THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 10

September

2019

DECISION

ZSPR. 421.2.2019

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 section 1 and section 2, art. 60, art. 101, art. 103 of the Personal Data Protection Act of May 10, 2018 (Journal of Laws of 2018, item 1000, as amended) in connection with Art. 5 sec. 1 lit. a and lit. f, art. 5 sec. 2, art. 6 sec. 1, art. 7 sec. 1, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b, lit. d, art. 32 sec. 2, art. 58 sec. 2 lit. and and with Art. 83 sec. 3, art. 83 sec. 4 letter a, art. 83 sec. 5 lit. a 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 UE L 119 of 04/05/2016, page 1 and, Journal of Laws UE L 127 of 23/05/2018, page 2), after administrative proceedings regarding the processing of personal data by Morele.net Sp. z o. o. with headquarters in Krakow at ul. Fabryczna 20A, President of the Personal Data Protection Office finding a breach by Morele.net Sp. z o. o. with headquarters in Krakow at ul. Fabryczna 20A, the provisions of Art. 5 sec. 1 lit. a and lit. f, art. 5 section 2, art. 6 sec. 1, art. 7 sec. 1, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b, lit. d, art. 32 sec. 2 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 UE L 119 of 04.05.2016, p. 1, and Journal of Laws UE L 127 of 23.05.2018, p. 2), hereinafter: "Regulation 2016/679" imposes on Morele.net Sp. z o. o. with headquarters in Krakow at ul. Fabryczna 20A, a fine in the amount of PLN 2,830,410 (equivalent to EUR 660,000), according to the average EUR exchange rate announced by the National Bank of Poland in the exchange rate table as of January 28, 2019.

JUSTIFICATION

On [...] November 2018, Morele.net Sp. z o. o. with headquarters in Krakow at ul. Fabryczna 20A, (hereinafter referred to as the "Company"), reported to the President of the Personal Data Protection Office (hereinafter also referred to as the "President

of the Personal Data Protection Office") two violations of personal data protection, which related to the unauthorized access to the customer database of morele.net, hulahop online stores .pl, amfora.pl, pupilo.pl, trenkuje.pl, motoria.pl, digitalo.pl, ubieramy.pl, Meblekuje.pl, sklep-presto.pl, budkuje.pl and the unauthorized access to [...] , and as a consequence of obtaining personal data of customers making purchases in the above-mentioned online stores. Then, on [...] December 2018, the Company reported to the President of the Personal Data Protection Office another breach consisting in obtaining unauthorized access to [...].

From [...] to [...] January 2019, in order to control the compliance of data processing with the provisions on the protection of personal data, inspections were carried out at Morele.net Sp. z o. o. with headquarters in Krakow at ul. Fabryczna 20A. The scope of the control covered the processing of personal data of customers of online stores: morele.net, hulahop.pl, amfora.pl, pupilo.pl, trenuje.pl, motoria.pl, digitalo.pl, ubieramy.pl, Mebleuje.pl, sklep-presto. pl, buduje.pl, the administrator of which is the Company.

On the basis of the collected evidence, it was found that in the process of processing personal data, the Company, as the controller, breached the provisions on the protection of personal data. These shortcomings consisted in: breach by the Company of the principle of confidentiality of data expressed in Art. 5 paragraph 1 lit. f 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 UE L 119 of 04/05/2016, p. 1, and OJ L 127 of 23/05/2018, p. 2), hereinafter referred to as "Regulation 2016/679", reflected in the form of obligations set out in art. 24 paragraph 1, art. 25 sec. 1 and art. 32 sec. 1 lit. b and d, art. 32 sec. 2 of Regulation 2016/679 consisting in the failure to ensure the security and confidentiality of the processed personal data, which resulted in unauthorized persons having access to the personal data of the Company's clients and in violation of the principle of legality, reliability and accountability expressed in art. 5 paragraph 1 lit. a and art. 5 sec. 2 of Regulation 2016/679, detailed in art. 7 sec. 1 and art. 6 sec. 1 of Regulation 2016/679, by failing to prove that personal data from installment applications collected before May 25, 2018 were processed by Morele.net Sp. z o. o. with headquarters in Krakow on the basis of the consent of the data subject.

The President of the Personal Data Protection Office, on the basis of the collected evidence, determined the following facts of the case:

The core business of the Company is retail sale via mail order houses or the Internet. The company runs the following online stores: morele.net, hulahop.pl, amfora.pl, pupilo.pl, trenuje.pl, motoria.pl, digitalo.pl, ubieramy.pl, nazwa się.pl, sklep-presto.pl, buduje.pl .

The company, in connection with its activities, processes the personal data of customers who have registered on the morele.net website (and the websites of other stores, mentioned above, whose administrator is the Company). The number of people whose data is processed by the Company is approximately 2,200,000 (approximately two million two hundred thousand). The scope of this data includes: name, surname, e-mail address (e-mail), telephone number and address for service, and access to this data is granted to [...]. Until December 2018, the Company also processed data from installment applications. The scope of this data included: name, surname, e-mail address (e-mail), telephone number, PESEL number, series and number of an identity document, date of issuance of an identity document, expiry date of an identity document, education, registration address, correspondence address, source income, monthly net income, household costs, number of dependents, marital status, amount of monthly other liabilities in financial institutions, information on the amount of maintenance and other obligations resulting from court judgments (collected since 2016). Their total number was about 35,000 […].

[…].

On [...] November 2018, the Company was informed by customers that they had received short text messages (SMS) informing them of the need to pay an additional fee of PLN 1 to complete the contract. The message contained a link to a fake DotPay electronic payment gateway. The company immediately notified the Police about the incident and attempted to clarify the matter.

[…]

The breach of personal data protection was identified by the Company on [...] November 2018.

Following monitoring activities, on [...] November 2018, the Company reported the breach to the President of the Personal Data Protection Office. Moreover, the Company posted information on false text messages on its website. The same information was sent to customers by e-mail and text messages. On [...] December 2018, the Company re-informed the data subjects of the breach, informing, inter alia, about the potential access to data from installment applications.

As indicated in the notifications and supplementary notifications sent to the President of the Personal Data Protection Office,

the Company started work on introducing additional technical security measures, including as […].

On [...] November 2018, the Company received an e-mail from an unknown person informing about the theft of the Company's customer database.

On [...] November 2018, the Company notified to the President of the Personal Data Protection Office a violation regarding the potential unauthorized access to the Company's customer database. The infringement affected approximately 2,200,000 (approximately two million two hundred thousand) users.

On [...] December 2018, the Company sent 2,200,000 (approximately two million two hundred thousand) e-mails to customers containing a notification of unauthorized access to the customer database (the content of the notification of data subjects was sent to the Office in addition to the notification of violation ). In the above information addressed to customers, the Company informed that it does not process data from loan applications.

On [...] December 2018, the Company identified another unauthorized access to [...], used to resend fake text messages, about which 600 people were informed to whom the unauthorized person had access. [...] On [...] December 2018, this breach was reported to the President of the Personal Data Protection Office.

Due to the fact that the notification of data subjects did not meet the requirements set out in Art. 34 of the Regulation 2016/679, on [...] January 2019, the President of the Personal Data Protection Office pursuant to Art. 52 sec. 1 of the Act on the Protection of Personal Data of May 10, 2018 (Journal of Laws of 2018, item 1000, as amended), sent an application to the Company ordering re-notification of data subjects about the breach of their personal data and advising these people on how to minimize the potential consequences of the breach. In response to the request of the President of the Personal Data Protection Office, the Company again sent a notification of a personal data breach to 35,000 (thirty-five thousand) people.

In order to determine the circumstances of data protection violations reported by the Company and to determine the technical security measures applied by the Company, measures to minimize the effects of the breach and prevent similar events, on [...] January 2019, the President of the Office for Personal Data Protection sent a request to the Company to provide explanations.

In response to the call of [...] January 2019, the Company, in a letter of [...] January 2019, provided extensive explanations, including: a description of the activities carried out by the Company after the incident, a description of the Company's technical and organizational security measures , description of the procedure for handling requests from data subjects.

To the clarifications of [...] January 2019, the Company attached the financial statements for the financial year from 01/01/2017

to 31/12/2017, which show that the amount of net sales and equivalent revenues is: [...] .

As established during the inspection, prior registration is required to make purchases in online stores administered by the Company. The necessary information to set up an account includes the e-mail address (e-mail) and the password to the user account entered by the customer of the store. After logging in, the user has the option to enter their first name, surname, address and telephone number (for the purposes of determining the basic data necessary to deliver the purchased goods). The user account exists in the Company's system until the termination of the contract, ie until the user [MB1] deletes the account.

As it was established during the inspection, in 2016 the documentation concerning the processing of personal data applicable in the Company was updated. In 2017, the Company began work related to the application of the provisions of Regulation 2016/679, in the field of adapting the website, user profile, newsletter, adapting documents within the Company, document circulation in the Company, physical and technical security measures. As indicated in the explanations adopted during the audit, the risk analysis was carried out by the Company on an ad hoc basis for individual processes, in an informal manner. During the inspection, a copy of the internal documentation of the Company was obtained, entitled "Report after the database theft" (Annex B10 to the control protocol), […].

[…].

As it was established during the inspection, the servicing module […] does not save the information entered by the client in the Company's database. […]

According to the explanations adopted during the inspection, the Company has never collected data on scans of identity cards belonging to clients submitting […]. From around [...] October 2018, the installment purchase form had a place to enter only the amount of maintenance obligations or the amount of obligations resulting from other court decisions. The company does not confirm that such data was recorded in the database removed in December 2018.

In a letter of [...] February 2019, the Company applied to the President of the Personal Data Protection Office with a request for an urgent examination of the case, indicating that due to the media nature of the case and the uncertainty as to how the case will be resolved by the President of the Personal Data Protection Office, the possible lengthy consideration of the case may pose a threat to the functioning of the Company. […].

In connection with the above, on [...] June 2019, in the letter: ZSPR.421.2.2019 / 43412, the President of the Office for

Personal Data Protection initiated ex officio administrative proceedings regarding the identified deficiencies, in order to clarify the circumstances of the case.

In response to the notification of the initiation of administrative proceedings, the Company's representative (power of attorney in the case files), by letter of [...] July 2019, provided explanations in which he indicated, inter alia, that:

In the opinion of the Company, the findings made in the course of the inspection do not indicate that the Company violated Art. 5 sec. 1 lit. f, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b and d, art. 32 sec. 2 of Regulation 2016/679.

During the inspection (as requested by the inspectors), the company presented the content of the consent clause legalizing the processing of data from installment applications, therefore it cannot be considered that the Company processed data from installment applications without a legal basis and, consequently, the statement of the President of the Office of Protection is not correct. Personal Data that in this respect the Company violates Art. 5 sec. 1 lit. a and art. 5 sec. 2 of Regulation 2016/679.

The company had technical and organizational security measures adequate to the identified threats, taking into account the conditions set out in Art. 24 and in art. 32 of Regulation 2016/679.

The company performed the risk analysis of the existing threats on an ongoing basis and implemented new and up-to-date methods of ensuring the security of the processed data, taking into account the conditions specified in Art. 24 and in art. 32 of Regulation 2016/679.

The company does not agree with the allegation that it did not perform an ongoing assessment and did not monitor potential threats to the rights and freedoms of the persons whose data it processes, because the Company has been regularly conducting research, verifying threats, and hiring external companies to conduct security audits for many years. On this circumstance, during the inspection, the Company provided a number of pieces of evidence [...]

The company also referred to the list of applied security measures submitted during the inspection.

In the Company's opinion, indirect evidence confirming the fact of ongoing monitoring of threats and the introduction of adequate security measures is the Company's reaction to the suspected data leak, which took place in November 2018. The Company updated its risk position and implemented new safeguards [...] and suspended the data collection process from installment forms. These activities were not of a one-off nature (caused by a security incident). The Company always took appropriate actions when the IT team or IOD recommended the necessity to update, modernize or extend the security of personal data processing.

Confirmation of the monitoring of collateral in the Company are orders that are drawn up in order to improve collateral, [...].

The company also disagrees with the allegation that potential threats are not monitored on an ongoing basis. This claim is not supported by any evidence gathered during the audit. On the contrary, in the opinion of the Company, the collected material indicates that actions in the above scope were undertaken. The President of the Personal Data Protection Office did not specify to what extent, in his opinion, the Company breached the obligation to monitor threats on an ongoing basis, which makes it impossible to refer to the formulated allegation more precisely and to formulate additional evidence conclusions.

Regulation 2016/679 imposes on administrators the obligation of appropriate (to threats) safeguards, and not effective safeguards in all circumstances. The processing risk always exists, regardless of the measures used. The administrator's task is to minimize them by applying adequate measures, which the Company has done and is doing.

Contrary to the claims of the President of the Personal Data Protection Office regarding the selection of ineffective measures at the level of network traffic monitoring, the Company monitors network traffic, as evidenced by the adopted technical security measures including network traffic monitoring, i.e. […].

The Company also points out that the "Report after the database theft" (Annex B10 to the control protocol) would not arise if the Company did not monitor the traffic (see the table showing the level of network traffic).

In the opinion of the Company, there are no grounds to conclude that the Company did not check the level of data security on an ongoing basis and did not adjust it to the identified threats.

In the opinion of the Company, the allegation that the risk of gaining access to […] was not assessed is not confirmed by the evidence collected during the inspection. The risk analysis carried out by the Company shows that only authorized persons (employees of the Company) who were granted appropriate permissions had access to [...].

The company also points out that Regulation 2016/679 requires the analysis and evaluation of personal data processing processes, and not individual IT systems. IT systems (and their security) are only applied technical measures, referred to e.g. in art. 24 sec. 1 of Regulation 2016/679 or in art. 32 sec. 1 of Regulation 2016/679.

The analysis of the facts and the reassessment of the risks resulted in the Management Board of the Company making a decision to […].

Due to the fact that the President of the Personal Data Protection Office, summarizing the allegations, stated that the earlier implementation and introduction of additional measures could significantly reduce the risk of obtaining unauthorized access,

the Company notes that this thesis was not supported by any arguments, as well as justification why, taking into account the security measures applied by the Company, were they are inappropriate.

According to the Company's assessment, the applied technical and organizational security measures were adequate to the risks related to the processing of personal data, in accordance with Art. 24 sec. 1 and 32 sec. 1 of Regulation 2016/679. There are no grounds for contradicting theses in the evidence. The company's position is that the applied technical and organizational security measures were adequate to the threats and met the conditions set out in the regulations.

Referring to the objection of the President of the Personal Data Protection Office that the Company is not able to accurately indicate the date of launching the functionality of saving data from installment applications, the Company indicates that the content of the consent is on the first page of Appendix A22 and Appendix A23 to the inspection protocol. […]. Therefore, the objection of the President of the Personal Data Protection Office in the above-mentioned scope is incorrect and has no support in the collected evidence.

The evidence does not justify the allegation made by the President of the Personal Data Protection Office that the Company does not have a documented analysis of the data processing process in terms of the functionality of saving data from installment applications. The evidence shows that the Company verified, assessed and monitored the data processing process related to installment applications on an ongoing basis. An example of an analysis conducted is [...] determining the content of the consent, which was prepared in connection with the ongoing analysis of the processing process.

As an example of the analysis and application of appropriate (adequate) technical measures for personal data related to […]. Only the user (customer) of the store had the opportunity to display the data during the next filling in the installment form (Privacy-by-Default).

The company argued that, in accordance with the accountability principle, the controller is required to demonstrate compliance with Regulation 2016/679, but may use any means to do so, including, inter alia, system logs, procedures (regardless of whether they are in the form of a document or not). In the present case, accountability is exemplified by […].

Referring to the objection of the President of the Personal Data Protection Office that the Company removed personal data from installment applications without detailed analysis, the Company points out that Regulation 2016/679 allows and orders the deletion of data when the controller ceases to have the purpose of processing. The company has completed the processing of data, the processing of which was based on consent and had no other processing purposes, therefore the data was deleted.

The closing of the process was motivated by the risk analysis carried out in connection with the correspondence with the blackmailer.

Referring to the remark of the President of the Personal Data Protection Office that the Company has not documented the deletion of data, the Company indicates that due to the closure of the data processing process, the process has been removed from the Register of Processing Activities. The deletion of the database has also been documented […]. In addition, the President of the Personal Data Protection Office did not indicate a provision that the Company would breach in connection with the deletion of the database.

In the opinion of the Company, the evidence collected in the case does not justify the statement of the President of the Office for Personal Data Protection that the Company processed personal data from installment applications without a legal basis, i.e. without the consent of the data subject, because the content of the collected consents is included in Annex A22 and Annex A23 to the inspection report.

In addition, in a letter constituting a response to the notification of the initiation of administrative proceedings, the Company's representative requested the President of the Personal Data Protection Office for:

admitting and taking evidence from an expert opinion in the field of IT systems security in order to: a) establish technical standards and organizational security measures in the business activities of entrepreneurs in the area of e-commerce, with a scale and nature similar to the scale and nature of the Company's operations in 2018; b) assessing whether the technical and organizational measures applied by the Company met the standards of security measures in the economic activities of entrepreneurs in the area of e-commerce, with a scale and nature similar to the scale and nature of the Company's operations in 2018; c) assessing whether the technical and organizational measures used by the Company were appropriate, taking into account the state of technical knowledge, implementation cost and the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probability and severity of the threat;

attaching to the files of the proceedings a copy of the previous correspondence between the Personal Data Protection Office and the Company (letter of the Company of [...] January 2019, letter of the Company of [...] February 2019, as well as notifications of infringements made by the Company).

By a decision of [...] August 2019, the President of the Personal Data Protection Office refused to accept the Company's request to admit and to conduct an expert opinion.

In response to the decision of [...] August 2019 and the information on the collection of evidence on [...] August 2019, the attorney of the Company upheld the current position of the Company and requested that the administrative proceedings in question be discontinued. In particular, the Company upholds its previously expressed position that there is no evidence of a breach of the provisions on the protection of personal data by the Company, in particular with regard to the application of appropriate security measures, and does not agree with the statement of the President of the Data Protection Office contained in the notice of initiation of the procedure of [... ] June 2019 on infringement of the provisions of Regulation 2016/679.

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

1. Article 5 of Regulation 2016/679 lays down the rules for the processing of personal data that must be respected by all administrators, i.e. entities that independently or jointly with others determine the purposes and methods of personal data processing. Pursuant to Art. 5 sec. 1 lit. f of Regulation 2016/679, personal data must be processed 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 ("confidentiality and integrity") .

Pursuant to Art. 24 sec. 1 of Regulation 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons of varying probability and seriousness, the controller implements appropriate technical and organizational measures to ensure that the processing takes place in accordance with this Regulation and to be able to demonstrate it. These measures are reviewed and updated as necessary.

Pursuant to Art. 25 sec. 1, both when specifying the methods of processing and during the processing itself, the controller implements appropriate technical and organizational measures designed to effectively implement data protection principles (taking into account data protection at the design stage).

Pursuant to Art. 32 sec. 1 lit. b of the Regulation 2016/679, taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probabilities and severity, the controller and the processor implement appropriate technical and organizational measures to ensure the level of security corresponding to this risk, including, inter alia, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, as appropriate, and pursuant to Art. 32 sec. 1 lit. d of Regulation 2016/679, regular testing, measurement and evaluation of the effectiveness

of technical and organizational measures to ensure the security of processing.

Pursuant to Art. 32 sec. 2 of Regulation 2016/679, the controller, when assessing whether the level of security is appropriate, takes into account in particular the risk associated with the processing, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

The provisions of Art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 letter b and d and art. 32 sec. 2 of the Regulation 2016/679 are therefore a specification of the provisions referred to in Art. 5 sec. 1 lit. f of the Regulation 2016/679, confidentiality rules. Therefore, the case at hand should be analyzed in terms of meeting the conditions that determine the level of appropriate technical and organizational measures to be applied.

The principle of confidentiality, the correct implementation of which ensures that the data is not disclosed to unauthorized persons, was breached in the actual state of the case as a result of double access to […]. [...] and to the data of all customers from the Company's database system resulted in the materialization of the risk of violating the rights and freedoms of natural persons whose data is processed by the Company, in the form of a method called phishing, aimed at phishing data, including credentials to the bank account by impersonating the Company in SMS messages and using the fact that the customer has placed the order.

The said breach of confidentiality, in the opinion of the President of the Personal Data Protection Office, should be considered from the perspective of two events: obtaining unauthorized access to […] and obtaining data of all clients from the Company's database system.

In the actual state of the case, in the opinion of the President of the Personal Data Protection Office, an ineffective authentication measure contributed to the event of obtaining unauthorized access [...].

As indicated by the Company in the letter of [...] January 2019, immediately after the finding of a breach consisting in gaining access [...] by an unauthorized person, work was undertaken to introduce additional technical security measures, including as […].

The President of the Personal Data Protection Office, in the notification of the initiation of administrative proceedings, indicated that the Company had not fulfilled the obligation under Art. 32 sec. 1 and 2 of Regulation 2016/679 consisting in the selection of effective technical and organizational measures at the level of access control and authentication. In response, the Company

indicated that its employees receive appropriate authorizations and authorizations to access individual IT systems and databases, and that access is supervised by a team of administrators. Moreover, it indicated that the Company's IT team monitors the functioning of [...] on an ongoing basis and adjusts the solutions to market standards and threats, and that used in the Company [...] made it possible to detect unusual behaviors.

In the opinion of the President of the Personal Data Protection Office due to […]. As evidenced by the material collected during the inspection, the Company used external security auditors (Annexes B11 and B12 to the inspection protocol) and implemented their recommendations with regard to the identified vulnerabilities in the software code used to process personal data. In the opinion of the supervisory authority, the ability to ensure continued confidentiality was insufficiently assessed and the risk of unauthorized access was not taken into account […]. As indicated by the Company in response to the notification about the initiation of administrative proceedings, "it is not the aim of the regulation to fully eliminate the risk, which cannot be done, but only to implement appropriate and proportionate technical and organizational solutions, taking into account the assessed criteria" and that Regulation 2016 / 679 "imposes on administrators the obligation of adequate (to threats) safeguards, and not safeguards that are effective in all circumstances."

It should be noted here that access control and authentication are the basic security measures aimed at protecting against unauthorized access to the IT system used to process personal data. Providing access to authorized users and preventing unauthorized access to systems and services is one of the model security elements, which is indicated, among others, by PN-EN ISO / IEC 27001: 2017-06 standard. According to Art. 32 sec. 1 of Regulation 2016/679, one of the factors that should be taken into account when selecting the appropriate technical and organizational measures is the state of technical knowledge, which should be assessed taking into account market conditions, in particular the availability and market acceptability of a given technical solution. Guidelines specifying this subject are provided by the applicable standards and norms, in particular ISO standards, which are also subject to constant reviews and changes conditioned by technological progress.

The European Network and Information Security Agency (ENISA) in its Guidelines on the Security of Personal Data Processing issued in 2016 [1] taking into account the above-mentioned of the standard (in the version of 2013) and the provisions of Regulation 2016/679, as part of access control and authentication, it recommends the use of the two-factor authentication mechanism for systems that include access to personal data.

In line with the risk-based approach resulting, inter alia, from joke. 25 sec. 1 of Regulation 2016/679, the selection of the appropriate authentication measure should be based on the risk assessment of the transaction or service carried out with it. The PN-ISO / IEC 29115: 2017□07 standard ("Information technology - Security techniques - Framework for the reasonable assurance of the levels of authentication"), like recitals 75 or 85 of Regulation 2016/679, indicates the possible consequences and effects of failed authentication depending on the applied level, incl. unauthorized disclosure of confidential information or financial loss.

The legitimacy of using properly selected technical means in the field of access control and authentication is also indicated by other organizations dealing with information security.

The OWASP Foundation, an international non-profit organization whose goal is to develop and disseminate good practices addressed to software developers, in its document "OWASP Top 10 - 2017" [2], presents a list of the greatest threats to web applications along with methods of preventing them. One of them is breaking the authentication agent (usually one-step). As a preventive measure, it is recommended to use multi-step authentication as a way to significantly minimize the risk of security breaches.

This document and the standard cited above also refer to the development of the American federal agency - the National Institute of Standards and Technology (NIST) of the document - "NIST 800-63B: Guidelines for Digital Identity: Authentication and Management. application lifecycle ”(Digital Identity Guidelines: Authentication and Lifecycle Management) [3].

Both the PN-ISO / IEC 29115: 2017 07 standard, the NIST 800-63B document and the studies of the OWASP organization indicate that the selection of the appropriate authentication agent should be preceded by a risk analysis and should be constantly reviewed.

The risk, in the actual state of the case in question, concerned the risk of using a method called phishing, aimed at phishing data, e.g. credentials to the bank account by impersonating the Company in SMS messages and using the fact that the customer has placed the order. As indicated in the literature, phishing attacks include attacks targeting specific groups of people (the so-called spearphishing) and the attacker spends time to obtain information about the target and create a personalized message related to the situation of a given person (in this case - a person who made a purchase transaction), which means that messages of this type (in the case in question - a text message requesting an additional fee of PLN 1 to complete the order, together with a link to a fake DotPay electronic payment gateway) may be difficult to detect and defend .

According to the annual reports on the activities of CERT Polska for 2016, 2017 and 2018, phishing is one of the most common types of incidents and the most distinctive category among other attacks, and the percentage of such incidents remains at a similar level (in 2018 about 44 percent). As CERT Polska points out, the most common motive of criminals is the desire to obtain credentials for various websites, including banks. Moreover, the spoofing scenarios, as was the case in the present case, became the most popular attack against e-banking users in 2018, causing significant financial losses. CERT Polska indicates that the first internships of this type took place in 2017, which is also confirmed by press reports.

In the factual state of the case, in the opinion of the President of the Personal Data Protection Office, ineffective monitoring of potential threats to the rights and freedoms, the data of which are processed by the Company, contributed to the event of obtaining unauthorized access to customer data from the Company's database system.

As the Company points out in the letter of [...] July 2019, the indication by the President of the Personal Data Protection Office in the notification on the initiation of administrative proceedings that potential threats are not monitored on an ongoing basis "is not (...) confirmed in any evidence collected during the control ". In addition, the Company indicated that "contrary to the claims of the President of the Personal Data Protection Office regarding the selection of ineffective measures", it monitors network traffic and indicated the adopted technical security measures in this respect, inter alia, […].

In the opinion of the President of the Data Protection Office, despite the application of such a solution, the Company was not able to react to an unusual event in the monitoring system consisting in increased data transmission. In the document "Report after the database theft" (Annex B10 to the control protocol) it was indicated that in [...].

The presented facts indicate that the Company, from October 2018 to January 2019, was not aware of the reasons for the increased data transmission. […]. In the opinion of the President of the Personal Data Protection Office, the measures adopted by the Company could be effective if they were properly adjusted and a procedure for reacting to adverse events such as unusual network traffic was implemented. ENISA, in its guidelines on the security of personal data processing, also indicates that the monitoring of events in IT systems is an important element enabling the identification of potential internal or external threats. This task should be performed in the form of appropriate implemented procedures and notification system about adverse events.

As it is emphasized in recital 76 of Regulation 2016/679 (the recitals include the rationale for the provisions of the enacting terms (articles) of the act such as the regulation), the risk should be assessed on the basis of an objective assessment that

determines whether the data processing operations involve a risk or high risk. risk. At the same time, the reasons for the occurrence of the risk related to the nature of the data, the scope of their processing, context and purposes, as well as other elements indicated in recital 75 of Regulation 2016/679, should be taken into account, taking into account Art. 32 of Regulation 2016/679, including - in particular - the relation of these reasons to data security and the effects of failure to ensure this security (Article 32 (2)).

Pursuant to Art. 32 sec. 2 and having regard to recital 83 of Regulation 2016/679, when assessing whether the level of security is appropriate, the risk associated with the processing (in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data) is taken into account in particular. sent, stored or otherwise processed) and which may, in particular, lead to physical, property or non-material damage (recital 83).

In the actual state of the case, the Company, processing personal data of over 2,200,000 users, which should be considered the processing of personal data on a large scale, and taking into account the scope of data and the context of processing, was obliged to more effectively assess and monitor potential threats to the rights and freedoms of persons whose data are processed.

Regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing is the responsibility of each controller and processor under Art. 32 section 1 lit. d of Regulation 2016/679. The administrator is therefore obliged to verify both the selection and the level of effectiveness of the technical measures used. The comprehensiveness of this verification should be assessed through the prism of adequacy to risks and proportionality in relation to the state of technical knowledge, implementation costs and the nature, scope, context and purposes of processing.

In the actual state of the case, the Company fulfilled this obligation, partially verifying only the effectiveness of the implemented security measures in terms of known vulnerabilities in the implemented software - as evidenced by security audits of the IT systems already in operation used to process the data of the Company's clients [...]. In the opinion of the President of the Personal Data Protection Office, the Company therefore did not take any steps to assess the selection of technical and organizational measures through the prism of risk adequacy. Performing reviews and updating implemented solutions are also a requirement formulated directly in Art. 24 sec. 1 sentence 2 of the Regulation 2016/679, as well as resulting from Art. 25 sec. 1 of Regulation 2016/679, creating an obligation to ensure privacy in the design phase (privacy by design) and imposing an

obligation on the controller to implement appropriate technical measures both in the phase of determining the processing methods and in the phase of the processing itself. Taking into account the nature, scope, context and purpose of data processing and the resulting risks for the rights and freedoms of natural persons, the controller is obliged to implement appropriate technical and organizational measures.

It should be noted that the earlier application of the implemented [...] December 2018 [...] and implemented [...] would significantly reduce the risk of unauthorized access by an unauthorized person, and thus minimize the risk of violating the rights or freedoms of natural persons whose data is processed by the Company , i.e. sharing data with unauthorized recipients.

To sum up, in the opinion of the President of the Personal Data Protection Office, the Company applied technical and organizational measures that contributed to a limited extent to the fulfillment of the requirements of Art. 32 of Regulation 2016/679, as foreseeable risks have not been adequately minimized and limited during processing.

2. The requirement under Art. 5 sec. 1 lit. and Regulation 2016/679 imposes on the controller the obligation to process data in accordance with the law, fairly and in a transparent manner for the data subject. The requirement to ensure the lawfulness of data processing operations means, inter alia, the need to meet at least one of the conditions for the legality of data processing, as specified in art. 6 of the Regulation 2016/679 and the need to ensure compliance with other provisions on the protection of personal data.

Pursuant to Art. 6 sec. 1 lit. and Regulation 2016/679, processing is lawful if the data subject has consented to the processing of his personal data for one or more specific purposes. According to Art. 4 point 11 of Regulation 2016/679, the consent of the data subject means a voluntary, specific, informed and unambiguous demonstration of the will, which the data subject, in the form of a declaration or a clear affirmative action, allows the processing of personal data relating to him.

However, from the content of Art. 7 sec. 1 of Regulation 2016/679, where the processing is based on consent, the controller must be able to demonstrate that the data subject has consented to the processing of his personal data. The administrator should implement organizational or technical measures to prove the receipt of the consent of the data subject, in particular in a manner allowing for the consolidation of the fact of receiving the consent.

To be correct for the purposes of evidence, related to the administrator in accordance with art. 7 sec. 1 of Regulation 2016/679, the burden of proof is the collection and recording of information on who gave consent and what its content was, when it was given, what information was received by the data subject when submitting the declaration of consent, what

information was provided on the manner of consent, and whether consent has been withdrawn and if so, when. The administrator has the above-mentioned information on the consent expressed by the data subject constitutes a detail of the general principle of accountability formulated in Art. 5 sec. 2 of Regulation 2016/679. If the controller is not able to demonstrate that and what consent to the processing of data has been expressed by the data subject, this consent may be questioned.

As it was established during the inspection, the Company obtained data from installment applications, which was to make it easier for customers to submit subsequent applications for installment purchases (auto-completion of the installment form). As indicated in the explanations, these data were not used by the Company for any other purpose of its own. The company is not able to precisely indicate the date of launching the functionality of saving data from installment applications (probably in 2016) and does not have a documented analysis of the data processing process in this respect. Evidence shows that around [...] December 2018, the Company, on oral instructions from [...], removed the database containing customer data from the so-called "Installment applications". No detailed analysis has been carried out in this respect and no data deletion has been documented.

Referring to the explanations regarding the violation of the principle of compliance with the law, fairness and accountability in the processing of personal data from installment applications, it should be emphasized that the Company has not been able to demonstrate since when it collected personal data in order to facilitate the fulfillment of future applications [...] and in this respect, it did not provide declarations of consent to such processing. The printout [...] only states that it is only in connection with the amendment to the provisions on the protection of personal data ("in connection with the GDPR") that two consents should be added on the [...] page.

Due to the fact that consents were obtained after the entry into force of Regulation 2016/679, and the process itself lasted from 2016 (explanations by the Company), it should be assumed that the deleted database contained data collected without a legal basis. […].

In the course of the inspection, the Company did not present any clauses or templates of consents used before the application of Regulation 2016/679, therefore it should be stated that the controller has not proved that it has obtained appropriate consents from persons whose data it has collected in the period from 2016 (as indicated in the explanations - the period from which the Company started obtaining data from installment applications) until May 2018 for the processing of data from installment applications.

For these reasons, the Company's explanations regarding the completed data processing process, in the absence of other evidence, are not sufficient to conclude that the processing itself was carried out in accordance with the law, including on the basis of a properly formulated premise of consent.

This approach of the Company to the data processing process, despite the fact that the process itself is considered closed (the data has been deleted), violates the basic principles of data processing, including the principle of legality and reliability indicated in art. 5 paragraph 1 lit. and Regulation 2016/679, because the controller must always be able to demonstrate that personal data are processed in accordance with the law. On the other hand, the principle of accountability (Article 5 (2) of Regulation 2016/67) requires the controller to be able to demonstrate that it complies with its obligations under the provisions on the protection of personal data. These requirements apply to all stages of data processing, which also applies to situations where data protection breaches occur or the processing undergoes significant changes. On the other hand, accountability applies not only at the time of collecting personal data, but throughout the processing, regardless of the information communicated or the method of communication. The company sent customers a notice of unauthorized access to the customer database, in which it informed that the unauthorized access did not apply to the information provided in installment applications because it does not collect such data, which could mislead customers. For these reasons, the administrator's decision to delete data, which was not preceded by a consistent analysis, proves that the basic principles of personal data protection referred to above were not respected.

Bearing in mind the above findings, the President of the Personal Data Protection Office, exercising his powers specified in art. 58 sec. 2 lit. and Regulation 2016/679, according to which each supervisory authority has the right 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 this regulation, an administrative fine under Art. 83 of Regulation 2016/679, having regard to the circumstances set out in the proceedings in question, stated that in the case under consideration there were premises justifying the imposition of an administrative fine on the Company.

When deciding to impose an administrative fine on the Company, 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:

a) The company failed to comply with the obligation to apply appropriate technical and organizational measures to ensure a level of security corresponding to the risk of unauthorized access to personal data of its clients, which resulted in double

access to [...] by an unauthorized person or persons, and consequently also access to the database data of all customers of the Company in the total number of approximately 2,200,000 (approximately two million two hundred thousand) people; therefore, the Company's activities aimed at ensuring the security of data processing prior to the occurrence of the violation should be considered ineffective, as they did not contribute to the elimination of the risk of damage;

b) the violation of Art. 5 sec. 1 lit. f in conjunction joke. 32 sec. 1 lit. b and d in connection with joke. 32 sec. 2 of Regulation 2016/679 consisting in obtaining unauthorized access to the Company's employee panel by an unauthorized person or persons, and consequently also access to the Company's customer database, is of considerable importance and serious nature, as it creates a high risk of negative legal consequences for approximately 2,200 000 (approximately two million two hundred thousand) persons, to whose data the person or unauthorized persons had access; Importantly, due to the double breach of the confidentiality of the Company's IT system, the risk is proportionally higher than 600 (six hundred) people; breach by the Company of the obligations to apply measures to ensure the security of the processed data, before their disclosure to unauthorized persons, entails a potential, but real possibility of using this data by third parties without the knowledge and against the will of the data subjects, contrary to the provisions of Regulation 2016/679, e.g. to enter into legal relationships or commitments on behalf of the data subjects; The seriousness of the breach is also significantly influenced by the fact that the Company, which processes personal data in a professional manner, as part of its activities, has greater responsibility and greater requirements than the entity that processes personal data as part of a side activity, incidentally or on a small scale; when conducting commercial activities, and at the same time collecting data via the Internet, the Company, as the data controller, should take all necessary actions and exercise due diligence in the selection of technical and organizational measures ensuring the security and confidentiality of data; the factual findings made by the President of the Personal Data Protection Office prove that the Company did not meet this task at the time of the identified violations;

c) violation of Art. 5 sec. 1 lit. f, art. 32 sec. 1 lit. b and d and art. 32 sec. 2 of Regulation 2016/679, arose as a result of failure to exercise due diligence by the Company and was undoubtedly unintentional, nevertheless, the Company as the controller is responsible for any irregularities found in the data processing process; the fact that the Company, despite the declaration of monitoring the network system and reacting in the 24/7 system (twenty-four hours, seven days a week), did not find it in real time, i.e. on 07/10/2018 - 14/10, deserves a particularly reprehensible assessment. .2018, increased traffic on the server's gateway and did not take any remedial actions at that time to prevent access to data by approximately 2,200,000

(approximately two million two hundred thousand) natural persons who are the Company's clients. In this state of affairs, the Company's negligence should be considered gross;

d) the breach of failure to ensure the security and confidentiality of the data lasted at least from [...] November 2018 (when the Company's customers informed about receiving text messages calling for an additional fee of PLN 1 to complete the order with a link referring to the fake DotPay electronic payment gateway) by [...] December 2018 (i.e. introducing additional technical security measures by the Company) - which should be considered a relatively short period; however, this circumstance may not have a mitigating effect on the supervisory authority's decision, as the breach concerned a significant number of natural persons; data leakage of 2,200,000 (about two million two hundred thousand) people - even if it is a short-term or one-off event - should be assessed strictly, due to its nature and high importance and scope, and also due to its possible long-term consequences for data subjects .

When determining the amount of the administrative fine, the President of the Personal Data Protection Office also took into account the mitigating circumstances affecting the final penalty, i.e .:

a) taking all possible actions by the Company to remove the violation; as it was established in the course of the proceedings, consequently in relation to the reported violations, the Company introduced, inter alia, […];

b) good cooperation on the part of the Company, which, both in the course of the inspection and during these proceedings, cooperated with the President of the Personal Data Protection Office in order to remove the breach and mitigate its possible negative effects; within the prescribed period, the Company sent explanations and replied to the request of the President of the Office for Personal Data Protection, therefore the degree of this cooperation should be assessed as full;

c) there is no evidence that the data subjects have suffered material damage, nevertheless the breach of confidentiality of data in itself constitutes non-pecuniary damage (harm); this is because individuals whose data has been accessed without authorization may, at the very least, fear losing control of their personal data, identity theft or fraud, and finally financial loss;

d) it has not been found that the Company previously violated the provisions of Regulation 2016/679, which would be relevant to the present proceedings.

The fact that:

a) The Company does not apply the 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,

b) in the same case, the measures referred to in Art. 58 sec. 2 of Regulation 2016/679,

c) there is no evidence that the Company obtained financial benefits and avoids losses in connection with the breach.

Taking into account all the above-mentioned circumstances, the President of the Personal Data Protection Office decided that the imposition of an administrative fine on the Company is necessary and justified by the weight, nature and scope of the alleged infringements. It should be stated that any other remedy provided for in Art. 58 sec. 2 of Regulation 2016/679, and in particular stopping at a reprimand (Article 58 (2) (b)), would not be proportionate to the identified irregularities in the processing of personal data and would not guarantee that the Company will not commit similar acts in the future as in this negligence case.

Referring to the amount of the administrative fine imposed on the Company, the President of the Personal Data Protection Office stated that in the established circumstances of the case - i.e. in the event of a breach of the principle of data confidentiality, expressed in Art. 5 sec. 1 lit. f of Regulation 2016/679 (reflected in the form of obligations specified in Article 24 (1), Article 25 (1) and Article 32 (1) (b) and (d), Article 32 (2) of Regulation 2016/679), and, moreover, violation of the principles of legality, reliability and transparency, as expressed in art. 5 sec. 1 lit. a Regulation 2016/679 and the principle of accountability, expressed in art. 5 sec. 2 (detailed in Articles 6 and 7 of Regulation 2016/679) - Art. 83 sec. 5 lit. a regulation 2016/679, according to which the violation of the basic principles of processing, including the terms of consent, the terms and conditions of which are referred to, inter alia, in art. 5, 6, 7 of this regulation are subject to 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 being applicable.

At the same time, due to the finding by the Company of a breach of several provisions of Regulation 2016/679 as part of the same or related processing operations, pursuant to Art. 83 sec. 3 of Regulation 2016/679, the President of the Personal Data Protection Office determined the total amount of the administrative fine in an amount not exceeding the amount of the fine for the most serious breach.

In the presented facts, the most serious breach by the Company of the confidentiality principle specified in Art. 5 paragraph 1 lit. f of the Regulation 2016/679. This is supported by the serious nature of the breach and the group of people affected by it (approximately 2,200,000 - approximately two million two hundred thousand users of online stores administered by the Company). Importantly, in relation to the above-mentioned number of people, there is still a high risk of unlawful use of their

personal data, because the purpose for which an unauthorized person took steps to gain access to this information is unknown.

The breach by the Company of the principles of legality and reliability expressed in Art. 5 paragraph 1 lit. a and the principles of accountability under Art. 5 sec. 2 of Regulation 2016/679 should be considered a minor infringement. In the case of the second of the identified infringements, the group of people affected by it is much smaller (about 35,000 - about thirty-five thousand users submitting installment applications). The company also removed these data, considering that their further processing is associated with a higher risk. Collecting data from applications [...] without a legal basis, i.e. the consent of the data subject, took place before the application of Regulation 2016/679, and after the amendment to the regulations, the Company collected data on the basis of consent, which was proved during the inspection and during the proceedings.

Pursuant to art. 103 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2018, item 1000, as amended), the equivalent of the amounts expressed in euro, referred to in Art. 83 of the Regulation 2016/679, are calculated in PLN according to the average EUR exchange rate announced by the National Bank of Poland in the exchange rate table on January 28 of each year, and if the National Bank of Poland does not announce the average EUR exchange rate on January 28 in a given year - according to the average euro exchange rate announced in the table of exchange rates of the National Bank of Poland that is closest to that date.

Bearing in mind the above, the President of the Personal Data Protection Office, pursuant to art. 83 sec. 3 and art. 83 sec. 5 lit. a regulation 2016/679, in connection with art. 103 of the Act on the Protection of Personal Data of 2018, for the violations described in the operative part of this decision, imposed on the Company - using the average EUR exchange rate of January 28, 2019 (EUR 1 = PLN 4.2885) - an administrative fine in the amount of 2 830 PLN 410 (which is the equivalent of EUR 660,000).

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 of Regulation 2016/679, i.e. it will be effective, proportionate and dissuasive in this individual case.

In the opinion of the President of the Personal Data Protection Office, the penalty imposed on the Company will be effective, because it will lead to a state in which the Company will apply such technical and organizational measures that will ensure the level of security for the data processed, corresponding to the risk of violating the rights and freedoms of data subjects and the importance of the accompanying threats. the processing of this personal data. The effectiveness of the penalty is therefore

equivalent to the guarantee that the Company, from the moment of the conclusion of these proceedings, will follow the requirements of the provisions on the protection of personal data with the utmost care.

The applied financial penalty is also proportional to the infringement found, in particular its seriousness, the number of individuals affected by it and the risk they incur in connection with the infringement. In the opinion of the President of the Personal Data Protection Office, the fine imposed on the Company is also proportional to its financial situation and will not constitute an excessive burden for it. The amount of the fine has been set at such a level that, on the one hand, it constitutes an adequate reaction of the supervisory body to the degree of violation of the administrator's obligations, on the other hand, it does not result in a situation in which the necessity to pay a financial penalty will entail negative consequences, in the form of a significant reduction in employment or a significant decrease in the Company's turnover. In the opinion of the President of the Personal Data Protection Office, the Company should and is able to bear the consequences of its negligence in the field of data protection, therefore the imposition of a fine of PLN 2,830,410 is fully justified.

In the opinion of the President of the Personal Data Protection Office, the administrative fine will fulfill a repressive function in these specific circumstances, as it will be a response to a breach by the Company of the provisions of Regulation 2016/679, but also a preventive one, as the Company itself and other administrators will be effectively discouraged. to breach the provisions on the protection of personal data in the future.

In the opinion of the President of the Personal Data Protection Office, the applied fine meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the breaches found in the context of the basic requirements and principles of Regulation 2016/679 - in particular the principle of confidentiality expressed in Art. 5 sec. 1 lit. f of the Regulation 2016/679.

The purpose of the imposed penalty is to ensure proper performance by the Company of the obligations provided for in Art. 5 sec. 1 lit. f, art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 lit. b and d, art. 32 sec. 2 of Regulation 2016/679, and consequently to conduct data processing processes in accordance with applicable law.

Bearing in mind the above, 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 Office for Personal Data Protection (address:

ul. Stawki 2, 00-193 Warsaw). A proportional fee should be filed against the complaint, in accordance with Art. 231 in connection with Art. 233 of the Act of August 30, 2002, Law on proceedings before administrative courts (Journal of Laws of 2018, item 1302, as amended). 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.

Pursuant to Art. 105 paragraph. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2018, item 1000, as amended), the administrative fine must be paid within 14 days from the date of expiry of the deadline for lodging a complaint to Provincial Administrative Court, or from the date of the ruling of the administrative court coming into force, to the bank account of the Personal Data Protection Office at NBP O / O Warsaw No. 28 1010 1010 0028 8622 3100 0000.

[1] Guidelines for SMEs on the security of personal data processing - https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

[2] https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

2019-09-19