ALERT SAFE COMPANY

No. 8/2022

Ladies and Gentlemen,

Here is the August issue of our "Secure Company" alert, in which we discuss the most current and interesting information on counteracting money laundering and terrorist financing (AML), as well as on cybersecurity and personal data protection.
Our alert is focused primarily on topics relating to cybersecurity and personal data protection. We want to draw your attention to two issues relating to the processing of data by financial institutions. The first relates to the right to make photocopies of identification documents. The second, to the inability to continue to process the data of a borrower when no credit agreement was concluded.
The remaining extensively discussed points relate to new regulations: EU regulation on digital markets, and the planned Polish law on counteracting electronic communication abuses to make it easier to fight so-called spoofing.
We also include the most interesting, shorter cybersecurity related information.
We hope that the information presented in the alert will be useful and will make it easier to navigate cybersecurity, personal data and AML regulations and legislative trends.
Should you need more or more detailed information, please don't hesitate to contact our company and experts.

DR ANDRÉ HELIN, BDO Managing Partner

Banks not always allowed to photocopy client ID

Banks are not always allowed to photocopy client ID cards. According to the Office for Personal Data Protection (UODO), it is only permissible when it is necessary to apply security measures to prevent money laundering and terrorist financing.

According to information from the middle of August 2022, the UODO continues to be of the opinion that the copying of personal ID cards by financial institutions is legal only if it is necessary to apply security measures aimed at preventing money laundering and terrorist financing.

In accordance with Article 112b of the Banking Law, banks are allowed to process the information contained in the identification documents of natural persons for the purposes of their banking activities. This only means that the regulation grants them the right to process all of the personal data contained in the identity documents of their clients. It does not, however, permit them to make copies of those documents. In most cases it is enough to only present an identity document for inspection.

Whereas in accordance with the provisions of the Act on counteracting money laundering and terrorist financing, obligated institutions, including banks, but also investment funds, businesses that conduct currency exchange activities as defined in the Foreign Exchange Law, or notaries with respect to specific activities performed in the form of a notarial deed, have a right to photocopy identity documents for the purposes of applying financial security measures. Before applying financial security measures they must assess the risk of money laundering and terrorist financing. At the same time, the regulations clarify when obligated institutions apply financial security measures.

As controllers, financial institutions are required to comply with the provisions of the General Data Protection Regulation (GDPR). This means that before applying financial security measures they must determine if for these purposes it is necessary for them to process the personal data contained in a copy of an identity document. This is because in accordance with the principles of purpose limitation and data minimization referred to in Article 5 of the GDPR, personal data must be collected for specific, explicit and legitimate purposes, as well as adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

BIK must delete the data of would-be borrower if no agreement was concluded

Regulations do not allow for the processing of personal data after credit worthiness is assessed and risk analysis performed, in a situation where no obligation relationship arising from the conclusion of a credit agreement was formed.

The President of the UODO ordered SKOK and BIK to delete the personal data obtained in order to assess credit worthiness and analyze risk. The authority determined that the premise legalizing the continued processing of the data was no longer present, as no credit agreement was concluded. The President of the UODO stressed that under the provisions of the Banking Law, the processing of the personal data in question is possible in two situations: when performing a risk analysis and credit worthiness assessment (before concluding a credit agreement), as well as during the term and after the expiration of the credit agreement (for a period specified by law). The regulations do not, however, allow for the processing of personal data after the credit check and risk analysis are completed in a situation when no obligation relationship arising from the conclusion of a credit agreement was formed. Therefore, after the completion of the analysis and assessment, in the absence of a credit agreement, the premise legalizing the processing of the data in question is no longer present.

The matter was reviewed by a Voivodship Administrative Court (case file II SA/Wa 1128/21), which agreed with the UODO.

The Court did not agree with the argument raised in the complaint that BIK would process the data in order to build scoring models. Credit scoring is a method used to assess the credibility of an entity applying for a bank loan. It consists of determining a client's credit worthiness based on comparing his profile with the profiles of clients who have already obtained loans and are repaying them. After applying for a credit, the person demanding the deletion of data did not conclude a credit agreement with SKOK. Thus – as stressed by the Court – to cite scoring has no factual basis in this case. Binding regulations do not allow for the processing of data after credit worthiness is assessed and risk analysis performed in a situation when no obligation relationship resulting from the conclusion of a credit agreement was established. Therefore, after the completion of the analysis and assessment, as no credit agreement was concluded, the premise legalizing the processing of the data in question is no longer present. This means that the President of the UODO was justified in ordering the deletion of data that SKOK and BIK had no legal basis to process.

There will be a law on counteracting abuses in electronic communications

The proposed Act on counteracting abuses in electronic communications provides for the monitoring of electronic communications, introduction of a smishing message model, creation of a list of Internet domains used to defraud user data and funds, and a list of numbers used exclusively to receive voice calls.

The draft bill focuses primarily on counteracting so-called spoofing, i.e. stealing data (e.g. credit card information), or infecting phones with appropriately fabricated text messages, as well as on eliminating so-called Caller ID spoofing, i.e. changing the ID of the caller to one that is trusted or recognizable to the recipient in order to induce him to act in a certain way.

Once passed, the act will introduce the legal definitions of such terms as "electronic communication", "electronic mail", "voice call" or "interpersonal communications service". More importantly, however, it will also define "abuses in electronic communications". Considered to be such abuses will be the provision of a telecommunications service or use of telecommunications devices inconsistently with their designation or legal regulations, for the purpose or with the effect of causing harm to a communications business or end user, or for obtaining undue gains.

According to the bill, telecommunications companies will be required to block text messages with content consistent with the message model provided by CSIRT NASK, which in turn will be tasked with launching (within three months of the new act's effective date) a system that will provide the models of such messages. The system will connect operators, as well as the Chief of Police and the President of the Office of Electronic Communications.

Objections to treating a message as abuse and entering it in the system operated by CSIRT-NASK will be reviewed by the President of UKE. He will also impose administrative fines for such abuses.

The draft bill on counteracting abuses in electronic communications was published on 15 June 2022 on the website of the Government Legislative Center (UD402). It has already undergone inter-ministerial and public consultations and is currently being reviewed.

EU regulations on digital markets will soon go into effect

On 18 July 2022 the Council of the EU approved new rules for fair competition on the Internet (the so-called Digital Markets Act – DMA). The Digital Markets Act ensures a digital level playing field that establishes clear rights and rules for large online platforms ('gatekeepers') and makes sure that none of them abuses their position.

The Digital Markets Act establishes new rules for large online platforms ("gatekeepers"). Thus the scope of the DMA will only cover entities whose annual turnover in the EU amounts to €7.5 billion, or whose global market value amounts to €75 billion. Gatekeepers must also have at least 45 million monthly individual end users and 100 000 business users. Moreover, they must control at least one "core platform service", such as market places and app stores, search engines, social networks, cloud services, advertising services, voice assistants and web browsers.

Under the new regulations gatekeepers have to: ensure that unsubscribing from core platform services is just as easy as subscribing; ensure that the basic functionalities of instant messaging services are interoperable, i.e. enable users to exchange messages, send voice messages or files across messaging apps; give business users access to their marketing or advertising performance data on the platform; inform the European Commission of their acquisitions and mergers.

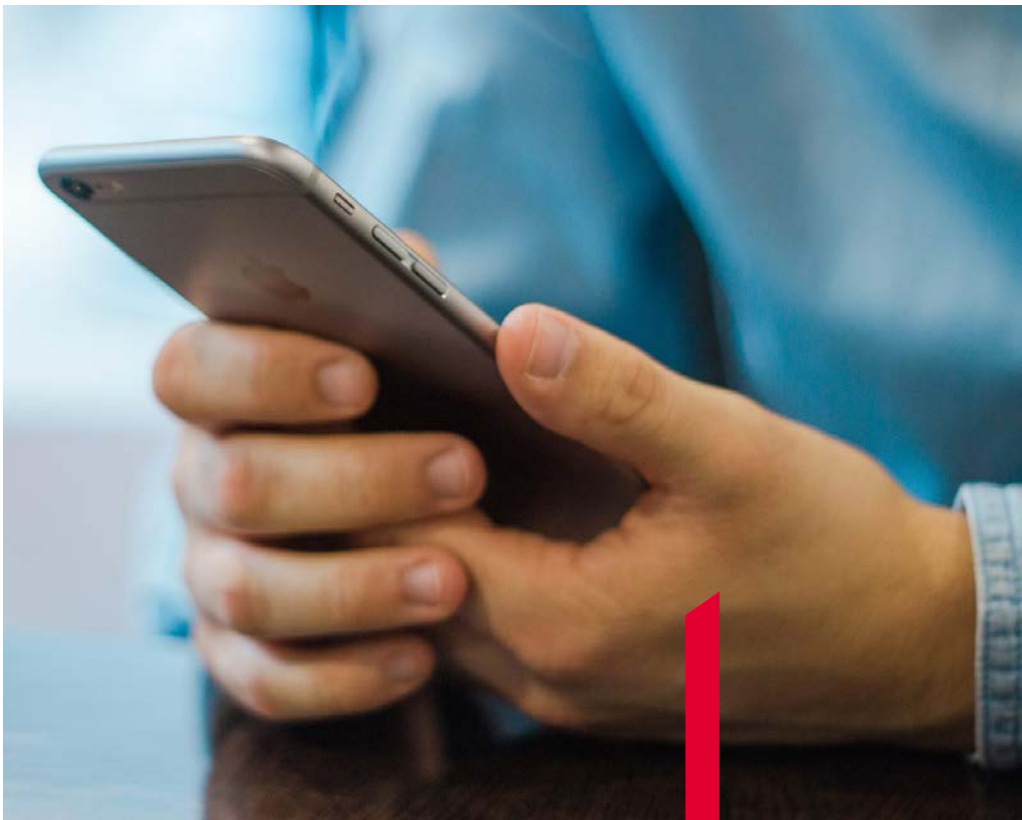
Gatekeepers can no longer: rank their own products or services higher than those of others (self-preferencing); pre-install certain apps or software, or prevent users from easily un-installing these apps or software; require the most important software (e.g. web browsers) to be installed by default when installing an operating system; prevent developers from using third-party payment platforms for app sales; reuse private data collected during a service for the purposes of another service.

If a large online platform is identified as a gatekeeper, it will have to comply with the rules of the DMA within six months.

If a gatekeeper violates the rules laid down in the DMA, it risks a fine of up to 10% of its total worldwide turnover. For a repeat offence, a fine of up to 20% of its worldwide turnover may be imposed.

If a gatekeeper systematically fails to comply with the DMA, i.e. it violates the rules at least three times in eight years, the European Commission can open a market investigation and, if necessary, impose behavioral or structural remedies.

The provisional agreement on the DSA that was reached by the Council and the European Parliament on 23 April 2022 and adopted in European Parliament on 5 July was to be adopted by the Council in September 2022. On 18 July the Council approved the position of the European Parliament, which means that the act has been adopted. The new regulations will go into effect six months after their publication in the Official Journal of the European Union.



In short:

New tracker-free e-mail

DuckDuckGo has released a new e-mail service that may be used to avoid spam sent by companies, as well as unwanted online marketing. This free e-mail is in fact a service that forwards messages to the user's primary e-mail address. The forwarded messages are, however, free of all trackers. It is therefore not possible to track the recipients of promotional newsletters and other marketing mailings for the purposes of targeted advertising or to collect their personal data. The service removes all trackers, including those in links, changes the unencrypted http protocol to https, and allows e-mails to be answered from an address in the duck.com domain.

Samsung phones with Internal Security Agency (ABW) certificate

Samsung has been granted a cryptographic protection certificate covering selected Samsung Knox security mechanisms. This was done as part of a process conducted by the Internal Security Agency. Certification was conducted within the Cybersecurity Cooperation Program (PWCyber), which is a public-private partnership initiative implemented by the Chancellery of the Prime Minister (formerly Ministry of Digitization) for the National Cyber Security System.

New provisions on digital signatures criticized by the industry

Association Digital Poland has notified the Chancellery of the Prime Minister of its position on the government's plans to amend the Civil Code with respect to the use of electronic signatures. It is the Association's opinion that the planned provisions stating that in civil law relationships, from a security standpoint, it seems sufficient to perform a verification at a level required for an advanced electronic signature, is a concept that downgrades and lowers standards and requirements, and does so at such a special time when the proposed EU regulation eIDAS2 tightens identification requirements.

NASK to publish a scientific yearbook on cybersecurity

The issues of cybersecurity and of Internet governance in public spaces are being addressed by a new English-language academic journal, Applied Cybersecurity & Internet Governance, published by the National Research Institute NASK. The call for articles for the first issue has just begun. Among the topics that NASK PIB, as publisher, would like to cover in the journal are: network and critical infrastructure security, the potential of the Internet of Things (IoT), the development of artificial intelligence (AI), digital infrastructure, the fight against cybercrime, cybersecurity education, the legal aspects of information security.

As many as 64 percent of companies believe they were the target of foreign cyber attacks

Two-thirds of companies have modified their cybersecurity strategies in the wake of the war in Ukraine and 64 percent of companies believe that they were targeted by cybercriminals sponsored by foreign states – indicates a report by Venafi. 66 percent of surveyed entities have modified their cybersecurity strategies as a result of the war in Ukraine. Every CEO and

every board member must realize that cybersecurity is one of the most important business risks faced by businesses today, regardless of industry – the report said.

Municipality cannot share information about water usage

A water utility cannot provide a municipality with information on the amount of water a resident has used, even if the resident is suspected of not paying for sewage, the Office for Personal Data Protection has said. The UODO has reiterated that in accordance with the Act on maintaining cleanliness and order in municipalities, it is up to the mayor to control the possession of contracts and evidence of payments for services consisting of the disposal of municipal waste and liquid waste collected on a property, or to otherwise document the performance of these obligations.

LinkedIn account management made easier

Business Manager is a new LinkedIn platform.
Its purpose is to make it easier for users to manage several accounts from a single dashboard.

In addition, Business Manager enables users to manage permissions and accesses, with a centralized listing of all connected profiles and users. Its users will also be able to share data about matched recipients across ad accounts. This will provide a streamlined way to utilize custom audiences and related info across profiles.

Thousands of apps can take control of Twitter accounts

More than 3200 applications have errors that allow Twitter's programming interface keys (API) to leak (in this case it is Consumer Key and Consumer Secret). In some cases this makes it possible to take over user accounts, if they were previously linked to the flawed software. The software errors were reported by the cybersecurity company CloudSEK.

Remote work in the Labor Code: occupational health and safety, personal data protection

According to the proposed bill, work may be performed at any location indicated by the employee and approved by the employer. This will, however, require the fulfillment of a greater number of formalities. The employer will be required to prepare an occupational risk assessment for remote work and health and safety information for employees. Another document to be prepared will be procedures for the protection of personal data during remote work.

New security vulnerabilities in Apple products

Apple has disclosed serious security vulnerabilities in iPhones, iPads and Macs, which can potentially allow attackers to take total control of those devices. Security experts have advised users to update the vulnerable devices – iPhone6S and later models; several iPad models, including generation 5 and later, all iPad Pro and iPad Air2 models, as well as Mac computers running MacOS Monterey.

PayPal has joined the TRUST network focused on AML for cryptocurrencies

PayPal has joined Travel Rule Universal Solution Technology (TRUST).
It is a group of companies building a system of counteracting money laundering (AML) for transactions performed in cryptocurrencies. The announcement was made after the American company introduced an infrastructure that allows its users to send and receive crypto assets between the company's own application and external portfolios and exchanges. PayPal has joined TRUST to increase the compliance of its activities with regulations on digital assets.

Malicious software from China in App Store

Several malicious apps that exploit vulnerabilities present in Mac Book computers have found their way to the App Store. They make it possible to take complete control of the infected devices. The fake Mac Book apps found in the App Store are: PDF Reader for Adobe PDF Files – Sunnet Technology; Word Writer Pro – TeamIdentifier; Screen Recorder – TeamIdentifier; Webcam Expert – TeamIdentifier; Streaming Browser Video player – TeamIdentifier; PDF Editor for Adobe Files – TeamIdentifier; PDF Reader – TeamIdentifier.

**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**