HAVEL & PARTNERS

CONNECTED THROUGH SUCCESS

PRAGUE | BRNO | OSTRAVA | BRATISLAVA

EU Legal News

II/2018

Strategic thinking I Individual approach I Excellent legal team I Long-term partnership

The Largest Czech-Slovak Law Firm with an International Approach

The most successful law firm in the Czech Republic and Slovakia based on the number of nominations and awards in all years of the competition

Law Firm of The Year

Best Law Firm of the Year in the Czech Republic (2017, 2018)

GLOBAL AWARDS CorporateLiveWire 2018

Czech Law Firm of the Year (2011–2012, 2014–2018)

WHO'S WHO LEGAL WWL

No. 1 legal advisor according to the number of M&A deals in the Czech Republic

EMIS (2016–2017)

Mergermarket An Acuris company (2009–2017)

M&A Law Firm of the Year in the Czech Republic and Slovakia (2016)

CorporateINTL GLOBAL AWARDS WINNER 2016

Summary

Introduction

Dear Clients and Business Friends,

Let us present you with the summer issue of our EU Legal News, which we have been using for a number of years to update you on key changes and new trends in the EU law and the way they are reflected in the Czech national law.

We keep you posted on some burning personal data protection topics even after 25 May 2018 when the key EU regulation, better known as the GDPR, came into effect. In this issue, we focus on the institution of consent as a legal title used in connection with personal data protection, which has, in our opinion, been overused by data controllers, thus posing certain risks. We therefore summarise and comment on the corresponding recommendations and notes of the European Personal Data Protection Board (formerly the Article 29 Working Party). Apart from the GDPR, we also focus on another much-debated topic linked to privacy protection – the draft ePrivacy regulation. After the GDPR came into effect, a number of entities became obliged to designate their data protection officer. This is why we also introduce to our readers Fair Data Professionals a.s., our sister company, which provides data protection officer services. The privacy topic is also closely linked to the draft Privacy Code of Conduct in mHealth applications, which we analyse in one of our articles and which should become the focus of attention primarily by mHealth application developers and device operators.

We also focus on two new draft directives dealing with the use of digital tools and technology in corporate law. The drafts are part of a long-term EU strategy to support namely SMEs and start-ups in their effort to expand the business to other member states by means of cross-border transformations.

Brexit will be one of the top issues in the months to follow. In this EU Legal News issue, we bring more information on the impact Brexit will have on the protection of IP rights.

Another key topic in this issue is the consumer law, which we address in two articles. One of them focuses on the New Deal for Consumers, a policy aimed at boosting consumers’ rights online and increasing fines for infringements of consumer rights and also introducing other tools to streamline corresponding enforcement mechanisms. The other article addresses a new regulation governing the performance of competent national authorities responsible for the surveillance of consumer protection rules and their cooperation when enforcing consumer rights EU-wide.

Finally, this issue, like all the previous ones, also brings you a competition law update prepared by our award-winning cartel team.

I hope that you will find this EU Legal News inspirational and that you will enjoy the rest of the summer.

Robert Nešpůrek

Consent in the light of GDPR

*The concept of consent to the processing of personal data, as applied to date under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "**Directive**"), has undergone notable development with the new regulation taking effect. Unlike the Directive, the new General Data Protection Regulation 2016/679 (the "**Regulation**" or "**GDPR**") stipulates in great detail the requirements for receiving and demonstrating the data subject's valid consent to the processing of personal data. Further we explain what it means for the practical use of apparently the most overused legal ground for processing personal data.*

Consent as legal ground for processing personal data

While consent under the previous legal regulation used to be understood as the fundamental legal ground for processing personal data, which was implied by the "philosophy and concept of the entire legal regulation of personal data protection",[1] it ranks *pari passu* with other legal grounds for processing under the current legal regulation. Consent is thus one of the six legal grounds for processing personal data specified by Article 6 of the Regulation, and even though it is listed first before other legal grounds, it may not be applied for the purpose of processing based on a different legal ground. For instance, such legal grounds often include performance of statutory duties, performance of a contract and others arising from Article 6(1) of the GDPR.

Before initiating any processing operation, the controller must specify one of the legal grounds for and the purpose of the processing, assessing whether consent is a suitable legal ground or if there is any other legal ground for the intended processing. Consent may only be a suitable legal ground in situations in which natural persons as data subjects can properly control their data and have a realistic choice with regard to the given conditions for the processing: the principle of freedom and ability to withdraw given consent. In the controller's view, consent may be the ground least suited for processing personal data as it enables data subjects to have lasting control over whether and for how long their personal data will be processed.

Consequences of invalid consent

One of the objectives of the new regulation detailing the giving of consent to the processing of personal data is to prevent the spreading of the current incorrect practice of obtaining consent when there is another lawful ground for the processing, i.e. when data subjects are asked to give their consent by signature for the possibility of entering into a contract; or controllers did not sufficiently fulfil their duty to inform. The supervisory authority may assess the incorrect or unjustified demanding of consent, the obtaining of consent under not particularly "free" circumstances or without provision of appropriate information as a violation of the basic principles for processing, including the data subjects' rights, within the meaning of Article 83(5)(a) and (b) of the Regulation. In relation to their processing activity, controllers should therefore re-evaluate each and every purpose of processing personal data, for which they have required the data subject's consent to date, and abandon the practice of demanding consent if there is another legal ground for processing.

In particular, this will include performance of contractual or statutory obligations or the exercising of legitimate interests, i.e. processing personal data using a camera system under certain conditions. On the other hand, it is completely illogical to demand consent of the other party for the purpose of a contract because if the other party withdraws its consent, the data must be erased. Potentially, the purpose for processing should be changed as these data will still be necessary for further performance and possibly enforcement of the contract and may not be simply erased upon withdrawal of the other's party consent.

[1] *Kučerová, Nováková, Foldová, Nonnemann, Pospíšil. Zákon o ochraně osobních údajů (Personal Data Protection Act), 1st ed., C. H. Beck.*

Another objective of the Regulation and effort to change the rather frequent incorrect practice is to eradicate the incorporation of consent in the text of contracts, in general terms and conditions or other juridical acts not enabling data subjects to express their will and give their consent in a valid way. Giving consent to the processing of personal data is a unilateral juridical act that must reflect the acting person's will and enable a free choice in this respect in relation to the handling of personal data. The Regulation does not allow a complicated or unintelligible wording of the consent text or such a position that makes the consent text hard to notice. The GDPR expressly provides that if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

Elements of valid consent

Consent may be considered as given in a valid way if it meets all the requirements set forth by the Regulation. If the consent does not fully comply with the GDPR, the ground is invalid and the controller's processing activity becomes unlawful. The controller must be able to demonstrate the given consent for the entire duration of the processing.

The Regulation stipulates that consent is *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*. Besides the aforementioned definition of consent stipulated in Article 4 (11), the Regulation provides additional guidance in Article 7 and Recitals 32, 33, 42 and 43 on the controller's procedure to obtain valid consent. The definition particularly implies that the data subject may not be forced by the controller to give his or her consent as consent must be given as a voluntary expression of the data subject's will.

Freedom of consent

The term "free" indicates that data subjects must have a real choice in terms of processing personal data. The Regulation provides for a general rule under which consent is not a valid lawful ground for processing if the data subject does not really have a choice and is forced in any way to give his or her consent or if failure to give his or her consent may cause adverse effects to the data subject. If giving consent is, for instance, part of terms and conditions that cannot be changed, the consent is presumed as not freely given. Similarly, consent is regarded as not freely given if the data subject is unable to refuse or withdraw consent without unjustified detriment.

If consent is to be regarded as freely given, it should not be used to process personal data where there is a clear imbalance between the data subject and the controller. This is particularly the case where the controller is the data subject's employer or a public authority as the data subject is unlikely to have freely given his or her consent in such circumstances, having no other real choices but to accept the stipulated processing conditions. It does not mean that employers or public authorities can never rely on consent as a legal ground for processing but such consent may be regarded as freely given in specific situations only. Furthermore, consent is presumed not to be freely given if it does not allow separate consent to be given to each different personal data processing operation (purpose) despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance. Such a case requires what we call granularity of consent, meaning that it must be possible to give consent for individual specific processing purposes. The following criteria are important in assessing whether consent is specific enough: (i) stipulating the purpose as protection against adding further processing purposes, (ii) granularity of requests for consent and (iii) clear distinction between information regarding the consent and information about other facts.

Granularity and formal requirements of consent

Consent must always be given for a specific, explicit and legitimate processing purpose, which the data subject must know in advance. In line with the purpose limitation principle, consent may only cover several processing operations if these operations serve the same purpose. This requirement aims in particular at protecting the data subject against the gradual extension of processing purposes and thus gradual loss of control over personal data processing after he or she has already given his or her consent. The second requirement – the requirement of granularity – is closely connected with the condition of freedom of consent, meaning that the controller must enable the data subject to have a choice in giving separate consent for each purpose. Last, the controller should provide specific information on the consequences of giving consent along with the request for consent in compliance with the principle of transparency so that the data subject can assess all circumstances of the processing that might influence his or her choice.

If the data subject is, for instance, requested to give his or her consent to the processing of personal data without the controller stating a specific purpose for which the consent is requested, or the consent is requested for a purpose where there is another lawful basis, such request breaches the Regulation and the data subject may defend himself or herself by lodging a complaint with the Office for the Protection of Personal Data. The said procedure violates the transparency principle and the controller's duties set forth in Articles 5, 7 and 12 of the GDPR.

Last but not least, the Regulation emphasizes that in terms of formal requirements, consent is to be given as the data subject's statement or clear affirmative act, indicating that consent must be given by acting to make it clear that the data subject has given his or her consent for the specific purpose. Consent may be given by a written or oral statement or potentially by electronic means. The controller should bear in mind that, if needed, it must produce evidence before a supervisory authority that the controller has obtained the consent; that is why oral statements mostly cannot be regarded as suitable for obtaining consent. In any case, consent must not be obtained by the same act by which a contract is made or terms and conditions are accepted. While the Regulation is effective, pre-ticked boxes implying opt-outs may not be used as they are in breach of GDPR requirements.

Withdrawal of consent

Articles and recitals of the GDPR on the withdrawal of consent are based on interpretations of the opinions of the WP29 working party, which is replaced by the European Data Protection Board (EDPB) as of the date of effect of the Regulation. Article 7 of the Regulation explicitly stipulates that the data subject shall have the right to withdraw his or her consent at any time and it shall be as easy to withdraw as to give consent. The GDPR does not provide that consent must always be given and withdrawn in the same manner, but the controller may in no way hinder or condition the data subject's right to withdraw consent and must inform the data subject of this right before the processing as such. Provisions of the Regulation imply, however, that consent given via electronic means, e.g. through one mouse-click or keystroke, the data subject must be able to withdraw that consent equally as easily. If consent is obtained via a specific user interface, e.g. through a mobile application, user account, etc., the data subject must be able to withdraw consent via the same electronic interface. It might be an excessive effort for the data subject if he or she had to switch the interface only for the purpose of consent withdrawal. We must also bear in mind that the data subject must be able to withdraw consent without unjustified detriment. This is connected with the condition that withdrawal of consent must be free of charge.

The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Generally, the withdrawal of consent is without prejudice to all processing operations carried out based on that consent in compliance with the Regulation before its withdrawal. However, the controller must terminate all affected processing activities and erase or anonymize the personal data if there is no other lawful ground for processing them such as the legal duty to archive the data. In other words, in the event of consent withdrawal, the controller must stop processing the personal data only for the purposes defined in the consent and is not obliged to delete these data if they are necessary for the performance of a contract, for example. The data subject must be informed of any change of a legal ground for the processing in compliance with the duty to inform under Articles 13 and 14 of the Regulation as well as the general principle of transparency.

Renewal of consent in relation to the transition to GDPR

After the Regulation came into effect, the controller may only rely on consent that had already been given in line with the conditions for obtaining it under the Regulation. If consent was not obtained in accordance with these conditions, it will not constitute a lawful ground for processing personal data. Consents already given, including those which were given as required by the Regulation, naturally degrade over time, affecting the time of validity of already given consent. In order to assess whether the term of validity of consent has expired, the controller must consider *inter alia* reasonable expectations of the data subject at the time of giving the consent.

According to the EDPB, consent obtained in the past remains valid if it complies with the conditions stipulated in the GDPR. However, in case of meeting the duty to inform – which is one of the basic requirements for consent to be valid – as the conditions of the Regulation are broader, there is practically no consent given in the past that could meet the conditions of the GDPR. National regulations of Member States differed in the scope of information that had to be provided. If the controller sufficiently fulfilled the duty specified in Sections 5(4) and 11 of Act No. 101/2000 Sb., on the protection of personal data and on the amendment of some laws, as amended, it would not be desirable in the context of the retrospective application of the Regulation that the controller should obtain new consent. These conclusions can be implied from the fact that "addressees" of the later legislation could neither anticipate nor observe it. On the other hand, controllers had a two-year term provided for by the GDPR to familiarize themselves with the provisions of the GDPR and adjust the processing to the new conditions. Although the market practice is not the same – some controllers have decided to obtain new/confirm existing consents while some are fulfilling the duty to inform – we believe that already given consents need not be renewed if the processing of personal data fully complied with the national regulation and recommendations of the Office for Personal Data Protection. If the only thing that is not in compliance with the GDPR is the incomplete fulfilment of the duty to inform, it should be sufficient to hold an effective campaign informing data subjects who were not informed in the past about the processing aspects and their rights.

Conclusion

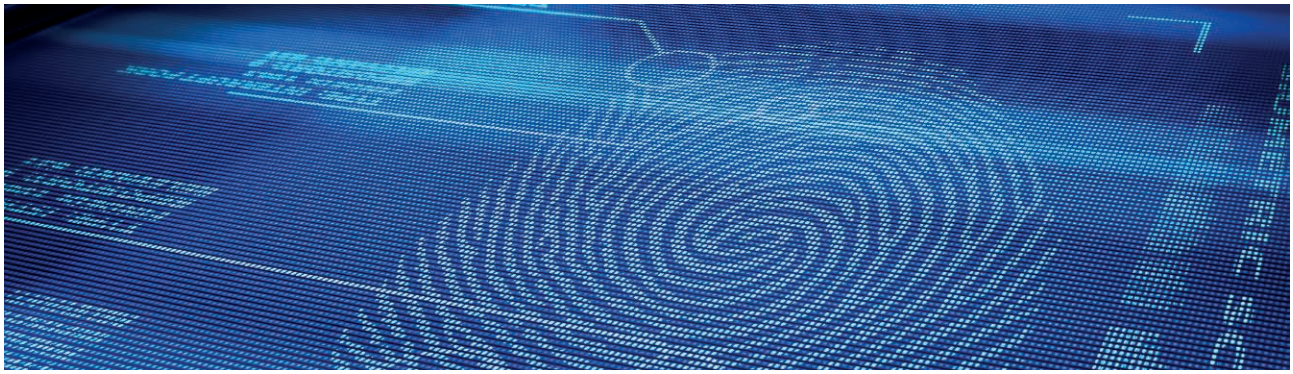
The Regulation toughens the mechanism of obtaining consent, introducing several new requirements for controllers to adjust their established procedures. If the processing of personal data has been based on consent obtained under Act No. 101/2000 Sb., on the protection of personal data and on the amendment of some laws, or Directive 95/46/EC, it is not necessary to request the data subjects again to give consent if such it complies with the requirements of the GDPR, and the controller may keep processing personal data after the Regulation became effective. What is particularly problematic in practice is the aforesaid conditionality of consent or its integration in general terms and conditions; such cases require a completely new set-up and new consents. If controllers collect new consents, they must do so fairly and in a transparent manner, especially justifying the collection by stating a specific purpose for processing personal data.

Authors:
Robert Nešpůrek | *Partner*
Jaroslav Šuchman | *Senior Associate*
Ján Jaroš | *Junior Associate*



We are the most attractive employer among law firms in the Czech Republic for the fourth consecutive year

Our law firm was voted the most attractive employer among law firms in the Czech Republic and ranked first in the TOP Employer Awards for the fourth consecutive year again in 2018. What's more, the best-performing law students placed our law firm first in the Lawyer category for the second time, a category dominated by international law firms in previous years. "*We highly appreciate the fact that the forthcoming generation of lawyers sees us as a prestigious and attractive employer. When I was a student, the ultimate goal of most students was to work for an international company. I'm glad to hear that we have managed to reverse this long-term trend, even among elite students who gave us the biggest number of preferential votes this year again*," Jaroslav Havel, the law firm's managing partner, comments on the awarded recognition.



DPOaaS: Outsourcing of DPO Services

Designation of data protection officer (DPO) is one of the most important new obligations for data controllers and processors under the General Data Protection Regulation (GDPR).

As DPO services may be provided also by a third party, many organisations consider outsourcing these activities. HAVEL & PARTNERS has years of experience advising on personal data protection and IT, so it decided to offer DPO services and further long-term support in the field of GDPR compliance in cooperation with **FairData Professionals a. s.**, a new company with full access to the capacities, know-how and experience of the law firm.

Offered services

- Outsourcing of the DPO services for controllers and processors of personal data that are obligated to appoint a DPO or decide voluntarily to appoint a DPO
- Professional support to DPOs appointed internally from among staff members and local support to foreign DPOs (designated e.g. on a group level)
- Acting as a quasi-DPO – an unofficial "officer" providing support to the organisation and monitoring its compliance with data processing requirements under the GDPR
- Further support and advice on data security and compliance

Advantages of our services

- **Stability and professionalism:** we have more than 12 years of expertise in the field of personal data protection and continue to build a strong and stable team with advantages you can benefit from in cooperating with a reliable partner on a long-term basis
- **Relevance:** we work in many sectors and know our clients' needs; GDPR rules should be applied proportionately to cover risks while still allowing business to be done
- **Increasing value:** we perceive the correct application of the GDPR as an opportunity to apply a modern approach to the use of data in business and to enhance reputation
- **Risk-oriented:** the most conservative solution is not always the best solution
- **Combined expertise:** our teams combine legal and IT expertise
- **Synergies:** DPO-related costs may not be marginal, but our service will take advantage of economies of scale
- **Efficiency:** thanks to detailed knowledge of your organisation, we can more efficiently assess the changes you are going to implement in the field of personal data processing
- **Prevention:** we will notify you of changes in legal regulations, new case-law or developments in the application of laws and provide you with company-specific change recommendations
- **Long-term support:** it is our vision to become one of the major providers of this type of service offering reliable long-term support to our clients

Robert Nešpůrek | *Partner* | *T: +420 255 000 949* | *E: robert.nespurek@havelpartners.cz*
Richard Otevřel | *Counsel* | *T: +420 255 000 943* | *E: richard.otevrel@havelpartners.cz*

"e-privacy Regulation": What changes will affect cookies?

*A new regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications (Regulation on Privacy and Electronic Communications) ("**Regulation**") is supposed to bring clearer and simpler rules for obtaining and dealing with cookie consent. The Regulation should repeal Directive 2002/58/EC[1], known as the 'cookie law', and, among other things, should contain new rules for granting consent and for notices related to the use of cookies and other identifiers stored on end-user devices.*

Regulation, GDPR and further legislative development

Like the General Data Protection Regulation[2] ("**GDPR**"), the Regulation is part of the EU strategy to complete the Digital Single Market, i.e. a set of regulations laying down the free movement of data. In relation to the GDPR, it is a special regulation as it only applies to a specific area of personal data protection. As such, the Regulation has application priority over the GDPR in the event of discrepancies. In the alternative, matters not laid down in the Regulation will be subject to the GDPR (such as requirements for expressing consent by end users).

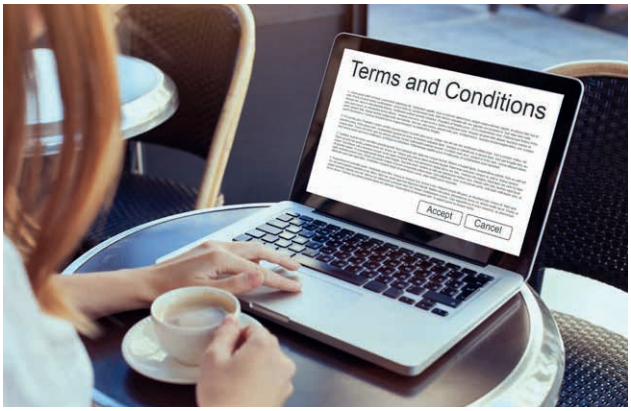
Although the Regulation was intended to become applicable on the same date as the GDPR, i.e. 25 May 2018, the legislative process was longer than expected and the final dates of validity and effect remain unclear, as well as for the definitive version of the Regulation. On 26 October 2017, the European Parliament ("**Parliament**") adopted a position on the Regulation proposal submitted by the European Commission ("**Commission**"). The proposal will now enter into "trialogue" negotiations in which representatives of the Commission, the Council and the Parliament will try to reach an agreement. Therefore, the text of the Regulation may change. As a result, this article discusses the Regulation proposal in its latest version as adopted by the Parliament on 26 October 2017.

The Regulation is to constitute EU-wide regulation of the right to privacy in electronic communications (including, without limitation, in respect of the internet, unsolicited emails, direct marketing, the internet of things and other related areas). The entities that will be most affected by the Regulation are mainly software (browser) developers and information society service providers.

This article analyses that part of the Regulation that affects nearly every website operator and, in fact, every internet user – cookie issues.

New rules for providing information to users and for cookie consent

The use of cookies, which allow end devices to be unambiguously recognised, is currently one of the most important and much discussed topics in internet privacy protection. Today, in Czech legislation, cookies are governed by Act No. 127/2005 Sb., on Electronic Communications. However, the practice (such as the use of cookie banners) is not wholly consistent. The Czech competition authority (Office for Competition Protection) itself has recently revised its approach to the duty to obtain user consent. In its recommendation[3] published on its website, the Czech competition authority states that cookie consent may be given through browser settings. The Regulation should presumably terminate the use of such banners for good.



The proposed change in cookie rules promises costs savings for information society service providers as it will bring the end of cookie banners, greater user-friendliness and perhaps more transparency in respect of cookie consent. On the other hand, the duty to obtain cookie consent for a large number of purposes may result in increased costs and the loss of a part of user databases for targeted advertising and other profit-making functions of websites.

In general, the Regulation proposal prohibits the use of the capabilities of end users' equipment for processing,

[1] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).*
[2] *Regulation 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 (General Data Protection Regulation).*
[3] *https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=29966&n=cookies%2Da%2Dgdpr.*

storing and collecting information from them, including software and hardware information. Nevertheless, the Regulation permits exceptions to this rule, such as for the purpose of carrying out a transmission in the electronic communications network or for providing an information society service required by an end user for a necessary period (such as to adjust the screen size or remember shopping cart items). Furthermore, this can include the necessity to obtain information about the technical quality or efficiency of the information society service provided or the end device's functionality, the necessity of privacy protection, security or safety of the end user, or the grant of consent (as defined in the GDPR[4]) by the end user.

As a result, consent to the use of cookies should not be required for the technical storage of or access to information that is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end user. This may include the use of cookies and other identifiers for the duration of a single established session on a website to keep track of the end user's input when filling in online forms over several pages.

If accompanied by appropriate privacy protection measures, such techniques can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Such measuring implies that the result of processing is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person. The no-consent regime should also apply to checks on configuration carried out by information society providers to provide the service in compliance with the end user's settings or the mere logging of the fact that the end user's device is unable to receive content requested by the end user.

Cookie settings in browsers and other software

The option to allow cookies should be provided in general settings upon installation of the browser (or operating system or communication application). Third-party cookies and cross-domain tracking will have to be disabled in basic settings, and the option should at all times be easily available to the user in the browser settings.

Nevertheless, browsers should allow end users to consent to cookies or other information stored in their end devices (although the GDPR prohibits any interference) and vice versa. On a specific page, browsers should allow users to grant separate consent to online tracking. In addition, browsers should allow users to set, for example, whether any software may be run or whether a website may collect information about the user's location or access specific hardware, such as a web camera or a microphone.

Besides the above, browser providers will be obliged to offer sufficiently detailed possibilities for giving consent to each individual category of purposes. These categories include at least tracking for commercial purposes or for direct marketing (behavioural targeting), for personalised content purposes, tracking localisation data, providing personal data to third parties (including unique identifiers that are equivalent to personal data available to third parties) or for analytical purposes.

Conclusion

If the Regulation is enacted as is, cookies may not be used without the active consent of the end user for purposes other than for ensuring the capabilities necessary for the correct functioning of websites. In addition, if most end users opt for "reject third-party cookies" settings based on the above rules for keeping default settings, it may become more difficult for online targeted advertisers to obtain consent outside the browser settings, i.e. by requesting end users directly. In consequence, these changes will have to be reflected by website operators in their cookie policies that will not comply with the Regulation.

Despite the fact that information society service providers may achieve savings resulting from the elimination of cookie banners for essential purposes, the obligation to obtain consent for a number of other purposes including marketing may lead to increased costs and the loss of a large part of user databases for targeted advertising and other profit-making website functions.

[4] *Consent (see the definition in Article 4(11) of the GDPR) is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. It is an active and voluntary manifestation of the data subject's will to which the data subject must not be forced.*

Authors:
Robert Nešpůrek | *Partner*
Petr Bratský | *Associate*
Vít Ferfecki | *Junior Associate*



European Commission's Initiative: Access to safe and high-quality digital services in healthcare

*In 2016, the European Commission ("**Commission**") published a draft Code of Conduct on privacy for mHealth apps ("**Code**").[1] Although prepared when the Data Protection Directive[2] was in force, the Code is to comprise a practical guide for mHealth app developers governed by the General Data Protection Regulation (Regulation (EU)2016/679, "**GDPR**"). Due to widespread criticism from the working party set up under Article 29 of the Data Protection Directive ("**WP29**") a year later, the Code has not been adopted to date. Yet the Code opens up a number of topics in privacy protection that merit the attention of healthcare facility operators and mHealth app developers.*

mHealth – current trend in healthcare

The term "*mHealth*" or "*mobile health*" refers to the use of mobile and wireless technologies, such as mobile phones and tablets or portable devices such as smart watches, for the purpose of providing healthcare services and information and collecting data concerning health.

The impact of *mHealth* is not negligible: according to the International Telecommunications Union, there were more than 7 billion mobile phones all over the world in 2015, out of which more than 70% were registered in low- and middle-income economies.[3] As a result, *mHealth* applications and mobile solutions (from text messages to comprehensive smart phone applications) are becoming more and more accessible. According to the World Health Organisation, digital health technologies have the potential to significantly change the way people will communicate with national health systems; *mHealth* applications increase the quality and coverage of care, increase access to health information as well as promote positive changes in health behaviours to prevent the onset of acute and chronic diseases.[4] However, as established by the Commission, there is a lack of trust in *mHealth* applications among the users in terms of privacy protection.[5]

Applicability and essential pillars of the Code

Not only for the reasons outlined above is the Commission trying to provide *mHealth* app operators and developers with comprehensible instructions as to how to apply EU data protection laws in respect of the specific features of *mHealth* applications. However, the Code expressly excludes from its applicability any overlaps among other areas of regulation, such as medical devices, consumer protection and e-commerce. In addition, the Code does not apply to mere 'lifestyle' data; according to the Commission, to determine whether it is health data, the general context and purpose of the data processing for which the application has been developed must be assessed. As an example of an application gathering health information, the Commission refers to an application allowing users to record their use of medicines or envisage the risk of a given illness. On the contrary, a pedometer application does not process health data unless it is concurrently linked to other data or to creating user profiles in terms of their physical condition.

Although the objective of the Code is to address app developers, the personal data protection community, associations and end-users of apps, in practice, its main focus is particularly on app developers, who are at the core of the Code.

According to the Code, a General Assembly will be established as an advisory body, with members made up of all of the parties referred to above. Decision-making powers would rest with a Governance Board elected from among members of the General Assembly. A Monitoring Body[6] would have an operational role which includes monitoring compliance with the Code in practice.

The General Assembly will supervise the governance and maintenance of the Code but will not have day-to-day

---

1 https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised.

2 European Parliament and Council Directive 95/46/EC of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 INTERNATIONAL TELECOMMUNICATION UNION. Measuring the information society report 2015 [online], [cit. 2 July 2018]. Available at: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf.

4 WORLD HEALTH ORGANIZATION. mHealth – Use of appropriate digital technologies for public health, Report by the Director-General at seventy-first World Health Assembly 26 March 2018 [online], [cit. 2 July 2018]. Available at: apps.who.int/gb/ebwha/pdf_files/WHA71/A71_20-en.pdf.

5 EUROPEAN COMMISSION. Green Paper on mobile health ("mHealth") 2014 [online], [cit. 2 July 2018]. Available at https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth.

6 Complying with requirements under Article 40(4), Article 41(4) and Article 41(2) of the GDPR.

decision-making powers. It will also provide annual financial contributions to secure the financial stability of the Code

If *mHealth* app developers wish to be bound by the Code, they must conduct a Privacy Impact Assessment[7], an example of which is contained in the Annex to the Code, and present it jointly with a declaration of compliance with the Code. Such developers would then be published in a centralised public register kept by the Monitoring Body, and they may add a trust mark to their app to indicate compliance with the Code. The Code also assumes third-party audits on app developers on a voluntary basis and alternative resolution of disputes and complaints before a panel appointed for the purpose.

Specific recommendations to *mHealth* app developers

The Code makes recommendations for developers in specific areas that are the most relevant in terms of data protection, particularly regarding obtaining the express and granular consent of app users to personal data processing. The consent could be obtained gradually at various stages of the use of the application always to the extent that the user wishes to use the *mHealth* application. Under the Code, any withdrawal of consent or cancellation of the app installation should result in the deletion of the user's data. Data must also be deleted after a certain period of time of non-use of the app or when it is no longer relevant for achieving the defined purpose.

Further, developers should also consider what specific personal data they need for the functioning of the *mHealth* application and for achieving the defined purpose, and they should not collect more data than necessary. Any secondary use of data (such as sale of the data to a drug manufacturer) must be anonymised or subject to the user's additional consent.

In general, applications should be developed in adherence to the principles of privacy by design and privacy by default and implement user-friendly interfaces that facilitate the exercise of users' rights under the GDPR (rights to access, correct, delete or restrict the processing of their data, and their rights to object and to data portability).

The Code also provides a summary of information that should be provided to *mHealth* app users by means of a condensed notice of data processing before app installation as well as a full privacy policy made available to the users within the *mHealth* app at any later time.

If an app developer or operator plans to show advertisements in the app, they should in accordance with the Code assess whether or not personal data is used to view the advertisement. In general, the use of contextual advertisements should be confirmed by the user before the *mHealth* app installation, and the user should be given the option to opt out from the contextual advertising at any time. If an advertisement is shown while personal data is shared with a third party or if it is a targeted advertisement using the user's personal data, the prior opt-in consent of the user must be obtained. However, under the Code, the use of an *mHealth* app as a whole may be conditional on the user's consent, i.e. exercising the opt-out right may result in the removal of the app from the user's device.

Criticism of the Code

When submitted to the WP29 for approval, the Code was met with criticism. The WP29 raised major comments that it recommended be incorporated in the Code. According to the comments, the Code does not bring sufficient added value and does not sufficiently address questions and problems encountered within the *mHealth* app sector. The Code is considered too general and, at the same time, too narrowly focused on data protection compliance, as it does not take into account legislation such as that governing cookies, unfair commercial practices and medical devices regulation, which can also play an important role for app developers. According to the criticisms, the Code insufficiently clarifies the roles of the parties involved in processing (app developers could assume the role of data controller, data processor, or joint controller). The WP29 also has doubts about the fact that consent would be the only legal ground for use in all cases of using an *mHealth* app and, at the same time, objects that all such consents might not always be freely given.

The Code is currently waiting to be amended and revised, after which it should be submitted for new approval to the European Data Protection Board, the successor of the WP29 under the GDPR. Nevertheless, app developers may still declare their adherence to the Code and start to comply with it in practice. However, in view of the ambiguities of the approach mainly as to the legal grounds of data processing, it is more practical to wait until the final version of the Code is delivered. Irrespective of whether the Code is adopted or not, *mHealth* app developers will be required to address privacy protection issues in their apps not only under the GDPR but also under all other applicable laws.

[7] *Under Article 35 of the GDPR.*

Authors:
Václav Audes | *Partner*
Lenka Teska Arnoštová | *Senior Associate*
Kateřina Tumpachová | *Junior Associate*



Commission proposes new rules to make cross-border transfers of companies simpler, faster and cheaper

*At the end of April 2018, the European Commissioner for Justice, Consumers and Gender Equality Věra Jourová presented two new proposals for Directives regarding the use of digital tools and processes in company law[1] and the rules of cross-border conversions, mergers and divisions of companies[2] (the "**Proposals**"). The Proposals should amend the Directive relating to certain aspects of company law[3] and aim in particular at making the use of freedom of establishment simpler for companies in practice. To that end, the main aspects of national legislations governing cross-border conversions in the respective Member States should be unified, the administrative and financial load associated with setting up and restructuring businesses should be reduced and the possibilities for using electronic communication means before setting up a company and throughout its existence should be broadened. In this article, we would like to inform you of the most important features the Proposals introduce in corporate law.*

Current problems of corporate law from the perspective of the single market

The Proposals form a part of the EU's long-term strategy for supporting the development of small and medium enterprises and start-ups which often face administrative obstacles and legal uncertainty in an attempt to expand their business to other Member States by way of a cross-border conversion. One of the main reasons for these difficulties is the fact that, in the absence of harmonisation in this legal area, the respective Member States lay down their own rules serving to protect entities which may be most affected by a cross-border conversion (i.e. minority shareholders, employees or creditors). Consequently, the respective Member States have different requirements for entrepreneurs; moreover, these requirements are often incompatible with each other, thus creating an inadequate burden which may, as a result, practically prevent a cross-border conversion in some cases. But as a matter of fact, cross-border transfers of companies contribute to the creation of new jobs, attract investments also from countries outside the EU and consequently facilitate overall economic growth in the single market.

At the same time, the Proposals should help eliminate somewhat clumsy and outdated national legislations governing the registry proceedings and, in particular, the modes of communication with state administration bodies caused by the fact that various online tools are still not used to a sufficient extent in corporate law.

Specific aspects of the Proposals

The first Proposal envisages the introduction[4] of the possibility for companies and their branches to register online in all Member States without the need for the applicant or their representative to be physically present. Applicants should be enabled to submit all documents to the competent body which maintains the business register in digitalised form when setting up a company and during its existence. Administrative costs should be further reduced thanks to common templates developed in an official EU language for the instrument of constitution that comply with requirements of the respective national law and are made available to the applicants in electronic form. Member States may still require the physical presence of applicants before any competent authority only if there is a genuine, founded and reasonable suspicion of fraud.

With a view to the general acceleration of the registry proceedings, it is assumed that uniform time limits will be introduced for the competent bodies to complete the registration (currently a period of five working days from the day when the applicant fulfils all conditions and submits all documents required for registration is proposed). The prohibition to make the registration of a company or its branch conditional on obtaining any licence before the registration (unless it is indispensable for the proper control of certain activities) should prevent delays in the proceedings.

A very practical aspect of the Proposals is the attempt to enhance transparency and to introduce the obligation for the Member States to enable free access to basic information about companies (such as the business name, legal form, registered office, scope of business, and persons authorised to represent the company) by interconnecting business registers[5]. The fee charged for obtaining some

[1] *2018/0113 (COD).*
[2] *2018/0114 (COD).*
[3] *Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law.*
[4] *Member States will be able to apply certain exemptions such as the possibility of exempting certain types of companies from the regime of fully digitalised procedures for setting up such companies.*
[5] *The system was already launched in the first half of 2017 and enables searching for information on joint stock and limited liability companies (or their equivalents under the respective national laws) and their branches registered in the EU Member States, Iceland, Lichtenstein and Norway. The information can be searched at: https://e-justice.europa.eu/content_find_a_company-489-cs.do.*

other information and documents (such as the instrument of constitution or specified accounting documents) may not exceed the actual administrative costs incurred in this connection.

The other Proposal introduces standardisation of the key aspects in legislation governing cross-border conversions such as the conditions of conversions, the minimum scope of information to be made publically available, the drawing of a report for the shareholders and employees, the mandatory examination of such conditions by an independent expert, the procedure for their approval but also the governing law applicable at the respective stages of the cross-border conversion process. Also, a more active involvement of the competent national bodies is assumed. They should be obliged to contribute to preventing the abuse of cross-border conversions by thoroughly reviewing each conversion at least as per the defined criteria. The report of an independent expert will serve as an important basis for the assessment of cross-border mergers; it will not be possible to waive the report even if all shareholders agree.[6] The competent authority will not approve a cross-border conversion if it finds the conversion to be a mere artificial arrangement aimed at obtaining undue tax advantages or at unduly prejudicing the legal or contractual rights of employees, creditors or minority shareholders. Shareholders who did not vote for the approval of the draft terms of a cross-border merger or have no voting rights would have the right to sell their interests (shares) to the company, other shareholders or third parties (carrying out the conversion in agreement with the company) and receive adequate compensation.

Creditors in all Member States should be equally able to seek the protection of their rights which are potentially threatened as a consequence of a cross-border conversion from the competent administrative or judicial authority within one month from the disclosure of the draft terms of the cross-border conversion. In order to prevent unnecessary disputes, presumptions are defined: if such presumptions are met, the intended cross-border conversion is deemed not to have prejudiced the rights of creditors. Also, the rights of employees from companies participating in a cross-border conversion should be strengthened, and their informedness should be enhanced. Last but not least extensive digitalisation, online communication among the parties involved and acceleration of the whole process by setting out time limits are proposed for cross-border conversions.

Potentially significant effect in practice

The Proposals are primarily capable of eliminating factual obstacles and the unnecessary administrative load in implementing freedom of establishment for companies in the EU and supporting, in general, cross-border expansion of European companies by making it cheaper and more efficient. However, this goal should be achieved by simultaneously preventing the abuse of the system for the purposes of circumventing tax legislation or weakening the rights of shareholders, employees or creditors.

If the currently submitted versions of the Proposals are successfully passed in the legislation procedure and correctly and timely implemented in national legislations, new avenues will open even to Czech entrepreneurs for their expansion to other Member States. They may also support the inflow of new investments to the Czech Republic.

What's next?

Currently the EU Council and the European Parliament have just started discussing the Proposals, so there is still a rather long way ahead for them to pass through the legislative procedure. With regard to the time limits for deliberating the Proposals and the proposed transposition period, the new legislation described above could enter into force in the Member States in approximately three years. Of course, it cannot be excluded that changes will be made to the Proposals during the approval process. We will certainly monitor the latest developments and keep you updated in the future editions of the EU Legal News.

[6] *However, it is assumed that an expert's report on a cross-border conversion will not be required for small and micro enterprises pursuant to the definition given in the European Commission's recommendation 2003/361/ES.*

Authors:
Pavel Němeček | *Partner*
Zuzana Hájková | *Associate*

Brexit and IP rights – update

*Since our latest issue of EU Legal News, the negotiations between the European Commission ("**Commission**") and the UK have made major progress, and the protection of intellectual property rights has become more specific. The main drive behind this is the aim to allow Brexit to have the least impact possible on IP rights. Although most topics on the agenda seem to have been settled, some issues are still pending.*

In March earlier this year, the Commission and the UK published a joint draft of the Withdrawal Agreement ("**Agreement**"). The draft reflects the most recent outcomes of negotiations between the EU and the UK. IP rights are addressed in Articles 50 to 57. A deal has been reached on the most crucial issues regarding IP rights, which were defined by the Commission in its position paper in September 2017, as we covered in the article *What is the future of IP rights following Brexit?* in the latest issue of EU Legal News. The UK cabinet asserted that the final version of the Agreement should be ready by October 2018.

Currently it seems that the following IP right provisions are expected to apply in the future:

1. First of all, both parties have agreed on a ***transitional period*** from 29 March 2019 (the expected date of Brexit) to 31 December 2020. The acquis should still fully apply in the UK during this period.
2. **EU trademarks** (including international trademarks with EU designation), **Community designs and plant variety rights**, which were validly registered before the end of the transitional period, will automatically remain valid in the UK without any further review and will have the same priority as EU rights.
3. **Applications for the above rights** which have not been registered before the end of the transitional period will not be automatically registered in the UK. Applicants, however, will be entitled to file new applications in the UK within 9 months from the end of the transitional period in order to maintain the right of priority linked to the original EU applications. No decision has been reached yet on a fee for the application, if any. The EU proposed that no fees be charged for applications while the UK has not yet commented on this proposal.
4. If a **non-registered industrial design** is protected before the end of the transitional period, such non-registered industrial design will enjoy the same rights in the UK as those in the EU. The IP rights that have been exhausted pursuant to EU regulations both in the EU and the UK before the end of the transitional period will remain exhausted also after the end of the transitional period.
5. **Databases** created before the end of the transitional period will enjoy the same level of protection in the UK as those in the EU.
6. No final decision has been reached in the Agreement on the protection of **geographical indications, designations of origin**, and the applications for **supplementary protection certificates**; these rights thus still remain the subject of negotiations. The UK has no national legislation governing geographical indications and designations of origin, which was covered in our previous EU Legal News issue; it will therefore have to adopt its own national legislation on this matter sooner or later. Furthermore, no agreement has been reached yet on the issue of representation before EUIPO and the UK IP Office, which is a burning issue for a number of law and patent offices in connection with Brexit.

Another update closely linked to IP rights but not covered in the Agreement is the fact that on 28 March the Commission issued a *Notice to Stakeholders*. It follows from the document that as of 31 March 2019, the rules governing the top-level .eu domain names will no longer apply to the UK. Owners of .eu domain names seated in the UK will no longer be allowed to hold these domain names. Owners seated in the UK will no longer be allowed to register or renew the .eu domain names. Besides that the registrars will be authorised to cancel, upon their own discretion, domain names owned by persons seated in the UK.

Although the situation is much clearer than it was several months ago, a whole range of unresolved issues (e.g. representing applicants and owners of industrial rights before the EUIPO by UK representatives) as well as those addressed only marginally (exhaustion of rights, geographical indications and designations of origin, supplementary protection certificates) still remain on the agenda.

On 12 July 2018, the UK cabinet issued a White Paper implying future relations between the EU and the UK, with IP rights addressed only marginally in this document. What is crucial, however, is the explicit confirmation that the UK will adopt its own post-Brexit geographical indication regulations. Persons seated both in or outside the UK will be allowed to file applications.

We will keep monitoring the developments in this field and keep you updated in our next issue of EU Legal News.

Authors:
Ivan Rámeš | *Partner*
Tereza Hrabáková | *Associate*

Intellectual property law services

Intellectual property law is one of our major practice areas. We provide specialised legal services related to works of authorship, trademarks, industrial designs, patents, database rights, and other intangible property. With its 20 members, our IP law team is one of the largest in the Czech Republic and Slovakia.

For many years, we have also focused on the enforcement of IP rights, that is, in relation to **counterfeit and pirated goods** and related customs procedures and litigation.

IP law aspects are also reflected in our focus on unfair competition and media law: we address issues related to advertising and the protection of personal rights. We also have specific know-how in film rights and contractual relationships between individual participants in film production.

Ensuring adequate protection of IP rights

- trade mark strategies in the Czech Republic, Slovakia, the EU and the rest of the world
- comprehensive IP portfolio management services and brand value enhancement
- registration of rights at national and international levels
- research in connection with trademarks
- protection of copyrighted works
- dealing with organisations for collective management of IP rights
- protection against illegal and parallel imports

Transactional support and contract negotiations

- transfers and assignments of registered and unregistered IP rights
- licences to IP rights
- IP agreements with employees, employee work
- franchise agreements
- due diligence and other types of legal audits
- technology transfers

Dispute resolution

- representing clients in disputes related to trademarks, patents and in other IP disputes
- arranging preliminary rulings
- support in obtaining evidence
- defence against unfounded claims
- preparing appropriate strategies for defending and representing clients in court

Combatting counterfeit and pirated goods

- monitoring and seizing counterfeit and pirated goods in all sale and distribution segments: during imports to the Czech Republic, during export, in retail stores, at stands and market places both on the internal market and on the Internet
- arranging for the destruction of counterfeit and pirated goods, filing actions and criminal complaints against infringers, entering into agreements for damages
- active cooperation with the Customs Administration and the Czech Trade Inspection Authority

Film rights and use of film incentives

- defining suitable contractual arrangements for financiers, producers, co-producers and service companies
- identifying risks involved in state aid (in particular, risks associated with the non-transferability of claims arising from film incentives)

Ivan Rámeš | *Partner* | *T: +420 255 000 945* | *E: ivan.rames@havelpartners.cz*

New initiative for better consumer rights and enforcement in the EU introduced

*While the European Union already has some of the strongest rules on consumer protection in the world, the European Commission (the "**Commission**") introduced in April 2018 its New Deal for Consumers (the "**Policy**"), designed to further strengthen consumer protection, providing consumers with a tool for a more efficient enforcement of their rights. Even though some of the proposed changes can be considered as merely minor modifications of existing laws, others apply to areas that have not yet been harmonised within the EU.*

Strengthening consumer rights online

The Commission intends to further extend the information duties to be complied with by operators of online marketplaces. If the Policy is successfully passed, consumers will have to be clearly informed about **whether a particular e-shop is operated by a private person or by a trader**. The Commission expects this minor change to help consumers know whether they are protected by consumer rights.

In an effort to further strengthen the rights of consumers, the Policy proposes that operators of on-line platforms should be obliged to **clearly inform consumers when a search result is being paid for by a trader and is thus given preferential ranking over results that are not being paid for**. The consumers should also be informed about the parameters determining the ranking of the search results. Apart from Google and Seznam, this change would also have an impact on other search engines.

The Commission also proposes in the Policy that all consumers within the EU should have the **right to cancel their contract under which a digital service is provided to the consumer for free** (such a cloud storage services, social media, or e-mail accounts). For these digital services, consumers often provide their personal data to the operators, who can then use them for marketing or other purposes. Besides other protections afforded by the new General Data Protection Regulation (GDPR), the consumer should have the right to withdraw from a digital service contract for convenience within 14 days, thus preventing any further processing of the consumer's personal data. Similar rules currently apply to distance contracts for the purchase or provision of paid digital service.

Enforcement of consumer rights

In the Policy, the Commission proposes to repeal a directive[1] which ordered the Member States to make it possible for qualified entities to launch legal actions for the protection of consumers' collective interests. Such actions are currently available for qualified entities seeking the cessation or prohibition of any conduct which infringes EU laws and is contrary to the collective interests of consumers.

While the aforesaid directive is allegedly unable to effectively protect the interests of consumers throughout the EU, the Commission proposes a new directive,[2] a draft of which has been published together with the Policy. By the proposed directive the Commission intends to order the Member States to **implement representative actions** in their national laws, which can be perceived as the European form of class actions known particularly in the United States. The proposed framework of representative actions is based on the currently-effective directive, and considerably extends the scope of claims that can be sought by consumers. Such action should only be filed by qualified entities (in particular, not-for-profit organisations dedicated to the protection of consumer rights) to be nominated by Member States.

If the proposed directive is adopted, consumers harmed by unfair commercial practices will be able to obtain remedies collectively through a qualified entity not only in respect of the cessation and prohibition of the infringing practice, but will also be able to seek compensation for actual damages or replacement or repair of a defective product.

The introduction of representative action is a significant change as similar right to collective actions seeking redress is currently not available (to comparable extent) in all EU member States. The Commission's proposal is apparently a response to the *Dieselgate* case which has affected a large number of consumers within the EU.

We add for the sake of completeness that in early April 2018, the Czech Government approved a draft bill on representative action,[3] the aim of which is to introduce representative action also in the Czech law. The draft bill primarily works with the *opt-out* principle, which in simple words means that any person who has a similar claim in the same matter (such as all buyers of the same product) is considered a party to a representative action. Hence, such person would not have to actively join a representative action brought in court. The draft bill applies this principle particularly to proceedings that would have thirty (30) or more parties. On the other hand, the draft bill envisages that proceedings with fewer parties would be the subject of the *opt-in* principle, where each person has to actively join such representative action. As the draft bill is not yet even structured in sections, it is possible that the final text of the law will be substantially different, if enacted.

[1] *Directive 2009/22/EC of the European Parliament and of the Council on injunctions for the protection of consumers' interests.*
[2] *Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC.*
[3] *Draft bill on representative action, no. 153/17.*

Increased penalties for violations of consumer protection provisions

Another major change introduced by the new Policy entails the palpable increase of penalties that may be imposed by national authorities on those who infringe consumer protection laws.

In a related proposal for a directive,[4] by which existing relevant directives are to be amended, the Commission requires Member States, among other things, to provide for fines the maximum amount of which should be at least 4% of the infringing trader's annual turnover for widespread infringements. As regards widespread infringements with a Union dimension, the amount of the fines should be derived from the cumulative annual turnover of the infringing trader in all the Member States concerned. In transposing the proposed directive, Member States should be free to introduce higher maximum fines as necessary.

Equal treatment of consumers

The proposed Policy also tackles equal treatment of consumers in EU Member States. The Commission aims at eliminating competition practices where the same producer markets products under the same brand or with the same marketing statement as being identical but which are different in different Member States (cf. numerous tests for dual quality of food products bought in the Czech Republic and Germany).

The Commission hence intends to achieve that a product marketed in one Member State will have practically identical composition in other Member States. In this respect, a Europe-wide product quality and composition testing campaign took place in May 2018, the results of which should be available by the end of 2018. Regarding the dual quality of food products please see the article *European Commission Notice in Fight against Dual Quality of Food Products*.

Support of traders in respect of withdrawal from contract

While the Policy quite logically follows the current trend of consumer protection, it also responds, to a certain extent, to practical suggestions from traders. The consumer's right to withdraw from an off-premises purchase contract within 14 days has resulted in a significant increase in e-commerce but, on the other hand, there have been multiple cases of abuse of this right by consumers. The Policy therefore introduces the rule that consumers will no longer be allowed to return products that they have already used instead of merely trying them out as they would in a brick-and-mortar shop – which is after all a common practice already.

For example, consumers who "buy" a camera for a 14-day holiday, where they use it extensively, and subsequently withdraw from the contract on the last day of the deadline and claim a refund would not be successful and they should be denied the right to withdraw. Contrary to the current wording of the relevant directives, traders will be able to inspect the returned goods before making a refund.

Conclusion

The overall concept of the Policy can be assessed positively from the consumers' viewpoint, as the Policy aims at enabling consumers to enforce their rights more efficiently. On the other hand, the Policy will impose additional obligations traders will have to comply with vis-à-vis consumers. If the measures proposed in the Policy are adopted, we suggest undertaking a timely analysis of the status quo in order to verify whether a trader fulfils all his obligations vis-à-vis consumers stemming from the current as well as the proposed legislation. Any drawbacks should be dealt with in time, as potential penalties that may be imposed by government authorities, or claims that may be asserted by consumers via representative actions, can be considerable.

There still remains a long way to successful adoption and actual implementation of the proposed Policy, as four currently applicable directives need to be amended and one brand new directive needs to be adopted in order to implement the Policy. Due to the legislative process, the final shape of the newly-introduced rules may of course significantly differ from the current proposal. We will therefore keep monitoring the developments regarding the adoption of individual directives and the enactment of the consumer Policy in general.

[4] *Proposal for a Directive of the European Parliament and of the Council amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules.*

Authors:
Ivan Rámeš | *Partner*
Dalibor Kovář | *Senior Associate*
Tomáš Chmelka | *Junior Associate*



New model of cooperation when enforcing consumer protection regulations in the EU

The European Commission has been striving to streamline the activities of national authorities, to boost legal certainty for business people and to enhance the position of consumers in response to unfair practices of some traders. Its long-term effort has resulted in the adoption of a new regulation which is to make circumvention of regulations and harm caused to consumers more difficult. A survey carried out by European Consumer Centres showed that consumers most often complain about online cross-border purchases. The new regulation will in particular affect consumers shopping abroad and will make it easier to combat unlawful practices harming consumers in another member state.

Regulation of Consumer Protection Cooperation and the background of the modernised regulation

Regulation No. 2006/2004 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on Consumer Protection Cooperation, referred to as the "**CPC Regulation**") currently harmonises rules for cooperation between national authorities EU-wide so that their law enforcement measures are applicable throughout the single market. The CPC Regulation thus aims to ensure legal certainty on the single market by unified cross-border enforcement of the consumer acquis. Efficient cross-border cooperation among competent national authorities when enforcing consumer rights is crucial namely to prevent non-compliant traders from exploiting gaps in regulations and territorial or other restrictions in the enforcement powers of individual member states. At the moment, member states use alerts and mutual assistance mechanisms complemented by a series of minimum powers that national authorities need for efficient cooperation. The existing mechanism to combat malpractice involving more than two member states operates based on intervention and assistance from the European Commission ("**Commission**").

Pursuant to Article 21a of the CPC Regulation, the Commission carried out an external assessment of the effectiveness of the CPC Regulation launched in 2012, which aimed to assess the need for amendments. The Commission namely assessed the efficiency and application of the regulation and thoroughly investigated the possibilities to adopt further mechanisms. The outcome of the assessment, which was followed by a public debate in 2013 and 2014, a consumer summit in 2013, an assessment of the impact and the need for a bill carried out in 2015, and other actions, was the *Digital Single Market Strategy*[1] dated 6 May 2015. In it the Commission planned to submit a proposal to review the CPC Regulation to develop more efficient mechanisms of cooperation among national authorities in charge of enforcing compliance with EU consumer protection regulations, namely for reasons of a significant discrepancy between the practice and basic EU consumer protection rules.

Based on performed reviews, the Commission found out that the existing level of discrepancy between commercial practices and EU consumer regulations is suboptimal. The rate of non-compliance with basic consumer protection regulations, uncovered during coordinated examinations of e-commerce websites carried out on an ongoing basis from 2007, ranged from 32% to 69%. These results are confirmed by data from the European Consumer Centres, showing that two-thirds of the total of 37,000 individual complaints received by the centres in 2014 concern cross-border online shopping. The investigation of samples from five online sectors (clothing, electronics, recreation, consumer credit and package travel) shows that 37% of EU e-shops did not respect consumer law in 2014. According to the Commission's estimates, consumers shopping online cross-border in the surveyed sectors alone could suffer damage of up to EUR 770 million per year.

As a follow-up to these steps, the Commission issued a proposal of a new modernised regulation in May 2016, which was adopted on 12 December 2017 and published in the Official Journal of the EU on 27 December 2017. The key areas that the *Regulation (EU) No. 2017/2394*[2] *of the European Parliament and of the Council ("**Regulation**")*

[1] https://ec.europa.eu/commission/priorities/digital-single-market/.
[2] *Regulation (EU) 2017/2394 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws.*

addresses are a *mutual assistance mechanism, coordinated surveillance, investigation and enforcement mechanisms for widespread infringements.*

Who will be affected by the new regulation?

The new measures against a widespread infringement of consumer protection regulations by traders could significantly reduce consumer detriment across the EU. Consumers shopping for services and goods cross-border in an online environment are affected by the Regulation, as its main aim is to increase their protection in such markets. The Regulation may mitigate the risk of consumer detriment, e.g. when goods bought abroad are not delivered to them or when they are given misleading information about the payment arrangements or are being debited automatically without their express consent.

The European Consumer Centres, which provide information on the rights of consumers on the single European market as well as free assistance and advice to consumers in their disputes with traders from other member states, can obtain information that may significantly help improve the level of enforcement of consumer rights. Currently, the centres do not provide such data to cooperation authorities systematically, but under the Regulation they will be requested to do so. That could help national cooperation authorities to define priorities within the EU or to issue alerts to these authorities on new or widespread cross-border infringements.

The Regulation will also have an impact on the position of cooperation authorities and single liaison offices which currently bear high administrative costs as a result of inefficient cross-border cooperation. The enhanced coordination of law enforcement will eliminate the double effort and thus lower the costs, namely by combining sources to address widespread infringements.

The Regulation will also increase legal certainty for traders. More consistent and unified cross-border law enforcement will enhance the competitiveness of compliant traders, by ensuring a level playing field in the single market. The Regulation does not impose any new legal obligations upon traders but instead reflects the fact that traders suffer from unfair competition from non-compliant traders, who develop business models that allow them to evade laws and harm consumers from a different country. Diverging enforcement approaches among member states also made producers, retailers, e-shops, intermediaries and others look for the differing valid enforcement regulations in each individual jurisdiction concerned.

Last but not least, widespread infringements of consumer protection regulations require increased action from EU bodies. In particular, the Commission will benefit from a stronger position in the network of cooperating surveillance bodies, mainly thanks to coordinated actions against widespread infringements that meet the Union-dimension threshold.

Minimum powers of competent authorities

Competent authorities should have a minimum set of investigation and enforcement powers to apply this Regulation effectively, to cooperate with each other, and to deter traders from committing intra-Union infringements of consumer protection laws. Those powers should be adequate to tackle the enforcement challenges of e-commerce and the digital environment where the possibilities of traders easily concealing or changing their identity are of particular concern. These powers should ensure that evidence can be validly exchanged among competent authorities to achieve effective enforcement at an equal level in all member states.

Consequently, compared to the currently valid CPC Regulation, authorities have additional minimum powers, including the power to conduct necessary on-site inspections (and the power to enter premises, land, or means of transport, or to request other authorities to do so), which could prove an efficient tool when inspecting the sale of counterfeits or health or life-threatening goods, for instance. This could prevent certain traders from constantly avoiding checks by closing down stalls or shops or other similar conduct. The additional powers also include the power to make a purchase anonymously, i.e. without first presenting credentials, which would otherwise be their duty; the power to purchase goods or services undercover or the power to adopt interim measures and to impose sanctions and ensure indemnification of the consumer. Another crucial power is the power to block websites, domains or similar digital environments, services or accounts or their parts. Similar powers (disguised identity, access to locked premises, etc.) were already conferred on the Czech Trade Inspection Authority in the amended Act No. 64/1986 Sb., on the Czech Trade Inspection Authority, as amended,

effective from the end of 2017. This analogy shows that lawmakers both at the national and EU levels see their priorities in a functional and effective market with sufficiently protected consumers.

Certain minimum powers regulated in the CPC Regulation were defined in greater detail to ensure that their applicability and use will be identical throughout the EU. These powers include, for instance, the power to require that any individual or legal entity, including banks, internet service providers, domain registries and registrars and hosting service providers provide any relevant information, data or documents in any format or form.

Member states will retain the possibility to decide whether the competent authorities will exercise the minimum powers directly under their own authority or by application to courts. Where the member states decide that surveillance authorities exercise their powers by application to the competent courts, the member states should ensure that those powers will be exercised effectively and in a timely manner and that the cost of exercising those powers will be proportionate and will not hamper the application of this Regulation,

Mutual assistance mechanism

The mutual assistance mechanism consists of two instruments. The first of these is a request for information which enables competent authorities to obtain relevant information and evidence showing whether an intra-Union infringement has occurred and to stop such infringement. The other is a request for enforcement measures which enable one competent authority to request another competent authority in a different member state to take enforcement measures to stop or to prohibit an intra-Union infringement.

All measures defined in the Regulation concern cross-border issues (e.g. the trader is located in another member state) and widespread infringements of consumer protection regulations occurring simultaneously in more than one EU member state. The key reason was the fact that cross-border aspects of Union consumer *acquis* cannot be sufficiently achieved by member states' individual actions; in fact, member states alone cannot ensure efficient cooperation and coordination of their actions when enforcing these rights.

Follow-up

The Regulation includes a delayed entry into force for it to allow member states, competent authorities and the Commission to make the necessary arrangements and legislative changes. The Regulation will therefore apply from January 2020. The existing implementing measures will have to be replaced to take into account the changes brought about by the Regulation. For instance, the platform used to exchange information among cooperating authorities will have to be altered. All legislative as well as administrative measures, no matter how costly they may seem, have a potential to bring desirable outcomes and to shift the digital market one step closer to the coveted goal – an environment where the position of traders will be equal and the consumer protection level will be high.

Authors:
Ivan Rámeš | *Partner*
Laura Tadevosjanová | *Paralegal*

Acquisition International ranks us the best law firm in the real estate and construction

AI 2018 BUSINESS EXCELLENCE AWARDS

Our law firm was recognised by the UK's Acquisition International magazine published by AI Global Media Ltd. According to the review of legal advisory rendered in Central and Eastern Europe (the CEE region), HAVEL & PARTNERS is the best law firm in the real estate and construction industries (Best Real Estate & Construction Law Firm – CEE). "*Acquisition International's award proves our leading position among providers of legal consultancy aimed at the real estate and construction industries. Thanks to the numerous groups of excellent lawyers equipped with detailed knowledge of the real estate market and the broad range of services offered by our law firm, we are able to assist our clients with the most demanding real estate projects*," Jaroslav Havel, managing partner at HAVEL & PARTNERS, comments on the next award received.

Competition law update

EU competition law has recently seen a number of new developments and interesting cases. We would like to inform you about the most interesting ones in this edition of the competition flash.

Another record fine for Google[1]

In the middle of June 2018, the Commission announced that it fined Google EUR 4.34 billion for unlawfully strengthening its dominance in internet search engines through smart phones running on Android.

Google's strategy comprises three types of abusive practices. According to the Commission, its licensing conditions required manufacturers to pre-install Google Search and Google Chrome applications. Google offered its apps as a package – Play Store, Google Search and Chrome – while not allowing manufacturers to install some alternative applications. According to the Commission, Google also paid some manufacturers and mobile network operators for exclusively pre-installing Google apps on their devices. At the same time, Google allegedly prevented manufacturers from selling smart phones running on alternative versions of Android that were not developed directly by Google but by third parties on the basis of the published source code (so-called "Android forks") in exchange for the possibility to offer Google apps on these devices.

According to the Commission, as a consequence Google has cemented its position on the market for internet search engines (with a market share of over 90%) by which it denied rivals to compete on the concerned market on the merits and equal terms. The Commission also emphasises that Google's behaviour affected the whole smart phone industry.

Although the decision has not been published yet, it has triggered controversies and is already being sharply criticised. We will keep you updated on the latest developments in this case.

Judgment of the General Court of Justice – A fishing expedition against the Czech Railway Company?[2]

From 26 to 29 April 2016, the Commission conducted a dawn raid on the business premises of the Czech Railway Company (*České dráhy*). České dráhy defended itself against the dawn raid by filing a lawsuit at the General Court. The company objected that the Commission defined the subject of the investigation so broadly that it could focus on almost any practices occurring on almost any of České dráhy's railway lines over an excessively long period of time.

The General Court partly satisfied the objection of České dráhy. The subject of the dawn raid was defined unlawfully, authorising the Commission to investigate any anticompetitive conduct occurring on any railway line without possessing sufficient underlying documents and indications for such investigation. However, the General Court found the subject of the dawn raid justified to the extent to which the Commission examined the application of predatory pricing to the Prague-Ostrava line. At the same time, the General Court concluded that it was justified for the Commission not to precisely define the starting point of the period when the alleged unlawful conduct occurred.

The General Court also ruled on České dráhy's lawsuit against a second dawn raid the Commission conducted on the basis of documents seized during the previous dawn raid.[3] The General Court fully dismissed the second lawsuit. According to the general Court, the Commission obtained the documents in line with a duly defined scope of investigation.

New methodology for antitrust fines[4]

The Office for the Protection of Competition introduced a new procedure for the calculation of fines for anticompetitive practices. This procedure puts a greater emphasis on economic aspects of anticompetitive practices, practical experience and case-law of administrative courts.

Turnover on a sale of goods which a breach of competition rules relates to remains the basic criterion for determining the amount of a fine. At the same time, the Office increased the percentage rate of fines to up to 15% for more serious cases from the current 3%. Also, the method of calculation applicable to cases when mitigating and aggravating circumstances are taken into account has changed.

---

1 *http://europa.eu/rapid/press-release_IP-18-4581_en.htm*
2 *Judgment of the General Court of Justice no. T-325/16 from 20 June 2018 in the case České dráhy v. Commission.*
3 *Judgment of the General Court of Justice no. T-621/16 from 20 June 2018 in the case České dráhy v. Commission.*
4 *http://www.uohs.cz/cs/hospodarska-soutez/aktuality-z-hospodarske-souteze/2416-uohs-prepracoval-metodiku-pro-ukladani-pokut-za-protisoutezni-jednani-tresty-budou-spravedlivejsi.html.*

You can find more detailed information in our Competition Flash 05-2018.

Restricted retailers in Prague outlet centres[5]

The Office looked into agreements between the landlord of retail spaces in Prague Fashion Arena and its tenants. The agreements contained a provision restricting the tenants from operating a store in other outlet centres within an area reachable in 60 minutes.

According to the Office, as a result, these agreements disrupted competition. The Office prohibited the fulfilment of these agreements and imposed a CZK 1 million fine. At the same time, a landlord of another Prague outlet centre challenged the agreements before a civil court. These proceedings have not been finished yet.

Supreme Administrative Court and Constitutional Court rule on the period for filing an action against the unlawful interference of an administrative authority.[6]

At the end of last year, the Supreme Administrative Court issued a decision in which it assessed the admissibility of an action filed by Eurovia against the unlawful withholding of documents which were seized during dawn raids conducted as a part of proceedings before the Office in the matter of the so-called "large construction cartel". The Supreme Administrative Court decided that the action was filed belatedly as the period for filing it started upon the commencement of such interference rather than upon its termination.

The Constitutional Court cancelled the decision of the Supreme Administrative Court. According to the Constitutional Court, such an interference needs to be regarded as pending (the Office still holds the documents in seizure), so no period, subjective or objective, can commence for filing an action against an unlawful intervention of an administrative authority. The Constitutional Court emphasised that the nature of the particular interference should be taken into account.

Termination of a cooperation agreement as implementation of a concentration

In view of the contemplated concentration between two audit companies in Denmark - Ernst & Young and KPMG Denmark - the latter company terminated a cooperation agreement with the international network of KPMG. Based on this agreement, KPMG Denmark had an exclusive right to undertake business under the KPMG trademark. In this connection, the Danish competition authority issued a decision concluding that the concerned conduct constitutes a breach of the requirement that a concentration can only be implemented after the competition authority issues a decision on the concentration.

Eventually, the case was referred to the CJEU for a preliminary ruling. The CJEU decided that the conduct in question did not constitute a breach of the prohibition to implement a concentration without the prior consent of the competition authority as it did not consequently result in a change of control in the target company Ernst & Young.

CJEU ruling on disadvantaging competitors by differentiated pricing[7]

The Portuguese competition authority assessed the application of differentiated royalties by the Portuguese collective right management body as an abuse of dominance taking the form of discriminatory pricing. Following proceedings on a question referred for a preliminary ruling the case was forwarded to the CJEU.

In its judgment the CJEU stated that it is necessary to consider all relevant facts which have an effect on the customer's costs, profits and other interests in order to be able to determine whether the discriminatory pricing results or may result in advantaging one competitor over others. But if the effect of differentiated pricing on the costs or even profitability or earnings of the competitor that believes to have been harmed is not significant, it can be inferred that such differentiated pricing cannot have any impact on the competitive position of the competitor.

The final decision is up to the Portuguese competition authority though.

Another decision in the case of Delta pekárny[8]

The Supreme Administrative Court repeatedly dismissed a cassation complaint of Delta pekárny. A decision concerning dawn raids was remanded to administrative courts based on a judgment of the ECHR and the Constitutional Court. The European Court of Human Rights concluded that the right to respect for private life was breached as a consequence of insufficient procedural guarantees under Czech law.

After the case had been remanded the Regional Court in Brno dismissed the action again. Therefore, Delta pekárny approached the Supreme Administrative Court invoking the

[5] *http://www.uohs.cz/cs/hospodarska-soutez/aktuality-z-hospodarske-souteze/2409-urad-zasahl-proti-omezovani-obchodniku-outletovym-centrem.html.*
[6] *https://www.usoud.cz/aktualne/ustavni-soud-vyhovel-ustavni-stiznosti-spolecnosti-eurovia-cs-a-s-zaloba-stezovatelky/.*
[7] *CJEU judgment C-525/16 from 19 April 2018 in the case MEO – Serviços de Comunicações e Multimédia SA proti Autoridade da Concorrência.*
[8] *Judgment of the Supreme Administrative Court no. 5 As 256/2016 – 231 from 21 December 2017 in the case Delta Pekárny v. the Office.*

conclusions of the Constitutional Court and the ECHR. But the Supreme Administrative Court dismissed the cassation complaint. According to the Supreme Administrative Court, neither the ECHR nor the Constitutional Court dealt with the lawfulness of the contested dawn raid; rather, their main objections related to the absence of an effective subsequent review by Czech administrative courts. As to other aspects, there was nothing to object to regarding the dawn raids conducted by the Office. According to the Office, the Supreme Administrative Court did not deviate from the subject, which was based on the available circumstantial evidence and sufficiently defined the specific anti-competitive conduct.

Qualcomm fined for abusing dominance on the market for mobile chips[9]

At the end of January, the Commission issued a decision by which it punished the US manufacturer of telecommunication technology Qualcomm for abusing dominance on the European market. According to the Commission, the technological giant acted unlawfully from 2011 to 2016 by paying Apple billions of dollars for using only Qualcomm's LTE chipsets in their products.

Qualcomm's terms set out that they would stop the payments if Apple changed the supplier. Apple would even be required to return the payments that were made previously.

According to the Commission, Qualcomm, which holds over a 90% share on the market for LTE chipsets for mobile devices, precluded its competitors from participating in competition.

Chairman of the Office reduces fine for failure to provide data for timetables[10]

CHAPS – a company possessing the complete data for transport timetables in the Czech Republic – has long denied making the data accessible to other competitors. In 2016, the Office assessed CHAPS's behaviour as abuse of dominance by hindering other competitors from entering the market for automated transport connection searches. In its first-instance decision, the Office fined CHAPS over two million Czech crowns.

In remonstrance proceedings, the chairman of the Office changed this decision and reduced the fine by more than half to CZK 1,080,000. According to the chairman of the Office, the first-instance authority incorrectly applied the EU law, as only Czech law was to be used and the Office did not possess sufficient underlying documents for applying the Union law. At the same time, it was determined that the illegal conduct occurred for a shorter period of time.

Commission opens an in-depth investigation of a merger between Apple and Shazam[11]

Apple is interested in buying the most popular music recognition application for mobile phones. The Commission decided to perform a deeper analysis to consider its preliminary concerns about distortion of competition.

These preliminary concerns follow from the potential risk that Apple could gain access to sensitive data relating to customers of its competitors. It could then more easily target its music streaming services and try to attract these customers to the Apple Music service. Hence, the Commission will investigate whether other competitors will be damaged by this merger.

Regular news overview

We discuss with you these and other interesting EU and Czech competition law decisions at least twice a year at regular seminars held within the framework of the HAVEL & PARTNERS Academy. Follow the schedule and visit our autumn seminar.

[9] http://europa.eu/rapid/press-release_STATEMENT-18-427_en.htm.
[10] https://www.uohs.cz/cs/informacni-centrum/tiskove-zpravy/hospodarska-soutez/2380-pokuta-pro-chaps-byla-snizena-porusil-jen-narodni-pravo.html.
[11] http://europa.eu/rapid/press-release_IP-18-3505_en.htm.

Authors:
Robert Neruda | *Partner*
Lenka Gachová | *Managing Associate*


HAVEL & PARTNERS

CONNECTED THROUGH SUCCESS

Our team

200 lawyers | **400** employees

Our clients

1,000 clients | **70** of the Fortune 500 global companies
50 companies in the Czech Top 100 league | **7** companies in the Czech Top 10 league

International approach

Legal advice
in more than **80** countries of the world
in **12** world languages
up to **70**% of cases involve an international element

www.havelpartners.cz

PRAGUE

Florentinum, Reception A
Na Florenci 2116/15
110 00 Prague 1
Czech Republic
Tel.: +420 255 000 111

BRNO

Titanium Business Complex
Nové sady 996/25
602 00 Brno
Czech Republic
Tel.: +420 545 423 420

OSTRAVA

Poděbradova 2738/16
702 00 Ostrava
Czech Republic
Tel.: +420 596 110 300

BRATISLAVA

Zuckermandel Centre
Žižkova 7803/9
811 02 Bratislava
Slovak Republic
Tel.: +421 232 113 900