THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 21

April

2021

DECISION

DKE.440.28.2021

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2018, item 2096, as amended) and pursuant to 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) in connection with joke. 12 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 with Art. 57 sec. 1 lit. a) and f) Regulation of the European Parliament and the EU Council 2016/679 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 (Journal of Laws UE L 119 of 04/05/2016) , page 1 and Journal of Laws UE L 127 of 23/05/2018, page 1, as amended), after conducting administrative proceedings regarding the complaint of Mr. PJ about irregularities in the processing of his personal data by the Supreme Administrative Court, President of the Office Personal Data Protection:

refuses to accept the request.

JUSTIFICATION

On [...] July 2016, the Office of the Inspector General for Personal Data Protection (now the Office for Personal Data Protection) received a complaint from PJ, hereinafter also referred to as the "Complainant", about irregularities in the processing of his personal data by the Supreme Administrative Court, hereinafter referred to as also the "Company".

The content of the complaint shows that it is related to a hacking attack on the website [...], as a result of which the complainant's personal data in the form of a telephone number was made public on the Internet. In the content of the complaint, the complainant indicated that the Company did not provide him with information on (quoted) ,, (...) what personal data was or still is in the personal data file of N. S.A. and (...) which of these data were or still are processed by N. S.A. or cooperating and affiliated entities ”. Considering the breach, the Complainant requested the initiation of administrative proceedings against the Company in order to verify the manner of securing his personal data and to determine in detail how

unauthorized persons had access to the data collected by the Company.

On the basis of the evidence gathered in the case at hand, the following facts were established.

1. On [...] July 2016, the Complainant received a text message from the Company, containing information that unauthorized third parties had obtained his [...] telephone number from the Company's data files and that it was made public on the Internet.

2. In connection with the information received, the Complainant [...] sent an e-mail to the Company on [...] these data were or are still processed by it, an indication of how the Company protects the Complainant's personal data against third party access and an explanation of how third parties came into their possession. The complainant requested contact with the Information Security Administrator, hereinafter referred to as "ABI", regarding the breach of his data. Due to the fact that the Complainant's telephone number is used for banking transactions, as authorization codes from the bank come to that number, the Complainant requested an indication of the possibility of securing the confidentiality of the transmitted data in digital form.

3. In response to the above message, an employee of the Company's Technical Service Center sent an e-mail on [...] July 2016, in which he informed the Complainant that his personal data regarding the telephone number had been breached in connection with a hacking attack on the website [...]. The breach concerned only the data from the application form, ie the complainant's telephone number, contained on the [...] website, and not from the Company's systems. The company informed that all other personal data of the Complainant were safe. She pointed out that in connection with the sending of an appropriate message on the breach of personal data to persons, the need for ABI to contact them was eliminated. The company informed that, inter alia, takes steps to remove data from the network and cooperates with law enforcement authorities. Regarding the request to indicate the possibility of securing the confidentiality of the data sent in digital form, the Company informed the Complainant that the Complainant should contact the bank to determine whether it is dangerous for his account to have his telephone number by third parties without any other data.

5. In an e-mail of [...] July 2016, the Complainant, in view of the information received from the Company that ABI did not need to contact him, again demanded an explanation of how his personal data was secured in the Company's records. He also requested an indication of the method of encryption of his personal data and a manner of compensation for the infringement of his personal rights.

6. As it results from the letter of [...] August 2016 (ref. Mark: [...]) attached to the complaint, the Company informed the Complainant that, inter alia, processes his personal data in the field of e-mail address and telephone number for the purpose of

archiving and conducting proceedings before the Inspector General for Personal Data Protection, the Prosecutor's Office (the Company has reported a crime) and the President of the Office of Electronic Communications. She pointed out that she had been processing data since [...] November 2014 and obtained them directly from the Complainant in connection with completing the offer form, and the data is processed both in paper and electronic form. The company informed the Complainant that [...] July 2016, around g .: [...] as a result of a hacking attack, the personal data of the Company's subscribers and its potential customers who are natural persons were breached. As a result of the attack, the hackers gained access to user data provided via the website [...], including the Complainant's personal data. Such unlawfully obtained data was then published on the Internet. At the same time, the Company informed the Complainant that it uses technical and organizational measures in accordance with the requirements set out in the Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on the documentation of personal data processing and technical and organizational conditions to be met by devices and IT systems used for processing personal data (Journal of Laws No. 100, item 124). These measures ensure protection of the processed personal data appropriate to the threats and categories of data protected, and in particular, they protect the data against unauthorized disclosure, removal by an unauthorized person, processing in violation of the Act, as well as alteration, loss, damage or destruction.

7. In a letter of [...] September 2020, the Company informed the President of the Personal Data Protection Office that the Complainant's personal data had been obtained on the basis of his consent, ie based on the premise of Art. 23 sec. 1 point 1 of the Act of August 29, 1997 on the protection of personal data - Journal Of Laws of 2016, item 922, hereinafter also referred to as the "1997 Act". In order to use the services of the Company, the complainant provided his telephone number via the contact form available on the website [...]. The company indicated that it processes the complainant's personal data in the following scope: name, surname, address, e-mail address and telephone number. The data is processed on the basis of art. 6 sec. 1 lit. f of the Regulation of the European Parliament and the EU Council 2016/679 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 (Journal of Laws EU L 119 of 04/05/2016, p. 1) and Journal of Laws UE L 127 of 23/05/2018, p. 1, as amended), hereinafter also referred to as "GDPR", for the purposes of evidence and defense of the administrator's rights in connection with correspondence with the Complainant, as well as in connection with with explanatory proceedings before GIODO. The company explained that [...] in July 2016, there was a hacking attack on the website [...] as a result of which cybercriminals gained access to the data of potential customers

and made it available on the Internet. Due to the fact that the Complainant provided his telephone number via the contact form - the perpetrators came into possession of this number. The company informed that it reported the infringement to GIODO [...] July 2016, and [...] July 2016 sent supplementary reports. The company protects the complainant's personal data against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical measures, in particular related to access control and monitoring, backup management, protection against unauthorized access, as well as organizational measures, in particular related to the implementation of appropriate policies, procedures and instructions.

8. In connection with the hacking attack on the website [...], the Inspector General for Personal Data Protection carried out a control of the compliance of personal data processing with the provisions on the protection of personal data (reference number [...]. remedial actions taken to eliminate similar events in the future, the Company does not violate the provisions on the protection of personal data.

1) joining the program of the Ministry of Digitization in the field of responding to cybersecurity incidents called [...] called [...],

2) starting the implementation of the solution provided by the Internal Security Agency [...] called [...] consisting, inter alia, monitoring traffic from the address of N., including to the website with the address [...] and cooperation with the Internal Security Agency was established,

3) updating documents named: "Personal data security policy N. S.A." and "Instructions for managing the IT system of N. S.A.",

4) appointment of the Incident Reporting Team [...], keeping the "Register of violations" and launching a dedicated e-mail [...] where incident reports are received,

5) applying a solution [...] consisting in scanning the available services of N. located in the network of N.,

6) launching a dedicated website [...] with the content of the data breach message and an e-mail address [...] at which the Company could be contacted to provide information on what data was made public,

7) development of a "Guide" containing suggestions related to minimizing the effects of a personal data breach that took place as a result of a hacking attack on the website [...],

8) remodeling the system [...],

Moreover, during the control procedure it was found that the audit carried out for the Company by P. Sp. z o.o., in terms of the [...] vulnerability of the website to a hacker attack, he showed that the error in the code structure of the above-mentioned the

website that led to the data leak was not on the side of the Company.

After reviewing the entirety of the evidence collected in the case, the President of the Office for Personal Data Protection considered the following.

At the outset, it should be noted that on May 25, 2018, with the entry into force of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2018, item 1000, as amended), the Office The Inspector General for Personal Data Protection has become the Office for Personal Data Protection. 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 (Journal of Laws of 2016, item 922, as amended), hereinafter also referred to as the "1997 Act", in accordance with the principles set out in the Code of Administrative Procedure (Journal of Laws of 2017, item 1257, as amended), hereinafter also referred to as "Kpa ". All actions taken by the Inspector General for Personal Data Protection, hereinafter also referred to as "GIODO", before May 25, 2018, remain effective (Article 160, paragraph 1 and paragraph 2 of the Act of May 10, 2018 on the protection of personal data) .

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 / WE (Journal of Laws UE L 119 of 04.05.2016, p. 1 as amended), hereinafter referred to as "GDPR".

At the time when the event described by the applicant took place, the Act of 1997 was in force. the act defined the rules of conduct in the processing of personal data and the rights of natural persons whose data is or may be processed in data files (Article 2 (1) of the Act).

Pursuant to Art. 36 of the Act of 1997, the data controller is obliged to apply technical and organizational measures ensuring the protection of personal data being processed, appropriate to the threats and categories of data protected, and in particular should protect the data against unauthorized disclosure, removal by an unauthorized person, processing in violation of the Act as well as alteration, loss, damage or destruction (section 1). In addition, the data controller keeps documentation describing the method of data processing and the measures referred to in para. 1 (paragraph 2).

The above provision shows that one of the basic obligations of the controller is the obligation to apply technical and organizational measures ensuring the protection of personal data being processed, in particular securing the data against disclosure to unauthorized persons.

It should be emphasized that pursuant to Art. 18 sec. 1 point 1 of the Act of 1997, in the event of a breach of the provisions on the protection of personal data, GIODO, ex officio or at the request of the person concerned, by means of an administrative decision, orders the restoration of the legal status, and in particular 1) removal of the deficiencies; 2) supplementing, updating, rectifying, disclosing or not disclosing personal data; 3) application of additional security measures for the collected personal data; 4) suspension of the transfer of personal data to a third country; 5) securing data or transferring them to other entities; 6) deletion of personal data. At the same time, it should be pointed out that the assessment of the grounds for the application of Art. 18 sec. 1 of the Act of 1997 is justified and necessary only insofar as the Company would not remedy the deficiencies in data processing.

In connection with the Complainant's allegation that the Company did not fulfill the disclosure obligation, it should be noted that the Company fulfilled this obligation towards the Complainant in a letter of [...] August 2016 (ref. Mark: [...], i.e. after the submission by him a complaint.

However, when referring to the Complainant's request for information on the method of securing his data by the Company (including the encryption method used), it should be noted that such information is confidential information included in the internal documentation, and its disclosure poses a threat to the proper protection of personal data. Familiarizing third parties with the details of data security solutions and the architecture of systems used for their processing may make it easier for cybercriminals to interfere with these systems (e.g. stopping work or uncontrolled modification of the system, taking over, distorting or deleting data contained in it) by bypassing the applied safeguards or their "break". This information is made available only to a limited group of people in connection with the tasks entrusted to them by the data controller. These persons are obliged to keep them secret.

The findings made in the course of these proceedings showed that the infringement described by the Complainant, consisting in unauthorized access to his personal data in the form of a telephone number, as a result of a hacking attack on the website [...], had in fact taken place. Nevertheless, the decisive factor for the resolution in this case is the fact that, in the opinion of the President of the Office, the Company has taken appropriate remedial measures to eliminate such events in the future. This assessment is justified by the control of the compliance of personal data processing with the provisions on the protection of personal data carried out by the Company by the General Inspector for Personal Data Protection, which showed that the Company does not violate the provisions on the protection of personal data in the field of personal data protection.

Due to the above, the President of the Personal Data Protection Office had no grounds to apply the order under Art. 18 of the 1997 Act

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 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 lodged through the President of the Personal Data Protection Office (address: ul. Stawki 2, 00-193 Warsaw). The entry fee for the complaint is PLN 200.00. The party has the right to apply for the right to assistance, including exemption from court costs.

2021-07-15