IP/IT NEWSTICKER IN CEE/SEE

AUSTRIA

Trademark amendments to the Austrian Trademark Protection Act ("Markenschutzgesetz")

By implementing the Trademark-Directive EU 2015/2436 and the Regulation EU 2017/1001 on the European Union trademark the Austrian legislators have adapted the Austrian Trademark Protection Act (MSchG) to the European requirements. The amendments are effective since 1 September 2017 in most parts and bring numerous facilitations for the application process.

New Calculation method of the protection period starting 1.9.2018

So far the trademark protection begins with the day of the registration in the trademark register and expires ten years after the end of the month of the registration of the trademark. With the implementation of the new regulation, the ten year protection period starts with the day the trademark was filed. The new calculation method of the protection period applies without exception to all trademarks in Austria, thus to registered and filed trademarks.

Option of division of the filed or registered trademark

Since 1.9.2017, §§ 23a ff MSchG provides the option to divide the application/registration of a trademark in two or more applications/registrations, which have the same priority rights as the basic application/registration. Such applications for division might be interesting during the process of filing for trademark protection, in which the patent office has concerns about the distinctiveness of parts of the trademark. The division will be available for international trademarks as of 1.2.2019. Applications must be filed at the Austrian Patent Office.

Certification marks on a national level

As a counterpart to the EU Certification Mark a national certification mark was implemented. The certification mark is capable to distinguish goods or services in respect of material, mode of manufacture of goods or performance of services, quality, accuracy or other characteristics, from uncertified products. Explicitly excluded by the protection of the certification mark is the indication of the geographical origin.

CZECH REPUBLIC

Who owns the copyrights for the iconic Czech cartoon character Krteček?

When Zdeněk Miller, the illustrator of the most loved Czech character, a Little Mole, died in 2011, a bitter dispute over the licence to his works flared up. The licence agreement entered into between Mr. Miller and his granddaughter shortly before his death was challenged by the administrator of the illustrator's copyrights. In October 2017, the verdict of the Municipal Court in Prague proclaimed the licence agreement to be invalid. However, the decision is not final yet, as Miller's granddaughter appealed to the Czech Supreme Court. Profits from the Little Mole copyrights are estimated to millions of crowns a year.

Spreading of Cyber Security Obligations

The functionality of essential parts of the society shall be protected from cyber-attacks by the amended Cyber Security Act as of August 2017. The amendment enlarges the scope of subjects which are to secure their cyber networks in a better way, to monitor and to report any attacks or attempts for them. Subjects obliged by this amendment are the ones securing key social and economic purposes in key departments, e. g. medical care, energetics, drinking water. On top of that, the amendment establishes the National Office for Cyber and Information Security which was decided to be built up in Brno between years 2018 – 2023.

Personal data vs property protection

In 2012, an e-bike was stolen from a shop of ekolo.cz whilst the act itself was caught on a camera. After that, the company shared the photo of a suspected thief on their social media account with a call to help finding him. It was just after that the company informed the police and handed the camera records over to them.

The Czech Office for the Personal Data Protection (the Office) imposed a fine on the company for unlawful personal data usage. The company filed an action against the Office to the court as they found the fine unjust reasoning that the Personal Data Protection Act allows an exception from personal data processing rules when protection of other personal rights is triggered.

The case ended up before the Czech Constitutional Court which ruled that the fine was eligible. The Constitutional Court stated that the company's action, i.e. sharing the photo publicly, was not absolutely necessary as the purpose (i.e. the protection of the property right) could had been fulfilled differently, for instance by leaving the recording to the police.

However, after the decision of the Constitutional Court, the Office published an official statement contradicting the original resolution. In particular the Office stated that it would not impose such a fine again as "everyone should be allowed to appropriately

demand their statutorily recognized rights if they had been breached".

Shared economics in Czechia

Shared economics has reached other changing points in the Czech Republic. In October, the Financial Administration Office issued a statement in which it declared that Airbnb should be viewed not as a lease, but as a systematic economic activity which falls under more strict criteria. Then, the service is subject to a different tax system and persons providing it should have a trade license. Moreover, if the annual turnover of this activity exceeds CZK 1,000,000.00 (approx. EUR 38,400), the owner needs to register as a VAT payer and might be required to record sales in accordance with the Electronic Record of Sales Act. Due to this growing complexity, Prague launched a website, both in Czech and English, which offers the summary of rules both for the providers of the service and its recipients.

On the other hand, in Brno, second largest city in the Czech Republic, a more positive change for the shared economics came. The court cancelled the interim measure by which the Uber service had been prohibited in the city for several months.

POLAND

Lemon lost to Lennon

In March 2017 a lemonade manufacturer from Katowice received a pre-litigation cease and desist infringement letter regarding its "John Lemon" trademark. A few days later the company was served a notice of lawsuit letter with a scheduled hearing date before a Dutch court in The Hague. The trademark 'John Lemon' was registered by the lemonade manufacturer in the European Union Intellectual Property Office (EUIPO) as early as in 2014. The party initiating the infringement claim, Yoko Ono, is the owner of a trademark with the forename and last name of the dead artist, John Lennon, which had been registered in the EUIPO in December 2016. The Polish lemonade manufacturer decided to settle and one must ask why? It held all the rights to a trademark which was registered much earlier. The company's position should have been secure. Part of the answer surely must have been the high costs of court proceedings in the court in The Hague. Another consideration must have been that Yoko Ono's lawyers demanded that the company should immediately stop the production and sales of the lemonade sold under the John Lemon brand. If they would have succeeded this order would have been effective throughout the entire European Economic Area leaving the manufacturer and its distributors with full stocks. Settlement avoided these risks. The lemonade manufacturer decided to rebrand the product "On Lemon".

Data protection regulations

Drafts of the new Polish Personal Data Protection Act and Provisions Implementing the

Personal Data Protection Act were published on 14 September 2017. The Amending Act Draft amends 133 sectoral acts. The proposed regulations are to ensure the successful implementation of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016. Both drafts were subject to social consultations. The official results of consultation are expected soon as are the final version of acts.

National Cyber Security Act

In early November the Government Legislation Centre published a draft of the National Cyber Security Act. The draft was created in connection with the need to implement the Directive of the European Parliament and of the Council (EU) concerning measures for a high common level of security of network and information systems across the Union (Directive 2016/1148). A national cyber security system is to be established to ensure the security of information systems used for the provision of key services and digital services. The security system will include key service providers in many sectors, including banking, energy, transport, healthcare and digital infrastructure. Providers will be obliged to assess the risks associated with cyber security, implement security measures and report serious incidents. The draft law has been submitted for inter-ministerial consideration.

SERBIA

New Personal Data Protection Law announced

On 14 November 2017, Ministry of Justice of the Republic of Serbia announced that the work on the draft of the new Personal Data Protection Law has been finished and that the public debate shall be soon opened. According to this announcement the new law should replace the current one that was adopted more than eight years ago and which is outdated and lacks numerous provisions that such law must include. The Ministry emphasized that the new law should provide for an efficient mechanism to protect citizens and to enable international transfer of personal data.

The draft of the new Personal Data Protection Law has not been made public so far so it is yet to be seen whether and to what extent the Ministry had taken into account the rules envisaged under the EU General Data Protection Regulation.

SLOVENIA

Published new drafts: Data Protection Act and Act on Information Security

At the beginning of October, the Ministry of Justice published a draft of the new Personal Data Protection Act that, together with the GDPR, will provide a new data protection legal framework applicable as of 25 May 2018. The new draft Personal Data Protection Act has been subject to public consultation until 13 November 2017.

Since the GDPR is directly applicable, the new Data Protection Act regulates only certain specific areas of data protection (i.e. areas that were left to national legislators by the opening clauses of GDPR). In this regard, the new Data Protection Act provides for requirements for inter alia child's consent, appointment of the data protection officer, retention period and the implementation of video surveillance and biometrical measures.

Data controllers are urged to use the remaining months to get closely familiar with the provisions of the GDPR and the new Data Protection Act and implement all required measures. Non-compliance with the GDPR will be sanctioned with fines up to EUR 20,000,000 or 4 % of worldwide revenue, whichever larger.

Furthermore, the Ministry of Public Administration has prepared a draft of the Act on Information Security transposing the NIS Directive (EU) 2016/1148 into Slovenian legislation. The Act on Information Security provides for measures for attainment of high level of security for essential networks and information systems.

The providers of essential services and digital service providers must comply with two main obligations – implementation of minimal security requirements and notification of incidents. The providers of essential services are, in particular, entities that are engaged in industries referred to in Article 5 of the Act on Information Security (e.g. energy, digital infrastructure, health and banking).

Managing E-Mail Accounts of Former Employees

As part of data security measures, employers are required to have in place a policy for administration of e-mails of their employees. Such policy should also set out the rules for management of e-mails after the employment has terminated.

As already outlined in the guidelines of the Information Commissioner (Informacijski pooblaščenec), the employee must be given a chance to copy and/or delete e-mails of private nature before leaving his job after the employment relationship has terminated. The e-mail account of the former employee must not be left active or may not be redirected to the e-mail account of another employee. However, the employer and employee may agree that the e-mail account remains active for a specific period after

the termination of the employment.

In the event of termination of employment, the Information Commissioner recommended a practice where the e-mail account of a former employee is deactivated as soon as possible and automatic replies are set up, which inform the recipient that the e-mail account has been deactivated and refer them to a new addressee (more in the non-binding Opinion of the Information Commissioner no. 0712-1/2017/1538, dated 3 August 2017).

E-Mailing Contact Persons

The latest amendment of the Electronic Communications Act (Zakon o elektronskih komunikacijah; Official Gazette of RS, no. 109/12, as amended) has specified a new exemption with regard to the opt-in consent for electronic marketing communication.

According to the new Article 158 of the Electronic Communications Act, a natural person or a legal entity may use e-mail address of natural persons, if published by the company as its contact e-mail address. The rationale is that the business interest (i.e. conducting business with clients) prevails over the private interest and in such cases the e-mail of the employee is deemed as being an e-mail of the legal entity.

UKRAINE

Legal framework for cybersecurity

Ukraine continues to take actions to increase cyber security. Legal framework for cybersecurity is introduced by the recently adopted Law of Ukraine "On Key Principles of Ensuring Cybersecurity of Ukraine". Proposals of experts from NATO and the EU were incorporated into the text of the law.

In the first place the Law harmonizes the relevant terminology of the Ukrainian law (e.g. cybercrime, cyber-attack, cyber protection) with the EU legislation. Secondly, it provides legal ground for protection of interests of individuals, companies and the state, defines competence of state bodies, organizations, individuals and companies, and provides for basic principles of coordination of their activities in the area of cyber security. Namely, the State Service of Special Communication and Information Protection of Ukraine, the National Police, the State Security Service, the Defence Ministry, the General Staff of the Armed Forces of Ukraine, the intelligence services and the National Bank are the state bodies responsible for cybersecurity of Ukraine.

The Law will not be used as an excuse for censorship; therefore the following will be out of its scope: services and relations related to the content of information, processed in telecommunication or technological networks, social media, blog platforms, video hosting services and similar online resources as well as private networks.

Besides, the Law defines the main objects of cybersecurity constituting the critical infrastructure of the country, such as energy, chemical, transportation, information and communication technologies, electronic communication companies, banking and financial institutions, and companies having potentially dangerous production or technologies. The principles of the classification of companies as critical infrastructure objects, requirements to their cybersecurity, independent audit of their informational security will be defined in by-laws. The requirements to audit must be elaborated based on international standards as well as standards of the NATO and EU.

Use of Blockchain technology in eGovernment

In 2017 the Ukrainian government officially confirmed its intention to use block chain technology in order to keep the state registers. This would allow avoiding abuse of access by different parties, including state officials, to the electronic registers and illegal change of information contained therein, which occurred during the past years due to the liberalization of legislation on state registers. Similar projects have been implemented in Sweden, Estonia and Georgia.

In April 2017 Bitfury Group was chosen as a contractor for the implementation of the technological solutions. On 3 October 2017 a beta version of the Ukraine's State Land Cadastre on blockchain was rolled out. This project is implemented in cooperation with Transparency International, the Ministry of Agricultural Policy and e-Gov Agency of Ukraine. It is anticipated that land related transactions will also be performed with the use of blockchain at the later stages. It is also expected that in 2018 the Immovable Property Register of Ukraine will be maintained with the use of block-chain technology as the next stage.

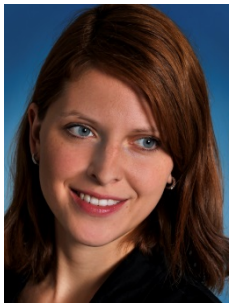
The use of blockchain and crypto currencies in Ukraine urged the Members of Parliament of Ukraine to introduce a legal framework for these activities. Thus, two draft laws have been submitted to the Parliament. The experts in the area are not satisfied with the regulation suggested by these drafts, thus another draft law will be developed by a working group which also includes the EBRD.

About WOLF THEISS

Wolf Theiss is one of the leading law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We have built our reputation on a combination of unrivalled local knowledge and strong international capability. We opened our first office in Vienna almost 60 years ago. Our team now brings together over 340 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region.

For more information about our services, please contact:

Georg Kresbach
Partner
georg.kresbach@wolftheiss.com
T: +43 1 51510 5090



Katerina Kulhankova
Associate
katerina.kulhankova@wolftheiss.com
T: +420 234 765 252