CHSHCEE NEWSLETTER

Keep up to date with the latest legal developments in Austria, Belarus, Bulgaria, the Czech Republic, Hungary, Romania and the Slovak Republic with our CEE newsletter.

Austria

Founder loyalty

Nadine Leitner and Albert Birkner explain a recent ruling of the Supreme Court that unsettled a lot of founders. **>> Read full article**

Belarus

Development of personal data protection regulations

Sergei Makarchuk discusses the first attempt to create consistent regulations on personal data protection in Belarus that will bring Belarussian law into line with international standards.

>> Read full article

Bulgaria

Implementation of the Fourth Anti-Money Laundering Directive

Boyko Gerginov gives an overview of certain details regarding the AMLD's national implementation that aims to strengthen existing anti-money laundering rules. **>> Read full article**

Czech Republic

The Prague Rules: Inquisitorial Rules on the Taking of Evidence in International Arbitration

Lenka Hrdlickova and Lukas Hoder analyse these new rules that aim to compete with the IBA Rules on the Taking of Evidence in International Arbitration. **>> Read full article**

Hungary

Unregulated issues and missed opportunities after the modification of the Privacy Act

Adrienn Dömök outlines a few of the changes introduced by the Hungarian Privacy Act. **>> Read full article**

Romania

GDPR – National legislation in Romania

Anda Nicoara highlights additional legislation at the national level in connection with the GDPR. **>> Read full article**

Slovak Republic

The Slovak Cyber Security Act

Jozef Bannert summarizes the recently introduced Slovak Cyber Security Act that imposes several obligations on service providers to prevent and detect cyber security incidents in networks and information systems. **>> Read full article**

CHSHCEE Austria

Founder loyalty

The Supreme Court unsettled a lot of founders last year when it ruled that the withdrawal of benefits by the founder of a private foundation conflicted with his duty of loyalty and that this constituted an abuse of rights. Founders normally wish to reserve the right to make major decisions, such as giving, amending and even withdrawing the benefits provided to beneficiaries. This is usually permitted and does not conflict with any duty of loyalty, not even in the wake of the Supreme Court ruling. However, the individual facts of the case are decisive.

Duty of loyalty and abuse of rights

The highly-publicised decision of the Supreme Court concerned an Austrian family of industrialists. The company's founder and his wife of many years had established a private foundation and transferred shares in the family business to the private foundation. During their divorce, the company's founder amended the rules governing beneficiaries in the deed of foundation. The changes were intended to ensure that neither his wife nor his children henceforth retained the status of beneficiary. The wife sued and the Supreme Court found in her favour. The Supreme Court found that special duties of loyalty exist between co-founders if only one of these co-founders is entitled to amend the deed of foundation.

In this specific case, the Supreme Court ruled that by excluding his wife and children, the founder – who alone was entitled to amend the deed of foundation – had acted in a way that constituted an abuse of rights. This is deemed to be the case if dishonest motives for exercising the right clearly outweigh any honest motive, or if there is a "huge imbalance" between the founder's own interests and the interests of third parties who are adversely affected. The company's founder wished to protect his life's work, which he felt was threatened by the actions of his family. However, this view held by the founder was grossly disproportionate in relation to the loss of benefits suffered by his family, in particular his wife who played an important role in building up the business and who herself had also contributed assets to the private foundation. The Supreme Court regarded the complete withdrawal of all financial benefits provided by the foundation as a form of disciplinary action against the beneficiaries and ruled that this was not in the interests of protecting the business.

Amendments to the rules governing beneficiaries remain admissible

Notwithstanding this ruling, any amendments to the rules governing beneficiaries cannot be assumed to be null and void on the grounds it constitutes an abuse of rights. The Private Foundations Act expressly provides that founders can reserve the right to amend the deed of foundation and the appendix to the deed of foundation. If a foundation was established by more than one founder, this amendment right can also be granted to just one or more than one founder. Where there are several founders, the amendment right can also be made subject to a majority decision of the founders. According to the Supreme Court, the exercise of the amendment right is subject to a content check and must be assessed on a case-by-case basis.

As before, amending the deed of foundation is permissible. It is also not possible to generalise and say that amendments to the deed of foundation or the appendix to the deed of foundation are no longer allowed to interfere with the rights of co-founders or beneficiaries. If one or more founders have reserved the right to make comprehensive amendments, interference with the legal positions of co-founders is permitted by law as well. This also applies in particular to amending the rules governing beneficiaries. Founders who in the deed of foundation have reserved an amendment right continue to be entitled to amend rules governing beneficiaries, give new benefits or even reduce the benefits paid to beneficiaries or completely remove them from the group of beneficiaries.

The specific circumstances do not have any significant impact on the admissibility of amending the rules governing beneficiaries. In this way, it can be an abuse of rights if a beneficiary descended from the founder who waived his/her compulsory portion of the estate in return for benefits is later stripped of his/her benefits. Any limitation placed on the founder's right to make amendments on the grounds that it may be an abuse of rights or because of a duty of loyalty must be assessed on a case-by-case basis. No general conclusions can be drawn from the Supreme Court ruling.

It would appear that in the case of the family in question the dispute meanwhile continues to rage: Most recently, the Constitutional Court ruled on the lawfulness of the shareholder squeeze-out. The wife lost her case. As a minority shareholder in the business, she was denied the protection of her legitimate expectations.

Authors:

Dr. Albert Birkner, Partner
Mag. Nadine Leitner, Attorney-at-law

For more information

Dr. Albert Birkner
Partner in Austria
albert.birkner@chsh.com
Tel: +43 1 514 35 431

CHSHCEE Belarus

Development of personal data protection regulations in Belarus

Introduction

The draft Law of the Republic of Belarus On Personal Data ("**Draft Law**") was recently made available for public discussion. It is the first such attempt to create consistent regulations on personal data protection in Belarus. At present, the protection of personal data is covered to a certain extent by Law No. 455-Z of the Republic of Belarus dated 10 November 2008 On Information, Informatization, and Protection of Information. However, in light of the current global trend towards developing personal data protection regulations, it is essential for Belarus to have a special purpose law regulating this issue.

Scope of the Draft Law

The Draft Law defines personal data as any information relating to an identified or identifiable natural person.

The rights relating to data protection in the Draft Law solely benefit natural persons. Legal entities are not granted any protection under the Draft Law.

As a general rule, all persons involved in the processing of personal data are subject to the data protection obligations laid down in the Draft Law; however, most of the obligations rest with the "Processor". A legal entity, a natural person, a public authority, and other bodies may act as a Processor.

The Draft Law applies to any processing of personal data in whole or in part by automated or non-automated means, which form part of a structured set of personal data accessible on the basis of specific criteria (e.g. card files, lists, databases, etc.).

It does not apply to certain types of personal data processing such as, for example, the processing of sensitive personal data collected, used and distributed in connection with intelligence and counterintelligence operations. The scope of the Draft Law also does not extend to personal data processing performed by natural persons solely for their personal or household purposes without any underlying commercial context.

Under the Draft Law, any cross-border transfer of personal data to countries in which personal data are not duly protected is prohibited unless special conditions are met (for example, consent is given by the subject of the personal data in writing or electronically or the data transfer is deemed necessary in order to protect the data subject or for

the purpose of providing healthcare services).

The Draft Law also lays down the rights and duties of the special body responsible for overseeing personal data protection. The special body will be nominated by the President of Belarus in due course.

Generally speaking, a significant portion of the Draft Law is similar to the EU General Data Protection Regulation ("**GDPR**"), but the Draft Law lacks the depth of the GDPR.

It is expected that the Draft Law will be put before the Belarusian Parliament for its consideration by the first half of 2019 and could be approved during the 2019 parliamentary session.

Summary

To date, there has been no comprehensive legislation regulating the protection of personal data in Belarus. The development of the Draft Law is a progressive step forward and, if enacted, will bring Belarussian law into line with international standards in this area. The adoption of the Draft Law would bring certainty to all activities undertaken by businesses in relation to the processing of personal data.

For more information

Sergei Makarchuk, LL.M.
Managing Partner in Belarus
sergei.makarchuk@chsh.com
Tel: +375 17 2663417

CHSHCEE Bulgaria

Implementation of the Fourth Anti-Money Laundering Directive

Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (**Anti-Money Laundering Directive** or **AMLD**) was recently transposed into Bulgarian law. The Directive was implemented by adopting the new Bulgarian Anti-Money Laundering Act (Act), which revoked and replaced the previous act of the same name.

The AMLD aims to strengthen existing anti-money laundering rules and introduces various changes to risk assessment obligations, transparency requirements about beneficial ownership, and customer due diligence, etc.

Below we outline certain details regarding the AMLD's national implementation.

Central register of beneficial ownership

The AMLD requires that information on the beneficial ownership of corporate and other legal entities be held in a central register. For Bulgaria, the following existing registers will be used to that end:

- Commercial Register – for companies
- Register of Non-Profit Organisations – for non-profit entities
- Bulstat Register – for trusts and similar legal arrangements

Registration requirements

The Act provides that all corporate and other legal entities incorporated in Bulgaria, as well as trusts and similar legal arrangements administered in Bulgaria, are required to have information on their beneficial owners entered in one of the aforementioned registers. The registration deadline is 31 May 2019.

Beneficial owner

The definition of "*beneficial owner*" in the Act corresponds to the definition in the AMLD: any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted. In relation to corporate entities, it should be noted that the threshold provided under the Act is smaller. Whereas under the AMLD an ownership interest of *more than 25 %* is an indication of direct ownership, a shareholding of *at least 25 %* is required for the same purpose under the Act.

Further implementation

Details on the application of the Act will be further specified in a regulation on

the implementation of the Act, which the Bulgarian government was required to adopt by the end of August 2018. The obliged entities are required to bring their anti-money laundering policies into line with the new rules within four months of the implementing regulation being adopted. As the government is struggling to meet the deadlines set by the Act, the actual enforcement of significant parts of the Act will be postponed.

The Registry Agency is also required to implement the necessary changes to the Commercial Register and Bulstat Register platforms to allow the registration of beneficial ownership data.

For more information

Boyko Gerginov
Managing Partner in Bulgaria
boyko.gerginov@chsh.com
Tel: +359 2 401 09 99

CHSHCEE Czech Republic

The Prague Rules: Inquisitorial Rules on the Taking of Evidence in International Arbitration

On 8 April 2018, a draft of the "Inquisitorial Rules on the Taking of Evidence in International Arbitration", known as the "Prague Rules", was released. These new rules aim to compete with the IBA Rules on the Taking of Evidence in International Arbitration, which are considered too heavily rooted in the common law tradition by the authors of the Prague Rules and in their opinion cause arbitration proceedings to be lengthy and expensive. The draft of the Prague Rules will be further discussed by the Working Group, with the final version due to be released before the end of 2018.

The goal of the Prague Rules

The development of the Prague Rules was initiated at the annual conference of the Russian Arbitration Association in Moscow in 2017. The stated goal was to oppose the "creeping Americanization of international arbitration" and what are claimed to be its negative effects. The authors of the Prague Rules primarily intend to make arbitration more cost-effective and less time-consuming by limiting the parties' scope of action and empowering the arbitral tribunal.

More specifically, the Working Group states that there are three main areas of taking evidence which cause international arbitration to be expensive and lengthy: 1) document production, 2) the hearing of too many witnesses, and 3) the lengthy examination of witnesses. These are the main focus of the new draft Prague Rules.

Therefore, unlike the IBA Rules, the Prague Rules follow an inquisitorial approach, providing a more active role for the tribunal, mostly in the areas of fact-finding, documentary evidence, factual witnesses, experts and the assistance provided by the tribunal in finding an amicable settlement of the dispute. The Prague Rules may be applied with the agreement of the parties as a binding document or merely as guidance. The tribunal can also suggest the use of the Prague Rules.

The differences between the Prague Rules and the IBA Rules

The IBA Rules adopted in 2010 have become a widely used tool for guiding the process of taking evidence in international arbitration. What are the differences between the IBA Rules and the Prague Rules?

First, Article 2 of the Prague Rules makes the arbitral tribunal responsible for managing the start of arbitration proceedings. The tribunal actively informs the parties which evidence it would consider appropriate to substantiate their positions and the tribunal may even order the parties to produce evidence.

Second, Article 4 of the Prague Rules states that only the production of specific documents can be requested. Therefore,

unlike Article 3(3) of the IBA Rules, the production of a category of documents, as well as e-discovery, is not allowed under the Prague Rules.

Under the Prague Rules, the role of the arbitral tribunal is shifted towards the inquisitorial model, which is in contrast to the role of the arbitral tribunal under the IBA Rules. Article 4.4 of the Prague Rules empowers the arbitral tribunal to call upon a party to produce any document if the tribunal considers it relevant. Article 3 entitles and encourages the tribunal to take an active role in establishing the facts of the case.

Third, the Prague Rules places limits on the power of a party to present witnesses and experts while giving the arbitral tribunal greater powers in this respect. The draft of the Prague Rules presents two alternative versions of Article 5, which contains rules for factual witnesses, with both versions to be discussed by the Working Group. Article 6 gives the arbitral tribunal powers related to experts.

Fourth, Article 5.6 of the Prague Rules stipulates that witnesses are to be examined under the direction and control of the arbitral tribunal. The Prague Rules clearly favour the examination of witnesses by the arbitrators, whereas the IBA Rules take the opposite approach favouring the parties.

Conclusion

The Prague Rules are a remarkable attempt at countering the dominant position of the IBA Rules. It will be interesting to see whether the Prague Rules receive such broad acceptance as its authors certainly expect. The Prague Rules are to be officially launched at a conference in Prague in December 2018.

Authors

Mgr. Lukáš Hoder, LL.M., Senior Associate
Mgr. Lenka Hrdličková, LL.B., Associate

For more information

JUDr. Petr Kališ
Managing Partner in the Czech Republic
petr.kalis@chsh.cz
Tel: +420 221 111 711

CHSHCEE
NEWSLETTER

CHSHCEE | Hungary

Unregulated issues and missed opportunities after the modification of the Privacy Act

Many Hungarian companies waited until the last moment before complying with the data protection regulation – presumably waiting, in vain, for a modification of the Privacy Act, the national data protection regulation. The modification was finally adopted in July, but employment law and sector-specific regulations (on the processing of financial, insurance or health-care data) have still not been adopted. The following article highlights a few of the changes introduced by the Privacy Act. Most of these changes do not add anything new to the GDPR rules, but they do appear to have caused many problems in practice.

Although the GDPR was adopted in 2016, it only became enforceable from 25 May 2018. Legislators, companies and other entities had two years to prepare and yet many took little action over this period to ensure their operations would comply with the provisions of the GDPR. The Privacy Act was modified in two stages: some provisions took effect on 26 July, the day following promulgation of the modification, while the rest took effect on 25 August. The modifications have not really added any new elements and do not represent much more than the transposition of the GDPR rules into Hungarian legislation. Unfortunately, detailed rules and regulations in response to issues that have been encountered in practice have yet to be adopted.

Confusion over legal bases

Although **the application of the GDPR as an EU regulation is mandatory**, i.e. there is no need for its transposition into national law, the modification of the Privacy Act was still necessary, for example to ensure it does not include any provisions that are incompatible with the GDPR. Additionally, **the GDPR provides numerous opportunities for the Member States to adopt their own national regulations**, for example in connection with employment-related data processing matters.

However, the modification of the Privacy Act ultimately appears to be a bit of a mixed bag, for example in the case of legal bases. The GDPR includes an **exhaustive list** that sets out six legal bases for processing, and therefore data processing is lawful if it is based on one of the following **legal bases**:

a. consent;

b. performance of a contract or the implementation of pre-contractual measures;

c. performance of the data controller's legal obligations;

d. protection of vital interests;

e. performance in the public interest or in the exercise of public powers; and

f. legitimate interests.

It is easy to see why points d. and e. do not have much relevance for businesses. What's more, companies try to avoid data processing based on consent because **consent can be revoked**. Processing conducted on the basis of **legitimate interests** is only possible if the interests of the data controller outweigh those of the data subject (e.g. an employee); nevertheless, it still appears to be a better solution than consent. Therefore, data processing by businesses generally takes place in connection with a **contract** or in order to perform a **legal obligation**.

However, the Privacy Act has slightly modified the terminology and it has consolidated data processing that is "inevitable for the performance of a legal obligation" (point c. in the list above) and data processing based on the "data subject's consent" into a single legal basis for data processing. We believe that this solution in its current form is **incompatible with the GDPR because it requires consent in addition to the existence of a legal obligation** and there is a good chance that it will give rise to problems in the future.

Data protection officer (DPO)

The term ***'belső adatvédelmi felelős'*** **(internal data protection manager) has been replaced in the Privacy Act by *'adatvédelmi tisztviselő'*, the term for data protection officer (DPO) that is used in the Hungarian version of the GDPR**. An innovation in the Privacy Act is that a DPO can hold that position for several data controllers and/or data processors at the same time. While the Article 29 Working Party, an EU committee on data protection, issued a guideline that deals with DPOs, the more specific and practice-oriented recommendations included in the guideline have not been incorporated into the Privacy Act. This is unfortunate because this guideline includes conflict of interest rules, as well as responses to questions often encountered in practice.

A **DPO must be appointed** if the data controller performs a public function that is laid down by statute, or if it is required by national or EU legislation. A **DPO can be appointed** in other cases, subject to the rules that otherwise apply to DPOs (e.g. reporting the appointment to the National Authority for Data Protection and Freedom of Information or NAIH). A workable halfway solution is if the person responsible for data protection issues is given a different title (e.g. data protection coordinator or manager). In that case, a related set of policies and procedures will have to be introduced, but a formalised approach will not be needed unlike in the case of a DPO.

Following the introduction of the modification, DPOs may only be appointed if they have **adequate knowledge of data protection**

regulations and the relevant case-law of the authorities and courts, but there are no requirements in terms of qualifications. (A degree in law, public administration, information technology or another equivalent field was required in the past.) While an internal data protection manager was previously required to work within an organisation and report directly to the leader of the organisation, now **it can be an external position in cooperation with the organisation**. The question of course is what is more effective: to train an employee to fill this position, which is both time-consuming and resource-intensive (training costs) and comes with certain risks (labour fluctuation, loss of know-how, certain protections under labour law) or to hire an external advisor (lawyer/organisation providing data protection services) who will need time to learn the ins and outs of the organisation's internal processes.

The NAIH will have an online system where DPOs can be registered, but for the time being the personal details of a DPO (name, postal address and e-mail) and any changes in such details must be sent by e-mail to the NAIH.

Data breaches

The new provisions of the Privacy Act only represent changes compared to the previous national legislation but in fact they reflect the rules of the GDPR. Under the new rules, a data breach must be reported to the NAIH immediately but in any event no later than 72 hours after its occurrence, except where the breach does not constitute a risk to the data of data subjects. The report must include a long list of elements that are stated in the Privacy Act. When it comes to understanding data breaches, it is better once again to rely on the opinion of the Article 29 Working Party rather than to look for guidance in the Privacy Act or the GPDR. The relevant Working Party guideline defines when a controller becomes aware of a data breach, what should be done if the data breach occurs at a data processor, and how to assess whether or not the data breach constitutes a risk to the rights of data subjects. Although data controllers may see this as a minor concern compared to recording obligations, in the light of the rather tight reporting deadline of 72 hours, it is advisable for them to adopt a policy that identifies what tasks should be carried out by whom and by what deadline in the case of a data breach.

Data subjects must be informed if a data breach is "likely to result in a high risk". The GDPR lists three exceptions to this rule, and the modified Privacy Act adds a new one (national security interest). Records must be kept of data breaches, and the information included in such records must be retained for a period of 10 years following the erasure of the relevant data. Data breaches must also be reported to the NAIH via an online system.

Data protection impact assessments

Data controllers are now required to determine what impact their proposed data processing activities will have on the rights of data subjects. If the data processing is likely to result in a high risk, a written data protection impact assessment must be prepared. Once again, guidance as to what qualifies as high risk should be sought from the Article 29 Working Group's relevant guidelines.

A data protection impact assessment must include at least a general description of the proposed data processing operations, a description of the risks identified and their type, and the measures implemented by the data controller in order to manage such risks.

Records and electronic logs

The provisions pertaining to records are included in a separate chapter in the Privacy Act. These provisions state that **records must be kept** of the processing of personal data, data breaches and the measures implemented in connection with the right of data subjects to access their data.

Electronic logs are not an element that has been transposed by the GPDR; the Privacy Act does indeed introduce a new term to the Hungarian data protection regime here. If personal data is processed electronically, an electronic log must be kept containing the following information:

- the type of personal data processed;
- the purpose and reason for the data processing;
- date and time of data processing operations;
- name of the person who carried out the data processing operations; and
- the recipient of any transmitted data.

In summary, while the modification was highly anticipated by lawyers in Hungary, it is not complete. The language of the modification mostly reflects the language of the GDPR, with provisions that are somewhat modified in certain cases. It remains an open question how the rules pertaining to data processing in various sectors and industries (health-care, banking or insurance) will be modified. Anticipation is particularly high among lawyers and other law practitioners who deal with employment law.

Author

Dr. Bernadett Török, Attorney-at-law

For more information

Dr. Tamas Polauf
Partner in Hungary
tamas.polauf@gp-chsh.ro
Tel: +36 1 457 80 40

CHSHCEE Romania

GDPR – National legislation in Romania

In the context of the application of Regulation (EU) 2016/6791 (GDPR), it is necessary for Romania to introduce the following additional legislation at the national level: (i) the law on the application of the GDPR (GDPR Law), and (ii) the law amending Law 102/2005 regarding the establishment, organization and functioning of the National Authority for Supervising the Processing of Personal Data (DPA Law).

DPA Law

The DPA Law focusses mainly on (a) control mechanisms and investigations, and (b) the competences of the DPA to resolve complaints.

(a) Control mechanisms and investigations by the DPA

The DPA has the option of imposing administrative fines and corrective measures for data protection violations. The minutes/decisions of the DPA may be contested before the Romanian courts. The decision of the court is not final and may be challenged before the superior court by the controller/processor; otherwise it is final without further formalities. The payment term for the administrative fine is 15 days from the date when the decision is handed over or communicated.

If a controller/processor fails to cooperate (e.g. by not providing the documents requested for an investigation), the DPA may impose a fine for each day of delay.

If the Romanian DPA is of the view that the data protection rules have been violated, it may make a court claim in this respect.

(b) Competences of the DPA to resolve complaints

Data subjects who believe the processing of their data does not comply with the applicable legal requirements have the possibility of registering a complaint with the DPA. Provision is made for a specific procedure before the DPA.

Notwithstanding the above, data subjects have the possibility of bringing violations of data protection rules to the attention of the courts. Any interested person may request that the court orders the reparation of damage caused by the processing of personal data.

GDPR Law

The GDPR Law lays down special rules regarding the processing of several categories of data.

- Special rules regarding the processing of genetic data, biometric data and data concerning health

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC

The processing of genetic data, biometric data or data concerning health for the purpose of automated individual decision-making, including profiling, is permitted if the data subject has given his/her express consent or if the processing meets the express legal requirements and provided appropriate measures have been taken to ensure the data is protected. The processing of data concerning health for public health purposes is also limited in accordance with the requirements of the law.

– Special rules regarding the processing of national identification numbers (NIN)

  The processing of a NIN, including by collecting or disclosing the documents containing such NIN, may be conducted in keeping with the GDPR. The Romanian GDPR Law requires additional safeguards in those cases where the NIN is to be processed on the basis of the controller's legitimate interest.

– Special rules regarding the processing of data at the workplace

  If electronic communication systems and/or video surveillance systems are used at the workplace to monitor employees, the processing of the employee's personal data for the purpose of pursuing the employer's legitimate interest is permitted only if specific safeguards for the benefit of the data subject are put in place.

– Other special rules regarding the processing of personal data

  There are specific exceptions with respect to the provisions of the GDPR in those cases where personal data is processed for archiving purposes, for general interest, for statistical purposes, or for science or historical research or journalistic/academic/literary purposes. In addition, the GDPR Law provides specific rules for certification bodies. Administrative fines are also addressed.

Author

Anda Nicoara, Senior Attorney-in-law

For more information

Mirela Nathanzon
Partner in Romania
mirela.nathanzon@gp-chsh.ro
Tel: +40 21 311 12 13

CHSHCEE
Slovak Republic

The Slovak Cyber Security Act

On 1 April 2018, the Slovak Cyber Security Act No. 69/2018 Coll. ("CSA") came into force. The CSA requires service providers to implement and comply with specific security processes through the use of modern security technologies and imposes an obligation on them to detect cyber security events in major networks and communications or information systems. Any failure by the service providers to comply with the obligations established by the CSA may result in the imposition of administrative fines of up to EUR 300,000.

Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to its transnational nature, substantial disruptions to those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

By adopting the CSA, the Slovak Republic transposed Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems ("NIS Directive"). Both the NIS Directive and the CSA aim to protect information systems and networks against disruption either from the technical devices themselves, the data processed on them or the services provided by them. The CSA sets out several obligations on public bodies and providers of basic services (e.g. in the fields of banking, transport, energy, digital infrastructure, post, pharmaceutical, metallurgical and chemical industries and health sector) and providers of digital services in the area of cyber security.

The CSA lays down minimum requirements for cyber security by introducing security measures outlined in Article 20 of the CSA. Article 20 also defines what is understood by security measures. However, specific security measures are issued by generally binding legislation.

A cyber security event is deemed to be any such event that causes or may cause disruption to the security of information in information systems or to electronic communications services and networks. The security breach itself is defined as a cyber security incident. Service providers are required to report cyber security incidents to the National Security Authority which has the status of a national unit of the Computer Security Incident Response Team ("CSIRT").

Providers of basic services

The identification criteria of the basic service and its providers are specified in the implementing regulation of the National Security Authority No. 164/2018 Coll.

According to Article 17 para. 1 of the CSA, if the provider of basic services exceeds the identification criteria provided by the implementing regulation of the National Security Authority, it is obliged to inform the latter, which must subsequently register the basic service in the list of basic services and its providers in the registry of providers of basic services.

The provider is obliged to adopt and follow general safety measures at least to the extent defined by the CSA, and if adopted, also according to the sectoral security measures.

In case the provider does not operate the network and information systems essential for the provision of its basic services and uses a third party – the supplier of network and information systems, it is obliged to conclude a contract with this third party to ensure compliance with security measures and notify obligations according to the CSA and for the whole duration of the supplier contract.

The CSA also regulates several notification obligations vis-à-vis third parties, the National Security Authority, the law enforcement authority in criminal proceedings or the police. The obligations of the basic service provider not only include the notification of the registration of services and its provider to the respective register or notifications of cyber security incidents but they also include an obligation to cooperate with the relevant authorities with regard to resolving cyber security incidents, providing essential information, with a view to securing evidence for the purposes of criminal proceedings and reporting a criminal offence relating to the cyber security incident.

Digital service provider

In Article 21 the CSA defines the provider of digital services. Digital services include online marketplaces, web search engines and cloud computing services provided by a legal entity or a natural person/entrepreneur who at the same time employs at least 50 employees and has an annual turnover or an annual balance sheet of more than EUR 10,000,000.

The digital service provider is required to notify the National Security Authority regarding the commencement of the provision of digital services. Following this notification, the digital service will be listed in the evidence of digital services and the provider of such service will be registered in the register of digital service providers.

As well as the basic service provider, the digital service provider is obliged to

adopt and follow appropriate safety measures, however according to special regulations addressing the risks associated with threatening the continuity of the digital services and the process of resolving cyber security incidents. In this regard, the provider must consider, in particular, the security of networks and information systems and its ability to prevent and deal with cyber security incidents, the necessary means of ensuring the continuity of digital services in the event of cyber security incidents, and the compliance of networks and information systems with security standards.

In addition, the digital service provider is subject to several notification obligations regarding the notification of cyber security incidents and related obligations to cooperate with authorities with respect to resolving cyber security incidents.

Administrative fines

The National Security Authority exercises control over compliance with the provisions of the CSA. In case the providers of basic services or digital services breach the obligations or fail to comply with requirements set out by the CSA, the National Security Authority may impose fines from EUR 300 to up to EUR 300,000. In every case the National Security Authority considers the seriousness of the administrative offence, in particular, the manner in which it was committed, the duration, the consequences and the circumstances in which it was committed.

Conclusion:

The CSA imposes several obligations on service providers to prevent and detect cyber security incidents in networks and information systems. It is important to stress that this also relates to the obligation to deal with a cyber security incident or cooperate with the relevant authorities in dealing with a reported cyber security incident. The providers of basic services and digital services should pay due attention to the obligations because failure to comply with the CSA may lead to the imposition of considerable fines.

For more information

JUDr. Jozef Bannert
Partner in Slovakia
jozef.bannert@sp-chsh.sk
Tel: +421 2 2064 8580

CHSHCEE NEWSLETTER

Media owner and publisher: **Cerha Hempel Spiegelfeld Hlawati Rechtsanwälte GmbH**, Parkring 2, A-1010 Vienna | Tel: +43 1 514 350 Fax: +43 1 514 35 35 | email: office@chsh.com | Although this newsletter was created with the greatest of care, we nevertheless do not accept any responsibility whatsoever for its content being correct, complete or up to date. | **Visit us at www.chsh.com** | **CHSH** Austria Belarus Bulgaria Czech Republic Hungary Romania Slovak Republic

CHSH Cerha Hempel Spiegelfeld Hlawati Rechtsanwälte GmbH