ALERT SAFE COMPANY

No. 7/2021

Ladies and Gentlemen,

Here is another issue of our "Secure Company" Alert, which this time contains information on counteracting money laundering and combating terrorism (AML), as well as on cybersecurity and personal data protection. We continue to hope that you will find it useful and interesting.

In this issue we dedicate a lot of attention to counteracting money laundering (AML). There are two reasons for this. Firstly, as of 31 July the group of so-called obligated institutions will be expanded as a result of the amendments to Polish regulations passed this spring. Most of them became effective as of 15 May, while others are about to go into effect. Secondly, the European Commission has announced a large package of changes to EU AML regulations. They are not only very interesting, but also important. In particular, they provide for several new solutions, such as the establishment of a new EU oversight authority, a ban on cash transactions in excess of 10 thousand euro, or a limit on anonymous payments in cryptocurrencies.

We would also like to draw your attention to the shorter pieces of information, including those on cybersecurity. As you will see, there are still serious problems, especially since the number of phishing attacks continues to be on the increase. A lot is also happening with regard to personal data protection, especially when it comes to the activities of the European Data Protection Board (EDPB).

We hope that another portion of information on the changes planned to AML regulations, as well as information on GDPR and cybersecurity, will be useful and will make it easier to navigate regulations and legislative trends, both Polish and European.

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, BDO Managing Partner

New groups of entities will report suspicious transactions

As part of counteracting money laundering, as of 31 July new groups of entities must verify the transactions of their clients and report those that are suspicious to the General Inspector of Financial Information.

31 July 2021 is the effective date of amendments to the Act on counteracting money laundering and terrorist financing (AML), which provide for numerous changes to the definition of so-called obligated institutions.

Although most of the amendments went into effect as of 15 May, some of the provisions of the Act will only go into effect after 3 months of its publication, i.e. counting from 30 April. It is therefore 30 July, so the new regulations will go into effect on 31 July. Among others, this will apply to changes in the definition of obligated institution. Under the amendments, as of 31 July the group of such institutions will, among others, include businesses whose main area of activity is the provision of services consisting of preparing returns, bookkeeping, providing tax or customs law advice, opinions or explanations, which are not other obligated institutions, i.e. to put it simply, most of all accounting offices. Up until now, the obligations arising out of the regulations in this area had to be fulfilled by entities that provided bookkeeping services.

This, however, is not the only such group. The same will apply to real estate agents and to businesses that sell or broker the sale of art, collectibles and antiques.

What is more, such entities will have to identify the beneficial owners of the companies they provide services to (those with actual impact on the client). The act indicates that beneficial owner can be any natural person who exercises direct or indirect control over a client — through powers arising from legal or factual circumstances, which enable this person to have a decisive impact on the activities or actions undertaken by the client, or any natural person on whose behalf a business relationship is established or an occasional transaction is conducted.

The Act of 30 March 2021 amending the Act on counteracting money laundering and terrorist financing, as well as certain other acts, published in the Journal of Laws on 30 April 2021 (item 815), became effective on 15 May with regard to other changes, including among others those relating to submissions to the Central Register of Beneficial Owners (CRBR), as well as with regard to penalties that may be imposed in connection with CRBR submissions. We discussed this in the previous issue of our alert.

Another group of regulations will become effective in another three months, i.e. as of the end of October.

The EU will reform its system of counteracting money laundering

The European Union wants to strengthen the centralization of the fight against money laundering and ban cash payments in excess of 10 thousand euro. The package of changes also includes a proposal to establish a new EU authority to fight money laundering.

On 20 July 2021, the European Commission presented an ambitious package of legislative proposals to strengthen the EU's anti-money laundering and countering the financing of terrorism rules. The package also includes a proposal for the creation of a new EU authority to fight money laundering.

The aim of the package is to improve the detection of suspicious transactions and activities, and close loopholes used by criminals to launder illicit proceeds or finance terrorist activities through the financial system. As recalled in the EU's Security Union Strategy for 2020-2025, enhancing the EU's framework for anti-money laundering and countering terrorist financing will also help to protect Europeans from terrorism and organized crime.

The package consists of four legislative proposals: a regulation establishing a new EU anti-money laundering and terrorist financing authority; a regulation on anti-money laundering and combating terrorist financing containing directly-applicable rules, including in the areas of customer due diligence and beneficial ownership; a sixth directive on anti-money laundering and combating terrorist financing replacing the existing Directive 2015/849/EU (the fourth AML directive as amended by the fifth AML directive), containing provisions that will be transposed into national law, such as rules on national supervisors and financial intelligence units in Member States; a revision of the 2015 Regulation on Transfers of Funds (Regulation 2015/847/EU) to trace transfers of crypto-assets.

The new EU anti-money laundering authority will be the central authority coordinating national authorities to ensure the private

sector correctly and consistently applies EU rules. The authority will also support financial intelligence units to improve their analytical capacity around illicit flows and make financial intelligence a key source for law enforcement agencies.

The EU anti-money laundering authority will in particular perform the following: establish a single integrated system of supervision over anti-money laundering and combating terrorist financing across the EU, based on common supervisory methods and convergence of high supervisory standards; directly supervise some of the riskiest financial institutions that operate in a large number of member states or require immediate action to address imminent risks; monitor and coordinate national supervisors responsible for other financial entities, as well as coordinate supervisors of non-financial entities; support cooperation among national financial intelligence units and facilitate coordination and joint analyses between them, to better detect illicit financial flows of a cross-border nature.

Whereas a single set of EU rules on counteracting money laundering and combating terrorist financing will harmonize the rules on counteracting such dealings across the EU, including, for example, more detailed rules on customer due diligence, beneficial ownership and financial intelligence units. Existing national registers of bank accounts will be connected, providing faster access for financial intelligence units to information on bank accounts and safe deposit boxes.

The proposed amendments will ensure full traceability of crypto-asset transfers, such as Bitcoin, and will allow for prevention and detection of their possible use for money laundering or terrorism financing. In addition, anonymous crypto-asset wallets will be prohibited, fully applying the EU's rules on anti-money laundering and combating terrorist financing rules to the crypto sector.

The Commission has also proposed an EU-wide limit of €10,000 on large cash payments. This EU-wide limit is high enough not to put into question the euro as legal tender. National limits under €10,000 will remain in place.

The legislative package will now be discussed by the European Parliament and Council.

There is a new computing cloud standard for the insurance industry

The Polish Chamber of Insurance, in cooperation with the Polish Chamber of Information Technology and Telecommunications, has developed a computing cloud standard for the insurance industry. It is a set of rules for the preparation and effective implementation of a cloud, in compliance with all of the applicable legal and regulatory requirements.

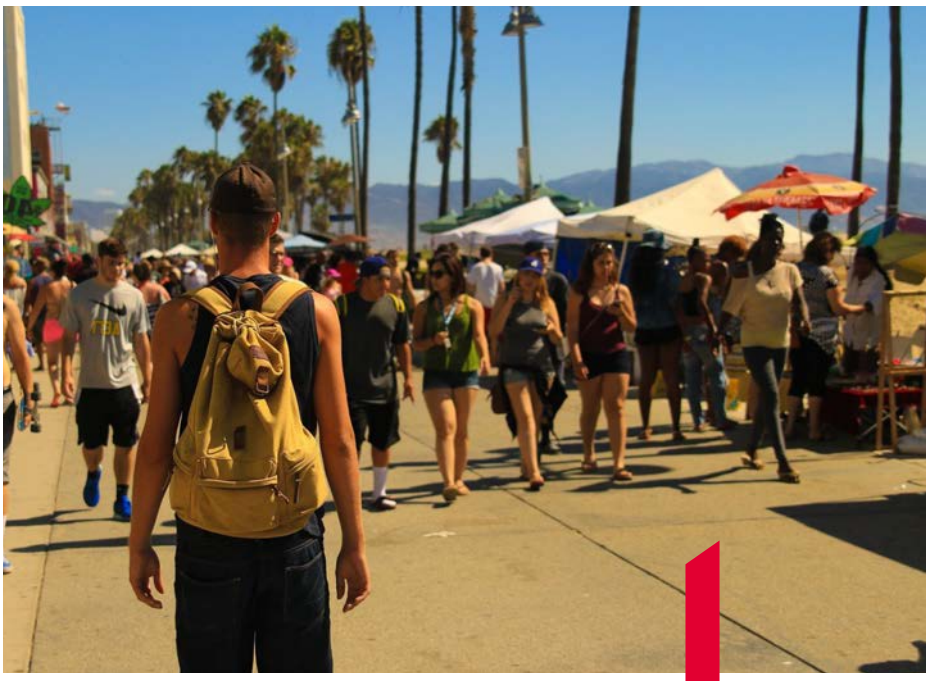
The standard refers to the requirements pertaining to the use of cloud solutions by entities covered by insurance supervision. It analyzes the relevant announcement and presents the requirements of the Office of the Financial Supervision Authority (UKNF) on the processing of information in a public or hybrid computing cloud by entities subject to insurance supervision.

The standard has been divided into chapters dedicated to regulations that affect the implementation of computing cloud services in the insurance sector.

And so for example, the guidelines on the classification and assessment of information explain that an insurance company classifies information in a documented manner, in accordance with the methods described in the Standard or another method adopted by the insurance company, including in particular ensures that: the classification of information divides information into categories; the classification of information divides information into at least legally protected and other information; the classification of information considers the basic security attributes, i.e. confidentiality, integrity and accessibility. The insurance company continually monitors changes in legal and regulatory requirements that would require the processed information to be reclassified.

With respect to risk, the standard recommends for insurance companies to at least once a year verify the factors that significantly affect risk assessment (including legal, regulatory, organizational and technical requirements) and, if such factors exist, reassess the risk.

The standard also states that in order to ensure security of the data processed in a computing cloud (or intended to be processed), the insurance company should ensure an appropriate level of competency of its employees and associates, where an appropriate level of competency is generally defined based on a the results of a risk assessment. Maintaining and gradually raising competency (qualifications, knowledge and skills) should be a part of the insurance company's good practices. Any deficiencies should be addressed by acquiring competencies such as external and internal training, transfer of knowledge, or support from companies that provide computing cloud related advisory services. Depending on the computing cloud model, the insurance company should define the competencies needed to implement or maintain cloud solutions.



In short:

Polish version of facial recognition guidelines available

On 28 January 2021, the Council of Europe's Committee on Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data adopted the "Guidelines on facial recognition". The document pertains to the use of facial recognition technologies, including live facial recognition technologies. The guidelines contain a number of recommendations on the rules that should be complied with and applied in order to ensure the integrity of human dignity, human rights and fundamental freedoms of every person, including the right to the protection of personal data. An unofficial translation of the guidelines is currently available on the UODO's website. Facial recognition is the automatic processing of digital images containing individuals' faces for identification or verification of those individuals by using face templates.

Gmail will use the organization verification standard

Gmail will get another function. Last year Google introduced BIMI (Brand Indicators for Message Identification) as part of its GSuite. Now the option will appear in Gmail. BIMI will help users verify whether a given email actually originates from a business (a sender successfully verified by Google). To this end, Gmail will show the logos of the companies that may write to us. The purpose is to show that the given senders have been successfully verified by Google and instead of an avatar, they have their own logo.

117 security errors in Microsoft products corrected in July

In the middle of July Microsoft began the distribution of the newest security updates as part of its July Patch Tuesday. Nearly 120 bulletins have been prepared for this month. Patches were applied to various products, including Windows and Microsoft Office, SharePoint, Excel, Microsoft Exchange Server, Windows Defender, Windows SMB. The July Patch Tuesday brought with it a total of 117 security bulletins, i.e. many more than the one in June. 13 of the gaps had the status of critical.

Guidelines on the concept of controller and processor adopted

At its 51st plenary on 7 July 2021, after public consultations, the EDPB adopted the final version of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR. The document is made up of two main sections: the first explains the concepts of "controller", "joint controller", "processor", "third party", whilst the second contains a description and explanation of the consequences of attributing different roles in data processing. The guidelines also contain a diagram that provides further practical guidance and makes it easier for entities to better understand the said concepts.

EDPB adopts guidelines on codes of conduct

At its plenary session, the EDPB adopted Guidelines on codes of conduct as tools for transfers. The main purpose of the guidelines is to explain the application of GDPR articles that provide that once approved by the competent supervisory authority and having been granted general validity within the Union by the Commission, a code of conduct may also be adhered and used by controllers or processors not subject to the GDPR located in third countries for the purpose of providing appropriate safeguards to data transferred to third countries. The guidelines complement the EDPB Guidelines 1/2019 on codes of conduct, which establish the general framework for the adoption of codes of conduct. Guidelines 1/2019 explain the procedures and methods for the submission, approval and publication of codes of conduct at both national and EU level.

Serious security flaw detected in Google Chrome

Older versions of the Chrome browser have a security vulnerability (CVE-2021-30561), the existence of which has been officially confirmed by Google. It is therefore necessary to urgently

update to the browser's newest version. In this specific case, the problem relates to the JavaScript V8 engine, which is the heart of the browser. The problem affects an unknown function of the v8 component. Manipulation using unknown input data may result in an unauthorized access vulnerability. This affects confidentiality, integrity and accessibility. The vulnerability has already been fixed in Chrome's newest version (91.0.4472.164).

Ireland will not adopt final measures against Facebook

At its 52nd plenary the European Data Protection Board (EDPB) adopted its first urgent binding decision pursuant to Article 66 par. 2 of the GDPR following a request from the Hamburg supervisory authority, after the supervisory organ had adopted provisional measures towards Facebook Ireland Ltd (Facebook IE) on the basis of Article 66 par. 1 of the GDPR. The Hamburg supervisory authority ordered a ban on processing WhatsApp user data by Facebook IE for their own purposes following a change in the Terms of Service and Privacy Policy applicable to European users of WhatsApp Ireland Ltd. The EDPB decided that the conditions to demonstrate the existence of an infringement and an urgency are not met. Therefore, the EDPB decided that no final measures need to be adopted by the Irish supervisory authority against Facebook IE in this case.

GUS will collect fewer data from water and sewage companies

Following an objection by the President of the UODO, the Main Statistical Office (GUS), as part of its statistical studies in 2022 will not collect the following data on the customers of water and sewage service providers: first and last name, PESEL number, residence address, mailing address, e-mail address or phone number. Previously, in his opinion on the draft regulation, the President of the UODO stated that the provisions of the Act of 7 June 2001 on the collective supply of water and collective disposal of sewage do not indicate that agreements for the supply of water or disposal of sewage authorize water and sewage companies to obtain their clients' PESEL numbers, phone numbers and e-mail addresses. The President of the UODO stressed the inadmissibility of situations where for the purpose of performing the tasks of another controller (in this case GUS), the data providing controller (in this case the water and sewage company) would be required to collect personal data that are not appropriate for its own purposes and to provide them to another, new controller.

Fake Allegro, Lotus and WP pages phish user data

The Polish financial sector's Computer Security Incident Response Team CSIRT KNF warns against a webpage that bears a striking resemblance to the Allegro auction service. Cybercriminals are trying to phish users' login and payment card data. The allegro.pl with a fake extension looks very much like the original. It enables a standard login and in the next step — the provision of payment card data. The same institution has warned against the webpages of Lotos and Wirtualna Polska, which have also been created in order to phish for data.

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