THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 07

September

2022

DECISION

DKN.5131.29.2022

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended), art. 7 sec. 1, art. 60 and art. 102 paragraph. 2 and sec. 3 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), hereinafter referred to as "uodo", as well as art. 57 sec. 1 lit. a) and h), art. 58 sec. 2 lit. i), art. 83 sec. 1 and 2 and article. 83 sec. 4 lit. a) in connection with Art. 28 sec. 1, 3 and 9 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general on data protection) (Journal of Laws UE L 119 of May 4, 2016, p. 1, Journal of Laws UE L 127 of May 23, 2018, p. 2 and EU Official Journal L 74 of March 4, 2021, p. 35), hereinafter referred to as: "Regulation 2016/679", after conducting the administrative proceedings initiated ex officio regarding the infringement by Sułkowicki Ośrodek Kultury with its seat in Sułkowice at ul. May 1, 70 provisions on the protection of personal data, President of the Office for Personal Data Protection

finding an infringement by the Sułkowice Cultural Center with its seat in Sułkowice at ul. 1 Maja 70, the provisions of art. 28 sec. 1, 3 and 9 of Regulation 2016/679, consisting in entrusting Mr. K. G. running a business under the name of [...] with the processing of personal data without a written entrustment agreement and without verifying whether the processing entity provides sufficient guarantees for the implementation of appropriate technical and organizational measures to the processing complied with the requirements of Regulation 2016/679 and protected the rights of data subjects, it is imposed on the Sułkowicki Cultural Center with its seat in Sułkowice at ul. On May 1, 70, an administrative fine in the amount of PLN 2,500 (say: two thousand five hundred zlotys).

Justification

The President of the Personal Data Protection Office, hereinafter referred to as the President of the Personal Data Protection Office, on [...] May 2020, received a notification of a personal data breach made by Sułkowicki Ośrodek Kultury with its seat in

Sułkowice at ul. 1 Maja70 (hereinafter referred to as "SOK" or "Administrator"), registered under the file number [...], informing about a breach of personal data protection of 30 people - employees and former employees of the Administrator. SOK (in accordance with its statute constituting an appendix to Resolution No. XII / 72/2015 of the City Council in Sułkowice of September 30, 2015) is an organizational unit of the commune established to carry out its own obligatory tasks in the field of culture.

In the course of the investigation, conducted in connection with the reported breach of personal data protection, it was found that SOK entrusted the processing of personal data with the above-mentioned persons to Mr K. G. running a business under the name of [...] with a place of business in T. No. [...], hereinafter referred to as "[...]" or "Processor", without entering into a written entrustment agreement and without verification of the processor, whether it provides sufficient guarantees of the implementation of appropriate technical and organizational measures to ensure that the processing meets the requirements of Regulation 2016/679 and protects the rights of data subjects. As established, the Administrator commissioned the above-mentioned the entity: keeping accounting books, records and preparing reports (in the area of finance, taxes and the Social Insurance Institution), processing personal data with the necessary attachments, storing documentation (VAT records, records of fixed assets, VAT declarations) - thus entrusting him with the processing of personal data of employees and former employees of the Administrator in the form of: names and surnames, parents' names, dates of birth, bank account numbers, addresses of residence or stay, PESEL registration numbers, e-mail addresses, data on earnings and / or property, mother's family names, series and numbers ID cards, phone numbers, and health data. In addition, SOK explained in its letters of […] November and […] December 2021 and […] April 2022 that 'There has been no entrustment agreement with the processor. The processor was asked for information, clarification and return / sharing of the processed data, but to no avail "," No contracts with SOK were concluded with the company [...]. (...) It is highly probable that Mrs. G., on the authority of the then Director, performed such activities using the ZUS Płatnik program outside the seat, transferring the database or the new database she created "," (...) (the administrator) does not have any documents confirming the start and termination of cooperation with the company [...] (...) "and" (...) (the administrator) does not have any documents confirming the verification of the terms of cooperation with the company [...] (...) ".

Attached to the letter of [...] November 2021, the Administrator presented letters of [...] June 2020, addressed, inter alia, to to the Director of SOK in 2015 - 2019, acting as Director of SOK in 2019-2020, chief accountant of SOK in 2017-2019 (p. B. G.)

and chief accountant of SOK in 2019-2020, asking for information "on what legal and factual basis this company [note: [... ]] kept the documentation of the Center, whether a civil law contract was concluded with this company, what was the scope of this contract and what was the scope of the company's obligations towards the Sułkowice Cultural Center ". The administrator also indicated in a letter dated [...] December 2021 that attempts to obtain explanations from Ms B. G. (who was described as a representative or employee of [...]) were unsuccessful.

In view of the above, in a letter of [...] May 2022, the President of the Personal Data Protection Office (UODO) initiated ex officio administrative proceedings against the Administrator regarding the breach by Sułkowicki Ośrodek Kultury, as the data controller, of obligations under Art. 28 sec. 1, 3 and 9 of Regulation 2016/679 (letter reference [...]).

The administrator did not respond in writing to the above-mentioned notifications about the initiation of administrative proceedings.

After reviewing all the evidence gathered in the case, the President of UODO considered the following.

The President of the Personal Data Protection Office is an authority competent for the protection of personal data (Article 34 (1) of the Personal Data Protection Act) and a supervisory authority within the meaning of the provisions of Regulation 2016/679 (Article 34 (2) of the Personal Data Protection Act).

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 Regulation 2016/679 (point a) and conducts proceedings on the application of this regulation (point h). An instrument for the implementation of the tasks referred to in Art. 57 of the Regulation 2016/679, there are in particular the remedial powers granted pursuant to Art. 58 sec. 2 of the Regulation 2016/679 - incl. to apply, in addition to or in place of the measures referred to in this paragraph, an administrative fine under Article 83, depending on the circumstances of the specific case (point i).

Pursuant to Art. 28 sec. 1 of Regulation 2016/679, if the processing is to be carried out on behalf of the controller, he or she uses only the services of such processors that provide sufficient guarantees to implement appropriate technical and organizational measures to ensure that the processing meets the requirements of this Regulation and protects the rights of data subjects. Pursuant to Art. 28 sec. 3 of Regulation 2016/679, processing by the processor takes place on the basis of a contract or other legal instrument, which are governed by Union law or the law of a Member State and are binding on the processor and the controller, determine the subject and duration of processing, nature and purpose of processing, type of

personal data and the categories of data subjects, the obligations and rights of the controller. This contract or other legal instrument provides in particular that the processor:

a) processes personal data only on a documented instruction of the controller - which also applies to the transfer of personal data to a third country or an international organization - unless such an obligation is imposed on it by Union law or the law of the Member State to which the processor is subject; in this case, prior to processing, the processor informs the controller of this legal obligation, unless the law prohibits the provision of such information due to important public interest; b) ensures that persons authorized to process personal data have committed themselves to secrecy or are subject to appropriate statutory obligation of confidentiality; (c) take all measures required under Art. 32; (d) complies with the terms of use of the services of another processor, referred to in paragraph 1. 2 and 4; e) taking into account the nature of the processing, as far as possible helps the controller, through appropriate technical and organizational measures, to fulfill the obligation to respond to requests of the data subject in the exercise of his rights set out in Chapter III; processing and the information available to him, helps the administrator to fulfill the obligations set out in art. 32-36; g) upon termination of the provision of processing services, depending on the controller's decision, deletes or returns to him any personal data and deletes any existing copies thereof, unless Union law or the law of a Member State requires the storage of personal data; h) provides the controller with all information necessary to demonstrate compliance with the obligations set out in this Article, and enable and contribute to the performance of, and contributes to, audits, including inspections, by the administrator or an auditor authorized by the administrator.

In connection with the obligation set out in the first subparagraph a. (h) the processor shall immediately inform the controller if he or she considers the instructions to be given to it infringe this Regulation or other Union or Member State law on data protection.

On the other hand, pursuant to Art. 28 sec. 9 of Regulation 2016/679, the contract or other legal act referred to in para. 3 and 4, shall be in writing, including electronic form.

The collected evidence shows that the Sułkowicki Cultural Center, entrusting the processing of employees' personal data, did not conclude a written entrustment agreement with the entity processing this data, which was K. G. running a business under the name of [...] with the place of business in T. No. [...] containing the elements indicated in art. 28 sec. 3 of the Regulation 2016/679. When assessing this state of affairs, we should start with explaining the function performed by these two entities

and their mutual relationship.

Pursuant to Art. 4 point 7 of Regulation 2016/679, "controller" means a natural or legal person, public authority, unit or other entity that alone or jointly with others sets the purposes and methods of processing personal data, and if the purposes and methods of such processing are specified in law Union or Member State law, the controller may also be designated under Union law or the law of a Member State, or specific criteria for its designation may be laid down. On the other hand, "processor" means a natural or legal person, public authority, agency or other entity that processes personal data on behalf of the controller (Article 4 (8) of Regulation 2016/679).

The fact that in the analyzed situation there was no contract for entrusting the processing of personal data within the meaning of art. 28 sec. 3 of the Regulation 2016/679 does not deprive Sułkowicki Ośrodek Kultury, or […], of the status of, respectively: controller and processor. It follows from Guidelines 07/2020 that "The concepts of controller (...) and processor are functional concepts in the sense that their purpose is to allocate obligations in accordance with the real roles of the parties and autonomous concepts in the sense that they should be interpreted mainly in accordance with with EU data protection law ". In the case at hand, there is no doubt that the Sułkowice Cultural Center was the administrator of the personal data of its former and current employees that it processed. Responsibility for the selection of the processor should be assigned to the SOK, as it is the controller that entrusts the processing of personal data to a natural or legal person of his choice - in Guidelines 07/2020 (describing who can be the controller), it is indicated that "In practice, however, it is usually an organization as such, and not a natural person in the organization (e.g. CEO, employee or board member), acts as an administrator within the meaning of the GDPR ". Therefore, from the point of view of the subject matter of this proceeding, it is irrelevant which of the persons included in the organization (ie SOK) and why decided to establish cooperation - even informal - with [...].

Due to the fact that pursuant to Art. 5 sec. 1 lit. a) and f) of Regulation 2016/679, personal data must be processed lawfully, fairly and in a transparent manner for the data subject ("lawfulness, fairness and transparency") and in a manner ensuring adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organizational measures ("integrity and confidentiality"), very important from the point of view of the data controller is the entity entrusted with the processing of this data. Art. 5 sec. 2 of Regulation 2016/679 provides that the controller is responsible for the processing of personal data in accordance with these principles and must be able to demonstrate compliance with them ("accountability") - therefore it is so important from his point of view to

thoroughly investigate which entity (and on which basis) entrusts the processing of personal data. This thought is expressed directly in Art. 28 sec. 1 of Regulation 2016/679, according to which, if the processing is to be carried out on behalf of the administrator, he uses only the services of such processors that provide sufficient guarantees to implement appropriate technical and organizational measures to ensure that the processing meets the requirements of this Regulation and protects the rights of persons whose data relate to. Moreover, Guideline 07/2020 states that "The elements to be taken into account may be: professional knowledge of the processor (eg technical knowledge in the field of security measures and data protection breaches); the reliability of the processor; the processor's resources and the application by the processor of an approved code of conduct or certification mechanism "that:" The processor's reputation in the marketplace may also be an important factor that controllers should consider "and that» The controller is (...) responsible for assessing the adequacy of the guarantees provided by the processor and should be able to prove that he took all the elements provided for in the GDPR seriously. Guarantees "provided" by the processor are those that the processor is able to demonstrate to the satisfaction of the controller, as they are the only guarantees that the controller can effectively take into account when assessing compliance with its obligations. Often this will require the exchange of relevant documentation (e.g. privacy policy, terms of service, record of processing activities, document management policy, information security policy, reports from external data protection audits, internationally recognized certificates such as ISO 27000 standards). The controller's assessment of whether the guarantees are sufficient is a form of risk assessment, which largely depends on the type of processing entrusted to the processor and must be made on a case-by-case basis, taking into account the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedom of natural persons ". In the present case, however, there are no indications that the controller took these elements into account.

The fact described in a letter dated [...] December 2021 by the Administrator that the representative or employee of [...] was (at the time of the infringement) Mrs. B. G. - employed as the chief accountant in the Administrator's organization in 2017-2019 is irrelevant with from the point of view of the Administrator's compliance with the obligations arising from art. 28 sec. 1 of Regulation 2016/679. Any personal ties do not constitute in this case the basis for a reliable assessment of the Processor's competences. As mentioned above, Guidelines 07/2020 clearly indicate which elements should be taken into account by the controller when assessing the processor.

Only after a sufficiently in-depth examination of the competences and adequacy of the selected processor (which is - as

indicated above - also an element of the risk assessment related to the processing of personal data), the controller may proceed to conclude an appropriate entrustment agreement. In Guidelines 07/2020 it was emphasized that "All processing personal data by the processor must be governed by an agreement or other legal act under Union or Member State law concluded between the controller and the processor, as required by Art. 28 sec. 3 GDPR. Such a legal act shall be in writing, including electronic form (…). Therefore, unwritten contracts (irrespective of their degree of detail or effectiveness) cannot be considered sufficient to meet the requirements of Art. 28 GDPR ". Guidelines 07/2020 also clearly indicate the consequences of failure to maintain the appropriate form of concluding a contract:" As the regulation clearly establishes an obligation to conclude a contract in writing, where no other relevant legal act is in force, its absence is a violation of the GDPR "- while it was also noted that "(…) it can be considered that the controller-processor relationship continues in the absence of a written data processing agreement. However, this would be a violation of Art. 28 sec. 3 GDPR ".

Although Art. 28 sec. 1 of Regulation 2016/679 mainly indicates the obligations of the administrator wishing to entrust the processing of personal data to another entity, Guidelines 07/2020 indicate that "Both the administrator and the processor are responsible for ensuring the conclusion of a contract or other legal act regulating the processing (...) ". The contract is at least a two-sided legal act, and the seriousness of entrusting the processing of personal data requires the involvement of all parties. Meanwhile, on the basis of the evidence collected in the case at hand, it cannot be stated that the Administrator and the Processor have made even informal arrangements that included the elements listed in Art. 28 sec. 3 of the Regulation 2016/679.

Once the controller has carefully selected the appropriate processor, and then the contract is concluded, it should not be forgotten that the administrator's obligations to entrust the processing of personal data to an entity that meets the requirements set out in art. 28 sec. 1 of the Regulation 2016/679 shall last at least as long as the period of entrustment. As indicated in the above-mentioned of the guidelines »The obligation to use only the services of processors" providing sufficient guarantees "in Art. 28 sec. 1 GDPR is an ongoing obligation. It does not end when the contract or other legal act is concluded by the controller and the processor. Rather, the controller should verify the processor's guarantees at appropriate intervals, including through audits and inspections where appropriate (…) ".

As can be seen from the above considerations, the decision to whom the controller would be entrusted with the processing of personal data cannot be made unreasonably. The consequences of taking a hasty decision, lack of appropriate form or content

of the entrustment agreement, or neglect of the obligation of the administrator to constantly verify the guarantees referred to in art. 28 sec. 1 of Regulation 2016/679, because they may directly affect natural persons whose personal data has been entrusted to the processor. Meanwhile, when applying the provisions of Regulation 2016/679, it should be borne in mind that the purpose of this regulation (expressed in Article 1 (2)) is to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and that the protection of natural persons in connection with the processing of personal data, it is one of the fundamental rights (first sentence of recital 1). In case of any doubts, e.g. as to the performance of obligations by administrators - not only in a situation where there has been a breach of personal data protection, but also when making decisions regarding entrusting the processing of personal data to other entities - these values should be taken into account in the first place. These rights are consistently protected by the requirements of Art. 28 sec. 1, 3 and 9 of Regulation 2016/679, hence their violation must be associated with a response of the supervisory authority appropriate to specific circumstances.

In the case at hand, there is nothing to indicate that the Administrator has checked whether the Processing Entity provides sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements of Regulation 2016/679 and protects the rights of the data subjects. In a letter dated […] April 2022, SOK indicated that it did not have any documents confirming the verification of the terms of cooperation with […]. It is also irrelevant who specifically made the decision to entrust the processing of this data, as the Administrator is responsible for the selection of the processor. Therefore, it should be consistently assumed that the Administrator did not meet the requirements set out in Art. 28 sec. 1 of Regulation 2016/679, which results in its breach of this provision.

The explanations provided by the Administrator show that (despite the failure to fulfill the obligations under Article 28 (1) of Regulation 2016/679), the processing of data was actually entrusted [...]. In the notification addressed to the data subjects of the violation (which was made in accordance with Article 34 of Regulation 2016/679), the SOK, describing the violation, indicated that: " , taxes and ZUS) to an external entity. The processing of personal data was entrusted without concluding an appropriate contract for entrusting the processing of personal data. Documentation (VAT registers, fixed assets register, VAT declarations) was stored by an external entity. There was a possibility of a personal data breach by an external entity or employees (former or current). SOK is not in possession of a single document in any possible form regarding settlements with ZUS in the period September 2017-December 2018. This is due to the complete inability to perform actions resulting from ZUS

calls to explain the irregularities of the prepared documentation, calculate contributions and establish public and public liabilities. legal SOK, as well as the complete impossibility of making paper documents available at the request of the ZUS inspector. All documents (the entire database) for the period September 2017-December 2018, based on the assurances obtained, were handled outside the seat of SOK and on private equipment without authorization and appropriate security. "

Moreover, from the explanations provided by the Administrator in a letter dated [...] November 2021, it follows directly that no entrustment agreement has been concluded with the Processor, and asking him for information, explanations and return or sharing of the processed data turned out to be ineffective. To some extent, the administrator restored the data to which he lost access as a result of entrusting their processing [...] - in a letter of [...] December 2021, however, he indicated that only information from the Social Insurance Institution was available.

The information that the entrustment agreement had not been concluded was repeated by the Administrator in a letter of [...] December 2021, and in the explanations dated [...] April 2022, he additionally indicated that he did not have any documents confirming the commencement and completion of cooperation with […]. The fact that in the case in question there was a breach of the obligation to conclude a sub-processing agreement in an appropriate form (i.e. the obligation referred to in Article 28 (9) of Regulation 2016/679) and with appropriate content (which is specified in Article 28 (3) of the Regulation 2016/679) is therefore indisputable. From the information provided by the Administrator that the breach concerned data for the period from September 2017 to December 2018, it can be concluded that the cooperation between SOK and the Processor could end on [...] December 2018 at the earliest - while it could have ended at the latest. it should be completed on [...] June 2020, when Mr. K. G., running a business under the name of [...], died (according to the information contained in the Central Register and Information on Economic Activity of the Republic of Poland). The date of termination of cooperation determined in this way may also be associated with the end of the infringement of the provisions of Regulation 2016/679 - taking into account the fact that data availability was only partially restored. In turn, when this collaboration could have started remains unclear. Due to the fact that as a result of providing the Data Processor, the Administrator has lost the availability of data resulting from settlements with ZUS from September 2017 to December 2018, it can be assumed that the violation of the provisions of Regulation 2016/679 lasted from [...] May 2018, when the provisions of that regulation became applicable.

In the present case, it should be emphasized that one of the consequences of the Administrator's failure to fulfill the obligations under Art. 28 sec. 1, 3 and 9 of Regulation 2016/679, it is impossible to regain access to all personal data entrusted to the

Processor.

Bearing in mind the above findings, the President of the Personal Data Protection Office, exercising his powers specified in art. 58 sec. 2 lit. i) Regulation 2016/679, pursuant to which each supervisory authority has the power to apply, in addition to or instead of other remedial measures provided for in Art. 58 sec. 2 lit. a) -h) and lit. (j) of that Regulation, an administrative fine pursuant to Article 83 sec. 4 lit. a) of Regulation 2016/679, having regard to the circumstances established in the proceedings in question, stated that in the case under consideration there were premises justifying the imposition of an administrative fine on the Administrator.

Pursuant to Art. 83 sec. 4 lit. a) Regulation 2016/679, breach of the provisions on the obligations of the controller and the processor referred to in art. 8, 11, 25-39 as well as 42 and 43 are subject to, in accordance with sec. 2 an administrative fine of up to EUR 10,000,000, and in the case of a company - up to 2% of its total annual worldwide turnover from the previous financial year, whichever is higher.

In the present case, an administrative fine against SOK was imposed for violation of Art. 28 sec. 1, 3 and 9 of Regulation 2016/679 on the basis of the above-mentioned Art. 83 sec. 4 lit. a) of Regulation 2016/679, while taking into account the content of art. 102 paragraph. 2 of the PDPA, from which it follows that the President of the Personal Data Protection Office may impose, by way of a decision, administrative fines of up to PLN 10,000 on public finance sector entities referred to in Art. 9 point 13 of the Act of 27 August 2009 on public finances (Journal of Laws of 2022, item 1634, as amended) - ie state and local government cultural institutions. Joke. 102 paragraph. 3 of the Act on 2, the President of the Personal Data Protection Office (UODO) imposes on the basis and under the conditions specified in Art. 83 of the Regulation 2016/679.

When deciding to impose an administrative fine on the Administrator, the President of the Personal Data Protection Office pursuant to Art. 83 sec. 2 lit. a-k of the regulation 2016/679 - took into account the following circumstances of the case, aggravating and affecting the size of the imposed financial penalty:

1. The nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing, the number of data subjects affected and the extent of the damage suffered by them (Article 83 (2) (a) of Regulation 2016/679) - with In the imposition of a penalty, the fact that the provisions of Regulation 2016/679 were breached in this case, imposing on the controller one of his basic and key obligations for the security of the processed personal data: verification of the processor and conclusion of the entrustment agreement in an appropriate form and with appropriate content. Moreover, the consequence

of violating the provisions of Art. 28 sec. 1, 3 and 9 of Regulation 2016/679 was a breach of the confidentiality and availability of data of thirty former and current employees of the Administrator. This breach indirectly harms the interests of employees, whose specific SOK should protect, and may also have negative consequences in the light of the provisions of other areas of law (labor law, social security or accounting regulations). When considering the aspect of the purpose of processing, it should be noted that the personnel service of employment contracts requires special diligence, and there is an imbalance between the SOK (employer) and data subjects (employees). The violation of the above-mentioned provisions is of considerable importance and seriousness, also because it may cause material or non-material damage to the data subject, and the likelihood of their occurrence cannot be excluded. In addition, the risk arising from the wide range of data covered by the breach has to be taken into account. It should be emphasized that there is still a risk of unlawful use of their personal data in relation to the persons whose data has been violated, because nothing is known about the organizational and technical measures applied by [...] to ensure the security of processing entrusted data, and also, the data to which the Administrator lost access as a result of the entrustment in question was not returned. Data subjects entrusted with the violation of the requirements of Art. 28 sec. 1 of Regulation 2016/679, they may therefore continue to suffer material damage, and the very breach of data confidentiality is also non-pecuniary damage (harm). The data subject may, at the very least, feel the fear of losing control of their personal data, of identity theft or identity fraud, and finally of financial loss. In addition, the violation in question involves the loss of control over the data that is potentially needed by its entities (e.g. data on acquired employee rights) - proper verification of the Processor allows you to reduce the risk of entrusting the data to an entity that may not return it.

Although, on the basis of the evidence collected in the case, it is difficult to precisely determine the duration of the violation, it should be assumed that the duration of the violation was relatively long. As shown above, its starting date should be the date of application of the provisions of Regulation 2016/679 (ie […] May 2018). The breach could end at the earliest by the end of December 2018, and at the latest with the death of Mr. K. G. - the Processing Entity ([...] June 2020) - taking into account the fact that SOK still has not regained the availability of some data.

When assessing the premise of Art. 83 sec. 2 lit. and Regulation 2016/679, which has a generally aggravating impact on the penalty, it should also be noted that the Administrator conducts a non-profit, socially useful activity, and local government cultural institutions have been treated by the legislator in a special way by reducing art. 102 paragraph. 2 uodo of the

maximum amount of an administrative fine up to the amount of PLN 10,000. The scope of processing is small (local) and concerns a relatively small number of people - hence the number of injured persons is also small. Moreover, no material damages were found (no non-pecuniary damages were reported either) - as indicated above, however, there is still a risk of their occurrence in this case.

2. Intentional or unintentional nature of the breach (Article 83 (2) (b) of Regulation 2016/679) - it does not follow from the evidence collected in this case that the disclosure of personal data [...] without proper verification of this entity and without concluding a contract of entrustment in the form provided for by law and with appropriate content, took place as a result of actions aimed at the violation of Regulation 2016/679. But the fact that the controller's intentional act (knowledge and will to infringe) has not been proven does not in this case amount to assuming that this premise should not be assessed as aggravating. The degree of negligence shown by the Administrator when entrusting the Processing Entity with the processing of personal data of SOK employees is gross - it proves the lack of compliance with the basic principles of personal data protection resulting from ignorance or disregard of the provisions of Regulation 2016/679.

3. The degree of the Administrator's responsibility, taking into account technical and organizational measures implemented pursuant to art. 25 and 32 (Article 83 (2) (d) of Regulation 2016/679) - the findings made by the President of the Personal Data Protection Office allow the conclusion that the Administrator has not complied with the obligations set out in Art. 28 sec. 1 of Regulation 2016/679 (regarding the verification whether the Processor provided sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing complies with the requirements of this Regulation and protects the rights of data subjects), and also did not conclude a processing agreement in the form prescribed by law (Art. 28 (9) of Regulation 2016/679) and on the information referred to in art. 28 sec. 3 of the Regulation 2016/679 in content. As a result of informally entrusting the processing of personal data, not only their confidentiality was lost, but also their availability (to some extent) was lost, for which the Administrator is responsible. It is also impossible to state that entrusting the processing of personal data was in accordance with the organizational measures introduced by the Administrator (procedures or regulations constituting the obligation to verify the processor and specifying the manner of concluding contracts for entrusting the processing of personal data), which would ensure compliance with the requirements of art. 28 of Regulation 2016/679.

4. The categories of personal data concerned by the infringement (Article 83 (2) (g) of Regulation 2016/679) - personal data the processing of which has been entrusted in a manner that does not meet the requirements of Art. 28 sec. 1, 3 and 9 of

Regulation 2016/679, have a wide scope (first and last names, parents' names, dates of birth, bank account numbers, addresses of residence or stay, PESEL registration numbers, e-mail addresses, data on earnings and / or property , mother's maiden names, series and numbers of identity cards, telephone numbers, as well as data of a specific category within the meaning of Article 9 of Regulation 2016/679: health data), which also entails a high risk of violating the rights or freedoms of individuals affected by the violation. It should be emphasized that, in particular, the unauthorized disclosure of such a category of data as a PESEL number (in combination with a first and last name) may have a real and negative impact on the protection of the rights or freedoms of natural persons. PESEL number, i.e. an eleven-digit numeric symbol, uniquely identifying a natural person, containing the date of birth, serial number, gender (and a control number), and therefore closely related to the private sphere of a natural person and also subject to exceptional protection as a national identification number art. 87 of Regulation 2016/679 is a data of a special nature and requires such special protection.

When determining the amount of the administrative fine imposed on SOK, the President of the Personal Data Protection Office took into account the following premises as mitigating circumstances:

1. Actions taken by the controller to minimize the damage suffered by the data subjects (Article 83 (2) (c) of Regulation 2016/679) - SOK did not receive information about material damage to persons affected by the infringement. It should be pointed out that immediately after the disclosure of the breach of personal data protection, before the commencement of administrative proceedings, SOK took steps to clarify the circumstances of entrusting data processing [...] and to regain the availability of lost personal data. The decision indicated as an aggravating circumstance that data subjects may still suffer material damage, and the breach of confidentiality itself is also a non-pecuniary damage (harm), but taking measures to regain data availability should be assessed as a mitigating circumstance - these are actions taken to minimize the damage suffered by the data subjects.

2. Relevant previous violations of the provisions of Regulation 2016/679 (Article 83 (2) (e) of Regulation 2016/679) - until the moment of issuing this decision, the President of the Personal Data Protection Office found no violations of the provisions of Regulation 2016/679 by the Administrator;

3. The degree of cooperation with the supervisory authority in order to remove the breach and mitigate its possible negative effects (Article 83 (2) (f) of the Regulation 2016/679) - SOK has independently undertaken a number of actions aimed at, inter alia, regaining access to lost data - and thus: mitigating its possible negative effects.

4. Any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits obtained directly or indirectly due to the infringement or avoided losses (Article 83 (2) (k) of Regulation 2016/679) - the President of the Personal Data Protection Office did not state in in the course of these proceedings that, by committing the infringement of the punishable SOK, it obtained any financial benefits or avoided any financial losses.

The fact of applying to the Administrator in this case by the President of the Personal Data Protection Office of sanctions in the form of an administrative fine, as well as its amount, was not affected by other sanctions indicated in art. 83 sec. 2 of Regulation 2016/679 circumstances, that is:

1. The way in which the supervisory authority learned about the breach (Article 83 (2) (h) of Regulation 2016/679) - the President of the Personal Data Protection Office found a breach of the provisions of Regulation 2016/679 as a result of the notification of the breach of personal data protection made by the Administrator, however in connection with with the fact that by making this notification, the Administrator only fulfilled the legal obligation imposed on him, there are no grounds to recognize that this circumstance constitutes a mitigating circumstance for him. In accordance with the Guidelines on the application and determination of administrative fines for the purposes of Regulation 2016/679 Wp. 253 "The supervisory authority may become aware of a breach as a result of investigations, complaints, press articles, anonymous indications or notification by the data controller. Pursuant to the regulation, the controller is obliged to notify the supervisory authority of a breach of personal data protection. Mere compliance with this obligation by an administrator cannot be interpreted as a weakening / mitigating factor ”.

2. Compliance with previously applied measures in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679) - in this case, measures referred to in Art. 58 sec. 2 of Regulation 2016/679.

3. Application of approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of Regulation 2016/679 (Article 83 (2) (j) of Regulation 2016/679) - the administrator does not apply approved codes of conduct or approved certification mechanisms referred to in the provisions of Regulation 2016/679.

Taking into account all the above-mentioned circumstances, the President of the Personal Data Protection Office decided that imposing an administrative fine on the Controller is necessary and justified by the weight, nature and scope of the alleged infringement of the provisions of Regulation 2016/679. It should be stated that any other remedy provided for in Art. 58 sec. 2 of Regulation 2016/679, and in particular stopping at an admonition (Article 58 (2) (b) of Regulation 2016/679), would not be

proportionate to the identified irregularities in the processing of personal data and would not guarantee that the abovementioned the entity will not commit a similar negligence in the future.

In the opinion of the President of the Personal Data Protection Office, the administrative fine imposed on the Sułkowice Cultural Center based in Sułkowice in the amount of PLN 2,500 (in words: two thousand five hundred zlotys), under the established circumstances of this case, performs the functions referred to in Art. 83 sec. 1 of Regulation 2016/679, i.e. it is effective, proportionate and dissuasive in this individual case. At this point, the content of Art. 102 paragraph 2 of the Personal Data Protection Act, from which there is a limitation of the amount (up to PLN 10,000) of the fine that may be imposed on a unit of the public finance sector, referred to in art. 9 point 13 of the aforementioned Act of 27 August 2009 on public finance.

In the opinion of the President of the Personal Data Protection Office, the penalty imposed on the Controller is proportional to the seriousness of the breach in the context of the basic objective of Regulation 2016/679 - protection of the fundamental rights and freedoms of natural persons, in particular the right to personal data protection.

At the same time, in the opinion of the President of the Personal Data Protection Office, the penalty in this amount will be effective (it will achieve the goal of punishing the Administrator for a serious infringement with serious consequences) and dissuasive in the future (it will cause the Administrator, in order to avoid further sanctions, to pay due attention to the processing of personal data through and with the help of The Processing Entity).

Summing up the above, in the opinion of the President of the Personal Data Protection Office, the administrative fine imposed in this case meets the conditions (the penalty functions) referred to in Art. 83 sec. 1 of Regulation 2016/679, due to the seriousness of the infringement found in the context of the basic requirements and principles of Regulation 2016/679.

Bearing in mind the above, the President of the Personal Data Protection Office resolved as in the operative part of this decision.

[1] Guidelines 07/2020 of the European Data Protection Board on the concepts of controller and processor included in the GDPR (Version 2.0, adopted on July 7, 2021), hereinafter referred to as Guidelines 07/2020;

2022-09-16