ALERT SAFE COMPANY

BDO

No. 4/2021

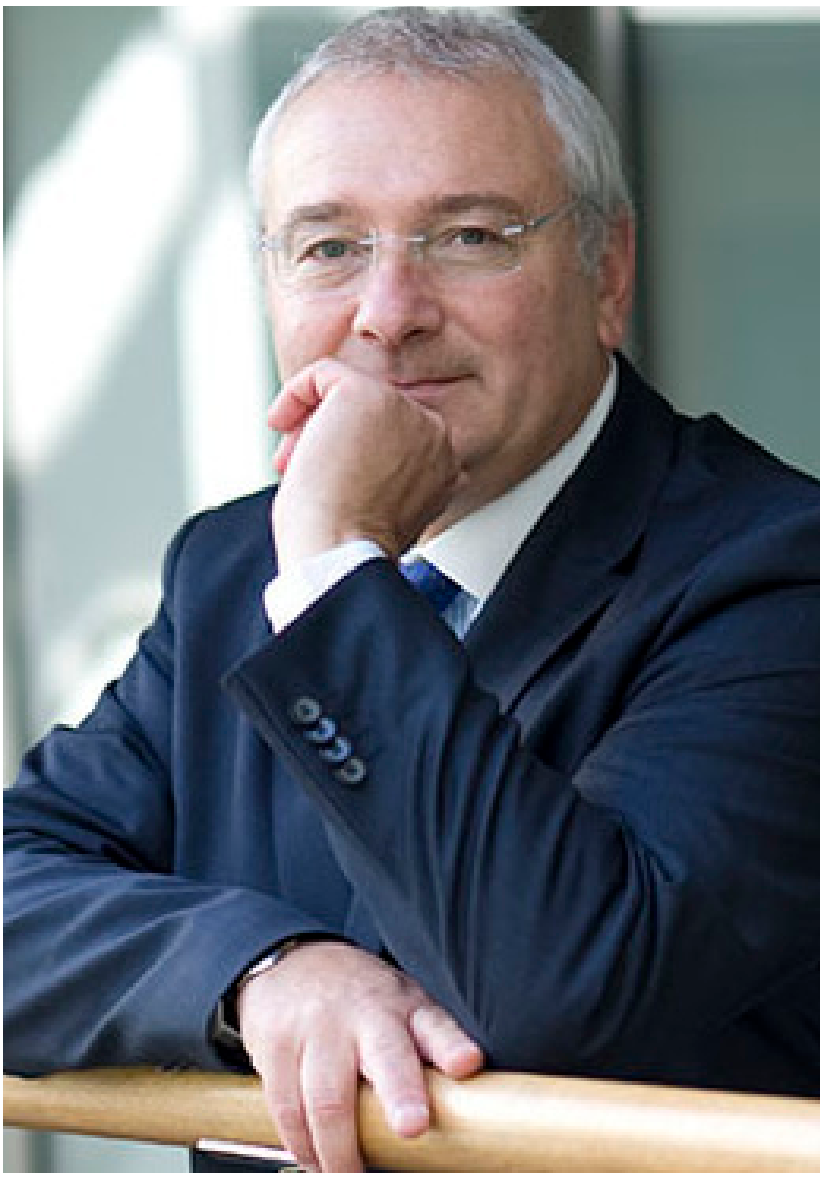
Ladies and Gentlemen,

Here is another issue of our "Secure Company" Alert. We hope that yet another portion of information on the changes planned to regulations on counteracting money laundering and terrorist financing (AML), along with interesting GDPR and cybersecurity related information, will turn out to be useful.

We would like to draw your attention to more changes to the Act on counteracting money laundering and terrorist financing, arising out of the amendments passed by the Sejm. In particular, we recommend the information on changes relating to the requirement to update the data submitted to the Central Register of Beneficial Owners (CRBR). They not only mandate the verification of the submitted data, but also introduce high penalties for failure to update the data already submitted to CRBR. Please note that we have regularly described the changes arising out of the amendments in our alerts in recent months.

Also noteworthy is the information contained in the other paragraphs of our alert, on securing data on social media accounts and on attempted break-ins to company systems using especially fabricated e-mails informing of inbox "overflow". These matters are quite important when it comes to information security.

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



DR ANDRÉ HELIN, Prezes BDO

Changes in regulations on counteracting money laundering signed by the president

The amendments to the Act on counteracting money laundering and terrorist financing and certain other acts, have already been passed. The new regulations are addressed to obligated institutions, on which they impose many new obligations.

At the beginning of April the president signed the amendments to the Act on counteracting money laundering and terrorist financing and certain other acts.

As a result of the amendments many new obligations have been imposed on so-called obligated institutions, which they should urgently include in their procedures.

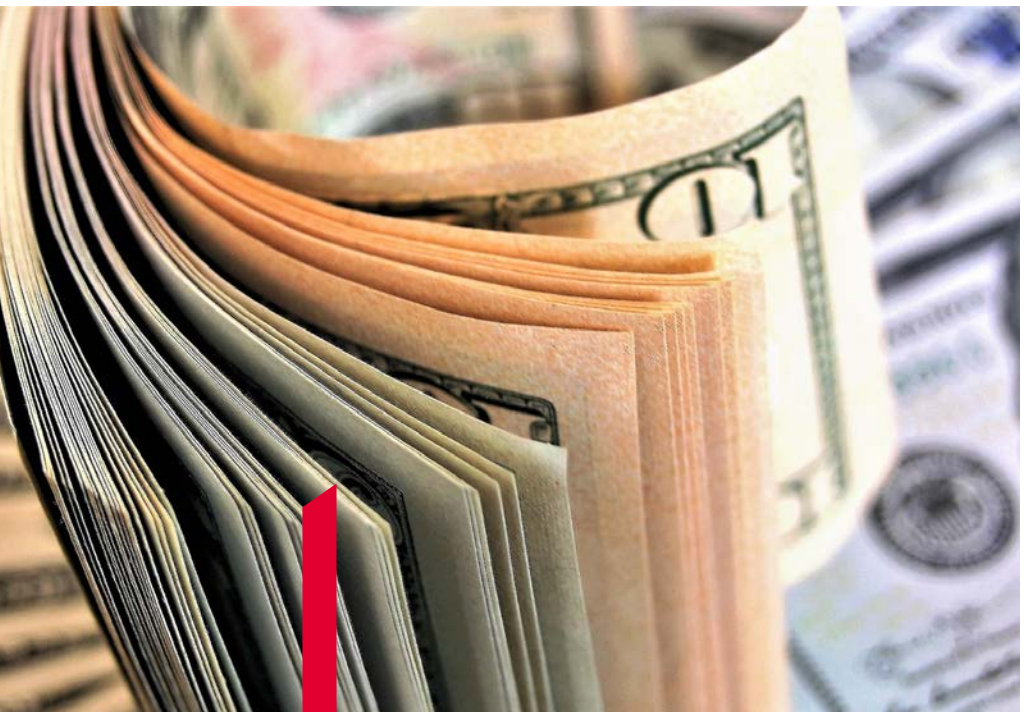
The new regulations: clarify the definitions of beneficial owner, member state and group; broaden the scope of statistical data collected by the General Inspector of Financial Information; specify the methods to be used by obligated institutions in the storage of documents and information obtained as a result of applying financial security measures, as well as the actions to be taken with regard to relationships with high risk third countries; introduce mechanisms for verifying data in the Central Register of Beneficial Owners and a requirement to register providers engaged in exchange services between virtual currencies and suppliers of virtual currency accounts; introduce a requirement to publish and update a list of public positions and functions that in accordance with local regulations qualify as politically exposed positions.

In addition to tax advisors who are already subject to the regulations, new obligated institutions will also include entities that provide services consisting of the preparation of tax returns, tax book keeping, providing advice, opinions or explanations on tax or customs regulations. The provisions of the act will also have to be applied by businesses whose activities consist of the sale of art, collectibles or antiques, including when such activities are conducted at art galleries or auction houses (when the value of a transaction or several related transactions amounts to 10 thousand euro). The same requirement will apply to entities whose activities consist of storing art, collectibles and antiques.

The amendments also require those who trade in virtual currencies to register in the new register kept by the minister of finance (the amendment introduces a requirement to register trade in virtual currencies on transactions in excess of 1 thousand euro).

The amendments also provide for new penalties. An entity that provides services to companies or trusts without registration will be subject to a cash fine of up to 100 thousand zł. The same fine may be imposed on entities that provide virtual currency services if they fail to register such activities.

The amendments had not yet been published in the Journal of Laws when we completed our alert.



A million zloty fine for error in CRBR filing

The Ministry of Finance will not only check if the companies required to submit data to CRBR have actually complied with this requirement, but also whether they have done it correctly. Submission of incorrect data will soon be punishable by a million zloty fine.

The amendments to the Act on counteracting money laundering and terrorist financing and certain other acts passed by the Sejm on 30 March 2021 introduce three important changes relating to submissions to the Central Register of Beneficial Owners (CRBR).

Firstly, they impose on obligated institutions a new requirement to verify the accuracy of the data submitted to the CRBR. Based on these regulations, the internal procedure of obligated institutions with regard to counteracting money laundering is to in particular specify the methods of recording differences between the information collected in the CRBR, and the information about the client's beneficial owners determined as a result of applying the provisions of the act.

Secondly, obligated institutions will have to record the differences between the information collected in the register, and the information they have obtained.

This means that obligated institutions (such as banks, insurers, real estate agents, exchange offices, notaries, auditors, tax advisors) will have to check the accuracy of the beneficial owner information provided by the client against the register, and if differences are found, report them to the tax authorities.

The third change pertains to penalties. Currently, in accordance with Article 153 of the Act on counteracting money laundering and terrorist financing, a fine of up to 1 million zloty may only be imposed for failure to submit beneficial owners to the CRBR. After the amendments, it will not only be the companies that failed to file information, but also those that failed to update information or filed incorrect information that will be subject to a fine of up to 1 million zloty. For those in management positions the fine will amount to up to 50 thousand zł. It should be remembered that even today's regulations require that information submitted to the CRBR be updated within 7 days of each change.

UODO advises on how to protect data on social media accounts

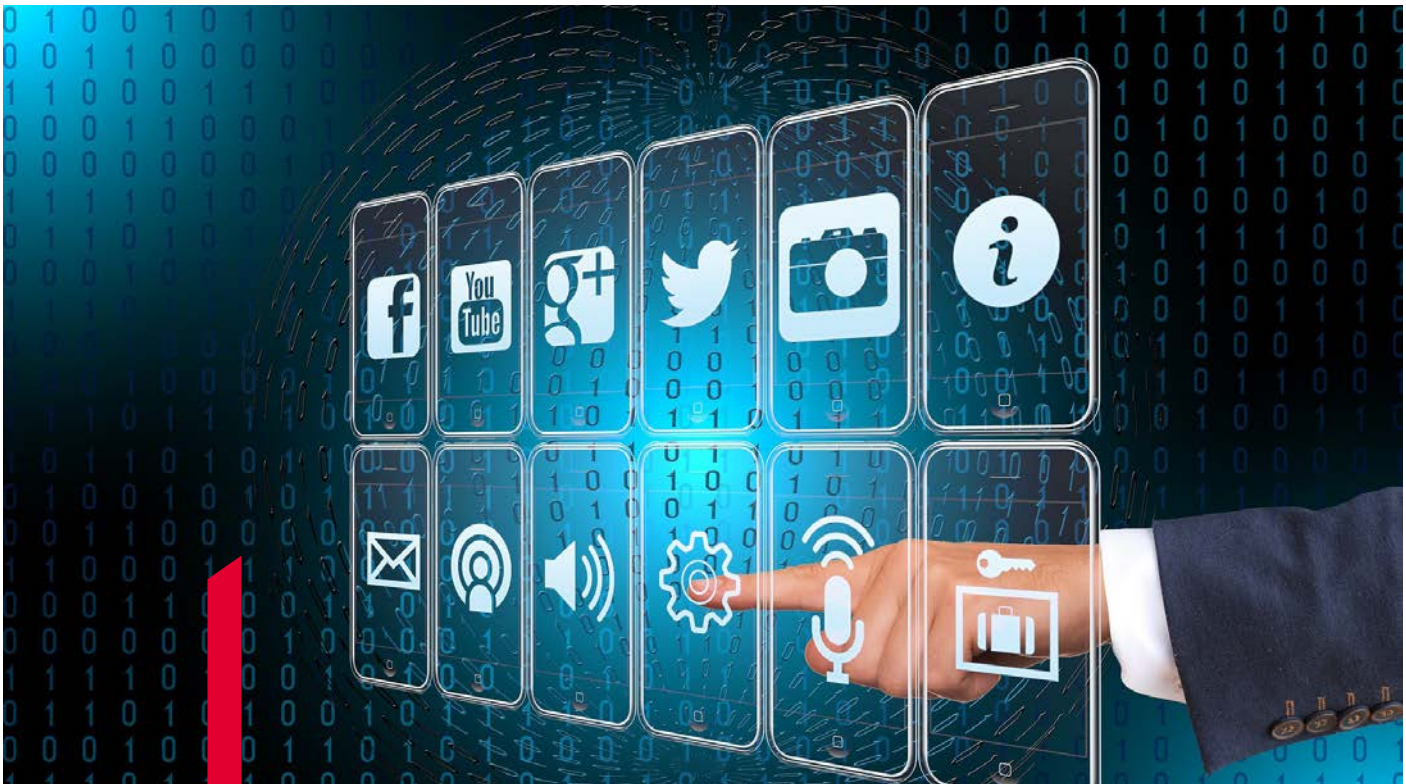
After the publication of data stolen from the accounts of social media users, the Office for the Protection of Personal Data (UODO) has published guidelines on data protection on such services, as well as on what to do if an account break in is suspected.

Recently published information on leaks of personal data from the accounts of Facebook users have prompted the UODO to publish guidelines on how to secure data on social media accounts. In the UODO's opinion, this aspect of internet use must be prioritized by all users due to the huge amount of data stored on such accounts.

The UODO recaps the rules that should be applied to minimize the risk of using social media. In this area it recommends: having a strong password — a password generator may be used; using multi-factor authentication — first you enter the login and password, then you confirm logging in with a token, because the use of such authentication key will effectively protect against hacking attacks (phishing, session hijacking). In addition, a token will not work when logging in on a fake page; not logging in on unknown devices; using different passwords for different portals and systems — a password manager can help; not using untrusted internet connections (public hot spots); limiting application permissions to log in using a social media account.

If a data leak is suspected, the UODO recommends to: absolutely and as soon as possible change your password, bearing in mind the rules for the creation of complex passwords; be on a lookout for phishing attacks, as according to the UODO, such attacks may intensify after a contact (e-mail) data leak; do not, under any circumstances, use the links included in an e-mail, especially one that was not expected or that originates from unknown individuals, institutions or companies; exercise caution against social engineering attacks conducted using phones. As explained by the UODO, a potential hacker may use data captured from social media, authenticate himself during a phone conversation with the victim, and then directly obtain more information, including access to the user's systems or devices.

It should also be stressed that the above rules apply not only to private, but also to company social media accounts. This is particularly important for small and mid-sized companies that often have no specialized IT departments.



The number of ransomware attacks is on the rise

The threat is still high of attacks on company computer networks, consisting of unlawfully encrypting data and decrypting them for ransom. Hackers gain access to company systems using, among others, fake e-mails about inbox overflow.

The ongoing COVID-19 epidemic and the resulting prevalence of remote work using company computers have resulted in a significant rise in ransomware attacks. This type of attack consists of blocking access to data on a computer or server. After gaining access to data, the perpetrators encrypt them and ask for a high ransom, most often in a virtual currency, for their decryption. Importantly, access to only one computer in the network is enough for the hackers to conduct an attack.

Computers are most often infected through a click on a link (also in the form of a photo or advertisement) included in an e-mail. Such e-mails are often designed in a way that they pretend to be a vendor and, for example, contain an invoice or payment demand, which is meant to provoke the recipient to click on the link and, in consequence, infect the computer with ransomware. Infections also take place with the use of so-called malvertising, i.e. the placement of malware in advertisements.

Another serious threat comes from e-mails that appear to contain messages relating to ongoing company business. For example, there is an increase in attacks using e-mails informing employees of the need to unblock an overflowing inbox. Clicking on such an

e-mail results in the hackers gaining access to the victim's computer and enables them to access the company's internal systems.

This is why nowadays security related matters require much more attention than before. This means the need to not only develop detailed security regulations the employees should comply with when working on company hardware from home, but also to consistently and frequently check whether these rules are actually adhered to. Another good protection against the loss of data that have often been collected for many years is to ensure appropriate frequent backups, of not only the data kept on company servers, but also of the data on local disks on the computers used by employees. In this case, the highest level of security would be achieved by keeping such copies outside the company network structure.

In short

The European Data Protection Supervisor against face recognition

Europe should implement a ban on the use of face recognition technology, because it leads to "an extensive and undemocratic interference" in the private lives of citizens – says the European Data Protection Supervisor (EDPS). This is the comment that appeared two days after the European Commission submitted a proposal of new regulations and standards on innovative solutions relating to artificial intelligence. At this time EDPS is focusing on setting precise boundaries for such tools and systems, which may constitute a threat to basic rights when it comes to data protection and privacy.

Green COVID-19 certificates must ensure personal data protection

In a joint opinion, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) call on EU member states to ensure that green certificates are fully compliant with the EU's data protection regulations. Data protection inspectors from the entire EU and the European Economic Zone have stressed the need to reduce threats to the basic rights of EU citizens and residents, which may arise out of the issue of a green certificate, including its unintended, secondary uses. The purpose of the green certificates is to make it easier to exercise the right to move freely in the European Union during the COVID-19 pandemic by establishing a common framework for the issue, verification and recognition of certificates on vaccination, testing and recovery.

EDPB has evaluated the adequacy of personal data protection in the United Kingdom

In mid April the European Data Protection Board (EDPB) adopted two opinions on the draft decisions confirming the adequacy of personal data protection in the United Kingdom after Brexit. The EDPB noted that there are two key areas of conver-

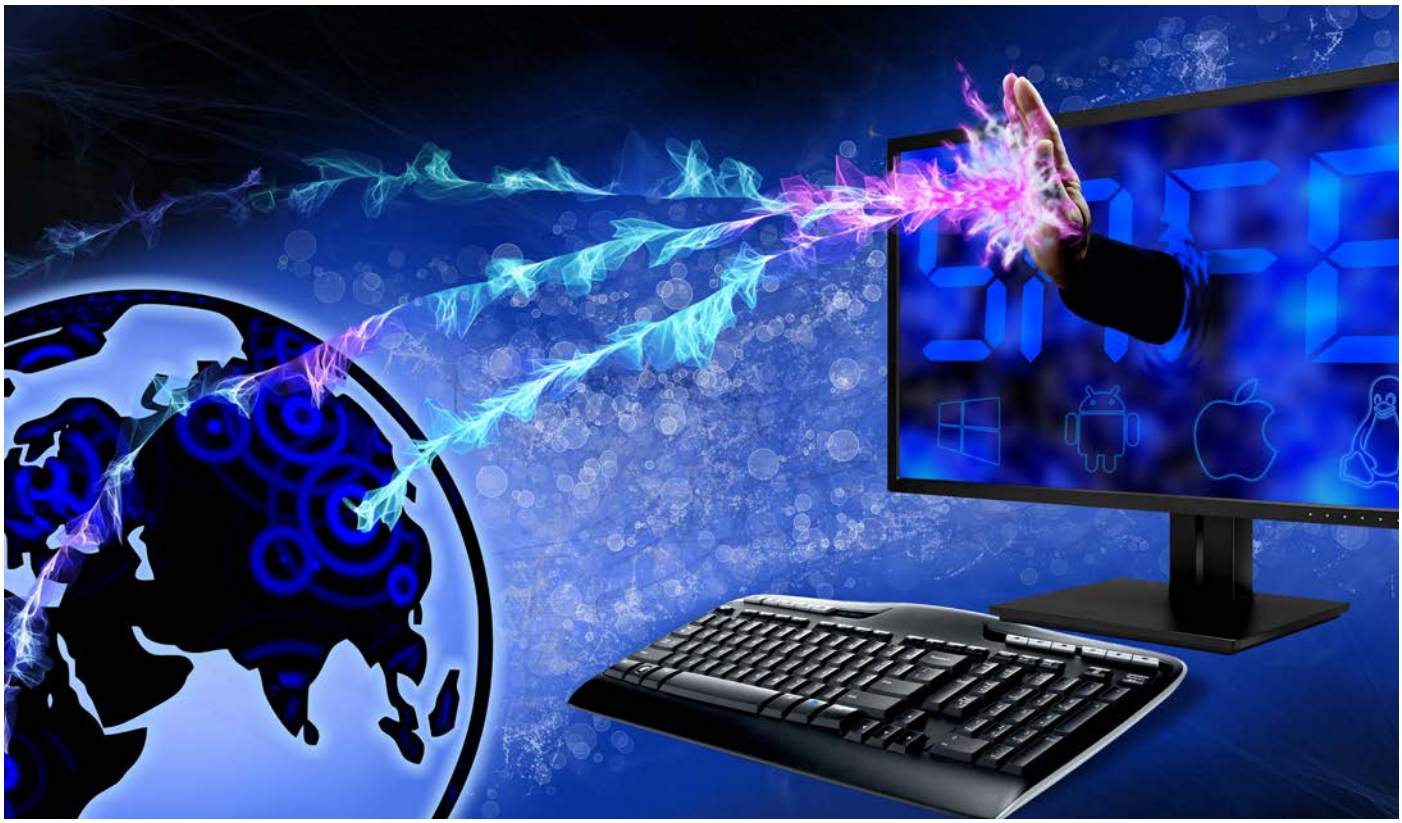
gence between the EU and UK data protection frameworks with regard to certain basic provisions, such as: the basis for lawful and fair personal data processing for legitimate purposes, purpose limitation, quality and proportionality of data, data retention, security and confidentiality, and transparency. In its opinions the Board did, however, identify some aspects the European Commission should review further or subject to strict monitoring.

Meetings via Teams after entering a special 13-digit identifier

By the end of May Microsoft plans to implement a new method of joining meetings in the Teams application. It will introduce a 13-digit code that will eliminate the need to use a link. All meetings will have a meeting identifier automatically assigned to a Microsoft Teams user and added to the invitation under the link to the meeting. Attendees will be able to join by entering the identifier. Pre-joining, lobby, and security will remain the same for all the meeting attendees.

Gaps in Microsoft Exchange dangerous for many companies

The recently announced gaps in the Microsoft Exchange Server have had a real impact on the security of companies throughout the world. The gigantic scale of the damage was reported, among others, by KrebsOnSecurity. Exchange Server, the world's most popular mail server, was hacked earlier this year, whilst Microsoft only patched the security gaps in March. This means that criminals had almost two months to launch their attacks. Check Point experts point out that any organization that has not implemented patches or does not have advanced protection systems may still be seriously exposed to attacks.



BDO spółka z ograniczoną odpowiedzialnością sp.k., ul. Postępu 12, 02-676 Warszawa;
tel.: +48 22 543 1600, fax: +48 22 543 1601, e-mail: office@bdo.pl