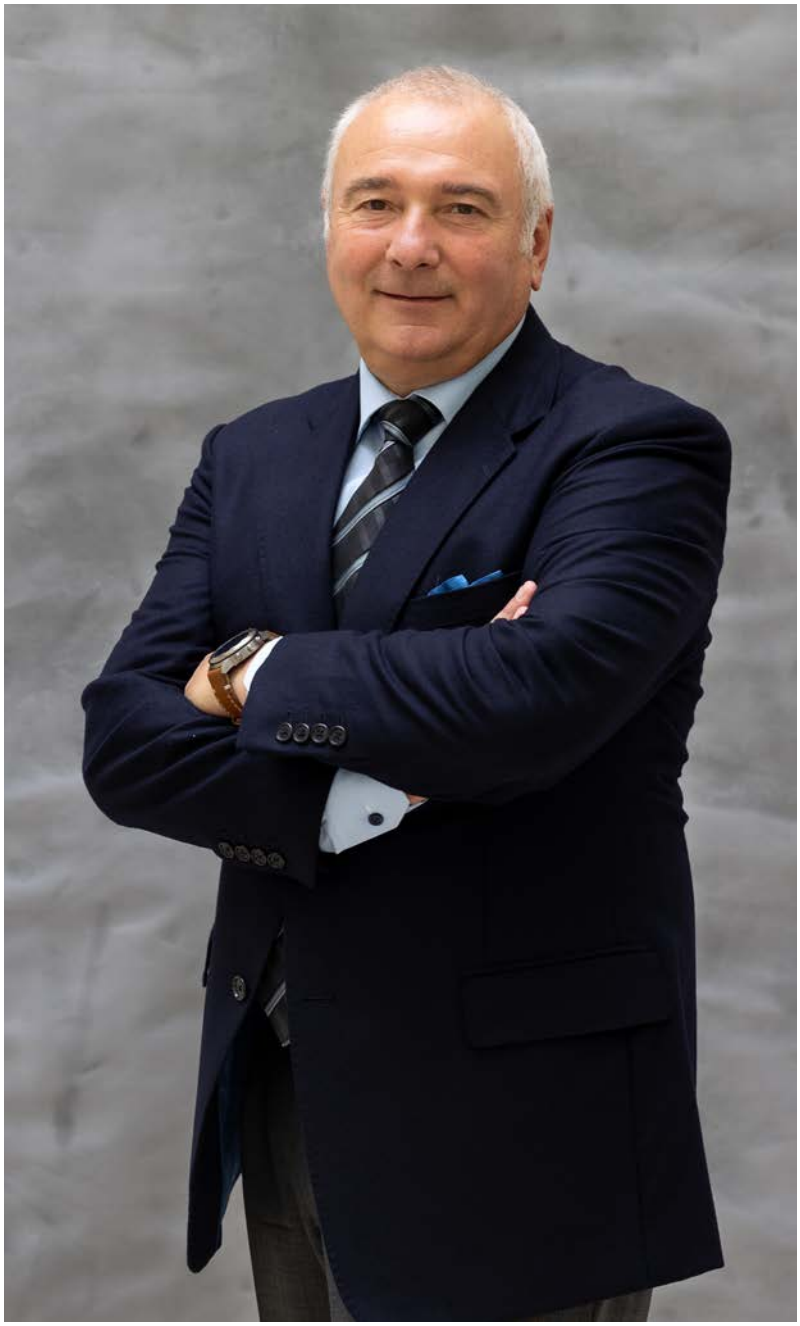
ALERT SAFE COMPANY

No. 9-10/2022

Ladies and Gentlemen,

Below please find the latest issue of our "Safe Company" alert, which discusses what we consider to be the most current and interesting information about anti-money laundering and anti-terrorism (AML), as well as cyber security and data protection.
This time we would first of all like to draw your attention to the planned changes in the operation of the Central Register of Beneficial Owners (CRBR) and the planned EU regulation, which is to define the rules for marketing products with digital elements in order to ensure the cyber security of such products. What is important here is that the new act will be a regulation, and therefore will not require implementation but will apply directly in EU countries, without the need for national legislation.
In addition, as always, we present the most interesting shorter security information.
We hope you find the content of this alert useful, making it easier to smoothly navigate the regulations and trends related to cyber security, data protection and AML.
Should you need additional, more detailed information, feel free to contact our firm and experts directly.



DR ANDRÉ HELIN, Prezes BDO

The processor must provide guarantees for the protection of data subjects

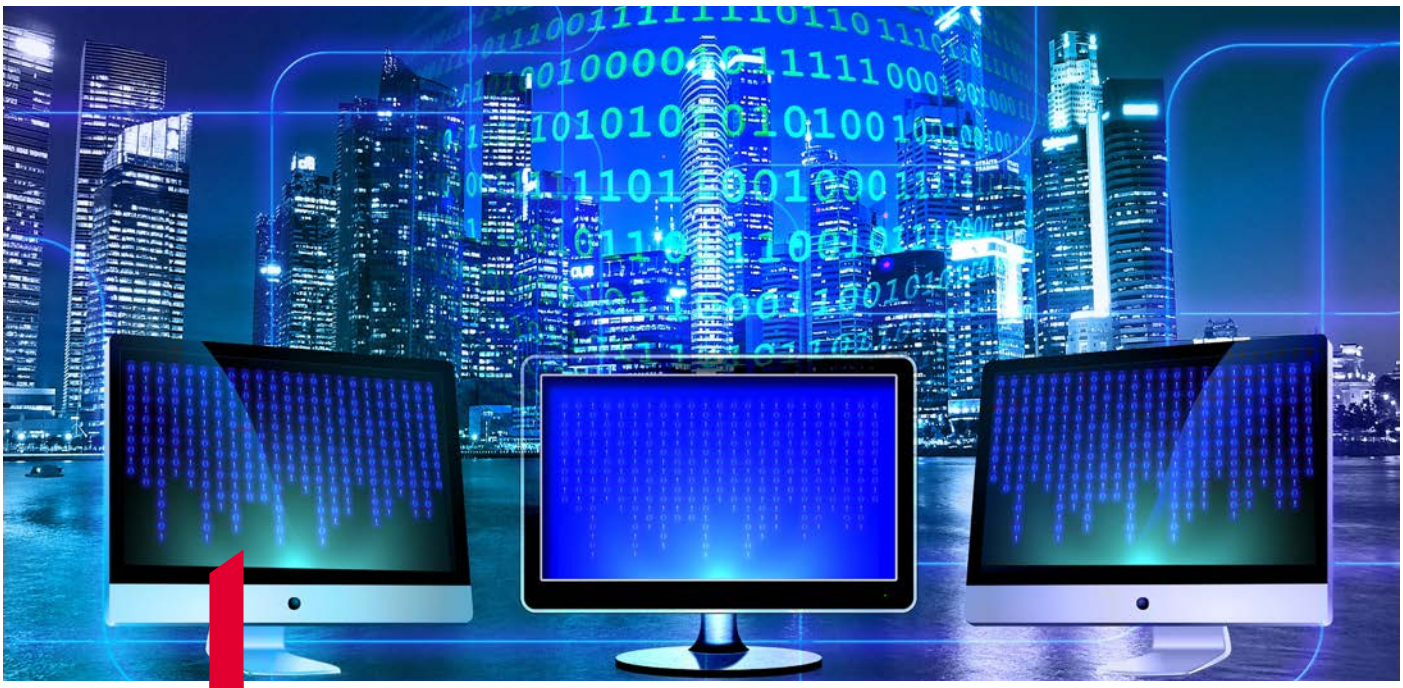
When deciding to entrust the processing of personal data to another entity, the controller should verify whether such entity offers sufficient guarantees of implementation of appropriate technical and organizational measures, and whether the processing will meet the requirements of GDPR and protect the rights of data subjects.

Failure to verify the processor and its guarantees for processing compliant with data protection regulations may entail consequences for individuals whose personal data has been entrusted to the processor, as e.g. loss of personal data. Therefore, the decision to whom the controller is to entrust the processing of personal data may not be groundless. It is only after the competence and adequacy of the chosen processor has been verified that the controller may proceed to conclude an appropriate data processing agreement.

Entrusting the processing of personal data without a written data processing agreement and without verifying that the processor provides sufficient guarantees for the implementation of appropriate technical measures may result in imposition of an administrative fine by the Office for Personal Data Protection (UODO) (as experienced recently by the Sulkowice Cultural Center).

The controller must also be in possesion of documents confirming verification of the terms of cooperation with the processor.

Pursuant to Article 28 GDPR, a controller wishing to process data with the assistance of another entity should only use entities that provide sufficient guarantees for the implementation of appropriate technical and organizational measures. The processing as such by is carried out by the processor under a written agreement between the controller and the processor. The agreement specifies, among other things, the subject, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller.



New EU regulation to tighten cyber security requirements

On 15 September 2022, the European Union published draft assumptions for a regulation whose main goal is to increase the level of cyber security in member states. From the document it follows that manufacturers, importers and distributors of digital products to the European market will have to comply with a number of rules in order for their devices to be legally sold in member states.

The proposed regulation would harmonize and streamline Community regulations by introducing cybersecurity requirements for products with digital elements and avoiding overlapping requirements from different regulations, the EU document reads. This would ensure greater legal certainty for operators and users across the Union and better harmonization of the uniform European market, creating more cost-effective conditions for operators seeking to enter the EU market.

The regulation would lay down: rules for the marketing of products with digital elements to ensure their cyber security; essential requirements for the design, development and manufacture of products with digital elements as well as cyber security obligations of business operators with respect to such products; essential requirements for the processes of handling vulnerabilities, introduced by manufacturers to ensure cyber security of products with digital elements throughout their life cycle, as well as the obligations of business operators with respect to such processes; provisions for market surveillance and enforcement of the aforementioned rules and requirements.

Under the essential cyber security requirements and obligations, all products with digital elements would only be made available on the market if - once they are reliably delivered, properly installed, maintained and used as intended or under conditions that can be reasonably foreseen - they meet the essential cyber security requirements of the new regulation.

The essential requirements and obligations would impost on manufacturers the obligation to consider cyber security in the design, development and manufacture of products with digital elements; to exercise due diligence with respect to security aspects in product design and development; to maintain transparency about cyber security aspects that must be communicated to customers; to provide security support (updates) in a proportionate manner; and to comply with vulnerability handling requirements.

With regard to the marketing of products with digital elements, obligations would be established for business operators, from manufacturers to distributors and importers, appropriately to their specific roles and responsibilities in the supply chain.

There will be changes in the operation of the Central Register of Real Beneficiaries

The government is planning to change the rules of the Central Register of Beneficial Owners (CRBR). Among other things, entity search in the registry by the KRS number and name of the entity, and also by the number under which the trust is registered, is to become possible.

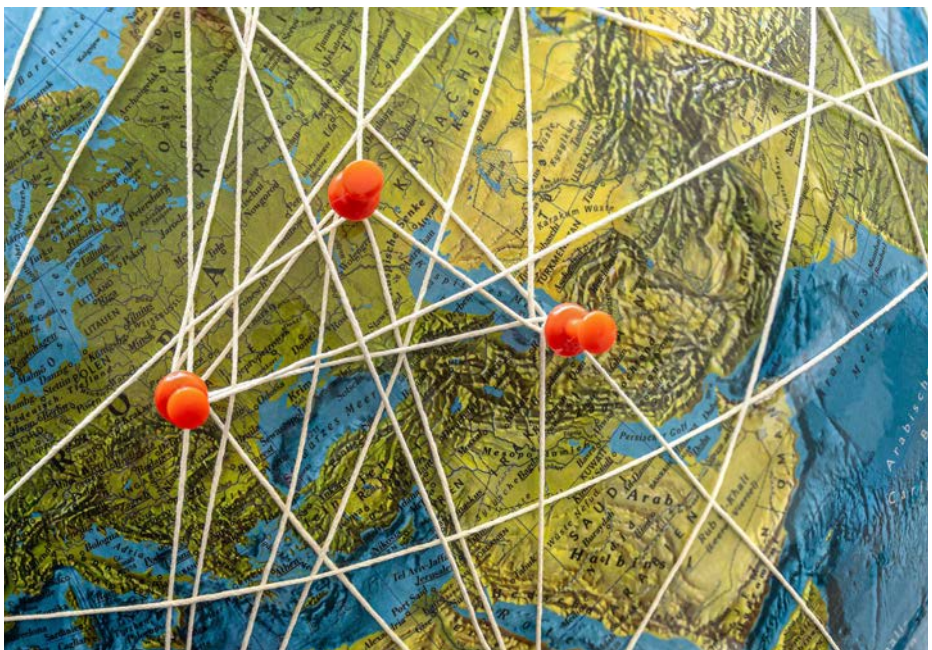
The Ministry of Finance has prepared a draft regulation amending the regulation on requests for and provision of information on beneficial owners (print 554).

It follows from the new regulations that in addition to the search criteria used so far (Personal Statistical Number PESEL, Tax Identification Number NIP, or full name and date of birth of the beneficial owner - in the case of beneficial owners entered in the Central Register of Real Beneficiaries as persons without PESEL), it will also become possible to search for entities by KRS number, as well as company name. Technically, the adopted solution will make it possibile to use of a part of the entity's name as a search criteria (by providing at least the minimum number of characters), and if more than one record is retrieved, information on the first records (maximum number of characters) will be provided as a search result and the entity name will have to be specified. The minimum and maximum number of characters will only be defined during modernization of the system.

In addition, in the case of entities governed by foreign law such as trusts and trusts-like legal arrangements that have not been assigned a tax identification number in Poland but have submitted information to the CRBR, the draft allows the CRBR to be searched by the technical number under which the trust was registered during the process of information submission to the CRBR.

This, however, is not the only change in the regulations. Namely, changes to the regulation are also to take into account the amended Act on counteracting money laundering and terrorist financing. The amendment extended the catalog of entities are required to report beneficial owner information to include trusts whose trustees or persons in equivalent positions are domiciled in the territory of the Republic of Poland, and trusts whose trustees or persons in equivalent positions establish business relations or acquire real property in the territory of the Republic of Poland in the name or on behalf of the trust. The obligation has been imposed on: partnerships; European economic interest groupings; European companies; cooperatives; European cooperatives; associations subject to registration in the National Court Register; foundations. Meanwhile, the regulation currently refers only to companies.

The new regulation is to enter into force on 1 January 2023. The draft is currently in the consultation stage.



In short:

Poles still unclear who to turn to for personal data protection

As many as 70 percent of Poles state they do not know who should deal with the negative consequences of a personal data leak, and 1/3 of those who are aware of the issue believe that it must be done by the victim. The remainder point to e.g. the police, the Office for Personal Data Protection (UODO) and data protection officers, and mainly expect them to provide detailed information about the incident and to recommend further action. This follows from a survey conducted by ChronPESEL.pl and the National Debt Register under the auspices of UODO.

EDPB has adopted a statement on the code of police cooperation

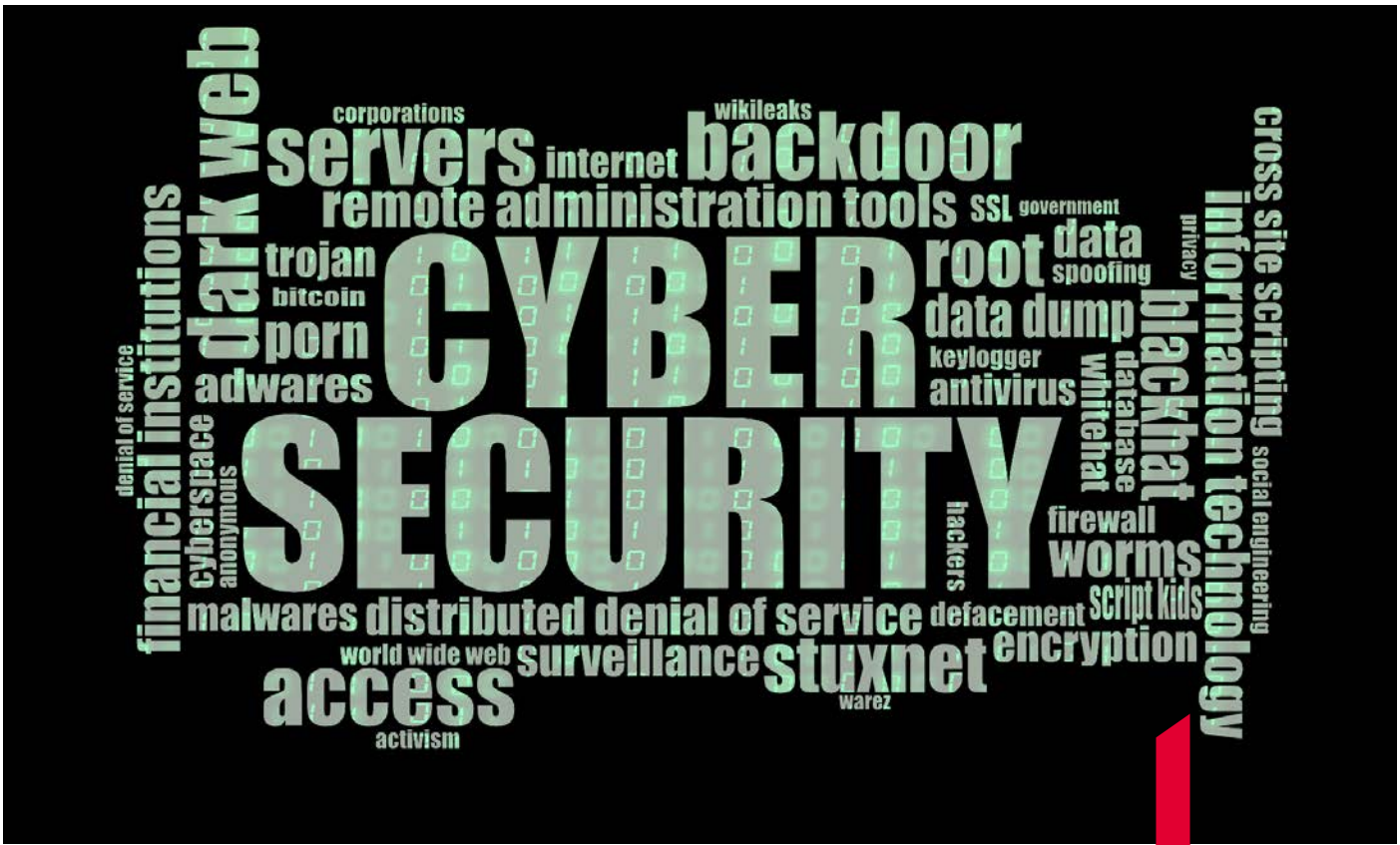
EDPB (European Data Protection Board), at its 69th plenary session, adopted a statement on the European Commission's proposal for an EU Police Cooperation Code, and selected the topic for a second coordinated enforcement action that will address the appointment and position of the Data Protection Officer. Among other things, EDPB recommends defining the types and severity of offenses that might justify automated searches of other member states' databases, and clearly distinguishing between personal data of different categories of data subjects, such as convicted offenders, suspects, victims or witnesses.

Remote workers are easier targets of cyber attacks

While often touting that remote work makes them more productive and easier to focus in the quiet of home, remote workers are also easier targets of cyber attacks, according to Cyberdefence24.pl. In total, nearly 30,000 security breaches were recorded in Poland in 2021 (CERT Poland data), 182 percent more compared to 2020. Therefore, 2022 can hardy be expected to score better in this regard, due to the war in Ukraine and the need for constant protection in cyberspace.

A sectoral anti-money laundering center is being established

The National Clearing House (KIR), Association of Polish Banks and individual banks are establishing a sectoral anti-money laundering center. They will exchange information on suspi-



cious transactions. The Sectoral AML Service Center is conceived as a structural and organizational aid to banks in fulfilling their numerous obligations under AML regulations. As the center's originators stress, it is not possible for a single bank to notice many circumstances beyond its specific area of operation. Only after receiving information from a larger number of banks is it possible to identify behavior patterns and interdependencies between transactions indicating their criminal nature.

Cyber security spending to grow to nearly $334 billion by 2026

According to a forecast by GlobalData, global revenues from cyber security will increase from $220 billion in 2021 to $334 billion in 2026. The ever-growing spending will be a consequence of the rapid increase in the number and sophistication of cyber attacks, the emergence of a large number of connected devices and their associated threats, and the prioritization of digital protection both within organizations and among consumers. Enterprise cyber security will prevail in terms of market demand (more than 90 percent revenue share in 2021).

New ways to attack inexperienced cryptocurrency users

Cyber security market analyst Serpent described on Twitter how fraudsters are currently targeting inexperienced cryptocurrency users. Among other things, they use fake websites, URLs, or hacked verified accounts. According to the expert, the criminals claim to be blockchain developers and seek out users who have fallen victim to a recent large-scale hack or exploit. They request a fee to implement a smart contract that can help recover stolen funds.

Most companies are unable to detect cyber threats on an ongoing basis

Three in etery four companies are unable to detect current cyber threats, according to a Dynatrace study. The report shows that early problem identification, prioritizing and mitigation of the impact of potential attacks is no longer an additional option, but a necessity. However, less than 40 percent of businesses use real-time vulnerability management features, and only 1/4 of security teams have access to accurate, constantly updated reports.

Hackers gained access to 140,000 payment terminals due to simple errors

Fintech Wiseasy was attacked by hackers. As a result, unauthorized persons gained access to 140,000 payment terminals. The case is reported by techcrunch.com, which at the same time notes that the intruders took advantage of a simple error: lack of two-factor authentication in the affected company's system. To make matters worse, the company responded belatedly to warnings from cyber security specialists, who had already reported on the data leak a few weeks ago.

Belgium sues IAB Europe before CJEU for violating GDPR

The Court of Justice of the European Union will look into complaints against IAB Europe and its ad tracking system, which may be inconsistent with GDPR. Belgium's data protection authority (APD) ruled in early February this year that the ad tracking system created by advertising industry association IAB Europe, which is used by 80 percent of websites, violates the basic principles of GDPR.

Revolut was hacked, but card data and passwords safe

The Times reports that Revolut was hacked. The total of 50,144 people were affected, including 20,687 Europeans and 379 Lithuanians. The hacker gained access to: full names, email addresses, addresses of residence, transaction information. Passwords and card data were not stolen.

**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**