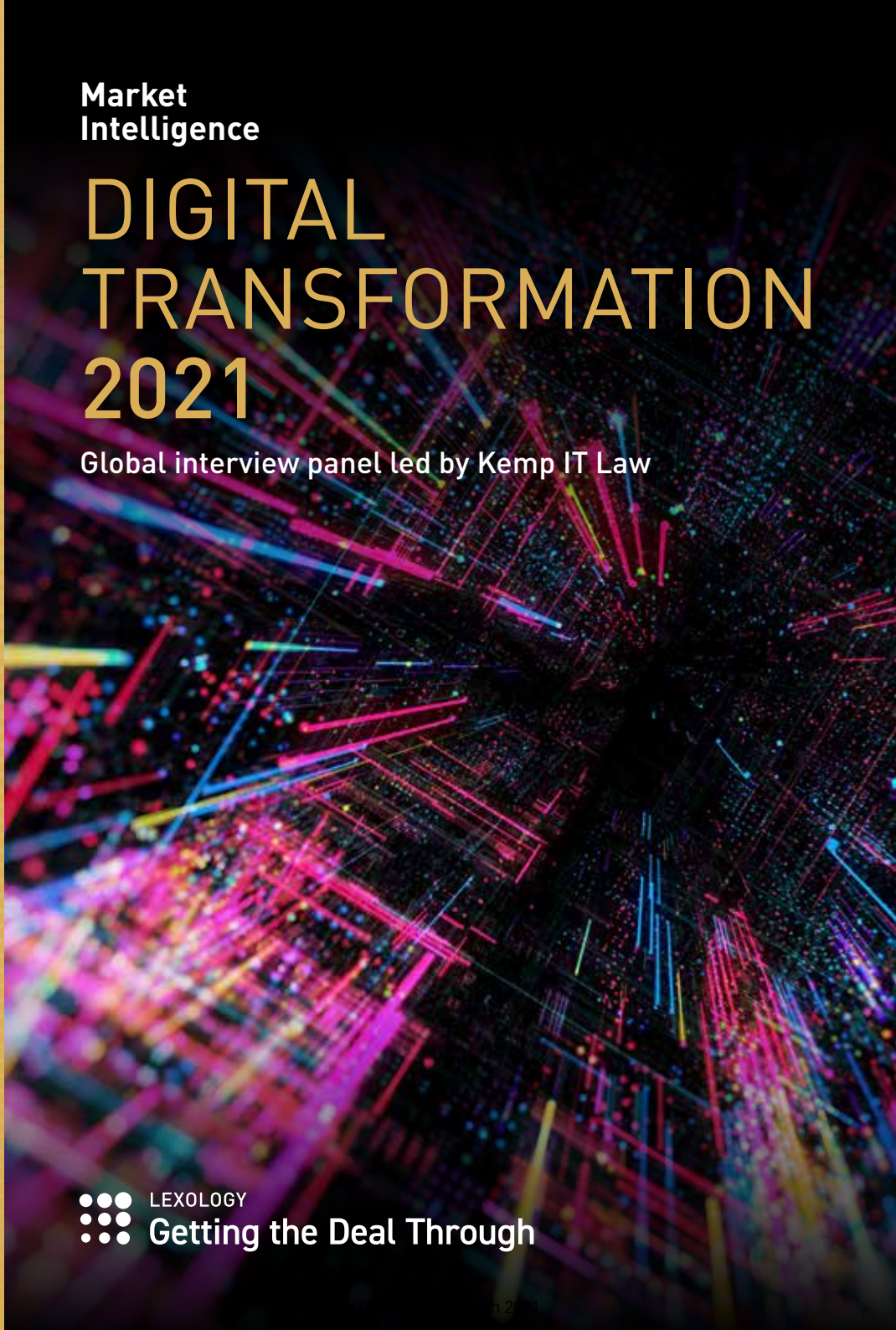
Market
Intelligence
DIGITAL
TRANSFORMATION
2021
Global interview panel led by Kemp IT Law
LEXOLOGY
Getting the Deal Through

LEXOLOGY
Getting the Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Printed and distributed by Encompass Print Solutions

DIGITAL TRANSFORMATION 2021

Belgium

Steven De Schrijver is a partner at Astrea and specialises in M&A, corporate law, IT and media, data protection and privacy and outsourcing. Steven has almost 30 years of experience in advising Belgian and foreign companies on corporate transactions and has been involved in numerous national and cross-border transactions in the IT, media, telecoms and life sciences sectors.

Steven also advises some of the largest Belgian and foreign technology companies, as well as innovative entrepreneurs on complex commercial agreements and projects dealing with new technologies, most of the time with a cross-border element.

Steven has been involved in many IT, outsourcing, software and cloud application development, digital transformation, telecom/media projects (establishment of first mobile telephone operator in Belgium, acquisition of Flemish broadband cable operator, joint venture to launch video-on-demand services) and data protection (now: GDPR) compliance projects. He has a passion for artificial intelligence, robotics and drones.

He is also active in the IBA Corporate and M&A Law Committee and the IBA Technology Law Committee and in ITechLaw. He is past-president of IFCLA and a member of the Tech M&A Committee of ITechLaw. He is an honourary member of AIJA and the Belgian member of EuroITCounsel.

Photo by Karol Kozlowski on Shutterstock

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

There are no Belgian laws or regulations that specifically and exclusively deal with digital transformation. This process is very broad and hence many fields of law will come into play, ranging from contract law to labour law (eg, employee participation and information requirements) to IP law (eg, the protection of trade secrets or the organisation's IP). Customers will usually perform internal audits to determine their needs; request information from potential suppliers (with or without signing a non-disclosure agreement); and request proposals and then negotiate with multiple suppliers to enter into final contractual negotiations with the chosen supplier. If the digital transformation involves the government and certain public companies, public tenders are also possible. Specific regulations and procedures relating to outsourcing can also come into play (eg, in the financial sector).

It is difficult to summarise the different laws that regulate digital transformation, as this process has the potential to involve every field of law. In any case, the most relevant are the Belgian Civil Code (which includes contract law); the Belgian Code of Economic Law (eg, unlawful B2B clauses, precontractual information requirements or IP); the EU General Data Protection Regulation 2016/697 of 27 April 2016 (GDPR), which deals with privacy and data protection; the Belgian Act of 30 July 2018 on the protection of personal data; the Belgian Act of 7 April 2019 on the security of Network and Information Systems (NIS Act); and the Belgian Act of 17 June 2016 on public tenders (as well as regional laws for Flanders, Wallonia or Brussels on public tenders). Any (other) relevant EU regulations and directives must also be considered.

There are no Belgian laws that specifically address data localisation as Belgium generally takes a liberal view, wishing to ensure that data is allowed to flow freely in line with European law on the free movement of date. This position is legally in accordance with Regulation 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. With regard to personal data, the GDPR (which also applies directly in Belgium) does not stipulate any data residency requirements, nor does it operate the concept of data localisation.

The GDPR, however, contains provisions restricting data transfers outside the European Economic Area (EEA) and lays out conditions for such transfers. Summarised, international transfers of personal data outside the EEA are possible if there is an adequacy decision on the data protection laws of a third country by the European Commission; there are appropriate safeguards in the contract (such as binding corporate rules or standard contractual clauses approved by the European Commission); or based on a number of derogations, such as explicit consent by


Steven De Schrijver

the data subject to the proposed transfers, subject to having received all necessary information about the risks related to the transfer.

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?

With millions of Belgians once again being forced to work from their home offices in Belgium's mostly service-based economy, the cry for cloud migration, cybersecurity, data protection and other digital aspects is louder than ever before. Organisations are addressing these needs extensively, creating opportunities for digital service providers as businesses move to video conferencing and other convenient ways to communicate online. However, not only bona fide organisations benefit from the digital transformation process. Cyber criminals take advantage of the fact that many SMEs do not have strong cybersecurity measures in place, for instance because such companies use the Bring Your Own Device approach that, in combination with teleworking, makes employees much more vulnerable to cyberattacks. We

anticipate that the initial implementation of 5G networks will, apart from its added benefits to the entire spectrum of industries and social activities, also bring severe security risks as a result of an increased interconnectivity of the entities operating with it. That is why EU member states are urged to promptly implement the EU 5G Toolbox set out in the new Cybersecurity Strategy (adopted March 2021), including robust and comprehensive measures for an EU coordinated approach to secure 5G networks. One of the most important measures is the EU-wide certification scheme for 5G networks that should help to address the risks related to the technical vulnerabilities of such networks.

Artificial Intelligence (AI) applications can help companies transform their business by improving prediction, personalising digital solutions, optimising operations and resource allocation. Apart from the economic and societal benefits to the entire spectrum of industries and society as a whole, the EU is also aware of the possible risks to its users and affected individuals. Hence, the EU has put forward a proposal for a regulation laying down harmonised rules on AI in April 2021 (the AI Regulation), which is set to regulate certain high-risk AI systems. However, the EU's quest in fostering the development and uptake of AI in the EU cannot be situated in a judicial vacuum. The safety of these products and services does not only rely on their design and production, but also on software updates and data flows feeding their algorithms. These features of digital technology and AI challenge the application of the traditional liability regime, governed by the 1985 Product Liability Directive (PLD) and national liability rules, which creates legal uncertainty for businesses and consumers. Since an ecosystem of excellence cannot be installed without trust, the European Commission is currently consulting on adapting the EU civil liability regime to new technologies in the digital age of ubiquitous interconnectivity and circular economy.

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

Customers will often have to find a balance between their needs and the possibly limited margin of negotiation when contracting with large players. The latter will usually impose their general terms and conditions from which they will only accept very limited derogations. It can also be useful to seek a basis for drafting an agreement in the ISO norms (ISO/IEC 17788, ISO/IEC 17789 and ISO/IEC 27018), which may offer the customer guidance in this respect.

An important factor is the security of cloud services. Not only it must be determined whether personal data are successfully and sufficiently protected. The same protection should also be sought to other business data that are uploaded in

> "Customers will often have to find a balance between their needs and the possibly limited margin of negotiation when contracting with large players."

the cloud. The customer may wish to include audit rights with respect to security measures. Customers can better select a cloud service provider that has good governance over the processing of personal data and IT security. Connected to this is a strong protection of the IP rights on creations uploaded or developed in the cloud. Customers may be reluctant to accept any rights of use of the supplier for data analytics in this respect. Clauses on the limitation of liability must be carefully reviewed, as too large an exoneration may effectively leave the customer without any damages in the case of losses, which have the potential to be large (especially in the case of a data breach).

In this context, applicable law and jurisdiction are also very important. If a Belgian customer needs to enter into a contract under English law with jurisdiction in the US, its enforcement position may be weaker. In addition to this, he or she would need to involve an English lawyer to review the contract as a Belgian lawyer would not be able to advise with his or her scope of jurisdictional expertise. This may come at a much larger legal cost than initially foreseen. But when assessing the costs of negotiation (and the overall costs), customers must also remember that the cheapest provider of services is not always the best. A detailed analysis of the

real services and contractual guarantees must be carefully made. A comparison on price alone is insufficient.

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?

Many of the key contracting points when procuring these types of services will be similar, especially when it comes to privacy; data protection (especially data access, use or control); liability; IP rights (whereby full ownership must remain with the customer); and dispute resolution (including adequate remedies). Sufficient confidentiality agreements must be concluded that protect the customer's trade secrets. Non-solicitation clauses may be useful. Service level agreements (SLAs) provided by suppliers will also have to be critically assessed, especially with regard to clauses on the availability of the services; maintenance; the solving of breakdowns; and the performance. With regard to cybersecurity, maintaining cyber insurance is becoming increasingly of importance to customers. Of course, the parties will also carefully negotiate representations on IP, privacy, IT security and the maintenance of IT systems.

Providers of telecommunication services are heavily based on technological advances, implementing revolutionary technologies such as 5G, artificial intelligence (AI) and the Internet of Things. When dealing with services that rely on these new technologies, customers must set aside the traditional interpretation of important clauses such as those dealing with liability. How, for instance, will the supplier be held liable for losses caused pursuant to a decision made by an AI system? If 5G services are being procured, the customer may wish to obtain the necessary guarantees that the network has been secured adequately and will remain sufficiently available. After all, due to more potential entry points and software reliance, the risk of attacks on a 5G network may be higher. The EU will resolve these questions at a higher level as to ensure the development of the internal market. The parties must also review whether any regulatory issues must be resolved (eg, notification to the supervising authority) or whether specific telecommunication laws apply (eg, when the parties intend to make use of radiofrequencies of operators for their system, the consent of the latter must be obtained for such use as it is the operator's responsibility to maintain a network without any disturbances).

When procuring data centre services, the localisation of the servers will be important to determine whether rules on international data transfers of the GDPR apply, in which case the necessary safeguards must be built into the contract.

Photo by velvetes on Shutterstock

Customers may request that the data are located with a local, or at least, a European provider. Clauses on sufficient technical and organisational security measures are also essential.

With respect to the acquisition of physical equipment (hardware), customers will often have to negotiate on the advance payments to the supplier, which often in the first draft of the contract amount to up to 50 per cent of the purchase price. Instead, it is much more accepted to include the following payment schedule: 25 per cent of the price at the delivery of the hardware; 25 per cent at the delivery of the software for the hardware; 25 per cent after positive acceptance test; and 25 per cent after the final acceptance of the hardware. Further key contract points will be, among others, related to: a time schedule for delivery; inspection of the supplier of the place of installation; the procedure and proof of final acceptance; amicable dispute resolution in the case of faulty delivery; and the guarantee period for the hardware.

In procuring virtualisation, the focus when contracting will lay on negotiating detailed SLAs, whereby measurable and enforceable terms and enforceable remedies

> "In the last five years, it seems that the most important changes in the terms of cloud service providers have been made after the adoption of the GDPR."

(eg, service credits discounts or damages) must be agreed upon. Maintenance and support services will be crucial, as they will become the backbone of this type of service together with system availability. Data ownership and data security will also be vital. Obviously, the customer must have sufficient safeguards that his or her data, which are essential for his or her business, remain secure when beyond his or her control.

We understand IT-related professional services engagements to also include consultancy agreements. Here, a large caveat must be made for labour law issues. Consultants must be considered and treated as independent parties, whereby customers must strictly avoid exercising any employer's authority (ie, giving consultants specific instructions on the organisation of their work and time). Because in Belgium you are either an employee (with an employment agreement) or a self-employed service provider, the risk exists that a consultancy agreement is requalified to an employment agreement if de facto the consultant is treated as an employee by the customer. This sham self-employment, a risk that is high in the Belgian IT sector, may cause the customer, pursuant to a requalification of the contract, to become responsible for all social security payments (which will be increased as a penalty with surcharges and interests) and all social expenses for

the de facto employee (holiday payments; end of year premiums; pension rights; bonuses; overtime pay; costs reimbursement, etc). This may be a considerable cost. Hence, drafting agreements with self-employed consultants must be done very carefully from a labour law perspective and the actual interactions between the principal and the controller need to be scrutinised.

In the last five years, it seems that the most important changes in the terms of cloud service providers have been made after the adoption of the GDPR. Cloud providers had to adapt their cloud terms by including or expanding wording on the processing of personal data; data transfers outside the EEA; security measures (the famous technical and organisational measures); and other GDPR-specific matters. The position of customers has also been strengthened thanks to these rules.

An interesting new development that has been introduced into Belgian law is a set of rules on unlawful B2B clauses, which are considered as mandatory law in Belgium. These rules entered into force on 1 December 2020 but their interpretation in practice is still awaited. In principle, they apply even when foreign law is selected, which means that they strengthen the position of Belgian customers and suppliers in cloud contracts. For instance, the rules require clauses to be more balanced and include rules on the limitation of liability, risk allocation and other important matters.

Another point of contention are the contractual clauses on the measures to be introduced by cloud and digital service providers pursuant to the NIS Act. The providers envisaged by the Directive must, from a technical point of view, provide adequate measures (which may differ from the GDPR) to protect the cloud system against incidents, depending on the size, importance and nature of the organisation and the technical knowledge available. From an organisational point of view, the supplier must have internal procedures, measures and action plans in the case of incidents or to avoid them. Customers may wish to include wording on these requirements so that they have the potential to invoke breach of contract in the case of an incident. These will become more important in the future with the NIS 2.0 Directive, which is set to expand the scope of the directive to many other entities.

Limitation of liability

The baseline for clauses limiting the liability of a party can, apart from the general rules in the Belgian Civil Code, be found in the Act of 4 April 2019. Even though its interpretation is yet to be awaited, it promises to prompt far-reaching extraterritorial effects. The Act introduces rules on unlawful B2B clauses applying to all agreements, including clouds service agreements. Beyond the obligation for clear and understandable contract terms, the protection consists of a blacklist of four clauses that are prohibited in any case and a gray list of eight types of clauses that are

presumed to be illegal unless the company shows that they are reasonable under the circumstances. Terms that are in any case prohibited include those limiting or excluding the right of access to the courts or those that irrefutably establish knowledge and acceptance of the terms and conditions. Furthermore, this blacklist also prohibits a co-contractor to reserve the right to interpret one or more clauses of the contract. Terms that are presumed to be unlawful, for example, are those that allow the company to change the price without justification, terms of tacit renewal of an unreasonable duration, terms that impose an undue economic risk on the other party, etc. Finally, a general standard considers as unlawful any term that, alone or in conjunction with one or more other terms, creates a manifest imbalance between the rights and obligations of the parties.

In conclusion, a contractual party is allowed to limit its liability, save for losses caused by willful misconduct; gross negligence or that of its employees; and except for cases of force majeure, for the non-performance of essential obligations that are the subject matter of the contract. Losses due to fraud cannot be excluded either, nor personal injury or death.

A supplier will also try to exclude liability for indirect losses. Belgian law foresees that the party that suffers losses must be indemnified for all foreseeable losses, but there is no clear definition of direct and indirect losses. It is therefore recommended to specifically list the types of losses that are covered or not.

Liability caps are possible, as the law on unlawful contractual clauses only deals with the exclusion of liability, not its limitation. However, these must always be reasonable and balanced. Typical examples are a cover that is not higher than the supplier's insurance cover or that is limited to the amounts paid under the contract for the performance thereof or to the amounts of the last 'X' invoices.

An alternative to clauses on the limitation of liability is to expressly qualify certain obligations as best efforts only, which means that the customer will have to present proof that the supplier did not make all reasonable efforts to perform his or her obligation. This burden of proof is heavier than the usual establishment of breach of contract due to non-performance of a certain contractual obligation.

Service credits

Service credits are generally accepted in service level agreements, but they should be drafted carefully as their legal nature has not been yet fully determined under Belgian law. If service credits are treated as a penalty clause in the contract, then they can be mitigated by a judge if they are exaggerated in comparison to what a reasonable contractual party would stipulate when placed in the same circumstances. Pursuant to this interpretation, the clause on service contracts will have to be balanced.

Photo by S-F on Shutterstock

Alternatively, service credits are viewed as a mechanism to establish the price for the services, whereby a lower quality of service leads to a lower price. Such qualification can avoid a risk of mitigation of the amounts in court. The downside here is that if the supplier does not meet its envisaged service levels, no breach of contract will be determinable with all consequences taking place in pricing only. It is therefore recommended to specifically include the parties' intention regarding the mechanism of the service credits in the contract.

Insurance

Belgian insurance clauses in IT contracts will usually not be as extensive as, for example, their US counterparts. In general, these will stipulate that the maintenance of an adequate insurance cover during the performance of the agreement is required, with the customer having a right to obtain proof hereof (eg, by receiving an insurance certificate). The types of insurance to be held by the supplier can be further listed, whereby a professional liability insurance is essential. In the context of digital transformation, it is advisable to seek cyber insurance cover for data breaches for both parties, which also covers the expenses of legal and forensic

> "The agreement upon which a long-term relationship can be built goes further and more in-depth than the identification, allocation and management of risks."

advisers and foreseeable. Due to strict labour law requirements, a sufficient work accidents insurance may also be required. It is rather unusual to list the specific amounts of the insurance cover.

Customer IP and IP indemnities

Belgian law in itself provides for solid protection of IP rights, such as copyright, patents, databases or trademarks. Contractually, it is recommended to foresee a mechanism that regulates the property rights of the IP. This can be done by making a distinction between the IP that existed before the entry into force of the contract (where there will be no discussion on the proprietary rights thereof) and the IP created during the performance of the contract. The latter category can be further distinguished between IP created on the demand of the customer (which will rather become its property, perhaps for an additional payment) and on the supplier's own initiative (which will rather remain its property). The customer will of course seek to gain ownership of all software developed during the performance of the contract. Whether the customer succeeds to obtain this, will depend on the strength of its

bargaining position, the value of the software and whether it is custom-made of standard software.

The use of 'licences' of the customer by the supplier to use certain IP for the performance of the contract is also frequent.

IP indemnification mechanisms for violations of IP rights, including those of third parties, are also common. The breaching party may also be held to defend the other party in court against the breach. Frequently, unlimited liability for the violation of IP rights are agreed upon as a deterrent. IP insurance is another possibility to be taken into account.

Termination

Contracts concluded for an indefinite period can be terminated at any time for convenience, but the parties can agree on a reasonable notice period. If the contract has a definite term, it will expire at the end thereof and cannot, save exceptions, be terminated earlier.

Belgian law grants each party the right to terminate the contract in the case of serious breach (sometimes with a remediation period), such as non-compliance with important contractual provisions like financial obligations for the customer, or non-compliance with key performance indicators for the supplier. The terminating party is in such a case also entitled to damages. In principle, a court judgment is required for this termination possibility. However, parties can agree on a termination clause without the involvement of a judge.

Sometimes the agreement will allow termination for convenience, but in that case, a lump sum indemnity and possibly a compensation for investments made by the supplier must be paid.

Mitigating supplier lock-in

The contract should seek to mitigate the risk of supplier lock-in by foreseeing the necessary support to re-source or in-source the IT services. A requirement of termination assistance by the supplier should be included, including wording on migration of applications and data to a new provider or in house and a transitionary period wherein the services may still be provided even if the contract has already been terminated or expired. This should also include a duty for the supplier to cooperate with his or her successor and other third parties to facilitate the transition. The cost for any transition or migration services should be agreed in the agreement between the supplier and the customer.

Migrating IT workloads and systems from on-premise to in-cloud during contract life cycle

Assistance by the supplier to the customer with respect to the transition from on-premise to in-cloud (including data migration) must be specifically agreed to in the contract as it is not supposed. It is not unusual to stipulate that the services will be provided 'as is' during a transitionary period, which can be viewed as a testing period. The terms of the SLA will then not yet apply. This gives the supplier the opportunity to carefully migrate to in-cloud and fine-tune the services where necessary.

TUPE or employee acquired rights when business services or functions migrate to the cloud

If an activity that can be considered as part of a business is transferred by the customer to the supplier, the employees are also automatically transferred based on identical employment terms (Collective Labour Agreement (CLA) 32-bis). The parties cannot contractually determine which employees transfer and which do not, neither can they contractually determine which employees form part of the activity as this is a question of facts. The application of these rules must be carefully assessed. The parties can work with a transfer plan that must be kept up-to-date and that is also clear about the allocation of costs and time spent by both parties in the process. Contractually, an indemnification clause can be agreed that foresees indemnification of the other party if certain assessments were wrong (eg, relating to losses caused by a wrong assessment of the employment rights that have been transferred). The transferee will usually require a warranty relating to any liability from the past, while the transferor will seek indemnification from claims by employees based on breaches of the CLA 32-bis procedure. The parties should work out in practice how to proceed with the obligatory requirements to inform and consult the employees and trade unions.

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

Belgian customers will, especially when entering into negotiations with large foreign digital services providers, have to cope with limited powers of negotiation. In many cases, cloud providers will simply present standard contracts from which they will not easily depart and that in most cases will be governed by a foreign law. The main points of contention will be the limitation of liability of the cloud provider; choice of law; wording on security measures; the use of best efforts clauses; a lack of sufficient guarantees in the SLA; the risk of vendor lock-in; the regulation of IP

rights; privacy; and rights of the supplier to suspend the services in certain conditions. Customers will need to negotiate balanced clauses whereby the limitation of liability of the service provider does not effectively render the customer without any rights of recourse. For instance, the liability can be set at the amount of the insurance cover and indirect losses can be excluded. Strong IP clauses that make sure that the customer's IP rights remain its ownership at all times will be crucial too. In connection hereto, the choice of law must be Belgian law, or a law in which the customer feels comfortable, so that the customer is not impeded from seeking indemnification in the case of a breach of contract (eg, if high legal costs would be incurred in a foreign jurisdiction).

However, the contract should not solely focus on the situation when something goes wrong. The agreement upon which a long-term relationship can be built goes further and more in-depth than the identification, allocation and management of risks. Both parties should clearly describe their expectations (what will be provided, when and the quality thereof); the roles and contributions of each of the parties; setting up a continuous governance process and what actions to take when discussions come to a halt.

Photo by K.Vilkas on Shutterstock

"The entry into force of the GDPR in Belgium has made organisations realise how important the protection of personal data and privacy is."

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

Apart from the GDPR, which contains certain legal cybersecurity obligations, an important part of the package of new measures under the New EU Cybersecurity Strategy (adopted March 2021) is the proposal for a Directive on measures for a high common level of cybersecurity across the Union. This Directive, informally called NIS 2.0, is supposed to repeal and build upon the 2016 NIS Directive. The personal scope will be broadened as entities will be classified based on their importance, and divided respectively in essential and important categories with the consequence of being subjected to different supervisory regimes. Essential entities in sectors such as energy, banking, health sector or digital infrastructure will now be joined by important entities in sectors such as postal and courier services, waste management, manufacturing, production and distribution of chemicals, food production, processing and distribution, manufacturing, with a possibility for member states to expand the latter category. Both categories are required to implement a non-exhaustive list of basic cybersecurity risk management measures ranging from risk analysis to use of cryptography and encryption.

Similarly to the 5G Toolbox, member states are encouraged to require essential and important entities to comply with the European cybersecurity certification schemes and to use European and international standards and specifications in the field of security of network and information systems. Importantly and contrary to the permissive 'may' wording of the old NIS Directive, the new directive will compel these actors to report significant cyber incidents to computer security incident response teams. Competent authorities will be empowered to issue fines of up to €10 million or 2 per cent of the total annual worldwide turnover of the respective essential or important entity. Companies across the EU should already familiarise themselves with the new proposal to start contemplating about the transposition into daily business. Of course, many proposals could already be applied in practice to boost an organisation's security.

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

The entry into force of the GDPR in Belgium has made organisations realise how important the protection of personal data and privacy is. While the heavier sanctions related to the breach of the GDPR are, of course, a key factor, general awareness of privacy matters has certainly increased overall in society as people are confronted

with privacy clauses and requests for consent more than ever. This puts additional pressure on organisations to address privacy concerns.

One of the most crucial changes in mindset, especially in the process of digital transformation, is the move from addressing privacy issues when they arise to the (obligatory) principle of privacy by design. Herewith, organisations are able to build privacy from the very beginning into their system, choose which types of personal data they really need to operate (data minimisation), foresee adequate protection measures and in general carefully assess each step in their set-up process out of a privacy and cybersecurity point of view.

Organisations are also increasingly aware of the risks associated with relying on a certain platform of other companies for their operations, especially if that platform is foreign. Restrictions on the transfer of data (and often entire change of the current law, such as with Schrems II, which requires immediate action and supplementary measures) and concerns about the security of the organisation's data abroad have certainly moved higher up the agenda of Belgian boards of directors.

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)?

Parties wishing to move from waterfall to Agile software development will focus less on negotiating liability clauses, but will set out detailed agreements on the development process and acceptance procedures. In contrast, in waterfall development, it can take months before the first results are presented and whereby only then it may turn out that the budget has been heavily surpassed, while the intended development has not been made in accordance with the customer's wishes. Heavy acceptance procedures that seek to verify whether the end result matches the extensive software specifications prepared at the time of the conclusion of the agreement are also more common in the case of waterfall development. In such a case, liability clauses are important to address the unforeseen costs.

Setting aside the general key contracting points, which have been sufficiently set out above, parties must agree on a clear outline of this process (eg, in a schedule to the agreement itself). In Agile development, it is important to foresee detailed and clear clauses to inter alia regulate short meetings to evaluate the current state of affairs (scrums or sprints); define the sprints; re-evaluate every step; have constant discussions between the customer and the supplier; maintain clear lines of communication between the parties; appoint representatives of each party; include testing; and regulate acceptance. Agile development represents a change of thinking whereby the focus should be on the training of staff; regular communication; faster

collaboration between teams; and flexibility on the form of the end product. As there is continuous delivery and acceptance, the risk of non-fulfilment of the expectations and wishes of the customer is much lower, resulting in a lower risk of liability too.

Customers must take into account that in DevOps development the development teams remain responsible for the operation of the software and continuous improvement thereof. Hence, contracts will not only address the development process itself (as in Agile), but they must also address what happens thereafter. The scope will therefore be much more open, as the DevOps team will be focused on the creation of value, improving the software and adapting to the customer's wishes, which will change over time rather than spending a lot of time and drafting and negotiating specifications that may anyway change during the course of the development. Outsourcing will frequently come into play, whereby clear outsourcing agreements will have to be negotiated. The main contracting points will be risk allocation and finding a balance between an open and closed scope, as well as agreeing how the scope may be changed. This is a difficult exercise, as the fees will depend on the anticipated risk, which is not always easy to define. The SLA will also be different in DevOps, as the accent lies on continuous monitoring and

Photo by MarinaD_37 on Shutterstock

reporting, as well as addressing flexibility and the constant change of needs, rather than monthly communications.

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

The process required for the digital transformation of an organisation will always depend on the type of organisation concerned. As the focus lies on transformation rather than on an ad hoc allocation of funds to develop or implement certain technology, the organisation must first perform a very detailed internal analysis of its digital needs and the needs of its customers. The board's role is crucial in this. The focus of the transformation may lie both on the improvement of internal operations and delivering better customer experience. Only when a vision has been established that can create value in the long term should further (legal) steps be taken, such as sending out Requests for Information to potential suppliers and subsequent Requests for Proposal. A due diligence should then be held with respect to the potential supplier to present a full overview of the risk's association with the supplier to the board. In general, the process must be marked by a drive to obtain as much information as possible on the needs and risks of the organisation's operation, also from employees, to fully address them throughout the further transformation. After all, the board's liability for an unsuccessful digital transformation may be at stake, as Belgian law requires all board members to act as reasonable, prudent board members placed in the same circumstances.

Digital transformation implies the use of data, often personal data, increased cybersecurity risks and reliance on technology. Therefore, with respect to any digital services that are being procured, organisations must apply the principles and requirements of the GDPR (and, if applicable, the NIS Act) in their process, such as privacy by design and by default, as well as the provision of technical and organisational measures. Companies should keep their eye on developments of the NIS 2.0 Directive, the AI Regulation and adapted liability regimes. They should not await their entry into force to implement the upcoming provisions in their long-term digital transformation journey.

Customers must also be made aware of the importance of good contract management when it comes to good governance. Of course, this is very important when preparing and executing the contract, but also and certainly afterwards. Organisations must ensure efficient obligation management, whereby the written agreements between the parties are frequently reviewed to make sure that the process that is being followed is in compliance with the parties' intention. Smart contracts may be an aid here. A (non-legal) summary of large and complex contracts

> "Customers must also be made aware of the importance of good contract management when it comes to good governance."

may be useful (certainly in the case of a detailed SLA), as well as setting deadlines in an internal electronic calendar to remain in control of the process and monitor it. The day-to-day operation teams that work on a certain project with external providers should be clearly informed about the contractual arrangements between the parties. It should also be foreseen that any meetings with external parties are minuted. The teams will be the first to be in a position to notify directors of any issues or contractual breaches that come up. Evidence on breaches can then also be immediately documented. Customers should also not be afraid to seek revisions and amendments if certain clauses seem not to work in practice after all.

Digital transformation may also be achieved through mergers and acquisitions (M&As) whereby organisations seek to acquire innovative businesses such as start-ups that develop promising technology that could assist them in becoming more digital, innovative, efficient and/or attractive for customers. In technology M&As, such organisations must prepare plans on how to integrate the acquired business and its technology into their organisation (and group). The original founders may continue to operate within the new organisation and must be assisted in this change (eg, to get used to the loss of control over their product). Often, organisations

will prepare an integration team that may even include former founders themselves who understand the issues of the integration process from a founder's point of view. Such a smooth integration will help to maximise the benefits of the acquisition.

Steven De Schrijver
sds@astrealaw.be

Astrea
Brussels, Belgium
www.astrealaw.be

The Inside Track

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

Automation is probably the lowest hanging fruit for digital transformation. However, data processing is a new frontier of AI-enabled automation. Automation will now not only reduce the amount of required manual data entry but also start to replace some of the human decision-making (eg, in HR). AI and machine learning will outgrow their niches and more widely embedded in all kind of business processes. The potential of data will be further unlocked and businesses will continue to invest in data analytics. Industries as retail, hospitality and healthcare will be revolutionised by providing digitised digital user interfaces (conversational, gesture, augmented reality). This will also be driven by new technologies, such as WiFi 6 and 5G. At the same time, companies and governments will have to further invest in cybersecurity and strong IT governance to protect organisational assets. The most interesting aspect for a digital transformation lawyer is that the trends and technologies constantly evolve.

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

Digital transformation is not an easy process. It requires a culture shift and can deeply impact your client's organisation. There are a lot of internal stakeholders involved (commercial, IT, security, legal, compliance). As a lawyer, you can only help your client to overcome this challenge by convincing him to engage you early in the process so that you can play your role as facilitator and identify and tackle legal and regulatory issues immediately when they arise.

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

As a digital transformation lawyer, you need to understand the technology at issue. You have to be able to think out-of-the-box and to apply legal principles that were not developed for the digital age to new technologies. You have to be able to build bridges between internal departments at your client and between your client and its customers and suppliers. By clearly identifying the key legal risks and assisting your client with its commercial risk assessment you can as lawyer contribute to the success of your client's digital transformation projects.

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by Kemp IT Law, this *Digital Transformation* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Covid-19 response
Government policy
Contractual negotiations
Cybersecurity & data protection