ALERT SAFE COMPANY

No. 9/2021

Ladies and Gentlemen,

We present the new edition of our "Secure Company" alert, containing information on anti-money laundering (AML) and counter-terrorism as well as cyber security and personal data protection.

In this edition, we would like to draw your attention to two issues related to further provisions of the amended Act on counteracting money laundering and combating terrorism, which are now coming into force. The first issue is extension of the list of entities carrying out so-called regulated activity to include business operators servicing companies and trusts. The other change involves the Central Register of Beneficial Owners (CRBR).

We would also like to draw your attention to issues related to so-called GDPR II, i.e. the EU regulation on privacy and electronic communications, which, due to its scope, will apply to virtually all companies conducting business using the Internet.

With the rising tide of spyware attacks on phones, we would also like remind you of the cyber security issues surrounding the use of company phones.

We hope that the next batch of information on planned changes in AML regulations and on GDPR and cyber security will prove useful and facilitate smooth navigation through regulations and legislative trends, on the grounds of both Polish and EU law.

Should you need additional, more detailed information, feel free to contact our firm and experts directly.

DR ANDRÉ HELIN, BDO Managing Partner

Starting from the end of October, new provisions for entities servicing companies and trusts come into force

The amended provisions of the AML Act, coming into force as of 31 October 2021, introduce an obligation to fulfill certain requirements and to make an entry in the register for, among other entities, business operators conducting activity for the benefit of companies and trusts (regulated activity). However, the obligation to obtain an entry in the register does not apply to legal counsels, lawyers and companies referred to in Article 8 of the Act on legal counsels and Article 4a of the Act on the bar.

As such, activities for the benefit of companies and trusts include: establishing a corporation or unincorporated entity; holding the position of member of the board of directors or enabling another person to hold that or a similar position in a corporation or unincorporated entity; providing a seat, place of business address or address for correspondence as well as other related services to a corporation or unincorporated entity; acting or enabling another person to act as trustee of a trust arising from a legal action; acting or enabling another person to act as person exercising the rights attached to shares or stocks for an entity other than a company listed on a regulated market that is subject to disclosure requirements under European Union law or to equivalent international standards.

Business operators conducting activity for the benefit of companies and trusts must also meet the statutory requirements of no criminal record, and have proven knowledge or experience in the area concerned.

The requirement of a clean criminal record means that the business operator should not have been sentenced for intentional offenses against: the activity of state institutions and local government; administration of justice; credibility of documents; property; business trading and financial interests in civil law transactions; money and securities trading; financing of terrorist crimes; offenses committed for financial or personal gain; or intentional fiscal offenses.

As regards the requirement to possess and provide evidence of knowledge or experience relevant to the regulated activity, completion of appropriate training or courses or involvement for at least one year in actions relating to activity for the benefit of companies or trusts will be sufficient.

The above requirements must be met, respectively, by natural persons conducting business activity in the scope concerned or members of managing bodies, persons who manage the performance of actions related to the conduct of regulated activities, beneficial owners of legal persons or organizational entities conducting regulated activities, as well as partners of such entities, as long as such partners are entrusted with management of the company's affairs or authorized to represent it.

Conducting regulated activity without obtaining an entry in the relevant register will carry a pecuniary penalty of up to PLN 100 thousand.

The Act of 30 March 2021 amending the Act on counteracting money laundering and terrorism financing and certain other acts, published in the Journal of Laws of 30 April 2021 (item 815), is generally effective from 15 May 2021. However, some of its provisions came into force on 31 July, and some only become effective on 31 October 2021.

Amended CRBR provisions to take effect in a month's time

The most important change in the area of CRBR's operation, which takes effect on 31 October 2021, is implementation of a mechanism for verifying the validity and truth of information contained in CRBR, which will now be the responsibility of obliged entities.

On 31 October 2021, provisions of the Act of 30 March 2021 amending the Act on counteracting money laundering and terrorism financing and certain other acts (Journal of Laws of 2021, item 815) come into force, in respect of changes relating to submissions to the Central Register of Beneficial Owners (CRBR), including penalties that may be imposed in connection with such submissions.

The amendment significantly expands the catalog of entities obliged to make submissions to CRBR. The catalog has been extended primarily to include trusts whose trustees or persons in equivalent positions reside or have their registered office, establish business relations or acquire real property in the territory of the Republic of Poland in the name or on behalf of trusts, as well as: partnerships; European economic interest groupings; European companies; cooperatives; European cooperatives; associations subject to registration in the National Court Register; foundations.

The amendment also specifies who can make a submission to CRBR. The person must be authorized to represent the entities covered by the obligation (and in the case of trusts – a trustee or person in an equivalent position). When making the submission, the authorized person has to provide his/her name and surname, citizenship, country of residence, Personal Statistical Number PESEL (or date of birth if the person does not have PESEL) and function entitling to make the submission.

The most important change in the area of CRBR's operation (which we have already mentioned in previous editions of our alert) is implementation of a mechanism for verifying the validity and truth of information contained in CRBR, which will now be the responsibility of obliged entities. This means in practice that each obliged institution will be required to analyze CRBR data when examining its clients. If any discrepancies are found between information submitted to CRBR and information the information gathered by the institution, it will be obliged to investigate the reasons of such discrepancies. If it turns out that data submitted to CRBR has indeed changed, the obliged institution will be required to inform the competent authority, via the IT system, about such discrepancies and to provide the relevant substantiation and documentation.

The so-called cooperating entities (as e.g. state and local government administrative bodies) will also be entitled to inform about any identified discrepancies between CRBR data and the actual status. Such entities (bodies) will also be entitled to post an appropriate note informing about the institution and completion of investigative proceedings, which will appear in CRBR, and to issue a decision on rectification of data in CRBR.

It also follows from the amendment that beneficial owners will be required to provide the entities obliged to make submissions to CRBR with all information and documents necessary to submit beneficial owner information or to update it timely. Failure to fulfill this obligation, resulting in the entity failing to timely submit the information or providing information inconsistent with the actual state of affairs, will carry a financial penalty of PLN 50,000 imposed on the beneficial owner.

The amendment also extends the catalog of sanctions imposed on entities subject to obligatory submission to CRBR to include a financial penalty for providing inaccurate information in the amount of up to PLN 1 million.

EU finalizes a regulation on e-privacy and electronic communications

Any company that provides telecommunications or instant messaging services, sends mailings and uses call-center services, as well as all organizations with websites that use cookies, should note the ongoing EU works on the privacy and electronic communications regulation (so-called ePrivacy or GDPR II).

The regulation on privacy and electronic communications (EPVO) is to replace the Directive on privacy and electronic communications (2002/58/EC, as amended), which has been in force since 2002.

The draft regulation on privacy and electronic communications, discussed since 2017, aims to protect confidentiality of communications, as well as confidentiality and integrity of users' devices. As opposed to GDPR, not only natural but also legal persons are protected. The regulation clarifies and supplements GDPR in its part relating to electronic communication data being personal data. It is intended to regulate areas such as e.g. the storage of communication data and metadata, ensuring that encrypted messages can be read in specific cases, direct marketing with the use of telecommunications devices, and utilization of cookies.

The regulation governs communication by classical voice telephony, text messaging and e-mail, communication by VoIP telephony, instant messaging and Internet e-mail services, as well as machine-to-machine communication (so-called Internet of things).

Among other things, the regulation is to introduce the principle of data protection already at the stage of design as well as data protection by default. Currently, the default cookie setting of most browsers is “accept all cookies”. Providers of software enabling the search and presentation of information on the Internet should therefore be required so to configure their products as to offer the option of preventing third parties from storing information on the end devices; this is often presented as the “reject third party cookies” option. End users should be able to choose from a range of privacy settings, from the highest (for example, "never accept cookies") to the lowest (for example, "always accept cookies") and intermediate (for example, "reject third-party cookies" or "accept administrator cookies only"). Such privacy settings should be presented in a visible and understandable manner.

It was originally assumed that the ePrivacy Regulation would come into force at the same time as GDPR. This, however, proved impossible. Recently, though, works have accelerated, the draft has already been approved by the European Commission and the Council of the European Union and now only needs approval of the European Parliament.

Once the ePrivacy Regulation comes into force, administrators will have many new obligations. Therefore, appropriate preparations are worth starting now.

Companies need measures to ensure the security of company phones

To ensure data security, companies should have strictly defined and followed procedures for constant monitoring of the status of programs installed on employees' company phones.

Today, taking care of the company's security, in the areas of both personal data and access to company secrets, is no longer limited to designing, implementing and applying procedures to ensure legal security or to regulating access to sensitive data. Procedures are also needed that relate to IT security, including the security of commonly used company smartphones, which no longer serve for communication purposes only (calls, e-mail), but often also for quick browsing and editing of data important to the company, financial data included.

Recent information about further attempts to add applications to the Google Play store the aim of which is to gain access to user data, or about ever more frequent text campaigns aimed at gaining access to confidential phone user data, should give rise to serious reflection on the security of company data stored on company phones. This applies also to personal data, whether data processed by the employee who uses the phone (third party data) or the user's own data. We must not forget that the phone remains owned by the company. The company is therefore jointly responsible for security of data stored on that phone.

To ensure such security, it is not enough to introduce appropriate regulations concerning the principles of using company phones and imposing appropriate restrictions and obligations on their users. What is also needed is an appropriate procedure for constant monitoring of validity of the operating systems installed on such phones so as to avoid the dangers related to software vulnerabilities and to ensure that they are constantly updated in the event of security patches. It is also necessary to monitor applications installed on the phones by employees so as to be able to eliminate, in a timely manner and on the basis of generally available information, the applications that may pose a risk of unauthorized access to the phone.

Most companies either fail to notice that danger or underestimate it. This is a serious mistake, which may prove costly for the company. And yet the security policy adopted in companies must absolutely cover that area of threats, providing for both the relevant rules and for procedures to ensure their implementation in the company's ongoing operations.

In short:

EDPB demands that the Irish supervisory authority reverse its decision on WhatsApp

The European Data Protection Board (EDPB) demands that the Irish supervisory authority reverse its decision on WhatsApp. The Board requests explanations on transparency and the calculation of fines for multiple breaches. The binding decision seeks to resolve a dispute arising from a draft decision issued by the Irish supervisory authority as lead supervisor in relation to WhatsApp Ireland Ltd. (WhatsApp) and subsequent objections expressed by a number of affected supervisory authorities. Thus for example, in relation to WhatsApp's collection of non-user data – when users choose the contact function – EDPB has found that, in the case in question, the procedure followed by WhatsApp failed to result in anonymization of personal data collected.

More and more attacks leading to theft of bank account access

Recently, there have been two large-scale text message attacks. The first one involves messages entitled "Quarantine". A link in the message directs to a page urging to download a "Flash Player" application. The application is malicious: once installed, it attacks the smartphone owners' bank accounts and robs them of their money. It affects smartphones with Android OS. Within the other attack, criminals send fake text messages impersonating multiple courier companies such as DPD and InPOST (Paczkomaty) and encouraging to install a new application for parcel collection. Having clicked a link in the message, the attack victim is directed to a website that imitates the courier company's site. Once there, the victim is urged to download an application. Once downloaded and installed, the application infects the phone with malware to steal money from victim's bank accounts.

Anonymization is to guarantee the security of the processed data

As reported by cyberdefence24.pl, BizTech Konsulting SA specialists have developed a solution to protect data in accordance with GDPR. Black Cargo ensures anonymization, i.e. permanent and irreversible erasure of personal data, which is replaced with fictitious data with the source database's relations and links preserved. As a

result, the person concerned cannot be identifies as the anonymized data is not associated with that person. Such data is no longer protected. Anonymization is used in various types of analysis, statistics, database testing, courts, research and many other purposes. Among other things, data contained in the databases of a training system can be anonymized for the purpose of statistical analyses of customers which allows the realization of statistical analyses of customers, as well as personal data under the right to be forgotten. The Black Cargo application comprises two modules: Black Cargo Masking and Black Cargo Scanning.

Xiaomi wants to assess the security of its smartphones

The Chinese corporation Xiaomi has hired an external expert to assess the security of its smartphones. The company's decision is a result of the Lithuanian government's appeal to citizens not to use devices of Chinese brands due to existing risks. Previously, similar appeals or recommendations were made by the governments of other countries as well. The Lithuanian National Security Center, which examined three smartphones from Chinese manufacturers, found four significant security risks. Three of them concerned Xiaomi Mi 10T 5G, and one – Huawei P40 5G. No such risks were detected in OnePlus 8T 5G.

Free Windows 10 upgrade to Windows 11 will be available

Microsoft has already released six Windows 11 updates. Now, it has announced that Windows 11 will be released on 5 October. Windows 10 users will be offered the option of free system upgrade provided that the hardware on which it is installed meets the minimum requirements of the new system. The free upgrade offer has no specific end date for eligible systems. However, Microsoft reserves the right to eventually end support for the free offer. As follows from its announcement, Windows 10 will be supported until 2025. Within the first 10 days of Windows 11 installation, the user will be offered the option of downgrading the system and reverting to version 10.

BDO is an international network of independent audit and advisory firms. Service provision within the BDO network is coordinated from the Brussels global office. BDO's beginnings go back to 1963. We have been present in Poland since 1991.
We have 5 offices in: Warsaw, Kraków, Poznań, Wrocław and Katowice.
BDO has for years been recognized in prestigious rankings of the activities performed by its Audit and Tax Advisory Departments, including most recently.

The last distinctions for the company are related to the Rankings:
Companies and Tax Advisors of Dziennik Gazeta Prawna for 2020:
- The Best Tax Advisor in the category of medium-sized companies (1st place)

The 2020 rankings prepared by the Rzeczpospolita and Parkiet dailies:
- Most Active Firm on the Stock Exchange (1st place)
- Best Auditor of Listed Companies (3rd place)
- Best Audit Firm (5st place)

**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**