ALERT SAFE COMPANY

No. 1/2021

Ladies and Gentlemen,

Here is another issue of our "Secure Company" alert. In it you will find information on more changes planned to regulations on counteracting money laundering and terrorist financing (AML), as well as interesting GDPR and cyber security related information.
We want to draw your attention to the changes in the Act on counteracting money laundering and terrorist financing (AML), which the government adopted at the end of December and which have been sent to the Sejm. We have been describing these changes in our alert for some time. Here we only want to remind you of some of the issues that are going to change.
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. The first, discussed in more detail, pertains to the controller's liability for the actions of a subcontractor. The second, shorter – the potential consequences of failure to verify an email address provided by a client. In connection with BREXIT it also seems important to review information on transferring personal data to Great Britain.
You should also take note of the new digital services regulations planned by the EU.
As always, 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, BDO Managing Partner

New regulations on counteracting money laundering have been sent to the Sejm

At the end of December the government adopted a draft bill of changes to the Act on counteracting money laundering and terrorist financing and certain other acts, submitted by the minister of finance, funds and regional policy. The amendments have already been sent to the Sejm.

The purpose of the amendments is to adapt Polish regulations to the EU directive on counteracting money laundering and terrorist financing.

The changes specify the institutions subject to the requirements of the Act on counteracting money laundering and terrorist financing. This includes businesses that conduct activities consisting of: trading or dealing in works of art, collectibles and antiques, as well as activities consisting of storing, trading or dealing in such goods — this applies to transactions with a value equal to or higher than the equivalent of 10 thousand euro — irrespective of whether the transaction is concluded as a single operation or several operations that appear to be related to each other.

The new regulations also clarify the provisions on the sharing of information by the General Inspector of Financial Information (GIIF) with domestic and foreign authorities and on the storing by relevant institutions of documents and information obtained as a result of applying financial security measures. The scope of statistical information collected by GIIF will also be widened.

The draft also clarifies the methods to be used by obliged institutions in the storage of documents and information obtained as a result of applying financial security measures.

It also introduces mechanisms for verifying data in the Central Register of Beneficial Owners (CRBR) and the requirement to register "providers engaged in exchange services between virtual currencies and fiat currencies" and "custodian wallet providers".

Under the new regulations it will be necessary to identify and verify the identity of the client and beneficial owner, as well as to continually monitor the concluded transactions in order to determine the final level of client risk. Financial security measures should be applied in cases such as when a change has occurred in the nature or circumstances of the business relationship, or if there has been a change in the data of the client or beneficial owner (we discussed these solutions in detail in past editions of our alert).

The new regulations detail definitions such as that of beneficial owner, member state and group. The draft defines beneficial owner as, among others, each natural person who exercises direct or indirect control over a client by holding powers arising out of legal or factual circumstances, which enable the exertion of decisive influence on the actions or activities performed by the client, or each natural person on whose behalf business relationships are formed or an occasional transaction performed (we discussed these solutions in detail in past editions of our alert).

The amendments are to become effective after 14 days of their publication in the Journal of Laws, with the exception of some provisions that will go into effect at different times.

More time to provide personal data to Great Britain

Free flow of data between the European Economic Area (27 EU member states and Iceland, Liechtenstein and Norway) and the United Kingdom will be maintained until 1 July 2021 at the latest.

This is a solution provided in a so-called bridging clause contained in the final provisions of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, which will regulate the future relationship between the EU and the UK.

During this period of transferring personal data to the United Kingdom, such transfers will temporarily not be treated as transfers of data to a third country. As a result, businesses and public entities will not have to meet the additional requirements specified in Chapter V of the GDPR. This also applies to the additional requirements on international transfers of data specified in Chapter 3a of the Act of 16 September 2011 on exchanging information with law enforcement authorities of European Union member states, third countries, European Union agencies and international organizations, which implements Chapter V of Directive (EU) 2016/680.

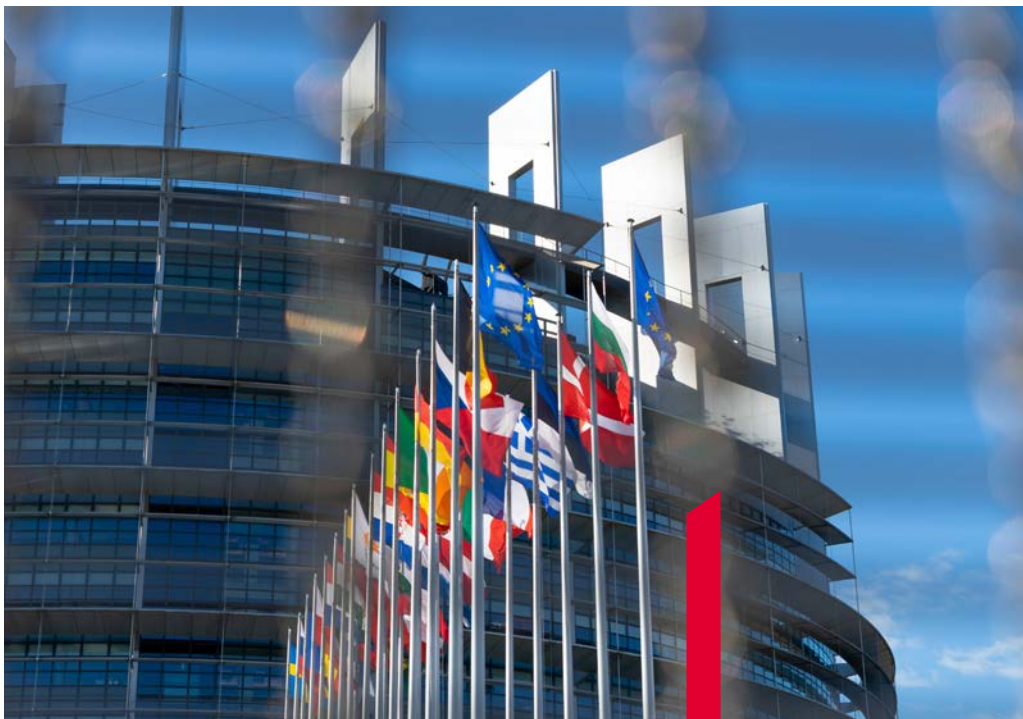
The transition period will end on 1 July 2021 at the latest, i.e. after six months from 1 January 2021. Although the agreement calls for four months, it will be automatically extended by another two, unless one of the parties to the agreement objects. The transition period may also end sooner.

In the transitional period the free flow of data will depend on the United Kingdom maintaining the personal data protection regulations based on EU law, i.e. the GDPR and Directive (EU) 2016/680 binding until 31 December 2020. During the transition period the United Kingdom will not be able to use its powers with respect to international data transfers.

Businesses that process the data of Polish citizens by providing their services from the territory of the United Kingdom must as of 1 January 2021 comply with the GDPR. This is because the GDPR also applies to the processing of data of persons present in the EU by controllers or processors without organizational entities in the EU, if those activities involve: offering goods or services to such persons present in the EU — irrespective of whether payment is required from such persons; or monitoring their conduct, providing that this conduct occurs in the EU.

Such businesses must designate in writing an EU representative in the member state of stay of the persons whose data are processed in connection with the offering of goods or services, or whose conduct is being monitored.

Businesses do not have to appoint a representative if the processing operations they perform are sporadic in nature, do not involve — on a large scale — the processing of special categories of personal data or personal data relating to convictions and prohibited acts and it is unlikely that due to their nature, context, scope or purposes they could constitute a threat to the rights or freedoms of natural persons.



Fines for failure to supervise subcontractor resulting in breach of GDPR possible

Inability to quickly detect and eliminate a threat caused the company to lose data. As a result, the President of the UODO found that the company failed to implement appropriate technical and organizational measures, which led to a breach of the data confidentiality principle, and imposed a fine on the company.

The fine imposed by the President of the UODO relates to a breach of information security (cybersecurity). The problem pertained to a subcontractor (processor). It is another in a series of fines imposed by the UODO in connection with leaks of data, which are a consequence of a failure to sufficiently protect networks and information, mainly by professional subcontractors.

In the course of the proceeding the UODO determined that the breach occurred when after the restart of one of the servers operated by a processor (hosting company) appropriate security configurations were not restored. The controller was notified of this by one of the cybersecurity specialists who discovered the vulnerability and showed a sample of publicly accessible information.

The controller, rather than thoroughly checking this information and monitoring the processor to ensure that they are handling the matter and checking security measures, had concerns that this could be an attempt at phishing for other data, which he stated in communications to the processor. As a result, the gaps in the system were not checked right away and a few days later data were stolen from the server.

It is the opinion of the UODO that the breach would not have occurred had the controller immediately reacted to the information that the data on his server are unprotected. The controller should have maintained the ability to quickly and effectively find all types of breaches to be able to take proper action. In addition, the controller should have been able to quickly examine the incident to determine if a breach of data has taken place and take appropriate remedial action.

The oversight authority further found that the absence of a quick enough reaction on the part of the processor to information about the vulnerability does not absolve the controller of liability for breach of data. It is the controller who must be able to detect, manage and report breaches – this is a key element of technical and organizational measures. In the UODO's opinion, although the company quickly notified the processor of a potential gap in server security, did not take sufficient action.

European Union is working on new rules on digital services security

The EU wants to introduce new regulations on digital services, including social media, online market places and other online platforms operating in the EU. They are also to cover such matters as the removal of illegal content from the Internet, protection of free speech, content moderation, online advertising.

Consultations are underway of the EU's draft regulation on digital services (Digital Services Act) and digital markets (Digital Market Act). The European Commission published the draft on 15 December 2020. Among others, it introduces new regulations on digital services, including social media, online market places and other online platforms operating in the European Union. The regulation is also to cover such matters as the removal of illegal content from the Internet, protection of free speech, content moderation by online platforms, online advertising.

The new regulation will strengthen the rights of users to appeal online platform decisions to remove or block content or the related account. In addition to the need for the platforms to create an internal system for responding to complaints, users will also be given the option to settle disputes out of court. Online intermediaries will also have to explain the decisions they make while moderating content.

Whereas the draft maintains a ban on imposing on intermediaries a general obligation to monitor content as part of the services they provide, which is fundamental to the protection of freedom of expression on the Internet.

The digital services act will also introduce provisions on removing illegal content from the Internet. Every user will be able to report such content. Special attention has been given to reports filed by courts or administrative organs. Priority treatment is also going to be given to reports made by trusted flaggers.

The regulation will also strengthen the transparency of online intermediaries. Among others, this will take place through an obligation to periodically report on the removal and blocking of content deemed to be illegal or contrary to the terms and conditions of the given intermediary's terms of service.

There will also be provisions to increase transparency in online advertising. Large platforms will be subject to stricter requirements when it comes to operational transparency.

The regulation recognizes the need to maintain proportionality in the imposition of obligations. The Commission wants very large platforms to have more obligations when it comes to exercising due care, which is why they should implement additional security measures. For this reason, in the proposed regulations it indicates that they will have to perform periodic assessments of the risk of exposing their services to dissemination of illegal content, as well as pay attention to the effect of their decisions on fundamental rights. They will also have to undergo periodic audits and ensure wider access to the data they hold.

In short

Attorneys at law have a standard for processing data in the cloud

The LegalTech Committee of the Warsaw bar association has prepared a "Standard for cloud processing of information by attorneys at law". Its purpose is to provide the methods and a set of tools for navigating this difficult and challenging area. It is primarily designated for those law firms that want to perform a large portion of their processes using a public or hybrid computing cloud. The guide clearly indicates what is, and what it is not a computing cloud.

Ministry of Labor will allow employers to check employees for sobriety

The Ministry of Development, Labor and Technology is working on regulations that will allow employers to perform preventative checks of employees for the presence of alcohol or similar substances and regulate the performance of such checks. There are also plans for the introduction of a comprehensive regulation setting out the basis on which employers can prevent intoxicated employees from performing work. The draft is currently being worked on within the ministry and will also contain GDPR related regulations.

Warning against cyber attacks relating to COVID vaccine

CERT Poland has issued a warning against potential attacks that take advantage of the start of registrations for coronavirus vaccinations. The CERT team has drawn attention to the need to be careful of suspicious emails, text messages, websites, applications and phone calls that ask for an immediate reaction. They have noted that coronavirus vaccinations are always free and voluntary. No payments or de-registrations are required.

Consolidated text of regulation on electronic communications with tax authorities has been published

The minister's of finance, funds and regional policy announcement of 26 November 2020 on the publication of the consolidated text of the minister's of development and finance decree on submitting declarations and applications and on the types of electronic signatures they should bear, has been published in the

2021 Journal of Laws (item 52).
According to the decree, declarations and applications may be signed with: a qualified electronic signature or electronic signature of the user on a tax portal that ensures the authenticity of declarations and applications, if they are sent via that portal, or with an electronic signature verified using a customs certificate, a trusted signature or personal signature, or another electronic signature that ensures authenticity of the declarations and applications. Personal signatures may be used if they are submitted via: a tax portal or the Central Register and Information on Business Activities, or the Electronic Tax and Customs Services Platform. The decree describes in detail what types of signatures may be placed on the various declarations and letters sent to the tax authorities.

UODO investigating a leak of data from a telemedicine platform during online consultations

The UODO has received a report of a breach of personal data from a company responsible for a telemedicine portal and remote consultations with doctors of various specialties. The case is currently being analyzed. The controller received information from a third party about a security error in one of the subsystems responsible for voice communications. Due to the gap in the system, an unauthorized person could, for a short time, have had access to the user's phone number, and if the consultation included an audio recording — could have been able to download it.

Incorrect email provided by client does not release controller from liability

The fact that a breach occurred as a result of an error made by a client, who provided an incorrect email address, cannot cause the event to not be classified as a breach of personal data. In permitting the use of email to communicate with clients the controller should be aware of the risks associated with, for example, the provision by a client of an incorrect email address. In order to minimize such risks the controller should implement appropriate organizational and technical measures, such as email address verification or encryption of documents sent by email. Also the fact of asking the unintended recipient to permanently delete the email cannot mean that the risk to the rights and freedoms of the data subjects is not high — states a decision issued by the UODO.