ALERT SAFE COMPANY

No. 3/2021

Ladies and Gentlemen,

Here is another issue of our "Secure Company" Alert. We hope that another portion of information on the changes planned to regulations on counteracting money laundering and terrorist financing (AML), along with interesting GDPR and cybersecurity related information, will turn out to be useful.
We would like to draw your attention to more changes to the Act on counteracting money laundering and terrorist financing, which this time were introduced by the Senate.
These changes should be followed as the amendments are nearly complete and the act should be signed into law in April.
We have described the changes arising out of the amendments in recent issues of our Alert.
Also noteworthy are the decisions and announcements made by the President of the Office for the Protection of Personal Data (UODO) on broadly defined liability for breaching GDPR.
Whereas with regard to information security, you should take note of the matters related to the consequences of a recent fire at the OVH data center, which for some time affected the operations of many companies, especially internet companies.
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

Biometric data may only be used in exceptional situations

The creation of any biometric data processing system should be preceded with an assessment of the impact on personal data protection, and any final decision to use it should take into account the fundamental principles of personal data protection — reminded the UODO.

According to the Office for the Protection of Personal Data (UODO), data controllers increasingly want to use biometric data. One of the reasons is the ease with which such data may be obtained (e.g. by placing a finger on a reader or eye to a scanner) and then identifying the person based on that data. Building or room access control based on a finger print, i.e. dactyloscopic data, is a good example. It is much easier and quicker to place a finger on a finger print reader than to enter an access code or use a proximity card that may be lost or provided to another, unauthorized person. As the use of biometrics spreads, the related issues are increasingly becoming the subject of proceedings conducted by European supervisory authorities.

As a result, the UODO reminds that biometric data processing constitutes a strong interference with privacy, leads to numerous threats, such as for example of a possible unauthorized disclosure of special data categories, or of discrimination. For this reason, the creation of any biometric data processing system should be preceded with an assessment of the impact on data protection, and any final decision to use the system should consider the fundamental principles of data protection, such as necessity, purposefulness and proportionality.

It should also be determined if biometric data identification is necessary and proportionate to the purpose of authentication or security. Where biometrics could be used to control access to rooms due to the need to ensure very high security, there is no justification for using them to access other rooms, such as for example a workshop.

The UODO has stressed that a controller may only process those data that are necessary to achieve a specific purpose. Allowing the processing of data that are not necessary, but may only help achieve the purpose, may lead to using this pretense for the processing of unlimited data. The controller could then explain that the data are not necessary, but may be useful in achieving the purpose. This approach would violate the principles of minimization and adequacy.

Money laundering: there will be a limit for real estate agents

The Senate has introduced an amendment to the changes to the Act on counteracting money laundering and terrorist financing and certain other acts, based on which real estate agents will not be considered obligated institutions if the value of monthly rent does not exceed 10 thousand euro.

At its 22 March 2021 sitting the Senate worked on the Act amending the Act on counteracting money laundering and terrorist financing and certain other acts. The (government's) draft implements the so-called fifth AML directive, which modifies EU regulations and increases financial transparency. It is meant to raise the effectiveness of the authorities entrusted with identifying funds originating from illegal activities or used to finance terrorism.

The amendments implement the provisions of the directive on preventing abuse of the financial system for money laundering and terrorism purposes. They also specify a list of obligated institutions, by including businesses that, among others, sell or broker the sale of art, collectibles and antiques, as well as store art, sell or broker the sale of art as part of transactions with a value equal to or higher than the equivalent of 10 thousand euro. In addition, the new regulations detail the principles of applying financial security measures and actions undertaken by obligated institutions with regard to relationships with high risk third countries. The amendments also clarify the methods to be used by obligated institutions to store documents and information obtained as a result of applying financial security measures. They introduce mechanisms for the verification of data contained in the Central Register of Beneficial Owners and the requirement to register entities that provide currency exchange services involving the exchange of virtual currencies, as well as suppliers of virtual currency accounts.

While working on the Act the Senate introduced an important amendment that was approved by the Ministry of Finance. The government's draft broadens the concept of obligated institutions by, among others, real estate agents. The Senate added a stipulation that this would not apply to real estate agency activities aimed at concluding an agreement for the rental or lease of a property or its part, with a monthly rental fee lower than the equivalent of 10 thousand euro.

It should be noted that the amendments will add to the group of obligated institutions those businesses whose main area of activity is the provision of services consisting of preparing returns, bookkeeping, providing tax or customs law advice, opinions or explanations, which are not other obligated institutions.

The Act has been sent back to the Sejm, which will review the changes made by the Senate.

Breaches of personal data protection must be immediately reported to supervisory authority

Sending an unencrypted email containing personal data and failing to inform the UODO of such a data protection breach within 72 hours, is subject to a fine.

The Office for the Protection of Personal Data (UODO) considered a case where an unauthorized recipient was sent an email with an attachment in the form of an unencrypted file containing the personal data of the addressee and others. In consequence, a security breach occurred which led to an accidental disclosure of personal data to an unauthorized person, i.e. to a breach of personal data confidentiality, constituting a breach of personal data protection.

In accordance with binding regulations, a "breach of personal data protection" means a breach of security leading to an accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to sent, stored or otherwise processed personal data.

The UODO reminds that in accordance with Article 33 par. 1 and 3 of the GDPR, in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification must at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In the matter reviewed by the UODO, the company had not complied with the requirement prior to the issue of the decision.

OVH data center fire will force companies to take greater care of IT security

The recent fire in an OVH server room has shown how important it is from the perspective of IT security to have correctly formulated agreements for the supply of server services, as well as appropriate business insurance if events should occur leading to a loss of data or business interruption caused by lack of access to essential IT infrastructure.

The recent high-profile fire of an OVH server room led to many problems for companies and individuals. The fire has shown that creating backup copies not frequently enough may threaten business continuity. The fire of an OVH server should be treated as a vital lesson in data processing security. In this context it would be worth it to consider insurance that will cover additional costs of restoring continuity and lost income during downtime caused by property damage (business interruption insurance).

Large trading platforms, financial institutions, etc., who have their own servers, but only some of their processes and data are held in a cloud, can expand their insurance by the so-called "customer and supplier extension clause". An insurance company liability limit is usually established for suppliers. If a supplier of in-cloud services experiences a loss in electronic equipment, resulting in an interruption of the activities of the entity that purchased the extension, then the insurance will cover it.

The situation of smaller companies is somewhat different. It should be remembered that electronic equipment policies for small and mid-sized entities usually cover data and software on media held by the insured business. In such cases it is necessary to pay attention to insurance contract provisions on the operator's contractual obligations with regard to: creating backup copies and being responsible for maintaining data and restoring them in the event of a breakdown or destruction of electronic equipment.

Regular creation of backup copies is of key importance when it comes to ensuring company IT security. This task should not, therefore, be neglected, especially since even if the company has an appropriate insurance policy, it constitutes a condition for any damage to be paid out. It should also be remembered that the insurance company's liability is usually limited to a specified amount.

Nonetheless, companies that use services like those offered by OVH should seriously consider purchasing appropriate insurance or insurance extension in the event of similar events. It should provide coverage for loss of data, as well as for loss of income caused by a temporary interruption of operations due to lack of access to necessary server infrastructure.

It is also important to better regulate the risk associated with such potential breakdowns in agreements concluded for the supply of such services.

In short

Work on amendments to the National Cybersecurity System Act taking longer

Work on amendments to the National Cybersecurity System Act is taking longer, apparently due to a difference of opinion between the draft's authors and the Ministry of National Assets and Ministry of Justice. Three provisions are said to be the most controversial. The first pertains to assessing the risk of suppliers of telecommunications equipment and mainly the problem of allowing Huawei to build a 5G network. The second relates to a strategic operator that is going to be responsible for telecommunications services for government, administrative and local government organs. The third issue concerns regulations entitling the President of UKE to discretionary allocation of 700 MHz frequencies without the need to open a tender.

Consultations on virtual voice assistants are underway in the EU

The European Data Protection Board (EDPB) is waiting until 23 April 20201 for comments on the Guidelines 02/2021 on virtual voice assistants. The guidelines on virtual voice assistants aim to identify the most significant compliance challenges for virtual voice assistants and provide the interested parties with recommendations on how to deal with them.

Consultations to be held on the processing of personal data for scientific research purposes

On 30 April 2021 from 10:00 am to 4:00 pm, the EDPB will hold a remote stakeholder event on the topic of applying the GDPR to the processing of personal data for scientific research purposes. The meeting is addressed to representatives from, among others, individual companies, sector organizations, NGOs, law firms and academia with an expertise in the field.

Consolidated text of Database Protection Act published in the Journal of Laws

The announcement of the Marshall of the Sejm of the Republic of Poland on the publication of the consolidated text of the Database Protection Act has been published in the 2021 Journal of Laws (item 386). Under the act, databases are subject to protection irrespective of the protection granted based on the Act on copyright and neighboring rights, which covers databases that meet the characteristics of a work.

Work is underway on enabling transfer of data to Great Britain

The European Commission has initiated a procedure to adopt two decisions confirming appropriate level of protection with regard to the transfer of personal data to the United Kingdom. One of the decisions is to be adopted based on the General Data Protection Regulation (GDPR), and the other based on the Data Protection Law Enforcement Directive (so-called law enforcement directive). The European Commission may, by way of an implementing act, adopt a decision that finds that a third party, territory or specified sector or sectors in that third country, or an international organization, ensure a proper level of protection.

Marketing agency lost with UODO before NSA

The Supreme Administrative Court has dismissed a complaint against a decision issued by the President of the UODO, imposing a fine on a company that hindered the exercise of a right to withdraw consent to process personal data (ruling of 10 February 2021, case file number II SA/Wa2378/20). In its decision to impose an administrative cash fine the UODO stressed that the company's process of consent withdrawal not only did not take into account the principle under which it should be as easy to withdraw consent as it was to grant it, but that to the contrary — the company's consent withdrawal procedure involved the application of complicated organizational and technical solutions.

Joint opinion of EDPB and EDPS on data governance

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have adopted a joint opinion on the Data Governance Act. On data sharing service providers, the joint opinion highlights the need to ensure prior information and controls for individuals, taking into account the principles of data protection by design and by default, transparency and purpose limitation. Furthermore, the modalities upon which such service providers would effectively assist individuals in exercising their rights as data subjects should be clarified.

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