ALERT SAFE COMPANY

BDO

No. 11/12
2021

Ladies and Gentlemen,

Here is the last issue of our "Safe Company" Alert for 2021, containing information about counteracting money laundering and terrorist financing (AML), as well as on cybersecurity and personal data protection.
We want to draw your attention to an interesting position by the UODO on the requirement to report breaches of personal data.
It indicates that information about such breaches must be given irrespective of whether as a result the data subject incurred an actual loss or not.
In the area of counteracting money laundering and terrorist financing (AML), we discuss the provisions of the Criminal Code that permit the punishment of not only direct perpetrators, but also their legal advisors.
We would also like to direct your attention to cybersecurity related matters. Recent months have brought increasingly concerning information about all types of threats.
We hope that another portion of information in our alert will be useful and will make it easier to navigate regulations and legislative trends, both Polish and European, as well as allow you to strengthen cybersecurity.
Should you need more or more detailed information, please don't hesitate to contact our company and experts.

DR. ANDRÉ HELIN, BDO Managing Partner

Personal data breaches must be reported even if there is no loss

Requirement to notify an individual of his personal data being breached is not conditioned on negative consequences for that individual, but on the very potential for their occurrence – reminds the UODO.

The UODO (the Office for the Protection of Personal Data) recently considered a matter where a courier service lost a shipment containing personal data, such as: first name, last name, PESEL number, residence address, bank account numbers, identification numbers assigned to bank clients. Although the bank notified the clients, but – as found by the UODO – the information was not sufficient – it did not comply with the requirements of the GDPR. The bank had also decided that since the risk of negative consequences to those affected was medium, it would not report this breach to the supervisory authority and thus did not completely fulfill the requirement to notify the affected data subjects.

As a result, the UODO has reiterated that it must be notified of those incidents where there is a likelihood (higher than small) of a damaging (unfavorable) impact on the rights or freedoms of the data subjects. When that risk is high, the breach has to also be reported to the data subjects. Such risks include: theft or identify forgery, financial losses, damage to good name. The wide scope of the data contained in the said correspondence may expose the data subjects to such consequences.

From the standpoint of the GDPR, given the potential for a damaging impact on the rights or freedoms of the data subjects, it does not matter if an unauthorized recipient did in fact acquire and familiarize himself with the data. What matters is that such a risk occurred. Of significance is also the matter of the scope of personal data affected by the breach, i.e. not just the first and last names, but also the PESEL numbers, which should be protected.

EDPD has published guidelines on international transfers of data

Adoption of guidelines on the interplay of Article 3 and Chapter V of GDPR – was one of the main decisions made by the European Data Protection Board during its 57th plenary session held on 18 November 2021. The document contains explanations to be used to ensure a common understanding of the concept of international data transfers.

The newest Guidelines 05/2021 issued by the EDPD (the European Data Protection Board) contain a clarification of the interplay between the territorial scope of application of the GDPR (Article 3) and the provisions on international data transfers contained in Chapter V. The Guidelines are meant to assist controllers and processors in the EU in identifying whether a processing operation constitutes an international data transfer.

The Guidelines specify three cumulative criteria that qualify processing as a transfer: firstly, the data exporter (controller or processor) is subject to the GDPR for the given processing; secondly, the data exporter transmits or makes available the personal data to the data importer (another controller, joint controller or processor); thirdly, the data importer is in a third country or is an international organization.

The processing will be considered a transfer, regardless of whether the importer established in a third country is already subject to the GDPR under Article 3. However, the EDPB considers that collection of data directly from data subjects in the EU at their own initiative does not constitute a transfer.

The Guidelines will be subject to public consultation until the end of January 2022.

Aiding in money laundering punishable also for lawyers and notaries

The Criminal Code provides for up to 10 years in prison for taking part in money laundering. Past court rulings indicate that even those who provide legal services or prepare contracts and land and mortgage register documents are subject to punishment for the crime.

Those obligated to counteract money laundering often forget that in addition to the provisions of the Act on counteracting money laundering and terrorist financing, penalties for money laundering are also provided for in the Criminal Code (Article 299). The article provides for penalties for receiving money; transferring or converting money; assisting in transferring its ownership or holding; other actions that may prevent or significantly hinder the ability to determine its criminal origins or location. In such cases the Code calls for imprisonment of 6 months to 8 years. It may be raised to 10 years in cases, when the perpetrator acted jointly with others, or obtained significant financial gain (of more than PLN 200 thousand) from his actions.

Receiving money should not be understood to only mean taking its physical possession, but also to book an amount or to prepare a financial document confirming an interbank transfer. Based on existing rulings it should, however, be noted that the issue of a power of attorney or payment to a bank account are not in themselves considered "receiving". Similarly, opening a bank account and making it available to another persons is not treated as "receiving".

Whereas the concept of assistance with transferring the ownership of money is very widely defined and may even pertain to legal services, a notary's preparation of a contract or documents from a land and mortgage register.

Importantly, an analysis of past rulings leads to the conclusion that very often considered to be the perpetrators of crimes from Article 299 of the Code are attorneys-in-fact or representatives acting on behalf of a legal person or other entities with specified property rights.

Other actions that may prevent or significantly hinder the ability to determine the criminal origins or location of money is a provision the enforcement organs can use against other behaviors (actions) that, in their opinion, fulfill the premises for attributing the perpetration of a crime from Article 299 of the Criminal Code.

Court websites with a short cybersecurity guide

Under binding regulations, cybersecurity is IT system resilience to actions that compromise confidentiality, integrity, availability and authenticity of processed data or related services they offer.

Advice on broadly defined cybersecurity has been published on the websites of Polish courts. The need to publish such information arises out of the Act of 5 July 2018 on the national cybersecurity system (2018 Journal of Laws, item 1560). In accordance with binding regulations, cybersecurity is "the resilience of IT systems to actions that compromise the confidentiality, integrity, availability and authenticity of the data they process or the related services they offer".

The guide lists the following as the most common threats in cyber space: malware attacks; identity theft; attacks meant to extort or damage data; blocking of access to services; unwanted e-mails (SPAM); social engineering; phishing.

To protect against such threats, the guide recommends: using updated anti-virus software (with real-time protection and automatic updates turned on); scanning all devices connected to the computer (pen drives, discs, memory cards, etc.) with anti-virus software; updating operating systems and software; not opening files of unknown origin; scanning all downloaded files with anti-virus software; not using bank, e-mail sites without a valid security certificate; periodic computer scanning with anti-virus software and checking of network processes; not visiting sites that offer free films, music or easy money (such sites often contain malware); not providing personal data on websites with respect to which there is no certainty that they are not visible to third parties; continued verification of e-mail sender addresses; password protection or encryption of e-mails containing confidential data (passwords should be provided using another form of communication); periodic backing up of important data; permanent firewall activation; paying attention to messages displayed on the computer screen.

In short:

Collecting consents using pop-ups violates GDPR

Pop-ups violate the GDPR – is the position of the Belgian personal data protection authority. In its opinion, this form of forcing users to be followed for the purposes of personalized advertising violates the provisions of the European data protection and privacy law. Once the Belgian authority's decision is confirmed, according to the GDPR's one-stop shop mechanism it will be sent to the relevant authorities in Poland and the Netherlands, where the entities complaining about IAB are based. The domestic authorities will have to prepare their positions within a month.

Representatives incorrectly notify of appointing data protection officers

The UODO reminds that the appointment (change in data or dismissal) of a data protection officer or his deputy may be reported by controllers (processors) via a representative. However, for the notification to be effective, the representative must remember to meet the conditions relating to electronic form of notification and electronic form of authorization, as well as to send stamp duty.

PESEL should not be IT system login

In its November newsletter the UODO reminds that the PESEL number should not be used as a login to an IT system or portal. Although the position of the Polish personal data protection authority on the use of PESEL numbers as logins to IT systems or portals has remained unchanged, such concerning solutions still continue to be used.

Facebook has circumvented security protections regarding data collection warning

Researchers are urging Apple users to remove not only Facebook, but also Instagram and WhatsApp from their devices. They say that despite efforts, those applications can still get users' private information, including location and IP address.

Facebook is said to be bypassing Apple's security measure that displays a warning for users with information about what data and for what purpose are collected by the application.

Digital water marks to be used to authenticate information on the Internet

Scientists from Japan, Poland and Spain are working on a tool that will help fight fake news. It will be detectable using digital water marks. A project entitled Detection of fake newS on Social Media pLAtfoRms (DISSIMILAR) is to result in a social media tool that will automatically check the credibility of information. It is to be based on algorithms of digital water marking of multimedia content, as well as on machine learning. The water marks are to be inaudible and invisible.

Apple sues NSO Group, creators of the infamous Pegasus

In a special announcement Apple has informed that it has filed a lawsuit against NSO Group, i.e. the creators of Pegasus in connection with the fact that it attacks Apple devices. Pegasus is a software used by governments to spy on their citizens, which attacks mobile devices, including iPhones, and lets the attacker take control of the device and obtain access to all of the data contained therein, as well as listen in on and surveil the user.

Another malware attack on Android smartphones

Android is being attacked by the AbstractEmu malware. Applications infected with the malware are being used by the attackers to "root" a smartphone, and thus obtain an ability to freely perform remote actions. Security researchers from Lookout Threat Lab have described 19 Android applications, 7 of which contained the AbstractEmu malware code. The malicious app could be found primarily in the Amazon Appstore and Samsung Galaxy Store, but one of the apps was also available via the Play Store, from which it had been downloaded more than 10 thousand times.

November security updates for Microsoft products published

Microsoft has published another set of patches as part of Patch Tuesday. The November update consists of 55 security bulletins, some of which are labeled critical. The November security updates solve problems in the following products: Microsoft Azure, Microsoft Edge, Chromium based, Microsoft Office (and the related Excel, Word and SharePoint), Visual Studio, Exchange Server, Windows Kernel and Defender. Patch Tuesday falls on every other Tuesday of the month.

EDPD guidelines on restrictions on the rights of data subjects

At its 56th plenary session, the European Data Protection Board (EDPB) adopted, after public consultations, the final version of the Guidelines 10/2020 on restrictions on the rights of data subjects under Article 23 of the GDPR. The guidelines are meant as a reminder of the application terms of restrictions by Member States or EU legislators in the light of the Charter of Fundamental Rights of the European Union and the GDPR. They contain a detailed analysis of the criteria for the application of restrictions, assessments to be complied with, the manner in which the data subjects can exercise their rights after the restrictions are lifted, and the consequences of violating Article 23.

**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**