
Market
Intelligence
DIGITAL
TRANSFORMATION
2020
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

Senior business development manager
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

Cover photo: shutterstock.com/Quardia

ISBN: 978-1-83862-564-1

Printed and distributed by Encompass Print Solutions

Digital Transformation 2020

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 is 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.

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

We are not aware of any Belgian laws or regulations which 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).

Clients will usually perform internal audits to determine their needs; request information from potential suppliers (with or without signing a non-disclosure agreement (NDA)); and request proposals and then negotiate with multiple suppliers to enter into final contractual negotiations with the chosen supplier. Regarding 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, pre-contractual 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


Steven De Schrijver

Commission); or based on a number of derogations, such as explicit consent by the data subject to the proposed transfers, subject to having receiving 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?

Belgian organisations have been at the forefront of implementing digital transformation in their daily operations for years. While already very advanced, the current covid-19 pandemic has boosted this transformation more than ever as working from home has been obligatory both during the first (18 March–3 May) and the second lockdown (as of 1 November 2020). Employers are even obliged to provide a certificate for employees who cannot work from home explaining why they must be physically present at work. With millions of Belgians working 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 great opportunities for digital services providers.

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

There are many factors to be taken into account when seeking cloud services. Clients 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 on the ISO norms (ISO/IEC 17788, ISO/IEC 17789 and ISO/IEC 27018), which may offer the client guidance in this respect.

An important factor is the security of the cloud services. Not only must it be determined whether personal data are successfully and sufficiently protected, but also other business data that is uploaded in the cloud. The client may wish to include audit rights with respect to security measures. Clients 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. Clients may be reluctant to accept any rights of use of the supplier for data analytics in this respect. The localisation of the servers must be reviewed to check whether any rules on international data transfers apply. Clients may request that the data are located with a local or, at least, a European provider. Clauses on the limitation of liability must be carefully reviewed, as too large an exoneration may effectively leave the client without any damages in 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 client 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 law specialist to review the contract as a Belgian lawyer would not be able to advise outwith 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), clients 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 only is insufficient.

"How will a supplier be held liable for losses caused pursuant to a decision made by an AI system?"

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 client); and dispute resolution (including adequate remedies). Sufficient confidentiality agreements must be concluded which protect the client'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 clients. 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 and the Internet of Things. When dealing with services that rely on these new technologies, clients 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 client 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 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. Clauses on sufficient technical and organisational security measures are also essential.

With respect to the acquisition of physical equipment (hardware), clients 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 (iv) 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 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 (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 client 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 is labour law. Consultants must be

Photo by velvetes on Shutterstock

considered and treated as independent parties, whereby clients 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 client. This sham self-employment, a risk which is high in the Belgian IT sector, may cause the client, 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 have had to adapt their cloud terms by including or expanding wording

"The Network and Information Systems Act is the first step in the Belgian legal cybersecurity landscape which will assist in raising awareness of cybersecurity within Belgian organisations."

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 clients 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 will be considered as special mandatory law in Belgium. As these rules enter into force on 1 December 2020, their interpretation in practice is still awaited. But in principle they could apply even when foreign law is selected, which means that they could strengthen the positions of Belgian clients 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 emerging point is the emergence of contractual clauses on the measures to be introduced by cloud service providers pursuant to the NIS Act, which also applies to digital services. Pursuant to this act, providers 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; and from an

organisational point of view, the supplier must have internal procedures, measures and action plans in case of incidents or in order to avoid them. Clients may wish to include wording on these requirements so that they have the potential to invoke breach of contract in case of an incident.

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, which introduces rules on unlawful B2B clauses applying to all agreements as of 1 December 2020. Summarised, a contractual party is allowed to limit its liability, save for losses caused by wilful 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 which 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 which is not higher than the supplier's insurance cover or which 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 client 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 damages 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.

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 reach his or her 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 client 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 insurance cover for data breaches as well, which also covers the expenses of legal and forensic 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 which regulates the property rights of the IP. This can be done by making a distinction between the IP which 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 he or she succeeds, will depend on the strength of his or her 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.

Photo by S-F on Shutterstock

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.

"An interesting new development that has been introduced into Belgian law is a set of rules on unlawful B2B clauses, which will be considered as special mandatory law in Belgium."

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 client.

Migrating IT workloads and systems from on-prem to in-cloud during contract lifecycle

Assistance by the supplier to the client with respect to the transition from on-prem 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 which can be considered as part of a business is transferred by the client to the supplier, the employees are automatically transferred as well 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 which is also clear about the allocation of costs and time spent by both parties in the process. Contractually, an indemnification clause can be agreed which foresees indemnification of the other party in case certain assessments were wrong (eg, relating to losses caused by a wrong assessment of the employment rights which 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 clients 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 which in most cases will be governed by a foreign law. The main points of contention will be too large a 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. Clients will need to negotiate balanced clauses whereby the limitation of liability of the service provider does not effectively render the client 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 which make sure that the client'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 client feels comfortable, so that the client is not impeded from seeking indemnification in case of a breach of contract (eg, if high legal costs would need to be made in a foreign jurisdiction).

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

The GDPR could be seen as a first step to introduce certain legal cybersecurity obligations in Belgium, as it foresees the need of adequate technical and organisational measures to protect the personal data that is being processed. This may include cybersecurity measures to protect digitally stored data against unauthorised access or hacking. The first real cybersecurity regulation entered into force in May 2019, which is the NIS Act. It applies to operators of essential services (eg, energy, banking, health sector, certain digital infrastructure and even search engines) and covers the protection of digital data. It cannot be excluded that the personal scope is further extended in the near future. This new act is the first step in the Belgian legal cybersecurity landscape which will assist to further raise awareness of cybersecurity within Belgian organisations.

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.

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 client's wishes. Heavy acceptance procedures which seek to verify whether the end result matches the extensive software specifications prepared at the time of the conclusion of the

Photo by K.Vilkas on Shutterstock

"Organisations are increasingly aware of the risks associated with relying on a certain platform of other companies for their operations, especially if that platform is foreign."

agreement are also more common. 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 in our contribution, 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; define the sprints; re-evaluate every step; have constant discussions between the client 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 client is much lower, resulting in a lower risk of liability too.

Clients 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 client's wishes which will change over time. 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 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 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 clients. 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 (RFIs) to potential suppliers and subsequent Requests for Proposal (RFPs). 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.

Clients 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 which 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 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 which 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. Clients 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 which 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 which 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 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 overcome this challenge by convincing your client 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

an LBR business

ISBN 978-1-83862-564-1