THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 19

November

2020

DECISION

DKE.561.21.2020

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended) in connection with Art. 7 and art. 60 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and pursuant to Art. 31 and art. 58 sec. 1 lit. e) in connection with Art. 58 sec. 2 lit. b) 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 data protection regulations ) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), after conducting administrative proceedings regarding the processing of personal data by K. Sp. z o.o., President of the Personal Data Protection Office, gives a reminder K. Sp. z o.o. for violation of the provisions of Art. 31 and art. 58 sec. 1 lit. a) Regulation of the European Parliament and of the EU Council 2016/679 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, as amended), hereinafter referred to as "Regulation 2016/679", consisting in the lack of cooperation with the President of the Personal Data Protection Office as part of the tasks and failure to provide information necessary for the President of the Personal Data Protection Office to perform his tasks.

Justification

The President of the Personal Data Protection Office (hereinafter also: "President of the Personal Data Protection Office") received a notification of suspicion of committing a crime submitted by K. Sp. z o.o. (hereinafter referred to as the "Company") to the Provincial Police Headquarters in G. This notification concerned the failure of the server operating in the Company the system of booking and selling hotel and catering services. The failure consisted in the encryption of database files located on the above-mentioned server via malware.

Due to the fact that the Company has not notified the breach of personal data protection to the supervisory authority pursuant to Art. 33 of the Regulation 2016/679, the President of the Personal Data Protection Office (UODO) initiated an explanatory procedure (reference number [...]) to determine whether, in connection with the notification by the President of the Company, a breach of security (failure of the server servicing the booking system and sale of hotel and catering services consisting in encryption of database files by malicious software), an analysis has been made in terms of the risk of data protection breach, resulting in the need to notify the President of the Personal Data Protection Office and persons affected by the breach of personal data protection.

In a letter of [...] February 2020, the President of the Personal Data Protection Office asked the Company to provide information on whether an analysis was made in terms of the risk of data protection breach resulting in the need to notify the President of the Personal Data Protection Office and persons affected by the breach of personal data protection. In addition, in this letter, the Company was informed about the obligation to report a breach of personal data protection in accordance with Art. 33 of the Regulation 2016/679.

This letter was delivered to the Company on [...] February 2020, which was confirmed on the "Confirmation of receipt of the letter-post item". Due to the lack of response to the above-mentioned a letter, an employee of the Personal Data Protection Office on [...] May 2020, conducted a telephone conversation with Ms L. C. representing the Company (tel. no. [...]) regarding the lack of response to the above-mentioned writing. Ms L. C. informed that she had not received this letter and asked for it to be sent again. Therefore, on [...] May 2020, a letter was sent to the Company with another summons to immediately provide explanations in the matter. This letter was delivered on [...] May 2020, which was confirmed on the "Confirmation of receipt of the letter-post item". The Company did not reply to this letter either. In view of the above, on [...] July 2020, another letter was sent to the Company with a renewed request to provide explanations immediately. The letter was delivered on [...] August 2020, which was confirmed on the "Confirmation of receipt of the letter-post item". The company did not reply to this letter either. Thus, despite the three effective summons to provide explanations, the Company did not provide relevant explanations in the matter.

By letter of [...] February 2020, the Company was informed that failure to respond to the requests of the President of the Personal Data Protection Office may result - in accordance with Art. 83 sec. 5 lit. e) in connection with joke. 58 sec. 1 lit. a) and e) of Regulation 2016/679 - imposing an administrative fine on the Company.

Due to the failure by the Company to provide the information necessary to settle the case with ref. No. [...], the President of the Personal Data Protection Office (UODO) initiated ex officio against the Company - pursuant to Art. 83 sec. 5 lit. e) Regulation 2016/679, due to the breach by the Company of art. 31 and art. 58 sec. 1 letter a) of the Regulation 2016/679 - administrative proceedings to impose an administrative fine on the Company (reference number DKE.561.21.2020).

The Company was informed about the initiation of the procedure by letter of [...] October 2020, properly delivered to the Company on [...] October 2020.

In response to the letter informing about the initiation of proceedings to impose an administrative fine on the Company, the President of the Management Board of the Company, in accordance with Art. 33 of the Regulation 2016/679, reported a breach of personal data protection, which allowed the President of the Personal Data Protection Office to conduct further proceedings in case no. […].

In addition, in a letter of [...] October 2020, the President of the Management Board of the Company explained that:

On [...] December 2019 at [...] there was a failure of the Company's server containing the hotel software database. The failure consisted in the inability to access the database located on a local server located in a hotel in a locked cabinet […]. The receptionist could not log into the system from the computer located in the hotel reception to serve the guests. The President of the Company, the network administrator and the personal data protection officer were immediately informed about this situation. As a result of the actions taken, it turned out that the database on the server was encrypted with software that the anti-virus did not detect. It has been established that the encryption was performed by a Trojan named Viki. As a result of further checks of the personal data breach, leakage of data on the server was excluded.

To the above-mentioned the event could have occurred in connection with the server's maintenance works that were in progress before and the works related to the installation of new and additional software related to the adaptation of the hotel system to the new accounting requirements and better system security.

The files on the server's disk were secured and transferred to the Provincial Police Headquarters in G., Department of Combating Cybercrime. The investigation in this case was discontinued due to the failure to identify the perpetrator, i.e. pursuant to Art. 322 of the Act of June 6, 1997, Code of Criminal Procedure (Journal of Laws of 2020, item 30, as amended) (proof: decision [...]).

The company purchased new disks and started installing the software from scratch.

As the justification for the lack of cooperation with the President of the Personal Data Protection Office, Ms L. Cz., Representing K. Sp. z o.o. indicated that the failure of the server operating in the Company for the booking system and sales of hotel and catering services caused a lot of stress both for her and for its employees (pre-holiday period). The difficult situation related to the event, as well as the difficult family situation (she brings up three children alone), resulted in greater focus on the correct resumption of the reception and the entire system operating the hotel, as on the tracking of the correspondence received by the Company. Also the situation related to the COVID-19 pandemic led Ms. L. Cz. to the fear of ensuring the safety of both the family, guests and the Company's finances.

In a letter of [...] October 2020, Mrs. L. Cz. apologized to the President of the Personal Data Protection Office for the lack of proper cooperation with him in connection with the proceedings under reference number [...], she asked for understanding of the difficult situation related to the above-mentioned incident (purchase and implementation of new drives), as well as taking into account its difficult family and financial situation, in particular related to the COVID-19 epidemic.

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. 57 sec. 1 lit. a) Regulation 2016/679, the President of the Personal Data Protection Office - as a supervisory authority within the meaning of art. 51 of Regulation 2016/679 - monitors and enforces the application of this regulation on its territory. As part of his competences, the President of the Personal Data Protection Office examines, inter alia, Complaints brought by data subjects shall investigate these complaints to the appropriate extent and inform the complainant of the progress and the outcome of these proceedings within a reasonable time (Article 57 (1) (f)). In order to enable the performance of such defined tasks, the President of the Personal Data Protection Office has a number of specified in Art. 58 sec. 1 of Regulation 2016/679, the rights in the scope of conducted proceedings, including the right to order the administrator and the processor to provide all information needed to perform its tasks (Article 58 (1) (a)) and the right to obtain access from the administrator and the processor to all personal data and all information necessary for the performance of its tasks (Article 58 (1) (e)).

Moreover, the President of the Personal Data Protection Office is entitled to a number of provisions specified in Art. 58 sec. 2 corrective powers, including reminders to the administrator or processor in the event of violation of the provisions of Regulation 2016/679 by processing operations.

Violation of the provisions of Regulation 2016/679, consisting in the failure of the administrator or processor to provide access to the data and information referred to above, results in a violation of the authority's rights specified in art. 58 sec. 1 (including the right to obtain data and information necessary to perform its tasks). Consequently, it is subject - in accordance with Art. 83 section 5 letter e) in fine of Regulation 2016/679 - an administrative fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year, with the higher amount applicable . It should also be indicated that the controller and the processor are obliged to cooperate with the supervisory authority in the performance of its tasks, as provided for in Art. 31 of Regulation 2016/679.

The President of the Personal Data Protection Office, acting pursuant to art. 58 sec. 2 lit. b) of Regulation 2016/679, it may also consider it justified to issue a reminder to the Company in the scope of the infringement of the provision of art. 31 in connection with Art. 58 sec. 1 lit. e) Regulation 2016/679.

Pursuant to recital 148 of Regulation 2016/679, for more effective enforcement of the provisions of the Regulation, sanctions, including administrative fines, should be imposed for breaches of the Regulation, in addition to or instead of appropriate measures imposed by the supervisory authority under this Regulation. If the infringement is minor, the fine may be replaced by an admonition. However, due attention should be paid to the nature, gravity and duration of the breach, whether the breach was not intentional, the steps taken to minimize the harm, the degree of liability or any previous relevant breach, how the supervisory authority became aware of on a breach, on compliance with the measures imposed on the controller or processor, on the application of codes of conduct, and on any other aggravating or mitigating factors.

Referring the above-mentioned provisions of the Regulation 2016/679 to the actual state of affairs established in this case, and described at the beginning of this decision, it should be stated that the Company - personal data administrator, - as a party to the proceedings conducted by the President of the Personal Data Protection Office (UODO) no. [...] undoubtedly breached the obligation to provide the President of the Personal Data Protection Office with access to additional information necessary for the performance of his tasks - in this case, to determine whether, in connection with the notification by the data administrator of a breach of security (failure of the server servicing the booking system and sales of hotel and catering services, consisting in the encryption of database files by malicious software), an analysis was made in terms of the risk of data protection breach, resulting in the need to notify the President of the Personal Data Protection Office and persons affected by the breach of personal data protection.

In response to the information about the initiation of administrative proceedings in the case with reference number DKE.561.21.2020. The President of the Management Board of the Company in accordance with Art. 33 of the Regulation 2016/679, reported a breach of personal data protection, which allowed the President of the Personal Data Protection Office to conduct further proceedings in case no. […]. Moreover, in a letter of [...] October 2020, the President of the Management Board of the Company provided detailed explanations justifying the short-term lack of cooperation with the President of the Personal Data Protection Office in connection with the proceedings with reference number […].

When deciding to impose a sanction in the form of a warning on the Company in this case, the President of the Personal Data Protection Office took into account the following circumstances affecting the assessment of the violation:

Nature, gravity and duration of the infringement (Article 83 (2) (a) of Regulation 2016/679).

The breach sanctioned in the present case affects the system of protection of personal data. An important element of this system, the framework of which is set out in Regulation 2016/679, are supervisory authorities with tasks related to the protection and enforcement of the rights of natural persons in this respect. In order to enable the performance of these tasks, supervisory authorities have been equipped with a number of control powers, powers to conduct administrative proceedings and remedial powers. On the other hand, administrators and processors have been imposed specific obligations, correlated with the powers of supervisory authorities, including the obligation to cooperate with supervisory authorities and the obligation to provide these authorities with access to personal data and other information necessary to perform their tasks.

In the opinion of the President of the Personal Data Protection Office, the Company's actions certainly resulted in a short-term lack of access to evidence indicating the obligation to report a breach of personal data protection to the supervisory authority referred to in Art. 33 of the Regulation 2016/679.

The Article 29 Working Party in the Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 adopted on 3 October 2017 with reference to the intentional or unintentional nature of an infringement indicated that, in principle, "intention" encompasses both knowledge and intent. due to the characteristics of a prohibited act, while "inadvertent" means no intention to cause an infringement, despite the controller or processor's failure to fulfill the legally required duty of care. Intentional violations are more serious than unintentional violations and, consequently, more often involve the imposition of an administrative fine. In the opinion of the President of the Personal Data Protection Office, the above-mentioned the breach was unintentional, one can speak of negligence. On the part of the Company, there was a will to

cooperate in providing the authority with all information (evidence) necessary to continue the proceedings under reference number […].

Lack of cooperation with the supervisory authority to remove the breach and mitigate its possible negative effects (Article 83 (2) (f) of Regulation 2016/679).

In the course of these proceedings, the Company expressed its willingness to cooperate with the President of the Personal Data Protection Office (UODO) in order to remedy the violation consisting, in particular, in providing explanations in the scope in which the conduct of the proceedings with reference number [...], she apologized for the lack of this cooperation, also justifying the lack of cooperation with the difficult epidemic situation in the country.

The other conditions set out in Art. 83 sec. 2 of Regulation 2016/679 did not affect (aggravating or mitigating) the assessment of the infringement made by the President of the Personal Data Protection Office (including: any relevant prior infringements by the controller, the manner in which the supervisory authority learned about the infringement, compliance with the measures previously applied in the same case , the use of approved codes of conduct or approved certification mechanisms) or, due to the specific nature of the breach (relating to the controller's relationship with the supervisory authority and not the controller's relationship with the data subject), could not be taken into account in the present case (in including: the number of injured persons and the extent of the damage suffered by them, actions taken by the administrator to minimize the damage suffered by data subjects, the degree of administrator's liability, taking into account the technical and organizational measures implemented by him, categories of personal data affected by the infringement zenie).

In connection with the above, acting pursuant to Art. 58 sec. 2 lit. b) of Regulation 2016/679, according to which each supervisory authority has the right to issue a reminder to the controller or processor in the event of violation of the provisions of this Regulation by processing operations, the President of the Personal Data Protection Office deems it justified to provide the Company with a reminder regarding the breach of the provision art. 31 in connection with Art. 58 sec. 1 lit. e) Regulation 2016/679.

The President of the Personal Data Protection Office decided that in this case, in the light of the criteria specified in Art. 83 sec. 2 GDPR, will be sufficient and at least as “effective, proportionate and dissuasive” as imposing a fine (see Art. 83 (1) GDPR).

It should also be noted that in the event of a similar event occurring in the future, each reminder issued by the President of the Personal Data Protection Office against the Company will be taken into account when assessing the premises for a possible

administrative penalty, in accordance with the principles set out in Art. 83 sec. 2 of the Regulation 2016/679.

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

The decision is final. The party has the right to lodge a complaint against the decision with the Provincial Administrative Court in Warsaw, within 30 days from the date of its delivery, via the President of the Personal Data Protection Office (address: ul. Stawki 2, 00-193 Warsaw). The fee for the complaint is PLN 200.

In the proceedings before the Provincial Administrative Court, the party has the right to apply for the right of assistance, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right to assistance may be granted at the request of a party submitted prior to the initiation of the proceedings or in the course of the proceedings. The application is free of court fees.

2021-02-05