ALERT SAFE COMPANY

BDO

No. 4/2022

Ladies and Gentlemen,

It is with great pleasure that we present to you the April issue of our "Secure Company" alert, in which we discuss the most current and interesting information on counteracting money laundering and terrorist financing (AML), as well as on cybersecurity and personal data protection.

This time our alert has been dominated by topics relating to personal data protection. There are two reasons for this. The first is the publication of the reasons for two exceptionally interesting Voivodship Administrative Court rulings. They both cover the responsibilities of data controllers. They also both have a very practical dimension. The second reason is the publication by the President of the UODO of a list of questions that will be asked as part of overseeing compliance with data protection officer regulations. We believe that it is a good idea to answer these questions even before an audit in order to avoid any possible deficiencies in this area.

The last extensively discussed topic relates to the recommendations issued by CERT in connection with an increase in cybersecurity threats during the conflict in Ukraine. These recommendations should be implemented or at least carefully analyzed.

We hope that the information presented in the alert will be useful and will make it easier to navigate cybersecurity related regulations and legislative trends.

As always, we wish you a pleasant read, and should you need more or more detailed information, please don't hesitate to contact our company and experts.

DR ANDRÉ HELIN, Prezes BDO

Employee cannot perform duties in place of the controller

A situation where the controller limits himself to only training the employees while failing to apply technical safeguards cannot be seen as the implementation of appropriate technical or organizational measures – found the Voivodship Administrative Court (WSA) in Warsaw in its ruling of 15 February 2022 (case file II SA/Wa 3309/21).

The Court upheld the supervisory authority's decision to impose a cash fine following the discovery of a data breach. The case pertained to the loss by a probation officer of an unencrypted pen drive type storage device. The device contained the data of 400 people under the officer's supervision and environmental inquiry.

In the reasons for its ruling the Court found that in the case it was clear that a data breach occurred as a result of the loss of an unencrypted pen drive. The data controller had issued unsecured devices for official use and required probation officers to secure them on their own.

The Court upheld the supervisory authority's position that an employee cannot replace the controller in the performance of his duties. In addition, an employee may not have the necessary knowledge with regard to the application of appropriate organizational or technical measures, or could implement inappropriate security measures that are not commensurate with the scope of the data that are being processed.

According to the Court, the controller breached the principles of confidentiality and integrity of personal data as he had failed to introduce appropriate organizational and technical measures that would be adequate to the data processing methods and objectives, and had reached for them only after the loss of the data storage device. In consequence, this omission enabled unauthorized access to the data.

In the Court's opinion, such organization of the process of determining and implementing data processing security measures deprives the controller of access to basic information. The result is a lack of knowledge about what safeguards are in place at the organization and whether they will be effective in case of potential threats.

Data protection is the responsibility of the entity acting as controller

Under the agreement for the provision of services concluded between the controller and the processor, data protection is the responsibility of the controller, who if necessary uses the help of the processor. If the controller decided that a copy of a data base should be deleted, it was his responsibility to check if that action has been performed – indicates a WSA ruling of 26 January 2022 issued (case file II SA/Wa 1384/21).

The case involved the disclosure of personal data associated with the kssip.gov.pl domain. As a result of unauthorized access to a file containing a copy of a data base, the data were published on the internet. Whereas a copy of the data base was created as a result of a test migration to a new training platform. During a proceeding before the supervisory authority, as well as before the Court, KSSIP attempted to show that responsibility for the incident rests with the processor. It was the employee of that company who at the controller's request had made a copy of the data base and left it on the server.

The Court, however, stressed that since it was the controller who had decided that the said copy of the data base should be deleted, it was his responsibility to check if this action had been performed. At the same time the Court pointed out that even if the processor's employee did not delete the copy, it was still the controller's responsibility to verify if its location ensures security of personal data processing. The Court noted that it is the controller that initiates actions as the entity that makes decisions on the objectives and methods of processing. It also stated that under the agreement for the provision of services concluded between the controller and the processor, data protection is the responsibility of the controller who, if necessary, uses the help of the processor.

In addition, the Court agreed with the UODO's charges relating to the absence of comprehensive provisions in the data processing agreement. In the Court's opinion, the supervisory authority was correct to point out that the data processing agreement did not sufficiently define the scope of the data. It did not contain the categories of subjects and did not specify the types of data by indicating their categories. In addition, KSSIP did not include in the agreement the processor's obligation to only process data on the controller's documented request.

More extensive verification of compliance with data protection officer regulations

The President of the UODO has published a set of nearly 30 questions that he will pose to data controllers and processors from the public and private sector as part of overseeing compliance with regulations on data protection officers.

Since the start of the application of the GDPR, the basic scope of audit activities has covered compliance with the proper appointment and performance of data protection officers (DPO). Now the scope of such audits will be significantly expanded. In the last days of March 2022 the President of the UODO published a set of nearly 30 questions that he will pose to controllers and processors from both the public and private sector as part of his oversight. According to the publication, the UODO will ask the following questions:

- Has a data protection officer (DPO) been appointed at the controller?
- Is the controller responsible for appointing a DPO (if so, on what legal basis), or has a DPO been appointed despite the absence of such a responsibility?
- Has the controller published the DPO's first and last name and contact information on his web page, or – if he has no web page, in a generally accessible manner at the place where he conducts his operations?
- Has the above information been placed in a generally accessible place (please indicate that place, if it is a web page, provide its address and link to the information)?
- Is the Data Protection Officer the controller's employee, and if not, on what legal basis does he perform his duties?
- Has the DPO been appointed solely at the controller, or does he also perform duties at other controllers?
- Based on what qualifications did the controller appoint the DPO (e.g. education, experience, knowledge)?
- What essential resources referred to in Article 38 par. 2 of Regulation 2016/689 does the controller provide to the DPO?
- How does the controller ensure the resources for the DPO to maintain his professional knowledge?
- What position does the DPO hold and who does he answer to in the controller's administrative structure?
- Has the controller appointed a deputy DPO and if so, when?
- Does the controller have a DPO team or another form of permanent support for the DPO with regard to his duties?
- How does the controller ensure that the DPO is appropriately and immediately included in all matters that relate to personal data protection (e.g. have methods been developed with regard to how such matters are to be consulted with the DPO, who and in what situ-

ations should consult the DPO, whether and on what terms does the DPO take part in management meetings)?

- How does the controller provide the DPO with access to personal data and data processing operations?
- Has the controller adopted any internal regulations on the work of the DPO (in particular in order to guarantee his independence and rights to access personal data and data processing operations, to involve him in all matters related to the protection of personal data, to avoid conflict of interests), and if so, in what internal document?
- How does the controller ensure that the DPO is not given instructions on the performance of his tasks?
- How does the controller ensure that the DPO is not penalized and dismissed for the performance of his duties?
- How does the controller proceed in a situation where he does not follow the DPO's guidelines or recommendations, e.g. does he document the reasons for not following those guidelines?
- How can the data subjects contact the DPO in accordance with Article 38 par. 4 of Regulation 2016/679?
- Does the DPO also perform other duties or perform another function in addition to those related to personal data protection, and if so, then: what are they and how much of his work time is allotted to the function of DPO and how much to other tasks; how did the controller determine that the said tasks do not lead to a conflict of interests as referred to in Article 38 par. 6 of Regulation 2016/679?
- With regard to the performance of other tasks, does the DPO answer to persons other than the controller's senior management?
- Has the controller developed a policy for the management of conflicts of interests or introduced another mechanism to ensure that no conflicts of interests occur?
- Does the DPO perform his duties only at the controller's offices, and if not, then at what other place and how is his constant availability for the management and employees of the controller ensured?
- Has the DPO developed (or does he systematically develop) his work plan, e.g. with respect to training, audits?
- Has the plan been presented to the controller for evaluation, does the DPO have sufficient resources and authorizations in areas that are covered by his tasks?
- How often and how does the DPO present the results of his audits to the controller?
- Has the controller asked the DPO for recommendations on assessing impacts on data protection, and if so, in what situations?
- Does the controller check the work of the DPO, and if so, how?

Businesses must take better care of their cybersecurity

In connection with the situation in Ukraine, CERT Polska has issued numerous recommendations on improving cybersecurity for businesses and citizens. In addition, CERT Polska recommends that businesses that collaborate with entities in Ukraine or have branches in Ukraine check the rules for network access and limit permitted traffic to a minimum.

Due to the current situation in Ukraine and the declaration of alert level CHARLIE-CRP, CERT has prepared cybersecurity recommendations to be implemented by citizens and businesses.

According to CERT, businesses should:

- Test the recovery of infrastructure from back up copies. It is essential that this be performed in practice on selected systems, not just procedurally.
- Ensure that the back up copies are isolated and will not suffer in an attack on the remaining infrastructure.
- Ensure that software is updated, in particular for internet-facing systems. Start with vulnerabilities on the list of those currently used in attacks.
- Ensure that any remote access to company resources requires two-factor authentication.
- Review business address services accessible from the internet and limit them to a necessary minimum. This may be done via, for example, the Shodan portal. In particular, services that allow for remote access such as RDP or VNC should not be directly accessible.
- Automatically update the signatures of security systems such as AV, EDR, IDS, IPS, etc.
- Implement domain filtering in the company network based on the warning list published by CERT. This will quickly block domains known to be malicious.

- Review the DdoS attack prevention guide prepared by CSIRT KNF and implement its recommendations.
- Review CERT's guide on how to strengthen protection against ransomware and implement its recommendations.
- Review CERT's materials on password security.
- Review CERT's article on message sender verification mechanisms and implement them for domains used to send e-mail.
- Where the business has a range of own IPs, joining the N6 platform is recommended. The platform provides current information about vulnerabilities and suspect activities observed by CERT in a given address range.
- Designate a person responsible for the coordination of actions in the event of an incident and practice response procedures.
- Make employees aware of the need to observe suspicious activities and inform them how to report them to the company's designated person.
- Provide CERT with a contact person, even if not required by law. This will allow CERT to quickly contact the right person to send a warning.

To recap, the CERT Polska Team operates as part of NASK – the State Research Institute which conducts scientific studies, operates the national .pl domain registry and provides advanced IT services. Since the effective date of the National Cybersecurity System Act of 5 July 2018 the team has been performing some of the tasks of CSIRT NASK (Computer Security Incident Response Team).

In short:

EDPB working on "dark patterns" guidelines

The European Data Protection Board (EDPB) is waiting until 2 May 2022 for comments on the "Guidelines 3/2022 on so-called dark patterns in social media platform interfaces: How to recognize and avoid them". "Dark patterns" are interfaces and user experiences implemented on social media platforms that cause users to make unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. The guidelines present best practices for different use cases and contain specific recommendations for designers of user interfaces that facilitate the effective implementation of the GDPR.

Land registers will make it possible to steal property owners' personal data

Disclosure of land register numbers makes it possible for anyone to easily obtain such information as names, surnames, parents' names, PESEL number, property address. This in turn may lead to dangers associated with unauthorized use of such information, such as for example identity theft, i.e. impersonating someone in order to commit a crime – stressed the President of the UODO and the Human Rights Ombudsman. The fact that the publication of a land register number makes it easy to indirectly identify property owners, making that number personal data, has also been confirmed by the Voivodship Administrative Court in Warsaw, which on 5 May 2021 dismissed a complaint filed against the UODO's decision by GGK.

Everyone has the right to personal data protection

Any activities performed for the benefit of Ukrainian citizens in Poland should respect the right to personal data protection and the right to privacy. Those who bring help to Ukrainian refugees should be careful to maintain an appropriate balance of interference in their fundamental rights. For this reason, data controllers who want to implement processes that facilitate and coordinate the Ukrainians' stay in Poland should determine whether, when it comes to personal data protection, those processes do not excessively interfere with the refugees' privacy, and whether they arise out of and comply with legal regulations, etc. – the explanations published by the President of the UODO indicate.

Trans-Atlantic agreement is no basis for data transfer

At its 63rd plenary meeting on 6 April 2022, the EDPB adopted Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework. At the

same time the EDPB stressed that the announcement does not constitute a legal framework on which data exporters can base their data transfers to the United States. It should therefore be remembered that data exporters must continue taking the actions required to comply with the case law of the Court of Justice of the European Union (CJEU), and in particular its Schrems II decision of 16 July 2020.

Windows 11 with new security functions

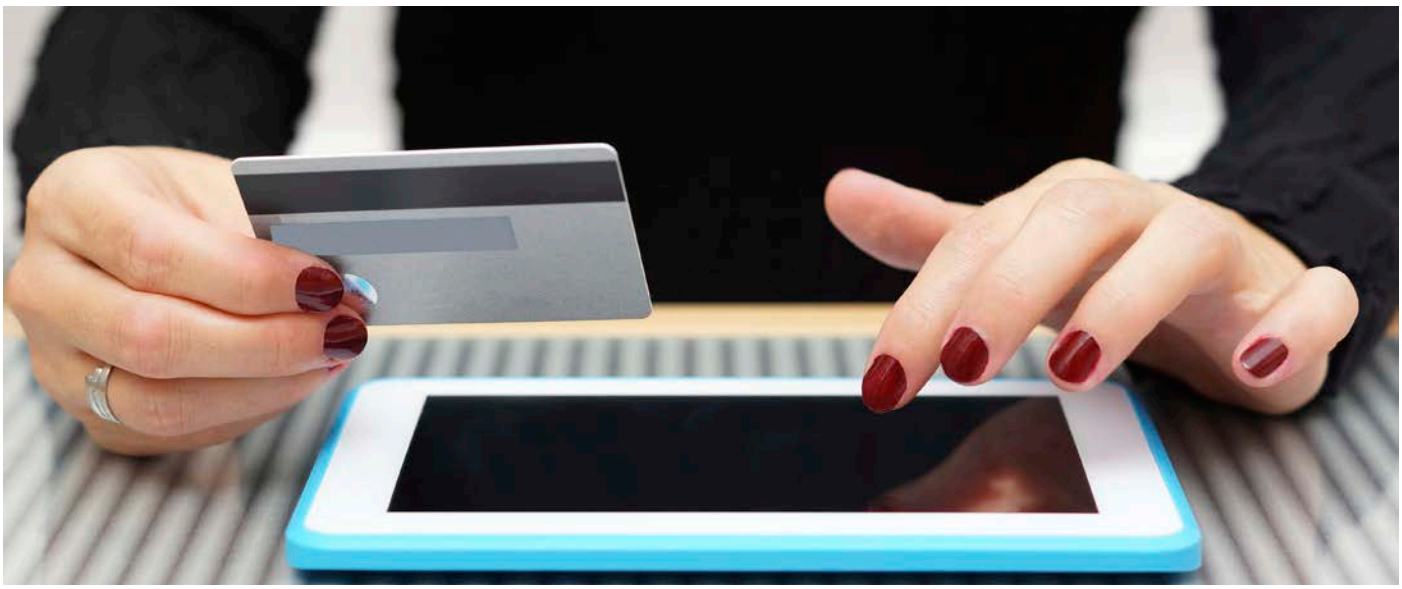
Microsoft has unveiled a new security feature for computers running the Windows 11 operating system. Test compilations for users registered in Windows Insider contain a solution called Smart App Control. In practice, it is a modern anti-virus that operates using cloud-based artificial intelligence. The whole process is used to block unknown and suspicious programs. To use the artificial intelligence based anti-virus, users will need to reinstall their Windows 11 operating systems. The newest solution has been included in Windows 11 operating systems with compilation number of 22567 or higher.

Another malware steals data from Android devices

Security researchers at the French company Pradeo have published information about another Android malware. The mobile device virus was identified in one of the applications in the official app store - Google Play. The French security researchers detected a malware called Facestealer in the source code of Craftsart Cartoon Photo Tools. The program, which turns photos into likenesses of cartoon and comics characters – in reality contained a malware code that was used to steal Facebook credentials.

Microsoft issues 100 security fixes

On 12 April 2022 Microsoft published more than 100 security bulletins (compared to 71 in March and fewer than 50 in February). They cover various products, including Windows, Microsoft Office, Dynamics, Edge, Hyper-V, File Server, Skype for Business and Windows SMB. 10 of the vulnerabilities have been classified as critical. Two are zero-days. This means that the vulnerabilities pose a real threat that may be used to launch an attack. The first relates to Windows User Profile Service, and the second to the Windows Common Log File System Driver. For a full list of released security fixes (2884 in total), visit the Microsoft Security Update Guide.



**BDO spółka z ograniczoną odpowiedzialnością sp.k., ul. Postępu 12, 02-676 Warszawa;
tel.: +48 22 543 16 00, fax: +48 22 543 16 01, e-mail: office@bdo.pl**