ALERT SAFE COMPANY

BDO

No. 7/2022

Ladies and Gentlemen,

Here is the July 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 we focus primarily on topics relating to cybersecurity and personal data protection. With respect to the former, we want to draw your attention to an interesting ruling on disclosing the salaries of data protection officers at public institutions, as well as recap some of the principles relating to the processing of employee personal data. When it comes to the latter, we discuss the EU's new cybersecurity rules (NIS2 Directive), as well as the new obligations of internet platforms to report online transactions to the tax authorities (implementation of DAC7 Directive).
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.
Should you need more or more detailed information, please don't hesitate to contact our company and experts.

DR ANDRÉ HELIN, BDO Managing Partner

EU to tighten cybersecurity regulations

The European Parliament's Committee on Industry, Research and Energy has approved an agreement with the European Council regarding the NIS2 Directive, which tightens cybersecurity regulations at EU member states.

The NIS2 cybersecurity directive (Directive on measures for a high common level of cybersecurity across the Union) will replace the currently binding NIS (Europe's first law on cybersecurity, adopted in 2016).

The obligations of EU member states will not change significantly under the NIS2 Directive. The draft calls for the governments of member states to, above all:

- ensure the operation of competent authorities on cybersecurity (including designate single points of contact and teams to respond to cybersecurity incidents – CSIRTs),
- adopt national cybersecurity strategies (and define appropriate policies to, among others, develop and promote a high level of cybersecurity), as well as
- ensure cooperation with the relevant authorities and CSIRT from other member states (as part of the CSIRT network and a member state Cooperation Group).

As a novelty in relation to the current NIS directive, NIS2 requires member states to put in place national plans to respond to large scale cybersecurity incidents and crises. Among others, such plans should include appropriate procedures, information flow channels or measures to prepare members states for large-scale cybersecurity incidents.

The most important and most significant, especially from the perspective of entities that provide digital services, is the change in the entities covered by the scope of the directive, i.e. those that will be assigned additional cybersecurity related obligations.

In addition to entities from the energy, transport, banking, financial or health sectors, deemed as essential from a cybersecurity perspective are, among others, cloud computing service providers – previously included in a "lower" category of digital providers; data center service providers – a new category of services that in particular includes centralized storage, processing and transport of data along with all of the necessary tools (e.g. facilities and infrastructure), as well as means (e.g. energy supply); content delivery network providers – a new category of services consisting of providing access to a server network to enable further distribution of internet content to users; trust service providers; providers of public electronic communications networks and electronic communications services; public administration entities of central governments.

Classified as important entities (i.e. those whose services are less critical from the perspective of cybersecurity than essential entities) are providers of online search engines and online marketplaces (previously classified as digital providers), as well as entities that had not previously been subject to the directive, such as providers of social networking platforms or providers of postal services. In addition, the category of important entities includes, among others, entities performing waste management, production and distribution of chemicals, or production and distribution of food.

Salaries of data protection officers at public institutions are public

Information about the salary of a data protection officer at a public institution, aside from components arising out of his family or social status, is related to the performance of a public function – the Voivodship Administrative Court in Warsaw has found.

The right to privacy will not always block the disclosure of information about the salary of a data protection officer. If the person who holds that position has actual influence over public affairs, than that person performs a public function. Therefore, information about his salary, aside from any components that arise out of his family or social status, is related to the performance of that function. This is the ruling of the Voivodship Administrative Court in Warsaw issued on 27 January 2022 (case file II SA/Wa 2930/21), the reasons for which have just been published.

According to the Court, the salaries of those who work for ZUS are financed with public funds, and under the provisions of the Public Finances Act, information about the management of such funds is public. It should, however, be remembered that the right to public information is subject to restrictions due to privacy or company secrets. Those restrictions do not apply to information about those who perform public functions, relates to the performance of those functions, including the terms of their performance, or in cases when the individual or business waives that right. The Court explained that under binding regulations, a "public function" is a function that involves the rights and obligations to perform tasks of public significance. Thus the term covers any person who has a real and specific influence on public affairs.

The Court found that a statement that a data protection officer is not a person performing a public function is incorrect. This is because the president of ZUS has given him the authority to perform tasks that have a real and specific influence over the rights of those whose data are processed on insured and premium remitter accounts and in registers. An analysis of internal legal documents indicated that he was granted significant and real influence to ensure that the entity's statutory duties are performed in compliance with legal regulations. He also had the power to manage matters associated with the performance of tasks by the public entity at which he performed the function. It cannot, therefore, be found that the data protection officer held a position of a service or technical nature.

Ministry of Finance to impose new obligations on e-commerce entities

The Ministry of Finance has prepared a draft of regulations directed at digital platform operators. They are to impose numerous obligations associated with reporting the data of their users to the tax authorities.

The Ministry of Finance has held short pre-consultations on the new obligations (applicable primarily to digital platform operators) imposed on selected e-commerce entities by EU Directive 2021/514 (so-called DAC7 Directive). Member states, including Poland, should implement the directive's regulations no later than by the end of 2022 so they can go into effect as of 1 January 2023.

The new regulations apply to digital platform operators that share their interfaces with sellers to make it easier for them to reach clients and sell goods and services.

The document indicates that the primary objective of implementing Directive DAC7 is to introduce a new reporting requirement for operators of digital platforms that make it easier for sellers to perform such activities as: real estate or parking space rentals, personal services, sale of goods, vehicle rentals (so-called relevant activities). Generally, subject to reporting will be income earned by individual sellers and additional data on those sellers and their real properties used for rental purposes (located in the EU). The main principle is to be that the reporting platform operator will report to the Head of National Tax Administration (Head of KAS) information about reportable sellers for the reporting period, by 31 January of the year following the calendar year in which the reporting platform operator identified the seller as a reportable seller.

The premises presented by the Ministry of Finance also indicate that in addition to reporting relevant information to the Head of KAS, digital platform operators will also have to inform the individual sellers of the scope of their data that will be reported to the tax authorities.

The new regulations will also introduce additional (aside from the reporting itself) obligations for digital platform operators covering three matters. Firstly, regulations on additional registration of digital platforms and the need for them to obtain another number to fulfill this specific obligation.

Secondly, regulations that introduce requirements to implement due care procedures (the new regulations will have an entire chapter on this) when verifying sellers, as well as to adapt systems to obtain appropriate data needed to properly perform the new reporting obligations. The regulations will require reporting digital platforms to verify whether the information collected for reporting purposes is reliable.

And thirdly, regulations on the introduction (or adaptation) of procedures to protect the data obtained in connection with the new reporting obligations (GDPR).

Records must be kept when employee data are processed

The General Data Protection Regulation (GDPR) provides that data controllers and processors are required to keep records of processing activities or records of categories of processing, respectively. This also applies to the processing of employee data that is not "occasional".

The GDPR lists the mandatory components of records of processing activities or records of processing categories (Article 30). Nonetheless it should be remembered that the President of the Personal Data Protection Office (President of the UODO) has prepared templates of a record of processing activities and a record of processing categories along with examples of how they should be completed and explanations on how to perform this obligation. They are available on the UODO's website. The templates are not binding in nature. The regulations permit many different models (structures) of such records. What matters is for the data controller or processor to be able to present the components listed in Article 30 par. 1 and 2 of the GDPR with respect to all of the data processing activities, in a clear and legible manner.

It should be noted that on 14 May 2018 the Article 29 Working Party (currently the European Data Protection Board – EDPB) adopted a standpoint in which it indicates that employers of fewer than 250 employees will not be exempt from the requirement to keep records of processing activities.

Under those guidelines, the obligation is to be fulfilled when the processing: may give rise to a risk of violation of the rights or freedoms of data subjects; is not occasional in nature; involves special categories of personal data referred to in Article 9 par. 1, or personal data relating to convictions and violations of law.

Any of those situations occurring independently is enough to give rise to this obligation. In such situations, however, a record of processing activities must only be kept for the types of activities listed in the guidelines. A good example is the regular processing of employee data, as such processing cannot be considered occasional.

In short:

New functionalities in group conversations on WhatsApp

New functionalities have been added to WhatsApp. This time they include group conversations. The first is the ability to mute a specific meeting participant. The second makes it possible to send messages to selected users during a meeting. At the same time, a new banner was added to notify when a new user joins a group conversation while it is already in progress.

Another batch of Windows security fixes

The June set of Windows 11 fixes, labeled KB5014697, has been published. This time the fixes apply to, among others, Office, Edge, Azure components, PowerShell, Defender or the Windows codecs library. Some more patches came in July. When it comes to Windows 11 it was the KB5015814 update, whereas Windows 10 got KB5015807 or KB5015811 depending on the edition. In the context of Windows 11 we should not forget about the upcoming update to version 22H2, which although ready in theory, will in practice not find its way to our computers until the end of the year.

Guidelines on certification as a tool for data transfers adopted

During its 66th plenary meeting the European Data Protection Board (EDPB) adopted guidelines on certification as a tool for data transfers and a binding decision based on Article 65 in a dispute relating to Accor. The guidelines are made up of four sections, each focusing on specific aspects of certification as a tool used to transfer data, such as: the object, scope and variety of entities involved; implementing guidelines on accreditation requirements for certification bodies; specific certification criteria to demonstrate the presence of appropriate data transfer security measures; as well as binding and enforceable commitments to be implemented.

Cybersecurity Department to review Uber and Bolt apps

The Cybersecurity Department of the Chancellery of the Prime Minister will review the apps that offer passenger transport services. According to cyberdefence24.pl, the objective is to improve the safety of women during trips with Bolt or Uber. New technological solutions will allow for a quicker reaction to dangerous events, as well as for easier driver verification.

NASK launches joint cybersecurity postgraduate program in Silesia

A two-major postgraduate Cyber Science program ran by NASK and Silesian universities – the Silesian University of Technology, the University of Silesia and the University of Economics in Katowice – will start this October. It will offer the following majors: "Tokenization and Process Automation in a Digital Economy" and "Cyber Security Management." This joint educational initiative is a response to the market challenges of a digital economy, which already involves not only modern technologies, but also management, psychology, law or sociology.

Another, third version of Whistleblower Act published

The third version of the bill on the protection of those who report violations of the law (UC 101) has been published on the website of the Government Legislative Center. The bill is to implement into the Polish legal system Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17).

Cybercriminals rarely profile their victims

Attacks where scammers specifically profile and target their victims are rare. In most cases, cybercriminals try to reach the broadest possible group of victims to maximize their profits – says Paweł Piekutowski, head of the Polish Financial Supervision Authority's Computer Security Incident Response Team (CSIRT KNF) operating at the Cybersecurity Department of the Office of the Polish Financial Supervision Authority (UNKF).

Germany is taking a look at Apple's privacy protection measures

The German anti-trust body (FCO) will take a look at Apple's privacy protection measures – the proceeding will check if Apple uses privacy to gain a compe-

titive edge. A similar proceeding was commenced last year by France, and the Polish UOKiK took an interest in the matter at the end of 2021. According to FCO, competition on the mobile apps market may be limited by the fact that although consumers choose to limit the transfer of data to third party mobile apps and advertisers, Apple will continue to have unrestricted access and will be able to compile them in any way it wants for marketing purposes.

Microsoft has ended support for Internet Explorer

Internet Explorer is officially no longer supported – at least in the "typical" Windows 10 editions. Microsoft recommends that those who need IE compatibility mode without exceptions use Edge, where such an option has been developed and has been available for some time. Internet Explorer has never been available in Windows 11, so there is no issue when it comes to its support.

**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**