THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 07

of December

2018

DECISION

ZSZZS.440.780.2018

DECISION

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2017, item 1257, as amended), 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) in connection with joke. 18 sec. 1 of the Act of August 29, 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922) and 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 (Official Journal of the European Union European, L 119, May 4, 2016), after conducting administrative proceedings regarding the complaint of Mr. DS, about the processing of his personal data, by the Kindergarten based in G., President of the Office for Personal Data Protection

refuses to accept the request.

Justification

The Office of the Inspector General for Personal Data Protection received a complaint from Mr. D.S, hereinafter referred to as the Complainant, about the processing of his personal data by the Kindergarten based in G., hereinafter also referred to as the Kindergarten.

In the content of the complaint, the complainant indicated that his personal data were not properly secured against disclosure to unauthorized persons and processing by unauthorized persons. He submitted that his personal files were kept in an unsecured room and that his personal data was on the hard drive of an unsecured computer. Moreover, the information in his possession shows that the Headmaster of the Kindergarten handed over for disposal computers containing his personal data on the hard drive. The complainant also pointed out that the Headmaster of the Kindergarten processes personal data of employees contained in copies (scans) of identity cards.

In the course of the administrative proceedings, the President of the Personal Data Protection Office established the following facts.

In the period from [...] September 2017 to [...] November 2017, the complainant was employed under an employment contract in a Kindergarten based in G .. Therefore, his personal data was processed by the employer to the extent and for the purposes resulting from from the Act of June 26, 1974, the Labor Code (Journal of Laws 2018.917, i.e. for the purposes necessary for the employment of an employee, documentation of the employment process, determination of the rights and obligations of the employee.

Due to the termination of the employment relationship, the documents containing the complainant's personal data were deposited in the archives of the Kindergarten based in G. They are kept by the above-mentioned the facility, i.e. by the former employer, to the extent and purpose consistent with the provisions of the labor law in a room without windows, which is locked. The key is in the safe, to which only the director of this facility has access.

The complainant's personal data regarding his private telephone number and e-mail address are not currently processed by the Kindergarten. The explanations submitted with the letter of [...] April 2018 show that the Complainant voluntarily provided his private telephone number and was the first to send a message to the Director from his private e-mail address.

The Headmaster of the Kindergarten does not have scans of employees' ID cards and their personal data contained in the documents are stored in personal files in a metal safe, to which only the Director of this facility has access. The employees' telephone numbers or their e-mail addresses are not stored in the personal files.

The desktop computer is located in the office of the Kindergarten Principal, whose doors are locked and the windows have bars. The computer has an access password and anti-virus software. On the other hand, the computer sent for recycling did not contain a hard drive. The facility has a wireless internet network protected by a password that is known only to the Headmaster of the Kindergarten.

The Headmaster of the Kindergarten does not use a private computer for business purposes and does not save any data regarding this facility on electronic media.

In the Kindergarten in G., on [...] January 2018, the documentation describing the organizational and technical measures to protect the personal data processed was approved.

In this factual state of the case, the President of the Office considered the following.

First of all, it should be noted that on the date of entry into force of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2018, item 1000) pursuant to Art. 166 paragraph. 1 of this Act, the Inspector General for Personal Data Protection became the President of the Personal Data Protection Office, and pursuant to Art. 167 paragraph. 1 of the same act, the Office of the Inspector General for Personal Data Protection became the Office for Personal Data Protection. On the other hand, pursuant to Art. 160 of the same Act, 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 (section 1) on the basis 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 PDA, in accordance with the principles set out in the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2017, item 1257) (section 2), hereinafter also referred to as Kpa The activities performed in the proceedings referred to in para. 1 remain effective (section 3).

In addition, it is necessary to emphasize that the President of the Personal Data Protection Office, when issuing an administrative decision, is obliged to settle the case based on the actual state of affairs at the time of issuing this decision. As argued in the doctrine, "a 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).

Moreover, in the judgment of May 7, 2008 in the case with reference number Act I OSK 761/07, the Supreme Administrative Court stated that "when examining [...] the legality of personal data processing, GIODO is obliged to determine whether, as at the date of issuing the decision in the case, the data of a specific entity are processed and whether it is done in a lawful manner ".

Referring the above to the established facts, it should be emphasized that the decisive factor for the decision that must be issued in the present case is the fact that the processing of the complainant's personal data began during the period when the Act of August 29, 1997 on data protection was in force. personnel, but is now being continued. Therefore, it should be stated

that the relevant provisions in this case are the application of the provisions in force at the time of issuing the decision on the case, i.e. 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 the repeal of Directive 95/46 / EC (Official Journal of the European Union, L 119, 4 May 2016), hereinafter also referred to as the GDPR, because the President of the Personal Data Protection Office must assess whether the questioned process of personal data processing as at the date of issue the administrative decision complies with the law.

The prerequisites for the legality of the processing of personal data were previously set out in Art. 23 sec. 1 of the Act on Personal Data Protection, according to which the processing of data was allowed only if: 1) the data subject consents to it, unless it concerns the deletion of data relating to him; 2) it is necessary to exercise the right or fulfill an obligation resulting from a legal provision; 3) it is necessary for the performance of the contract when the data subject is a party to it or when it is necessary to take action before concluding the contract at the request of the data subject; 4) it is necessary to perform tasks specified by law for the public good; 5) it is necessary to fulfill legally justified purposes carried out by data controllers or data recipients, and the processing does not violate the rights and freedoms of the data subject. Each of the above conditions was independent and autonomous, which means that the fulfillment of at least one of them determined the legality of the processing of personal data.

Referring to the current legal status, reference should be made to the equivalent of Art. 23 sec. 1 of the 1997 Act currently in force - Art. 6 sec. 1 of the GDPR, which defines the conditions for the lawfulness of data processing. In accordance with the above-mentioned provision, the processing of personal data is lawful only in cases where - and to the extent that - at least one of the following conditions is met: the data subject has consented to the processing of his personal data in one or more more than one specific purpose (point a); processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (point b); processing is necessary to fulfill the legal obligation incumbent on the controller (letter c); processing is necessary to protect the vital interests of the data subject or another natural person (point d); processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (s); processing is necessary for the purposes of the legitimate interests pursued by the administrator or by a third party, except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data,

in particular when the data subject is a child (f). In addition, recital 155 of the GDPR indicates that the law of the Member State may provide for specific provisions on the processing of personal data of employees in connection with employment, in particular the conditions under which personal data in connection with employment may be processed with the consent of the employee for the purposes of the recruitment procedure, performance of the contract employment, including the performance of obligations specified in regulations or collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work and for the purposes of individual or collective exercise of rights and benefits related to employment, and also for the purposes of termination of employment.

Moving on to the national legislation, it should be noted that in accordance with the wording of Art. 221 of the Act of June 26, 1974, the Labor Code (Journal of Laws of 2018, item 917) (hereinafter referred to as the Labor Code), the employer has the right to request the person applying for employment to provide personal data including:) and surname; 2) parents' names; 3) date of birth; 4) place of residence (correspondence address); 5) education; 6) the course of previous employment (§1). The employer also has the right to request the employee to provide, regardless of the personal data referred to in § 1, also: 1) other personal data of the employee; 2) PESEL number (§2), as well as personal data other than those specified in § 1 and 2, if the obligation to provide them results from separate regulations (§ 4). To the extent not regulated in § 1-4, the provisions on the protection of personal data (§ 5) shall apply to the personal data referred to in these provisions. By virtue of Art. 94 of the Labor Code is obliged to keep documentation in matters related to the employment relationship and personal files of employees (point 9a), as well as to store documentation in matters related to the employment relationship and personal files of employees in conditions that are not likely to be damaged or destroyed (9b). Pursuant to § 6 sec. 1 of the Regulation of the Minister of Labor and Social Policy of 28 May 1996 on the scope of keeping documentation by employers in matters related to the employment relationship and the manner of keeping personal files of an employee (Journal of Laws of 2017, item 894) (hereinafter referred to as also the Regulation), the employer establishes and maintains the employee's personal files, which include, inter alia, documents related to the termination of employment (§ 6 (3) of the Regulation).

In turn, according to Art. 125a paragraph. 4 of the Act of 17 December 1998 on pensions from the Social Insurance Fund (Journal of Laws of 2018, item 1270) (hereinafter also referred to as the Act on pensions and disability pensions), the contribution payer is obliged to keep payrolls, payroll cards or other evidence on the basis of which the basis for the calculation of the old-age or disability pension is determined, for a period of 50 years from the date of termination of work by the insured

person with a given payer. The same 50-year retention period applies to personal files, which results from 51 par. 1 of the Act of July 14, 1983 on the national archival resource and archives (Journal of Laws of 2016, item 1506, t. J.).

Regarding the issue of securing personal data, it should be noted that pursuant to Art. 36 sec. 1 u.o.d.o. the data controller was 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 change, loss, damage or destruction. In addition, the data controller was obliged to keep documentation describing the method of data processing and the above-mentioned technical and organizational measures, which were specified in detail in the Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on personal data processing documentation and technical and organizational conditions to be met by devices and IT systems used to process personal data (Journal U. of 2004, No. 100, item 1024).

However, according to Art. 5 sec. 1 letter f) of the GDPR, personal data must be processed in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by appropriate technical or organizational measures. Moreover, pursuant to Art. 25 of the GDPR, taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probabilities and severity resulting from processing, the controller - both when determining the methods of processing and during the processing itself - implements appropriate technical and organizational measures, such as pseudonymisation, designed to effectively implement data protection principles, such as data minimization, and to provide the processing with the necessary safeguards to meet the requirements of this Regulation and to protect the rights of data subjects.

Taking into account the above factual and legal status, it should be noted that the Kindergarten is currently processing the Complainant's personal data for the purposes and scope specified in the applicable legal provisions regarding the storage of documentation related to the employment relationship, which meets the criteria of the legality of the processing of personal data specified in art. 6 sec. 1 lit. c) GDPR, and previously in art. 23 sec. 1 point 2 u.o.d.o. As for the Complainant's personal data in the form of a private telephone number and e-mail address, the explanations provided by the Kindergarten in the letter of [...] April 2018 show that the data were provided by the Complainant voluntarily and are currently not processed. The

complainant, being an employee of the Kindergarten, was the first to send an e-mail to the e-mail addresses of the Headmaster of the Kindergarten and the Kindergarten, which contained a comparison of the installation monitoring of the facility with the costs of employing caretakers and a proposal to establish an access code to the Kindergarten. Therefore, the above-mentioned the complainant's personal data were processed by the Kindergarten in accordance with art. 23 (1) (5) of the Act An employer who is the administrator of personal data may process personal data that has not been requested from the employee, also when it is necessary to fulfill legally justified purposes pursued by the data administrator or data recipients, and the processing does not violate the rights and freedoms of the data subject.

In addition, referring to the complaint of the Complainant regarding improper protection of personal data against disclosure to unauthorized persons, removal by an unauthorized person and processing in violation of the Act on the Protection of Personal Data, it should be noted that the documentation describing organizational and technical measures to protect the processed personal data was approved in the Kindergarten in G. . The above document contains a detailed description of the basic principles of the organization of work on personal files processed using traditional methods and in the IT system, expressed in the Security Policy and in the Instruction for the management of the IT system used to process personal data. In addition, the explanations of [...] February 2018 show, inter alia, that only the Headmaster of the Kindergarten has access to the personal data of employees contained in the documents. The stationary computer at the facility is located in a room protected against unauthorized access, has anti-virus software and an access password. The Headmaster of the Kindergarten has also established a password for the wireless Internet network, which is known only to him. Moreover, a computer that did not contain a hard disk was sent for disposal, and not, as the Complainant pointed out, a computer containing personal data on the hard disk.

Therefore, the above explanations do not confirm the alleged improper protection of personal data against unauthorized disclosure, removal by an unauthorized person and processing in violation of the Personal Data Protection Act, as alleged by the Complainant. In such a situation, the public administration body may consider the facts of the case under consideration as established only on the basis of undoubted evidence and may not limit itself to making it plausible, unless the provisions of the Administrative Procedure Code provide otherwise (e.g. Article 24 § 3 of the Code of Administrative Procedure). As stated by the Supreme Administrative Court in the judgment of 9 July 1999 (reference number III SA 5417/98), "the body conducting the proceedings must strive to establish the substantive truth and, according to its knowledge, experience and internal conviction,

assess the evidential value of individual evidence, proving one circumstance for other circumstances ”.

Given the above, it should be stated that in the course of the investigation, no improper data protection, unauthorized disclosure of the Complainant's personal data, as well as the processing of personal data in violation of the Personal Data Protection Act before May 25, 2018, and currently the GDPR, were not found. The explanations of the Kindergarten based in G. show that the complainant's personal data was not disclosed to unauthorized persons. Both the computer equipment of the facility and the personal data contained in the documents have been secured against unauthorized access. Due to the termination of the Complainant's employment relationship, his personal data is stored in accordance with applicable legal provisions in the archives of the Kindergarten, which is also protected against unauthorized disclosure of personal data contained therein. Thus, there is no evidence that would make it possible to establish a breach of the provisions on the protection of personal data. The applicant also failed to provide such evidence in the course of these proceedings. Therefore, there are no grounds for the issuance of a decision restoring lawfulness pursuant to Art. 18 sec. 1 u.o.d.o.

In this factual and legal state, the President of the Personal Data Protection Office adjudicated as in the sentence.

Based on Article. 127 § 3 of the Act of 14 June 1960, Code of Administrative Procedure (Journal of Laws of 2017, item 1257), the party has the right to submit an application for reconsideration of the case within 14 days from the date of delivery of this decision. If a party does not want to exercise the right to submit an application for reconsideration, 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 delivery of the decision to the party. The complaint is lodged through the President of the Personal Data Protection Office. The fee for the complaint is PLN 200 (say: two hundred zlotys). The party has the right to apply for the right to assistance, including exemption from court costs.

2019-04-26