THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 18

February

2020

DECISION

ZSZZS.440.768.2018

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 Art. 7 sec. 1 and 2, art. 60, art. 102 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) in connection with Art. 5 sec. 1 lit. c, art. 9 sec. 1, art. 58 sec. 2 lit. f, lit. g and lit. and with Art. 83 sec. 2 and 3, art. 83 sec. 5 lit. a, art. 83 sec. 7 of the Regulation of the European Parliament and of 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, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws of the EU L 119 of 04/05/2016, p. 1, with the amendment announced in the Official Journal of the European Union L 127 of 23/05/2018, p. 2), after the administrative procedure on collecting children's fingerprints for their biometric identification when they use the services of the school canteen by the Primary School in Gdańsk, for which the governing body is the City of Gdańsk, President of the Office for Personal Data Protection,

finding that the Primary School in Gdańsk infringed the provisions of Art. 5 sec. 1 lit. c and art. 9 sec. 1 of Regulation 2016/679 of the European Parliament and of the Council of the EU and of 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, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 04/05/2016, p. 1, with the amendment announced in the Official Journal of the European Union L 127 of 23/05/2018, p. 2), consisting in the processing of biometric data of children when they use the services of the school canteen:

orders Primary School No. 2 in Gdańsk to delete personal data in the scope of digitized information about the characteristic fingerprint points of the fingers of children using the school canteen services,

orders Primary School No. 2 in Gdańsk to cease collecting personal data in the field of digitized information about the characteristic fingerprint points of the fingers of children using the school canteen services,

imposes on Primary School No. 2 in Gdańsk a fine of PLN 20,000.00 (in words: twenty thousand zlotys) for the violation stated in this decision.

Justification

The Office for Personal Data Protection learned about irregularities in the processing of personal data of students of the Primary School in G., hereinafter referred to as the School, consisting in collecting fingerprints of children using the services of the school canteen. As a result of the above, an ex officio proceeding was initiated regarding irregularities in the processing of personal data by the School.

In the course of the proceedings conducted in this case, the President of the Personal Data Protection Office (hereinafter referred to as the President of the Personal Data Protection Office) established the following facts:

The school uses a biometric reader, called […], located at the entrance to the school canteen, which identifies children collecting meals in the school canteen to verify that payment for the day's meal has been made. The school obtains data based on the written consent of the parent (legal guardian).

The school has been using a biometric reader since [...] September 2015. In the 2018/2019 school year, 1247 students attended the School, of which 603 used a biometric reader and 2 students from an alternative identification system. In the 2019/2020 school year, 1,121 students attend the school, of which 680 students use a biometric reader, and 4 students use an alternative identification system.

According to the explanations of the School of [...] December 2018, the School does not have any collection containing children's fingerprints. The data related to the fingerprint reader is collected only in the reader itself in the form of a string of bytes. During the reading process, the reader compares whether there is an appropriate sequence of bytes, and if so, it sends only the position number to the program. A position number is assigned to a specific child.

Two persons have access to the data in the reader: the system administrator and the authorizing officer - authorized employees of the School.

According to the explanations of the School of [...] December 2018, the parent in the contract for the use of meals in the school canteen has the option of: agreeing or not consenting to the use of the fingerprint reader. Parents are informed about this possibility on the school canteen website.

In accordance with the rules for serving lunches on the website of the school canteen - students who do not have biometric

identification pass all and wait at the end of the line (point 3), and when all students with biometric identification enter the canteen, admitting students individually without biometric identification (point 9).

According to the explanations of the School of [...] December 2018, after the termination of the contract for the use of lunches in the school canteen, the data needed for fingerprint identification, i.e. the sequence of bytes stored in the reader, is deleted. After removal, an archival copy is made on a micro SD card, which is stored in a secure room.

According to the explanations of the School of [...] September 2019, in a situation where the parent of a given child does not withdraw the consent to use the biometric reader and the child stops using the school canteen services (without terminating the contract for the use of lunches in the canteen the biometric pattern stored in the reader is stored until it is dissolved or until the end of the school year. The biometric pattern saved on the reader and on the SD card remains during the holidays. In the event of non-renewal of the contract for the use of lunches in the school canteen for the new school year, the above-mentioned data shall be erased by […] September each year at the latest.

According to the explanations of the School of [...] September 2019, after signing the contract and consenting to the use of the biometric reader by the parent, the child is registered in the payment and meal registration system (SEWiP) by entering his / her name, surname, class and name, surname , e-mail address, contact phone number of the parent. Then (if the parent has consented), the child's fingerprint pattern is registered in the reader. From that moment on, the pattern is identified by the above-mentioned system using an ordinal number in the reader. When the reader finds a biometric pattern that corresponds to the fingerprint applied at a given moment, the reader sends to the system the number that is assigned to the person in the system and then reads the lunch status (paid / unpaid).

In the School's opinion, the system does not save any data that would constitute biometric data.

The SEWiP program (payment and meal registration system) is installed on the school server. The server is protected against unauthorized access with a password. The server also has anti-virus protection with a firewall. An authorized employee of the School has access to the server.

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

Pursuant to Art. 9 sec. 1 of 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 of Laws No. EU.L.2016.119.1), hereinafter referred to as the GDPR, it is prohibited to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership as well as genetic and biometric data processed in order to uniquely identify a natural person or data relating to that person's health, sexuality or sexual orientation. In turn, according to art. 4 point 14 of the GDPR, biometric data means personal data resulting from special technical processing, relating to the physical, physiological or behavioral characteristics of a natural person, and enabling or confirming the unambiguous identification of that person, such as facial image or dactyloscopic data. It should be emphasized that children require special protection of personal data, as they may be less aware of the risks, consequences, safeguards and rights they have in relation to the processing of personal data (recital 38 of the GDPR). The Member States of the European Union also have the right to specify national provisions related to the processing of a specific category of personal data (including biometric data) to specify the conditions that determine the lawfulness of the processing of the above-mentioned data. personal data (Recital 10 GDPR). If the processing of personal data is carried out in order to fulfill a legal obligation imposed on the controller, the basis for its processing should be Community law or the law of a Member State. It is not required that there is a specific legal regulation for each individual processing. It is sufficient that a given legal regulation is the basis for multiple processing operations resulting from a single legal obligation (to which the controller is subject), or the processing is necessary for the performance of a task carried out in the public interest (Recital 45 GDPR). It should be emphasized that biometric data, due to their characteristics, are particularly sensitive in the light of fundamental rights and freedoms, and therefore require special protection. The context of their processing may pose a serious risk to fundamental rights and freedoms, therefore, as a rule, such data should not be processed, and the conditions legalizing this process included in the GDPR are an exception. However, the law of the Member States may include specific data protection provisions adapting the application of the provisions of the GDPR so that legal obligations can be fulfilled or a task carried out in the public interest or in the exercise of official authority vested in the controller can be performed. In addition to the specific requirements applicable to such processing, the general principles and other provisions of this Regulation should apply, in particular as regards the conditions for lawful processing (Recital 51 GDPR).

The biometric system identifies those features that are, as a rule, unchanged and, often (as in the case of dactyloscopic data), impossible to change. Due to the uniqueness and stability of biometric data, which translates into their invariability over time, the use of biometric data should be carried out with particular care and caution, therefore it should be noted that any leakage

of biometric data will result in a high risk of violating the rights and freedoms of natural persons. This applies in particular to the biometric data of children, because the decision to share this type of child's data by legal guardians and their possible leakage will not be reversible in time, even after the child reaches the age of majority.

On the basis of the collected evidence, it should be stated that from children whose parents have agreed to their identification and to identify their entitlement to receive the meal (on a given day), a fingerprint image is obtained using a fingerprint method. From this image, the controller [...] automatically selects selected features of the fingerprint and converts them into a digital record (biometric template), which it stores in its memory. The digital recording is assigned a position number (from 1 to 3000) after putting a finger to the reader, the system compares it with the biometric patterns in the reader's memory. Later, he combines the item number with the same number in SEWiP to which his name, surname, class, permission to collect a meal on a given day are assigned, as well as name, surname, e-mail address, contact phone number of the parent. In the opinion of the President of the Personal Data Protection Office, the data obtained by the School, including information on characteristic points in the fingerprints of the fingers, processed into a digital record, constitute biometric data within the meaning of the provision referred to above (Article 4 (14) of the GDPR), contrary to the explanations submitted by the School. As a result of compiling the biometric pattern registered on the device with the child's finger against the biometric reader, as well as other information (including the item number, first name, surname, class and authorization to collect dinner), its identification is possible.

The processing of a specific category of personal data, which includes biometric data, is governed by Art. 9 sec. 1 GDPR, according to which the processing of personal data revealing biometric data in order to uniquely identify a natural person is prohibited. The above-mentioned paragraph does not apply, inter alia, when one of the following conditions is met: the data subject has expressly consented to the processing of such personal data for one or more specific purposes, unless Union law or the law of a Member State provide that the data subject may not lift the prohibition referred to in sec. 1 (a). The catalog mentioned in art. 9 sec. 2 GDPR is closed. Each of the premises legalizing the processing of personal data is autonomous and independent. This means that these conditions are, in principle, equal, and therefore the fulfillment of at least one of them determines the lawful processing of personal data. In addition, the processing of personal data must comply with the principles set out in Art. 5 sec. 1 GDPR. These principles include, inter alia, data minimization (c). The aforementioned principle requires that the processing process is adequate, relevant and limited to what is necessary for the purposes for which they are

processed.

In the submitted explanations, the school indicated that the processing of biometric data is based on the voluntary consent of the students' parents (legal guardians). Pursuant to Art. 4 sec. 11 GDPR, "consent" of the data subject means the free, specific, informed and unambiguous demonstration of will, which the data subject, by means of a declaration or a clear affirmative action, authorizes the processing of personal data relating to him. However, in recital 43 of the GDPR, the EU legislator states that, in order for consent to be freely given, it should not constitute a valid legal ground for the processing of personal data, in particular in a situation where there is a clear imbalance between the data subject and the controller. Pursuant to Art. 106 of the Education Law of December 14, 2016 (Journal of Laws of 2019, item 1148), in order to ensure the proper implementation of care tasks, in particular to support the proper development of students, the school may organize a canteen. Therefore, it should be stated that the basis for the processing of any personal data of children in connection with the implementation of this school task could not be consent, because the basis for the processing of children's personal data by the School for this purpose is Art. 6 sec. 1 lit. e GDPR, according to which the processing is lawful, inter alia, when the processing is necessary to perform a task carried out in the public interest or in the exercise of public authority entrusted to the administrator. This means that the School processes the student's personal data on the basis of legal provisions, performing its statutory tasks. Therefore, it does not need a separate consent of parents or an adult student for the processing of personal data in connection with the performance of these tasks, i.e. the provision of services by the school canteen. By providing this service, the School may only process the student's personal data that is necessary for the provision of school canteen services. It should be noted that the provisions of generally applicable law indicate the type of data that the School may obtain from its students. None of them allow the School to process (acquire and collect) biometric data (the processing of which is in principle prohibited in Article 9 (1) of the GDPR) of students in order to perform this task.

In such a situation, the parent's consent cannot be a premise legalizing the processing of biometric data, because consent is the basis for legalizing the processing of personal data only if there are no other grounds for this processing. Recognizing the fact of giving consent by the parents of children as a circumstance that legalizes the collection of data from children other than those indicated by the Polish legislator, would circumvent these provisions. It is worth emphasizing that in accordance with the rules for serving lunches posted on the website of the canteen run by the School, students who do not have biometric identification pass everyone through and wait at the end of the queue (point 3), and when all students with biometric

identification enter the canteen, starts admitting pupils one at a time without biometric identification (point 9). The above-mentioned principles introduce unequal treatment of students because they clearly promote students with biometric identification.

In view of the above, it should be considered that the School did not have a legal basis allowing the processing of biometric data of children using the services of the school canteen. Therefore, due to the fact that the School does not have any of the conditions set out in Art. 9 sec. 2 GDPR, such conduct violates Art. 9 sec. 1 GDPR and the principles of data minimization established in the GDPR, according to which the data controller, i.e. in this case the School, should not obtain data excessively, but only those that are necessary to achieve the goals. It should be noted that the processing of biometric data is not necessary to achieve the goal of identifying the child's entitlement to receive lunch. The above-mentioned identification may be carried out by the School by other means, less interfering with the privacy of a child using the school's canteen services. The collected evidence shows that the School enables the use of the school canteen by means of a fingerprint, electronic card or based on the name and contract number. Thus, at the School there are alternative forms of identifying a child's entitlement to receive lunch. It should be emphasized that biometric data can be used, inter alia, for the purposes of ensuring personal and industrial security, information protection in order to verify suspects and assess their participation in crimes, issue identification documents (passports), control access to specific security areas - in these cases, these processes may be considered as justified due to the subject matter protection or the seriousness of the goal pursued, and the scope of the data used is adequate. Meanwhile, the verification of who intends to use the services of the school canteen and whether they are entitled to receive lunch through the biometric data obtained from students is, in the opinion of the authority, too much interference with their privacy, compared to the seriousness of the purpose for which they are to be processed.

Bearing in mind the above findings, the President of the Office for Personal Data Protection, exercising his powers specified in art. 58 sec. 2 lit. f and lit. g GDPR, orders the School to delete personal data in the field of digitally processed information about characteristic fingerprint points of fingers of children using the school canteen services and orders to stop collecting personal data in the field of digitally processed information about characteristic fingerprints of fingers of children using the services school canteen,

Pursuant to Art. 58 sec. 2 lit. and GDPR, each supervisory authority has the right to apply, in addition to or instead of other remedial measures provided for in Art. 58 sec. 2 of this GDPR, an administrative fine pursuant to Art. 83 GDPR, depending on

the circumstances of a specific case. The President of the Personal Data Protection Office states that in the case under examination there are conditions for imposing an administrative fine on the School.

Pursuant to art. 83 sec. 2 GDPR, administrative fines are imposed, depending on the circumstances of each individual case, in addition to or instead of the measures referred to in Art. 58 sec. 2 lit. a-h and lit. j GDPR. The President of the Personal Data Protection Office, deciding to impose an administrative fine on the School and determining its amount, in accordance with Art. 83 sec. 2 lit. a-k GDPR took into account the following circumstances of this case:

Children's biometric data were processed without a legal basis in violation of the principle of minimization, this state of affairs has been in effect from [...] May 2018 until now. It currently affects 680 children. The authority has no evidence that the data subjects have suffered material damage, but the very breach of the principle of data minimization of a special category may constitute non-pecuniary damage. The action of the School may lead to an unjustified differentiation of the situation of students using the services of the school canteen (nature, severity and duration of the violation);

The infringement found in the present case is of considerable gravity and serious nature, as it concerns the processing of data of a specific category and these are the data of children. The processing takes place without a legal basis and violates the basic principle of minimization with regard to the processing of personal data (Article 5 (1) (c) of the GDPR). The infringement found continues to date (nature, gravity and duration of the infringement);

The school made a conscious decision, motivated by the willingness to efficiently identify children collecting meals in the school canteen in order to verify the payment of the payment for the meal on a given day, which means that it should be attributed a willful act that violated Art. 5 sec. 1 lit. c and art. 9 sec. 1 GDPR (intentional or unintentional nature of the breach);

The administrator did not take steps to minimize the potential non-pecuniary damage because he did not qualify his action as unlawful (actions taken by the administrator to minimize the damage suffered by the data subjects);

The breach found is not related to the implementation and quality of the School - pursuant to Art. 25 and 32 GDPR - organizational and technical measures, therefore there is no need to determine in this context the degree of responsibility of the School (the degree of responsibility of the administrator taking into account technical and organizational measures);

The School has not been found to have previously breached the provisions of the GDPR that would be material to this proceeding (any relevant prior breaches by the controller or processor);

The breach concerned biometric data - categories of data subject to special protection (categories of personal data concerned

by the breach);

The President of the Personal Data Protection Office obtained information about unlawful processing of the above-mentioned personal data by the School ex officio (the manner in which the supervisory authority learned about the breach);

In the same case, the measures referred to in Art. 58 sec. 2 GDPR (compliance with measures imposed on the controller in the same case);

The school does not apply any approved codes of conduct pursuant to Art. 40 GDPR or approved certification mechanisms pursuant to Art. 42 GDPR (application of codes of conduct or certification mechanisms);

The President of the Personal Data Protection Office considered the circumstances mentioned in the above-mentioned aggravating circumstances which had an impact on the penalty. points 1, 2, 3 and 7. On the other hand, the circumstances indicated in the above-mentioned points 4, 5, 8, 9 and 10.

In the opinion of the President of the Personal Data Protection Office, the applied administrative fine performs the functions referred to in Art. 83 sec. 1 GDPR, i.e. it is effective, proportionate and dissuasive in this individual case.

It should be emphasized that the penalty will be effective if its imposition leads to the fact that the School adjusts its data processing processes to the lawful state. The application of an administrative fine in the present case is necessary considering also that the School completely ignored the fact that the biometric data of children were processed by stating that it did not process the data in the above-mentioned range.

In the opinion of the President of the Office for Personal Data Protection, the administrative fine will fulfill a repressive function, as it will be a response to the violation of the GDPR provisions by the School, but also a preventive one, as the School itself will be effectively discouraged from violating the provisions of personal data protection in this way in the future.

In the established circumstances of the present case, i.e. in view of the violation of the principle of minimization resulting from Art. 5 sec. 1 lit. c GDPR and art. 9 sec. 1 GDPR, Art. 83 sec. 7 GDPR, according to which, without prejudice to the remedial powers of a supervisory authority referred to in para. 58 sec. 2, each Member State may determine whether and to what extent administrative fines may be imposed on public authorities and entities established in that Member State. According to Art. 102 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), hereinafter referred to as the Act of 2018, the President of the Personal Data Protection Office may impose, by way of a decision, administrative penalties cash in the amount of up to PLN 100,000, incl. on units of the public finance sector, referred to in article 1. 9 points

1-12 and 14 of the Act of 27 August 2009 on public finances (Journal of Laws of 2019, item 869).

In connection with the above, it should be noted that the fine in the amount of PLN 20,000.00 meets the conditions referred to in Art. 83 sec. 1 GDPR due to the seriousness of the breach found in the context of the basic principle of the GDPR - data minimization.

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

Caution: The decision is final. Based on Article. 7 sec. 2 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) in connection with joke. 13 § 2, art. 53 § 1 and art. 54 of the Act of August 30, 2002, Law on Administrative Court Proceedings (Journal of Laws of 2019, item 2325, as amended), a party dissatisfied with this decision has the right to lodge a complaint 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 for Personal Data Protection (address: Office for Personal Data Protection, ul. Stawki 2, 00-193 Warsaw). The fee for the complaint is PLN 200. The party has the right to apply for an exemption from court costs or the right to assistance.

Pursuant to Art. 105 paragraph. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the administrative fine must be paid within 14 days from the date of expiry of the deadline for lodging a complaint to the Provincial Administrative Court, or from on the day the ruling of the administrative court becomes legally binding, to the bank account of the Personal Data Protection Office at NBP O / O Warsaw no. 28 1010 1010 0028 8622 3100 0000. Moreover, pursuant to Art. 105 paragraph. 2 above of the Act, the President of the Personal Data Protection Office may, at the justified request of the punished entity, postpone the date of payment of the administrative fine or divide it into installments. In the event of postponing the payment of the administrative fine or dividing it into installments, the President of the Personal Data Protection Office shall charge interest on the unpaid amount on an annual basis, using a reduced rate of late payment interest, announced pursuant to Art. 56d of the Act of August 29, 1997 - Tax Ordinance (Journal of Laws of 2019, item 900, as amended), from the day following the date of submitting the application.

2020-03-04