ALERT SAFE COMPANY

BDO

No. 11/2022

Ladies and Gentlemen,

We are pleased to present the new edition of our "Safe Business" alert discussing the latest and most interesting information on anti-money laundering and combating the financing of terrorism (AML) and in the scope of cybersecurity and personal data protection.

This time, we would like to draw your attention to two important EU regulations, i.e. the Digital Services Act (DSA) and Digital Markets Act (DMA) as well as the position of the Polish Financial Supervision Authority (KNF) addressed to the participants of the insurance market and regarding cybersecurity.

Apart from that, as always, we present the most important brief information concerning safety and remind the AML regulations regarding aiding and abetting.

We hope you will find the portion of information served in this alert useful, making navigating the regulations and trends related to cybersecurity, personal data protection and AML easier.

As always, enjoy your reading, and should you need any further, more detailed information, do not hesitate to contact us and our experts.

DR ANDRÉ HELIN, BDO Managing Partner

New EU regulations on digital services and markets

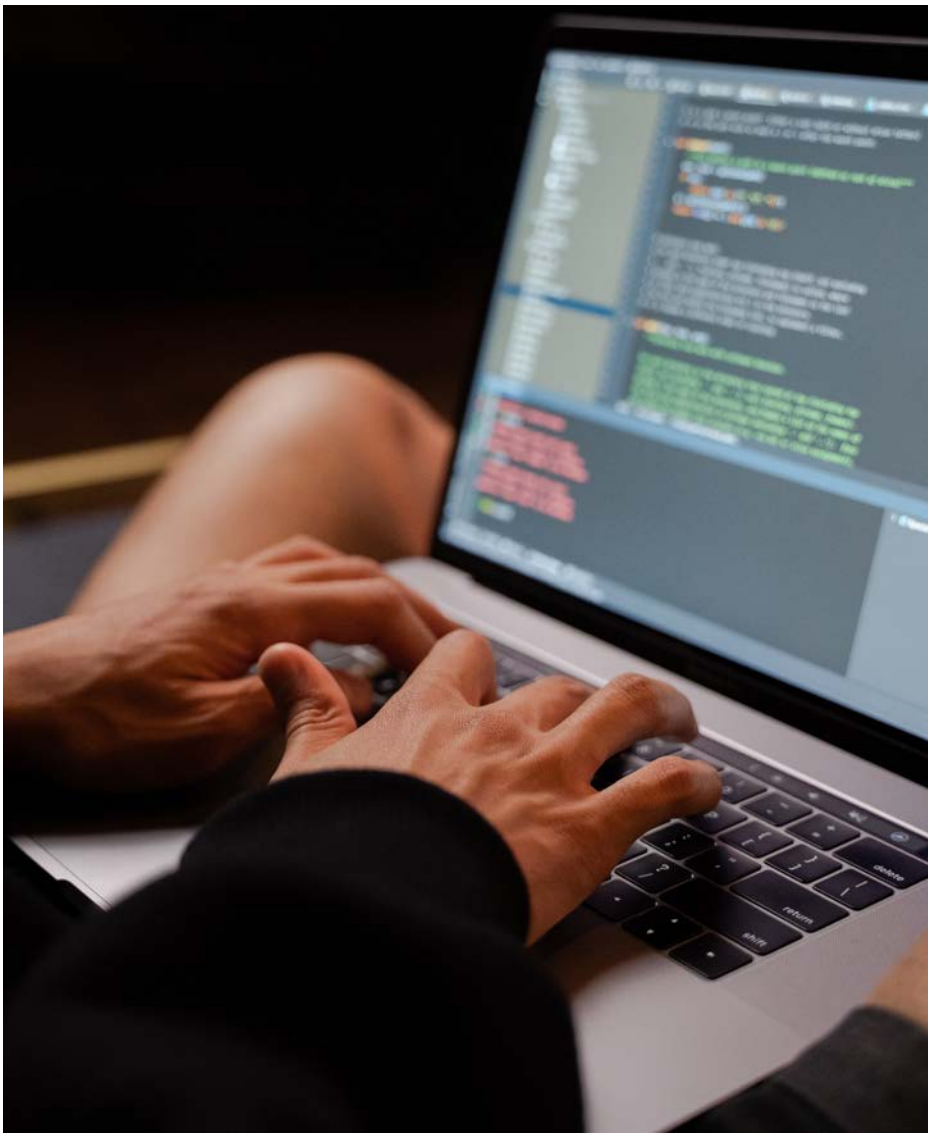
The EU Digital Services Act (DSA) entered into force on 16 November. It was adopted as part of the Digital Services Act Package comprising two EU regulations: Digital Services Act (DSA) and Digital Markets Act (DMA) – a regulation regarding the biggest platforms having a material impact on the functioning of the market and society.

DSA was published in the Official Journal of the European Union on 27 October 2022 and entered into force soon after (16 November). The law will become effective in the entire EUR in February 2024, but the new rules will become binding for the biggest platforms and search engines earlier.

The new EUR Act implements a principle according to which whatever is illegal outside the Internet, should also be illegal on the Internet. The DSA applies to: agency services offering network infrastructure (Internet access providers, domain name registrants); hosting services, such as cloud processing and Internet hosting services; large Internet search engines; online platforms associating sellers and consumers (e-commerce platforms, app stores, sharing economy platforms and social media platforms); big online platforms that can pose particular risk of dissemination of illegal content and cause social damage.

The regulations will oblige digital service providers, among other things, to carry out an obligatory risk assessment, implement risk mitigating measures and ensure transparency of the so-called recommendation systems, i.e. algorithms deciding what is displayed to the users. The new regulating will also entail the obligation of incorporation of provisions regarding respect for freedom of speech and media plurality in terms and conditions as well as guarantee of exercise of the right to anonymous payment for and use of digital services.

The Digital Markets Act lays down new regulations for large online platforms ("gatekeepers"). The DMA will, therefore, apply



only to businesses who annual turnover in the EU is EUR 7.5 billion or whose global market value is EUR 75 billion. The gatekeepers must also have at least 45 million monthly individual end users and 100 000 business users. Furthermore, such businesses must control at least one “core platform service” such as app markets and stores, search engines, social media, cloud computing services, advertising services, voice assistants and Internet browsers.

Under the new regulations, the gatekeepers must: make sure unsubscribing from core platform service subscriptions is as easy as subscribing; ensure interoperability of core functionalities of instant messaging services, i.e. they must enable exchange of text messages, voice messages or files between different messengers for the users; provide business users with access to their data regarding results of marketing or advertising activities on the platform; notify the European Commission of any mergers and acquisitions.

The gatekeepers no longer can: rank their services and products more favourably than similar services and products offered by other market entities (favour their own products or services); preinstall certain applications or software or prevent the users from easy uninstalling such applications or software; require installation of the most common software (e.g. Internet browsers) when installing an operating system; prevent application sellers from use of third-party payment platforms; re-use personal data collected when providing one service for the purpose of another service.

If a large online platform is considered a gatekeeper, it must ensure compliance with the provisions of the Digital Markets Act within six months.

If the gatekeeper breaches these provisions, it can be charged with a fine not exceeding 10% of its total global turnover. In case of a repeated breach, the fine can increase up to 20% of the total global turnover.

In case of systematic non-compliance with the Digital Markets Act, i.e. if the gatekeeper breaches the regulations at least 3 times within 8 years - the European Commission may open a market investigation and, if needed, apply behavioural or structural measures.

No active links in communication with clients of insurance institutions

The Polish Financial Supervision Authority (UKNF) has published a position on activities of insurance and reinsurance institutions in terms of cybersecurity. Among other things, it provides for the obligation to apply the "security first" rule, multi-factor authentication in electronic access channels and avoidance of active links in communication with clients.

As UKNF informs in its position, in their ongoing activities and in relation to planned activities, especially in the area of services involving electronic access channels, the Institutions should consistently apply the paradigm referred to as "security first". It consists in prioritising security and making decisions regarding the form of processes and products based on reliable risk analyses which must factor in not only the issues of of security of the Institution's ICT environment, but also threats connected with use of its services by the clients. Needs for cost or process optimisation, that could be the reason for reorganisation of the method of conducting the business, cannot affect the assumptions and models of those analyses, and their results must be used for effective risk control.

The analyses should cover also the requirements regarding provision of distance services to ensure maximum level of security of funds and data of clients achievable in the given conditions as well as factor in the current threat trends, vectors of attacks on clients, operating method of cybercriminals and potential risks resulting from the activities planned by the Institution, not only in relation to its own clients, but also in the context of potential impact of such activities on the entire sector of financial services.

In particular, the analyses should also regard the Institution's methods of confirmation of identity of clients using electronic access channels. These methods should be selected taking into consideration the risk connected with such channels, especially whether and to what extent application of multifactor verification of identity could contribute to improvement of the level of security of funds and data of clients. This applies also to use of other securing mechanisms, such as verification of the time and place of logging into the electronic access channel and the device from which the user logs in. UKNF is of the opinion that in the light of intensified activity of cybercriminals, lack of strong multifactor authentication of clients is an unacceptable risk. Such client authentication should be applied if the user gains access to information subject to insurance secrecy via remote access channels of the Institution and if the client executes operations connected with insurance product management that could entail financial effects, such as setting of bank account numbers or execution of cash transfers. Resignation from application of multifactor authentication in such cases is admissible only if the Institution, based on conducted analyses, assesses the risk for the client as low.

The supervisory authority is also of the opinion that sending active links to websites in e-mail (including embedding such links in images) and text messages addressed to the clients contravenes the message created and communicated to the clients for years regarding the risk of loss of data and funds, and the Institutions should make effort to limit this practice in favour of static information or information supplied to clients via mobile applications or other electronic channels that do not generate the risk of fraud.

Penalties for aid in money laundering also for employees and notaries public

The Penal Code provides for up to 10 years of prison for participation in the money laundering crime. Judicial practice shows that those persecuted for this crime may include even persons providing legal services, notaries public drafting contracts or preparing land and mortgage register documents.

Those responsible for counteracting money laundering often forget that in addition to the Act on Counteracting Money Laundering and Financing of Terrorism, sanctions for money laundering are provided for also in the Penal Code (Article 299). This provision stipulates penalties for acceptance of money; execution of a transfer or conversion of money; aid in transferring its ownership or possession; taking of other actions that may prevent or significantly hinder determination of its criminal origin or place of depositing. In such a case, the statutory law provides for the penalty of deprivation of freedom from 6 months to 8 years. The penalty of deprivation of freedom provided for in this regulation may be increased to 10 years if the perpetrator acts in agreement with other persons or gains a significant financial advantage from his or her actions (in excess of PLN 200 thousand).

Acceptance of money means not only physical coming in possession, but also booking of a specific amount or preparation of another financial document confirming the transfer in inter-bank settlements. Based on judicial practice, however, it must be noted that the mere fact of issue of a power of attorney or depositing money in a bank account is not an "acceptance" yet. Similarly, mere opening of a bank account and making it available to another person is not treated as an "acceptance".

On the other hand, accepting aid in transfer of ownership of funds is understood very broadly in judicial practice and may apply even to provision of legal services, drafting of a contract by a notary public, preparation of land and mortgage register documents.

It must be emphasised that analysis of judicial practice leads to a conclusion that perpetrators of the offence under Article 299 of the Penal Code are very often attorneys-in-fact or representatives acting on behalf of a legal person or other entities who are holders of the given property rights.

Taking of other actions that may prevent or significantly hinder determination of its criminal origin or place of depositing is a phrase that could let the law enforcement accept other behaviours (actions) as "technically" satisfying the criteria allowing to attribute perpetration of the offence under Article 299 of the Penal Code.

In short:

Two out of three businesses attacked with ransomware have probably paid the ransom

The European Union Agency for Cybersecurity (ENISA) has published its annual report. It concludes that over 10 terabytes of data is stolen monthly by ransomware gangs, and ransomware itself is the most significant threat. The analysis shows that the first step in most ransomware attacks was phishing. According to the report, 60% of ransomware attack victims could have paid the ransom to the criminals. Nearly ¼ of attacks were launched against government administrations and institutions.

EDPB is working on recommendations regarding binding corporate rules

The European Data Protection Board (EDPB) has adopted the "Recommendations on the application for approval and on the elements and principles to be found in Controller Binding Corporate Rules" (BCR-C). The Recommendations contain additional guidelines for controllers and aim at ensuring equal principles of operation for all entities applying for BCR approval. They also align the existing guidelines to the requirements provided for in the judgement of the Court of Justice of the European Union in the Schrems II case. Binding corporate rules are a tool that can be used by enterprises or groups of enterprises in a joint economic activity to transfer personal data outside the European Economic Area to controllers or processors within the same group.

The attack involving infected Python libraries has been on since October

As reported by niebzepiczenik.pl outlet, criminals are trying to infect programmers' computers with the W4SP Stealer Trojan horse. Since mid-October, someone has been regularly trying

to infect Python programmers this way. For this purpose, various libraries have been cloned and a malicious command has been added to them. The libraries are made available under slightly changed names (usually one letter is changed in the name).

Reporting personal data protection breaches by the courts may be required

The Personal Data Protection Office (UODO) has prepared the publication entitled "Processing of personal data by courts in the context of reporting of personal data protection breaches" in response to the question whether the President of UODO is the authority proper to receive reports of personal data protection breaches and audit on case of courts – and if so, to what extent. The publication informs that, in principle, the rules of GDPR apply to the activities of courts and other justice system authorities in the scope of reporting of personal data protection breaches referred to in Article 33 of GDPR. Therefore, in case of any incident, the controller (e.g. a court) is obliged to assess whether the given incident is a breach of personal data protection and if so – whether the breach regarded processing of data by the courts in performance of justice system tasks or not.

Polish Post (Poczta Polska) warns against a phishing campaign

The CERT Poczta Polska appointed to respond to online security breach incidents warns against a new phishing campaign involving use of the brand of the state postal operator. The fraud consists in extorting personal data and payment card data. The content of misleading communications published on social media include a false information regarding alleged resale of packages not collected by the clients of Poczta Polska. Poczta Polska does not resell uncollected packages and never asks for any additional fees for the package via text messages or electronic mail.

Data of 2.6 million Polish WhatsApp users for sale

Data of 487 million WhatsApp users have been put on sale on one of hackers' forums. The victims include 2.6 million Poles. The data offered by cybercriminals are phone numbers. Most of them are valid. The matter was brought to light by Cybernews outlet - they asked the hackers advertising themselves on one of the forums for a sample of data sold by them. The editors confirmed authenticity of the phone numbers in the sample and their connection with WhatsApp contacts.

Order of the US president on data transfer from the EU

On 7 October, the US president issued the executive order regarding implementation of the announced EU-US data privacy agreement in the US law. The order aligns the US law with the requirements of the requirements of the Court of Justice of the European Union presented in the so-called Schrems II judgement, adapting, among other things, the broad access to data in the context of national security as well as the complaint and appeal procedures

Data of European TikTok users will be available more broadly

TikTok is changing its privacy policy – the data of European users are to be available to application employees around the world – users who wish to log into the application, will have to agree to remote access to their personal data by service employees all over the world. Access will be granted to Brazil, Canada, China, Israel, Japan, Malaysia, Philippines, Singapore, South Korea and USA. Information has also popped up that Chinese Internet companies, such as TikTok, WeChat, or AliExpress, have made algorithm-related data available to the Chinese authorities.

**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**