ALERT SAFE COMPANY

BDO

No. 2/2021

Ladies and Gentlemen,

Here is the February issue of our "Secure Company" alert. In it you will find information on regulations on counteracting money laundering and terrorist financing (AML), as well as interesting GDPR and cyber security related news.
We would like to draw your attention to the new Financial Information System Act, which is to allow government organs to gain quick access to information about any bank accounts, both active and those that have already been closed.
Also noteworthy are the decisions issued by the President of the Office for the Protection of Personal Data (UODO) on broadly defined liability for breaching GDPR. This time the decision relates to liability when a breach occurred as a result of a controller not having updated software. The decision is important because many companies do not pay much attention to updating their software to newer versions.
As it turns out, using software that is no longer supported and updated by the manufacturer could be quite expensive.
You should also take note of the information on changes in the approach to the structuring of passwords in a way that will improve information security.
We wish you a pleasant read, and should you require more or more detailed information, please don't hesitate to contact our company and experts.

DR ANDRÉ HELIN, Prezes BDO

You can be fined by UODO for using outdated software

The Office for the Protection of Personal Data (UODO) issued a reprimand to a company after the controller lost access to personal data as a result of a malicious ransomware attack.

The UODO's proceeding showed that the data controller chose ineffective security measures for their information systems. In addition, the controller failed to perform tests of their sensitivity to various types of threats. The company only tested the efficiency of the software components, i.e. their tolerance of various types of breakdowns. In the UODO's opinion, the company did not fully check the technical and organizational security measures of the systems used to process personal data.

The controller had outdated operating systems and other software that had not been updated, as the manufacturers no longer offered technical support. As a result, the software was not updated for, among others, security measures.

The UODO has stressed that had the security been properly tested, the controller would have found it necessary to install updated operating systems and software supported and updated by manufacturers. This would have allowed the controller to minimize the risk of breaches.

As shown by the said case, having updated software is necessary to ensure proper protection of personal data by the data controller. Using software that is outdated and lacking manufacturer support is a circumstance that weighs on the controller when personal data protection turns out to be ineffective.

The relatively low penalty imposed on the company (controller) was the result of the fact that the data breach did not result in a loss for the data subjects and that immediately after its discovery the company replaced the outdated software, i.e. that the controller took immediate remedial action.

Minister of finance will create a new system to collect account data

A draft of a new bill on the Financial Information System (paper U66) has been submitted for public consultations. It is meant to supplement the AML system in Poland. It would allow the government organs, including the tax authorities, quicker access to citizens' accounts, including those that have been closed.

The new Financial Information System (SInF) would be used to help counteract money laundering and the terrorist financing; detect serious crimes or aid in serious criminal proceedings, as well as help identify, detect or secure assets originating from such crimes; and for other purposes specified in the act.

The Ministry of Finance has stressed that currently no regulations are in place that would make it possible to quickly and effectively obtain information about accounts kept for persons and entities involved in serious criminal activities. To obtain full information, public organs must conduct time consuming and costly activities, which include having to correspond with numerous financial market institutions or having to use paid commercial solutions, such as central account information kept by KIR S.A. For this reason, to make their operation easier and faster, the ministry wants to create the Financial Information System (SInF).

The central registers or central electronic search systems operating as part of SInF are to enable timely identification of any natural or legal person holding or controlling a payment or bank account identified via IBAN.

SInF would collect, process and share information on open and closed accounts, including bank accounts, savings and credit union (SKOK) accounts, payment accounts with other institutions, securities accounts along with the summary accounts used to service them. The system would also include data on safe deposit box agreements.

In the reasons for the proposed bill the ministry explains that the planned register will not be used to collect information on financial transactions or the amounts held in accounts or other products. To obtain such data it will still be necessary — as is the case now — for the public organs to direct a request to the relevant institution where the given account or product is kept. SInF will only make it possible — in specified cases — to efficiently locate an account or another product used to collect, store or invest funds belonging to a given person or entity, and will not provide the ability to obtain information about the assets held or transactions performed therein.

Institutions obligated to provide information to the system will include those institutions that provide the products and services that make it possible to collect, store and invest funds.

Information from SInF will be used for the purposes of performing the statutory tasks of courts, prosecutors, appropriate services: the Police, the Central Anti-Corruption Bureau, the Internal Security Agency, the Military Counterintelligence Service, the Foreign Intelligence Agency, the Military Intelligence Service, the Military Police, the Border Guard, the General Inspector of Financial Information and the National Tax Administration.

From 3 months to even 10 years in jail for violations associated with money laundering

As many as 10 years in jail is the punishment for anyone who helps hide illegally obtained funds, also in situations of failure to report a transaction despite being required to do so, or receipt of funds from an illegal source, even though there was a reasonable suspicion that they could have come from such a source.

In the previous issues of our alert we described the amendments to the Act on counteracting money laundering, which have been sent to the Sejm and await consideration. This time we want to remind you that matters associated with penalties for violating AML provisions (on money laundering) are also regulated by the Criminal Code. Such penalties are set out in Article 299 of the Criminal Code.

Punished first are actions relating to aiding in the concealment of proceeds from criminal activities.

Subject to punishment is anyone who accepts, holds, uses, transfers or exports, conceals, converts, aids in the transfer of ownership or possession, or performs other actions that may prevent or make it significantly more difficult to determine the criminal origins or location, or to detect, seize or confiscate money, financial instruments, securities, foreign exchange, property rights or other movable or immovable assets, originating from a prohibited act.

What is more, subject to the same punishment are the employees of a financial institution. The Criminal Code provides that such punishment may be imposed on a person who is an employee or acts on behalf of or for a bank, financial or credit institution, or another entity required by law to register transactions and persons who perform transactions, who contrary to the law accepts money, financial instruments, securities, foreign exchange, transfers or converts them, or accepts them in other circumstances that give rise to a reasonable suspicion that they are the subject of a prohibited act, or who provides other services that are meant to conceal their criminal origins or protect them from seizure.

The extent of liability is therefore relatively broad.

In both cases, the maximum penalty is 8 years in prison. However, the court may not sentence such a person to less than 6 months of imprisonment.

If the above described actions are conducted in collusion with another person, or the person who commits the crime achieves a significant financial gain, the punishment increases. This is because a court cannot impose a sentence that is lower than one year and longer than 10 years in prison.

What is more, the Criminal Code provides that the mere preparations to commit the described crimes may result in a sentence of as many as 3 years of imprisonment.

Punishment may be avoided if the perpetrator voluntarily confesses to the crime. This is because the criminal regulations provide that no punishment is imposed on whoever voluntarily discloses to a law enforcement organ information on persons taking part in the commission of a crime and the circumstances of its commission, if this prevented the commission of another crime. If, however, the perpetrator only made efforts to disclose such information and circumstances, the court shall apply an extraordinary mitigation of punishment.

Passwords should be long, but instead do not need to be constantly updated

Passwords to computers and systems should be long, but easy to remember. There is also no need to change them regularly. They should only be changed if there is an indication of a break-in.

The guidelines on security policies for passwords used in IT systems are changing. Until now it was recommend for the passwords to be made up of numerous characters, including special characters and numbers, and to be completely changed on a regular basis.

The recommendations issued in 2003 clearly stated that: to optimize the level of security, passwords must be reset and changed every 90 days, contain a combination of small and capital letters, numbers and a special character". At many companies it is also not possible to choose a password out of a pull of those recently used in previous months. This of course makes it difficult to remember the passwords and is a real nightmare for users. As it now turns out, completely unnecessarily.

Whereas the new security expert recommendations state that passwords should be long, but easy to remember, and that they should be changed when there is an indication of a break-in. There is no need to change them regularly. It turns out that in reality, cyclical password changes instead of increasing, actually decreased security. All because users continued to use similar passwords anyway, with one additional character often being the only difference.

Back in 2011 it had already been calculated that a password made up of four random words ("correct horse battery staple"), without special characters, would take computers around 550 years to decipher. In comparison, a password created using the old methods on a word could be broken in a few days. This is because it is not the characters used in the password, but the length of the password that matters the most.

It is therefore now recommended that passwords be long, made up of many words (within the limit imposed by the system) and it would be best if it rhymed, as this makes it easier to remember. The words should, however, be random, and not be a quote from a favorite poem. Experts also recommend for passwords to contain a special character, but preferably not an exclamation point at the end of a sentence.

In short

EDPB holding consultations on data protection guidelines

The European Data Protection Board (EDPB) is waiting until 2 March 2021 for comments on the Guidelines 01/2021 on examples regarding data breach notification. The guidelines contain a list of the most common cases of data breaches, such as: ransomware attacks; attacks consisting of data exfiltration and instances of lost or stolen devices and paper documents – prepared based on the experiences of supervisory organs.

EU has adopted opinions on standard contractual clauses

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have adopted joint opinions on two sets of standard contractual clauses: an opinion on standard contractual clauses between controllers and processors, and an opinion on standard contractual clauses for data transfers to third countries. The standard controller-processor clauses will apply throughout the EU and are meant to ensure full harmonization and certainty of EU law with regard to contracts between data controllers and processors.

KNF warns against fake bank applications

The Polish Financial Supervision Authority has warned users against a fake application that impersonates IKO, PKO BP's mobile app. The Computer Security Incident Response Team (CSIRT) of the Polish financial sector, operating at the KNF, has warned on its Twitter profile that the fake application contains the Alien malware used to steal online banking passwords.

EDPB on the law enforcement directive and privacy policy

During its 45th plenary session (2 February 2021) the EDPB adopted: recommendations on Article 36 of the law enforcement directive on the adequacy of protection, an opinion on H3C/PCAOB administrative arrangements, a statement on the new draft of the second additional protocol to the Convention on Cybercrime, a response to the EC questionnaire on the processing of personal data for scientific research, as well as discussed WhatsApp's new privacy policy.

Victims of trading system failures entitled to damage compensation

Clients of brokerage houses may be affected by trading system failures that prevent them from placing orders at prices quoted at a given moment. The President of the Office of Competition and Consumer Protection (UOKiK) has initiated a proceeding to determine whether brokerage houses unjustifiably exclude their liability for the consequences of such failures, and how they handle complaints from customers affected in such situations. If a consumer suffers damage related to a failure of a brokerage house trading system, he/she should first contact that financial institution and file a complaint.

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 2019:

- **1st place The Best Tax Advisor in the category of medium-sized companies**
- **3rd place for tax projects implementation**

The 2019 rankings prepared by the Rzeczpospolita and Parkiet dailies:

- **Best Audit Firm** (5th place);
- **Firm Most Active on the Stock Exchange** (5th place)

BDO spółka z ograniczoną odpowiedzialnością sp.k., ul. Postępu 12, 02-676 Warszawa;
tel.: +48 22 543 1600, fax: +48 22 543 1601, e-mail: office@bdo.pl