2011 on consumer credit; lending institutions and entities referred to in art. 59d of the Act of 12 May 2011 on consumer credit - on the basis of reciprocity, information constituting respectively banking secrecy and information provided by loan institutions and entities referred to in art. 59d of the Act of 12 May 2011 on consumer credit, to the extent necessary to assess the consumer's creditworthiness, as referred to in art. 9 of this Act, and credit risk analysis.

The Bank is currently processing the Complainant's personal data in connection with the conclusion of an agreement with the Complainant on maintaining bank savings and checking accounts No. [...].

The President of the Personal Data Protection Office, examining the basis for disclosing the Complainant's personal data, concluded that in the above-described circumstances of the case in question, there were no grounds for making an order against the Bank.

Regarding the Complainant's claim that an employee of the Bank disclosed his personal data to an unauthorized person, it should first be pointed out that the President of the Data Protection Office does not have any legal instruments that would make it possible to offset the effects of the unauthorized disclosure of his personal data, in the opinion of the Complainant.

This disclosure is an irreversible fact in the sense that it is not possible to lead to the situation which would have occurred had the infringement not taken place. Moreover, the condition for issuing a decision by the authority is the existence of a state of violation of the right to personal data protection at the time of issuing the administrative decision. However, in the case at hand, if, in the opinion of the Complainant, the disclosure was incidental, there are no grounds to assume that the actions questioned by the Complainant would be repeated in the past. The President of the Office is not authorized to issue an order in this case concerning possible unauthorized processing (disclosure) of the Complainant's personal data in the future. It should be

emphasized that an administrative decision is a specific and individual act and always concerns a strictly defined, established and current state of affairs at the time of the ruling. The President of the Office is not authorized to issue a decision with regard to future and often hypothetical situations.

It should be pointed out, however, that if, in the opinion of the complainant, a prohibited act was committed to his detriment, the complainant may apply directly to the law enforcement authorities with an appropriate notification about the possibility of committing a crime and seek protection of his rights through proceedings before the law enforcement authorities and then before a common court.

Notwithstanding the foregoing, I would like to inform you that if, in the Complainant's opinion, his personal rights were infringed, which pursuant to Art. 23 of the Act of 23 April 1964 Civil Code (Journal of Laws of 2018, item 1025, as amended), in particular health, freedom, honor, freedom of conscience, name or pseudonym, image, secret of correspondence, inviolability housing, scientific, artistic, inventive and rationalizing works, he may pursue his claims in this respect by means of a civil action brought before the locally competent common court. According to the content of Art. 24 § 1 and 2 above of the act, the person whose personal interest is threatened by someone else's action, may demand that such action be discontinued, unless it is not unlawful. In the event of an infringement, he may also require the person who committed the infringement to perform the actions necessary to remove its effects, in particular, to submit a declaration of appropriate content and in an appropriate form.

Taking into account the above, it should be concluded that there was no reason for the President of the Personal Data Protection Office to issue a decision ordering the restoration of the lawful state, therefore it is not justified to issue any of the orders referred to in Art. 18 of the Personal Data Protection Act of 1997 and in Art. 58 of the Regulation 2016/679.

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 Civil Procedure of the decision, the party has the right to submit an application for reconsideration of the case within 14 days from the date of its delivery 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 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.

2021-02-17