Czech Republic

Robert Nešpůrek is one of the founding partners of HAVEL & PARTNERS law firm and currently manages the firm's commercial, IP & technology group. Throughout his professional career in law, he has specialised, among others, in contract law, information technology, intellectual property and data law. His clients include internet platforms, e-commerce businesses, IT companies as well as major corporates and technology start-ups. Before establishing HAVEL & PARTNERS, Robert worked at the Prague and subsequently London offices of a global law firm. He obtained an LLM in European Business Law from Radboud University Nijmegen in the Netherlands.

Štěpán Štarha is a partner of HAVEL & PARTNERS law firm specialised in IT and telecommunications law, intellectual property law, data protection, contract law and private international law. Štěpán also regularly lectures on these topics.

Dalibor Kovář is a managing associate of HAVEL & PARTNERS law firm specialising in intellectual property law, information technology, e-commerce, innovation and start-up projects, legal aspects of electronic legal acts, and the law of contract. Dalibor participated in the most essential digitalisation legislation projects in the past years.

Richard Otevřel is a counsel of HAVEL & PARTNERS law firm specialised in e-commerce, IT, and personal data protection. Richard has been cited by the independent international publication *Who's Who Legal* as one of leading international experts in the Czech Republic for the area of information technology, telecoms and media, data privacy and protection, and data security since 2011.

1 What are the key features of the main laws and regulations governing digital transformation in your jurisdiction?

One of the most important laws adopted this year is the Act on the Right to Digital Service (ARDS), the 'digital constitution'. The ARDS was drafted by the private sector and its enforcement has been without a doubt the key to the digitalisation progress of (not only) the public administration, but has been further endorsed by the administrator of the Ministry of Interior of the Czech Republic. The ARDS will provide for the gradual digitalisation of all partial steps (digital services) carried out by the public administration and those that can be theoretically carried out digitally. The administration must come up with a list of its obligations and types of actions with external impacts, namely, they must compile a 'service catalogue' and they have until February 2021 to do so. In the next four years, the government, together with other public authorities and bodies, will digitalise all non-digital agendas, primarily those that could be of benefit to the wider public as well as those generating the highest added value, and should be greeted by the public with general acceptance. It is thus about transforming processes that had previously been non digital or manual, to digital processes.

The service catalogue will be updated regularly, and it will be available online to facilitate the digitalisation of not only certain actions but also of entire agendas, and will modernise and optimise services provided by the public sector. The open catalogue will thus throw the digital service into an unknown sphere from which the private sector should benefit. This would also help digitalisation from the ground up. The ARDS will allow attaching an electronic certified signature from 1 February 2022, which will be the final farewell to the use of paper documents, which people previously had to sign themselves.

Further, the eGovernment cloud has also been introduced into Czech law this year, and has been three years in the preparation. The government is now expressly allowed to use cloud computing solutions that will introduce major savings and a simplification of state IT infrastructure once used in a coordinated way. Cloud computing will also have its own service catalogue (offer and demand) that will directly influence the use of cloud solutions. Existing solutions must be entered in the catalogue within three years from the force of the act, otherwise the public authority should disconnect such solution. In fact, the cloud is now poorly used by the government and IT vendors feel an opportunity to build their business on existing private sector solutions.

There have been few modifications to the Act on Cybersecurity. Recently, governmental bodies started to be very active in education and took preventive measures within the Czech market (in reaction to, for example, cyberattacks on


Robert Nešpůrek


Štěpán Štarha


Dalibor Kovář


Richard Otevřel

public hospitals). Particularly the biggest private, and almost all public, organisations are now more clearly focused when it comes to on cybersecurity.

Bank identification has also become a key feature of Czech digitisation laws as further developed in the following point.

2 What are the most noteworthy recent developments affecting organisations' digital transformation plans and projects in your jurisdiction, including any government policy or regulatory initiatives?

The recent development in digital transformation in the Czech Republic is led by private industry rather than by governmental policies.

The most noteworthy development in the Czech Republic is the upcoming electronic identification via Czech banks. The Bank ID initiative will enhance mainly the scope of activities carried out by banks, namely by providing electronic identification, authentication, and trust services as well as other related services. The basic element of provided services will be the means for electronic identification such as login tools in internet banking for bank clients. It is anticipated that everyone will have these tools and knows how to use them. This is the basic difference as compared to national means for electronic identification (ID card with electronic chip); using them requires a chip card reader, servicing application and knowledge of several numeric codes. It is little surprise that that the existing means have not been used widely. Bank ID should allow both logging-in to national digital services and (in synergy with the ARDS) concluding and signing a contract remotely, viewing an electronic file or verifying one's own identity with all online services providers and using these services from the comfort of one's own home.

From 1 January 2021, the upcoming Bank ID offers the government and the private sector up to 5.5 million potential users who already have and are familiar with their means of access. Along with the above, the connected legislation will allow banks and insurance companies to access basic registers and other selected public administration IT systems, and also to verify whether clients' data is up-to-date in order to comply with the obligations stipulated by the legal regulations. This development represents a digital transformation in terms of a new digital business model.

Aside from the above, organisations might benefit from more frequent technology partnerships built between Czech banks and technology companies (including start-ups) – for example, the wider facilitation of payments; the use of AI within interaction with the clients; and focusing on their (eventual) needs or building reliable platforms for various legal acts for the public.

"When negotiating contracts with a Czech provider, it is good for organisations to know that a liability for damages cannot be fully excluded."

3 What are the key legal and practical factors that organisations should consider for a successful Cloud and data centre strategy?

It is very important to assess what data and processes are to be operated within the cloud service or data centre, particularly whether they are critical or non-critical for the organisation and whether the cloud service is public or private. Many organisations in the Czech Republic rely on a public cloud but a private cloud is also not exceptional. In the Czech Republic, the main focus is usually on the areas (among others) of liability; personal data; and cybersecurity aspects which are slowly gaining importance. Despite there being many specialised providers of various services, Amazon, Google and Microsoft are the key players in the Czech Republic cloud services. There is a high number of providers specialising particularly in helping organisations with their cloud migration.

When negotiating a contract with a Czech provider (and it is expected that such a contract will be governed by Czech law unlike in the case of the international players mentioned above), it is good for organisations to know that liability for damages cannot be fully excluded, although providers are keen to do so in their

standard contract documents. Czech law forbids the limitation of liability for damage caused to a person's natural rights, intentionally or by a gross negligence. More importantly, it does not allow a limitation of liability towards a weaker party. The weaker party is a concept introduced into Czech law by the Civil Code effective from 2014 and it states that this can be any person in a business relationship with another party whereas the business relationship does not relate to the (weaker) party's own business (eg, a company buying a laptop from an e-shop for its employee) but it may also include situations when adhesion contracts (standard contracts with no possibility of any negotiation whatsoever) are concluded. A clause in such a contract that refers outside of the contract text (website, etc), may only be valid if the weaker party was acquainted with the clause and its meaning by the provider or the party must have known the meaning of such a clause. It is quite often that personal data processing matters are excluded from any limitation of liability.

If we focus on the specifics of the cloud, the key factors to consider include the quality of the service (specification, functions, ability to help achieve set goals); security (both physical and digital, externally and internally); availability (reasonably set uptime and reaction times); and accessibility (connectivity, speed of data processing, etc.). These areas have an effect deep within the factual and contractual characteristics internally and externally towards respective suppliers. Organisations should also consider any specific regulations having effect on their business. Such legislation may include data protection regulation (GDPR and local laws – in the Czech Republic, there is an Act on Personal Data Processing), cybersecurity laws (Act on Cybersecurity, implementing the Directive (EU) 2016/1148 of the European parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, but note that there is more in the Act on Cybersecurity than in the directive) or perhaps financial sector regulations.

Anything extra required from the supplier may affect the service price. That is why organisations should consider very carefully the scope of services they need to avoid paying for an attractive feature that no-one in the organisation uses.

4 What contracting points, techniques and best practices should organisations be aware of when procuring digital transformation services at each level of the Cloud 'stack'? How have these evolved over the past five years and what is the direction of travel?

The market has gone through a vast development in recent years. There are many more providers who believe a subscription-based Software as a Service (SaaS)

solution is the key to success. Therefore, before contracting with any new provider and giving them your valuable data for processing, the provider should be checked to avoid any unwanted and adverse effects on the organisation's business.

Providers usually tend to push their own template documentation. This is quite understandable since it keeps the legal costs per contract at a minimum. But organisations should review these documents thoroughly as they often miss some key assuring points. To describe a common practice, usually a non-disclosure agreement (NDA) (with a penalty for its breach) is signed before the provider is allowed anywhere near an organisation's internal database of information. We may often see a provider assessment process is initiated before or after signing the NDA. When personal data is in question, the providers usually tend to accept clients' own data processing agreement (DPA) particularly in cases if organisations are high-profile with regard to data processing (such as in the e-commerce sector).

Liability always has been and still is a big topic. Providers tend to limit their liability as much as possible and organisations tend to avoid it, which can create a certain level of friction. But in general the limitation of liability is standard. GDPR,

Photo by LALS STOCK on Shutterstock

"The area of liability for damage and the possibility of its limitation has undergone fundamental development in Czech law over the past 10 years."

however, made a big change to this, and greater liability of the provider is required; in fact, it is often unlimited.

Each level of the cloud stack requires a specific approach. With regard to the hardware part of the cloud (data centre), the main concerns are maintenance and physical security (access to the data centre, etc) but this does not always have to be the case particularly if your contractual party offers you a service without anything related to a specific data centre.

The connectivity layer (networking, firewalls, security) usually requires regular updates to the security infrastructure (software, firmware) and organisations should carefully assess necessary reaction times and require the provider to perform proactive monitoring of risks and their mitigating tools.

With regard to servers, storage, virtualisation and operating systems as well as development and analytic tools and databases, a proper licence structure should be established and managed to allow future changes with no unnecessary risks. A provider should advise with the proper licence model and guarantee that such a model has been duly assessed. The main topic regarding storage is backup. Reaction times and fix times are often the main parts of any service level agreement (SLA)

since they affect the organisation's ability to avoid major data losses. Organisations should specifically agree on who is responsible for backups as this is not a typical part of the service.

The main part visible to regular users – hosted applications and data – should have a proper licence acquired. Also, do not forget to add a technical specification of the applications (or a service, as often described in contracts) to the contract to be able to enforce the application quality at any time. Organisations should make sure that their data is encrypted, accessible at any time (including their backup) and always (or at least some time before the contract expires) ready for migration.

Despite this being rather a general rather than a cloud-specific matter, organisations should care about the governing law and setting up courts' jurisdiction since SaaS or other digital services are very often cross-border services and thus the governing law is often an important point for negotiations. If parties cannot agree, it is often recommended to settle with a neutral legal system which is close to both systems. For the Czech Republic, this is typically Germany or the Netherlands. Organisations should also push the provider to implement certain contractual penalties for breach of the most important obligations in the contract.

5 In your experience, what are the typical points of contention in contract discussions and how are they best resolved?

It is probably not surprising that even in the environment of Czech law the typical points of contention in contract discussions include the scope of liability for damage; the scope of the client's or customer's cooperation; the scope of granted intellectual property rights or a licensing arrangement; and data rights.

The area of liability for damage and the possibility of its limitation has undergone fundamental development in Czech law over the past 10 years. While 10 years ago under Czech law the exclusion of the right to compensation for damage and even its limitation was, to the surprise of foreign suppliers, considered inadmissible and therefore invalid, the situation is completely different today. Czech law allows validly negotiating not only on a limitation on the amount of compensation for damage, but also its complete exclusion (while respecting statutory restrictions that do not allow regretting the right to compensation for damage, for example in cases of an intentional breach of an obligation or interference with natural human rights). In this legislative situation, suppliers in the Czech Republic usually try to limit the compensation for actual damage and to exclude any other types of damage. At the same time, suppliers often exclude in their model documentation any indirect, consequential and similar types of damage that Czech law does not even explicitly recognise. On the other hand, clients (especially those in the public sector) are often reluctant to accept any

restrictions on the right to compensation for damage, despite this being a common standard abroad.

The first step in discussions that should be taken in the environment of Czech law is to think about the wording of the clause on limitation of compensation for damage from the viewpoint of Czech law and revise the wording of contractual documentation, which will often have been created under the influence of foreign law, and will contain references to various indirect or consequential damage, which is not clearly defined in Czech law. Either the parties will remove these 'monuments' of foreign model contracts or, on the contrary, they will define them more clearly, thus removing the first stumbling block. In further discussions, it is appropriate to attempt to agree on the limitation of compensation for actual damage and the amount of lost profit by a specific amount (usually through the amount of the agreed price or a percentage thereof). Clients in the Czech environment will finally agree to such a limitation if there are exclusions from the agreed limit that address the most pressing risks for clients. Such exclusions typically include possible penalties for breaches of personal data protection, or other penalties by the regulator (for example, the Czech National Bank in the case of clients falling under its supervision). In our opinion, in Czech practice an agreement constructed in this way, which is a compromise between the interests and objectives of the client and of the supplier, can be reached. And contracting authorities are gradually becoming more willing to do so when preparing tender documents for a public contract as well, when they realise (it is explained to them by advisers) that unlimited liability may only discourage responsible suppliers and support those who are not serious enough.

The second typical area in which discussions arise in the Czech Republic is the definition and scope of the client's cooperation during the delivery. Unfortunately, it is a standard (and negative) practice in the Czech Republic that the client's cooperation is not clearly defined and its entire arrangement is summarised in one sentence saying that the client shall provide all necessary cooperation. It is clear that such a reflection in the contract leads to the supplier and the client having diametrically opposed ideas about the extent to which the client and its employees should be involved in the entire delivery process. Therefore, in the Czech Republic, disputes concerning the delivery of IT solutions mostly end in disputes over whether or not the client has provided the agreed cooperation. In practice, when addressing this problem, we have found greater interconnection between the lawyers preparing the contracts and the IT staff, and consistency on the part of the lawyers in defining the requirements for cooperation and obtaining the necessary information from factual sponsors to be useful. The solution then differs depending on whether the delivery is executed through the traditional Waterfall model or through the Agile or even DevOps model. In any case, however,

Photo by Lanski on Shutterstock

it is necessary to define the capacities and roles that the client will provide, which is something that is still not standard on the Czech market.

Another area in which discussions often arise is the licensing arrangement or regulation of intellectual property rights. In the Czech Republic, from our experience, clients, whether from the public or private sector, often cling to the fact that they will have an exclusive licence to the delivered solution. This is, of course, something that is problematic for suppliers, and if it is accepted, it leads to an increase in the delivery price. However, this requirement is deeply rooted in the minds of Czech clients, despite it not often being preceded by any in-depth consideration. In practice, we have found it worth broaching this business question with clients and encouraging them to explain why they actually insist on an exclusive licence. Often, the client is able to easily accept a non-exclusive licence and request an exclusive licence only for those parts of the delivery that are custom-made and, at the same time, the exclusive licence makes sense in relation to them. Sometimes in practice, the solution for the client is to bind the supplier with a specific non-compete clause and confidentiality agreement and at the same time acquire only a non-exclusive licence. In addition to the issue of licence exclusivity, it is worth noting that there is still a debate in Czech law as to whether or

not a SaaS solution contract should also include a licencing arrangement. For the avoidance of doubt, most lawyers in the market are inclined to include the licencing arrangement in the SaaS contracts for prudential reasons.

The last of the main areas we would like to mention is data rights (both personal and non-personal data). Here, in our experience, disputes between the client and the supplier do not necessarily arise during negotiations, but, surprisingly, the parties often do not pay enough attention to this area. They often just prepare a general NDA or data processing agreement without a deeper analysis of business needs, which, however, do not correspond to the actual setting of the business case.

6 How do your jurisdiction's cybersecurity laws affect organisations on their digital transformation journey?

Despite cybersecurity in general as a topic, particularly in the covid-19 era, cybersecurity laws do not affect most organisations at all. The cybersecurity laws affect only a minor group of companies within the private sector (typically telecommunication providers) and thus all measures are usually implemented due to other requirements (personal data protection laws, compliance programs, company group rules etc.). Cybersecurity may, however, affect organisations when they provide services to the public sector. In such a case, they may be identified as an obliged entity under the cybersecurity laws. Even in such a case, the requirements more or less correspond to obtaining an ISO certification (ISO/IEC 27000 family).

7 How do your jurisdiction's data protection laws affect organisations as they undergo digital transformation?

Luckily, the GDPR brought at least some uniformity to what limits a local legislation may impose on data processing. On the other hand, Czech laws did not include any unpleasant rules such as localisation requirements even before 2018 and, interestingly, have been treating both paper and electronic documents equally (the only practical issue, not relevant to electronic data, is readiness of documents – producing paper evidence upon request of authorities may delay the whole process if kept in another country, for instance).

We experienced the tendency of some governmental agencies to include provisions requiring storage of personal data within the Czech territory, but this has never become an official strategy due to being clearly against EU law.

However, even without explicit localisation requirements, the CJEU's recent decision in the Schrems II case revealed how fragile business cooperation concerning the processing of personal data outside of the EU can be. The only

"The CJEU's recent decision in the *Schrems II* case revealed how fragile business cooperation concerning the processing of personal data outside of the EU can be."

functional and flexible measure remains the using of Standard Contractual Clauses (SCC), although this has its own caveats. First, everyone wishing to use SCCs, must reinforce those clauses when exporting personal data to a country where the SCCs themselves do not suffice, but it remains unclear how the private company should assess such risks and what the reinforcement should look like – we are still waiting for an official guidance at the EU level since the Czech Data Protection Authority does not seem to have developed its own recommendation beyond what is mentioned above here. Second, not all scenarios are covered by the approved SCCs – for example, a processor located in the EU may not use a sub-processor outside the EU without making a formal arrangement with the controller. And finally, customers have started to perceive any extra-EU processing as a sign of risk, thus the requirement to localise data at least within the EU is more frequent from the businesses themselves than legislators already.

Photo by Nature's Charm on Shutterstock

8 What do organisations in your jurisdiction need to do from a legal standpoint to move software development from (traditional) waterfall through Agile (continuous improvement) to DevOps (continuous delivery)?

In our experience, the problem of transition from the traditional Waterfall model through Agile (continuous improvement) to DevOps (continuous delivery) is mainly in the heads of lawyers and managers and not in the legislation. First of all, it is therefore necessary to change the reasoning of lawyers and managers in order to move away from the automatic requirements to define a fixed price for a specific predefined performance in each contract. This approach is incompatible with moving to Agile or DevOps. In Czech practice, clients are either not willing to agree with the change of this paradigm or, on the contrary, they approach it nihilistically, not providing for Agile and DevOps formally in contracts at all, and operating only on the basis of orders and payments for the use of the supplier's staff's capacity without further contractual arrangement. Obviously, neither approach is correct and even

deliveries executed through the Agile or DevOps model deserve proper providing for in contracts.

One specific area is the use of Agile and DevOps in the public sector, where the situation is more complicated than in the private sector due to public procurement law. Even here, however, in our opinion, in the environment of Czech law, it is possible to award a contract to a supplier for deliveries executed through Agile or DevOps. In order to use such a supplier, it is only necessary to go into the depth of the public procurement rules and not automatically announce a tender procedure only for services (the supplier's capacity), as is happening in the Czech Republic today. As for the market practice, however, we have unfortunately not yet come across a tender procedure for awarding a contract for delivery through the Agile or DevOps model.

9 What constitutes effective governance and best practice for digital transformation in your jurisdiction?

We are dealing with the common understanding that every organisation should shape up to the new reality that was present even prior to covid-19. The pandemic speeded up the processes and drive to adopt digital solutions. We believe that almost each organisation is now somehow facing the dilemma as to how to digitise and transform itself to be more effective, efficient and at the same time relevant on the market.

It is very fortunate to see that the biggest organisations do not hesitate to pay top-tier advisers to help with their digital transformation projects and share the relevant information throughout the market (including the impact on end customers and negative steps within the project). Further, the knowledge base and technical preparedness of the organisations' advisers has increased tremendously in the past years. Therefore, we experience rather detailed and well-built digitisation plans based on automatisation, robotisation, access management and overall hardening of the environment to be safe and sound without limitation of the user's comfort.

Without doubt, the best (and most necessary) practice of digital transformation is switching from on-premise solutions to cloud, to provide organisations, their workers, and clients more flexibility.

An effective transformation should benefit from the cross-functional co-operation of executive directors with CIOs and other senior managers of the organisation by connecting approaches focused on business with fast development models (Agile and DevOps). For example, all major Czech banks switched to the Agile method of organisation in the past years giving an example to other sectors with the aim to align transformation goals with business goals.

Technologies represent a necessary essence of digital transformation and are already present, but we perceive a new standard in the development of the digital competencies of employees and of other workers within organisations, as well as the sharing of a defined strategy. Digital transformation requires a change of thinking, new competencies, discipline, and personal courage to be implemented in everyday life. This approach is vital but has been neglected in the past. Defining a compelling communication strategy and vision to sell the transformation story to an organisation can thus also be perceived as best practice in digital transformation in the Czech Republic.

Robert Nešpůrek
robert.nespurek@havelpartners.cz

Štěpán Štarha
stepan.starha@havelpartners.sk

Dalibor Kovář
dalibor.kovar@havelpartners.cz

Richard Otevřel
richard.otevrel@havelpartners.cz

HAVEL & PARTNERS
Prague
www.havelpartners.cz

The Inside Track

What aspects of and trends in digital transformation do you find most interesting and why?

Robert Nešpůrek: It is the unprecedented growth of the ecosystem of IT solutions providers and the emergence of new players. We have worked on digital transformation projects with large multinational IT companies as well as medium companies both local and from around the world, as well as start-ups. Customers' options have multiplied. Digital transformation is transforming not only the corporate world but also the IT sector in the Czech Republic potentially delivering greater value to customers for their money and flexibility, thus addressing some of the issues carried by the 'old' IT world.

What challenges have you faced as a practitioner in this area and how have you navigated them?

RN: Advising on digital transformation requires a new approach to defining legal solutions for clients that reflect clients' practical requirements and demand a multi-disciplinary, multi-faceted perspective. We have reorganised our teams across our commercial, IT and regulatory practices to provide fresh understanding of what digital transformation means for our clients and how we can best contribute to clients' digitalisation efforts. It is exciting to be drafting new legislation enabling digitalisation on one day, the next day discussing with a progressive IT provider how best to tap the newly emerging market around BankID and the day after helping a major corporates to adopt paperless processes involving an integration of a digital signature solution into a SaaS-based DMS.

What do you see as the essential qualities and skill sets of an adviser in this area?

RN: Clients face a major challenge of managing digital transformation that is not only technically sound but also contributes to the success of their business. It is crucial that besides technical legal excellence we help to find the best business partners, weigh the benefits of digitalisation against the costs and possible business disruptions, provide markets insights and approach a project with open mind to mitigate risks and achieve key goals.