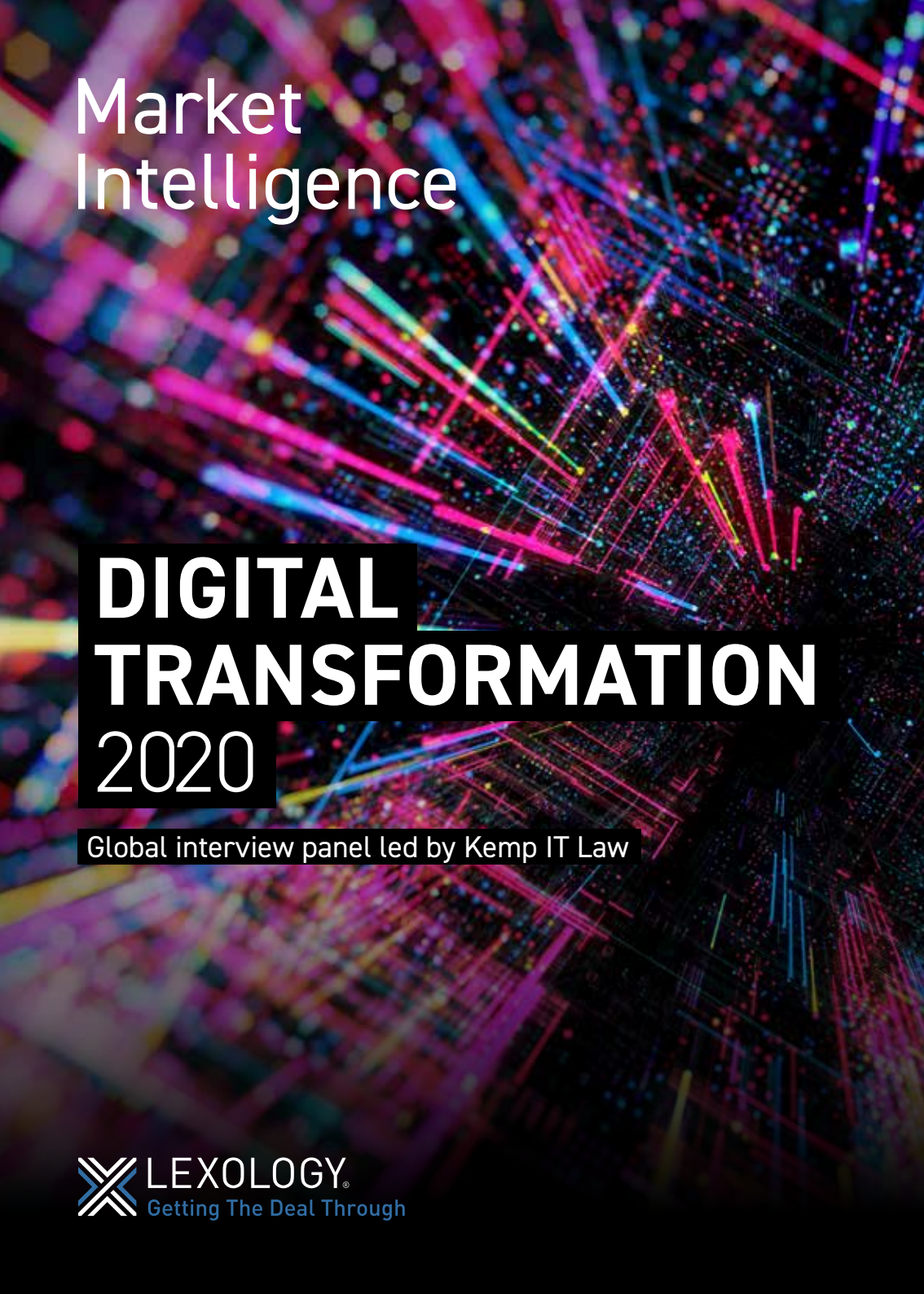

Market
Intelligence
DIGITAL
TRANSFORMATION
2020
Global interview panel led by Kemp IT Law
LEXOLOGY
Getting The Deal Through

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

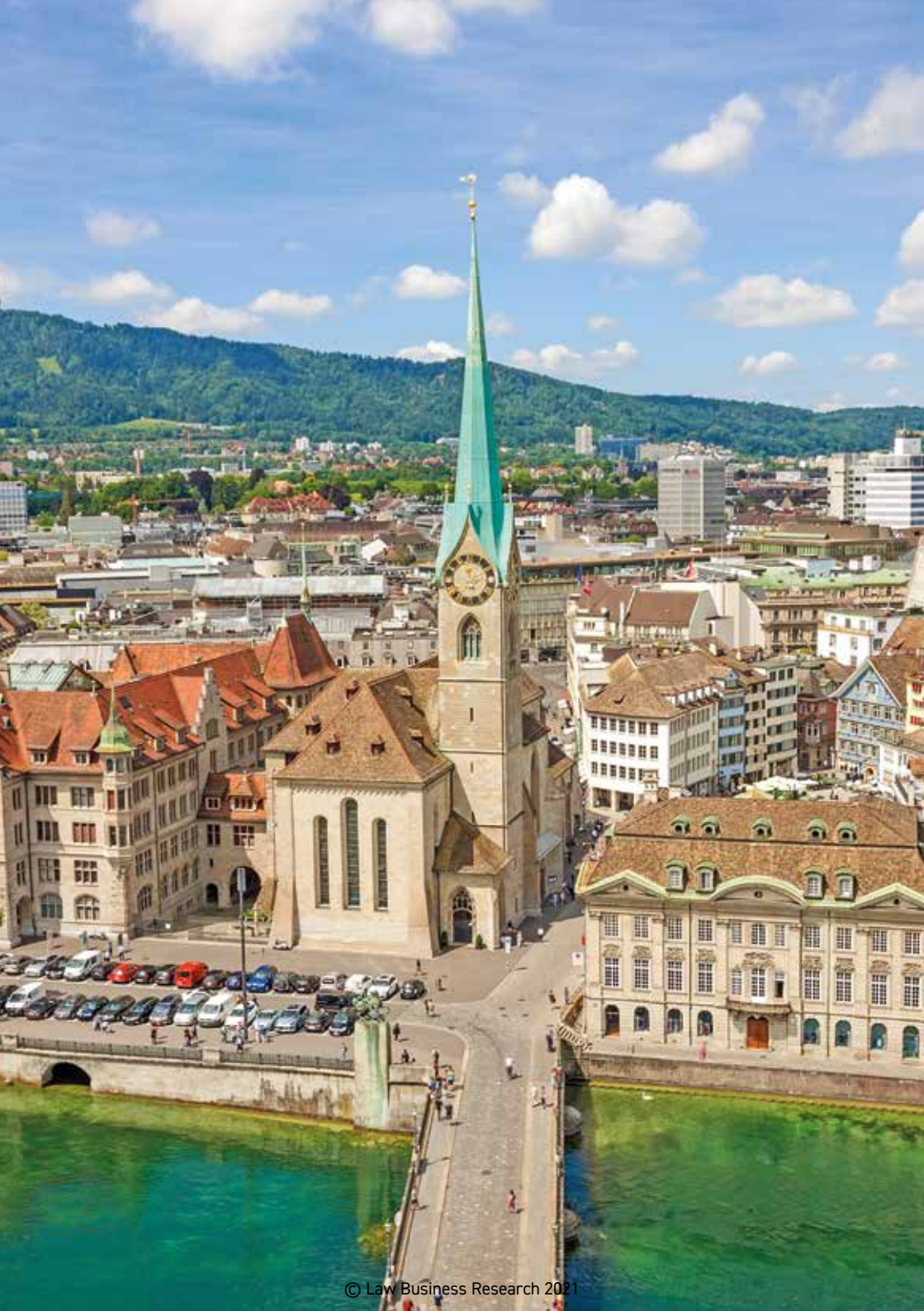
Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Cover photo: shutterstock.com/Quardia

ISBN: 978-1-83862-564-1

Printed and distributed by Encompass Print Solutions

Digital Transformation 2020



Switzerland

Angelica Dünner leads Streichenberg und Partner's technology practice. She has more than two decades of experience advising clients in the technology sector and represents a broad range of clients, be it world-known technology companies, leading multinationals in a number of sectors, or small and medium-sized firms. Having worked as an in-house counsel, Angelica has a comprehensive understanding of clients' internal processes and regularly supports her clients in negotiating or settling complex international deals involving existing and emerging technologies.

Matthias Stauffacher's practice is mainly in administrative and data protection law with a focus on the healthcare sector. He advises pharmaceutical companies on questions regarding the approval, pricing or trade of pharmaceuticals and supports these companies in the preparation and review of contracts with healthcare professionals and clinics. With his profound knowledge of regulatory requirements, particularly anti-corruption, data protection and contract law, he supports clinics, hospitals, doctors, pharmacies and other healthcare companies. He regularly works with start-ups and technology companies that develop new technological solutions for the healthcare sector.

Melanie Käser focuses on advising middle sized to multinational companies on different commercial law topics, especially supporting firms in getting their deal through – strategically and contractually. Furthermore, she specialises in advising companies who want to expand through managed distribution systems. Her background with a law and economics studies allows her to deeply understand the client's business needs. Melanie's clients appreciate her approach and support in settling disputes before they reach court as a positive and preventive measure for their projects.

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

'Digital transformation' is understood here as referring to 'investment in technologies, people and processes that supports the development of an organisation's digital capabilities'. It primarily includes cloud migration; cybersecurity; data protection; DevOps and governance, with automation; big data; AI; machine learning; and analytics also relevant to our practice.

In Switzerland, the notable key feature is the absence of up-to-date meaningful or specific laws governing digital transformation. It is thus mainly regulated by secondary legislation. Depending on the industry in which the digital transformation is conducted, sector-specific laws may apply (eg, strict regulations apply in the healthcare, finance and gambling sectors).

The following Swiss Federal Acts are most relevant for digital transformation in general: Code of Obligations; on data protection (DPA); on the surveillance of post and telecommunications; against unfair competition; on technical trade barriers; on certification services for electronic signatures and other applications of digital certificates; on the promotion of scientific research and innovation; and on electronic patient files.

For businesses, one advantageous feature of Swiss legislation is its flexibility, specifically, the approach whereby contract law only regulates certain ground principles, rather than any sort of detail. This enables business partners to jointly define tailored approaches in their contract, which is key for continuously and fast-moving technologies. On the other hand, this also mandates the business partners to think about the legal framework within which it is necessary to address key risks and requirements.

Overall, in Switzerland, for too long the focus on implementing digital transformation has been on technology rather than people and processes. Organisations looking towards the federal government for good examples of how to conduct such a transformation are basically looking in vain. This is partly due to the fact that in Switzerland, the federal government does not actually have (legal) sovereignty to regulate or purchase such projects in many areas, since such sovereignty lies with the cantonal and communal authorities. Additionally, our federal government is also lacking in experience with successful large digital transformation programmes in recent years, given that the large projects conducted were neither on time nor delivered at agreed cost, and nor with the expected quality. Organisations therefore need to look elsewhere for inspiration.


Angelica Dünner


Matthias Stauffacher


Melanie Käser

"The focus on implementing digital transformation has been on technology rather than people and processes."

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?

In the annual 2020 World Digital Competitiveness Ranking of the Institute for Management Development in Lausanne (IMD), Switzerland ranked as the sixth most competitive economy of the 63 economies evaluated. Time to relax?

No, is the consensus of all involved stakeholders, as was impressively demonstrated by the spread of the coronavirus and its consequences for the Swiss economy and social life. The latter constitutes the most noteworthy development furthering digital transformation in Switzerland like no single cause before. All of a sudden, living, working and being 'digitally (near-)native' is a must, and not optional anymore for a vast proportion of the labour population, schools, even kindergarteners and the elderly. Grandparents starting virtual dinners with their friends, and kindergarteners chatting to their teachers online, are fast becoming a reality.

The demand for digital solutions to all questions and areas of life has exploded in these last few months. Enterprises became painfully aware that availability of sufficiently sized, secure and stable IT infrastructure is not optional, but a must. Frantically looking through contracts and evaluating new options were requirements of the hour.

The focus has immediately (and rightfully) moved to keeping the human being as the central resource of the economy available and ready to work, and using digital solutions to enable this. Things we took for granted for so long, such as being able to travel, be it only to the workplace, all of a sudden became impossible in lockdown. Enterprises that had designed and had been embodying their digital transformation around this central resource – employees – were at a clear advantage.

What had been unthinkable a few months ago (corporations holding their annual general meetings by way of virtual meeting or in writing; working from home in the banking sector, for example) were suddenly the only means of keeping the Swiss economy running and compliant. Lawyers have been required to come up with new ways of holding meaningful voting via digital platforms, to ensure that they remain non -contentious and confidential.

There are other noteworthy developments though, if not so striking. With its recently updated Digital Switzerland Strategy and Digital Foreign Policy, the Swiss federal government aims to further reduce the obstacles for digital transformation in Switzerland and to ensure that Switzerland remains an attractive location in this respect, nationally and internationally. The commitment to reduce legal barriers for individuals and companies is enforced while enabling and further promoting the digital self-determination of consumers and employees. In accordance with

Photo by Alexandru Staiu on Shutterstock

this strategy, a wider range of laws is currently being or has recently been either newly created (be it the Federal Acts on electronic patient files; new regulations for Blockchain and Distributed Ledger Technology (DLT), or on electronic identification services, the latter subject to the Swiss people approving this act in a vote at the beginning of 2021); or updated (Federal Act on Data Protection, with an effective date of 1 January 2022). Also, further parts of the Swiss government are moving to offering their services via e-portals. Currently, only the Federal Finance Department for the Federal Tax and Customs Authorities are doing so.

Also, as a result of the close economic cooperation between Switzerland and the European Union (EU) and due to the exterritorial application of certain EU legislation, companies based in Switzerland, dealing with EU citizens, or exporting goods or services to the EU need to closely consider legal developments within the EU (eg, GDPR; e-privacy regulation; consequences of the EU–US Privacy Shield invalidation by the EU Court of Justice; digital tax of the OECD, etc.).

On 15 April 2017, the federal law on the electronic patient file came into force; it regulates the framework for the introduction and distribution of the electronic patient file. The electronic patient file is intended to strengthen the quality of medical

treatment; improve treatment processes; enhance patient safety; and increase the efficiency of the healthcare system. However, due to various technical problems, the fact that the exchange of the file with the patient or health insurers has not been included in the legislation, and probably also a lack of will on the part of those involved, means that implementation is not yet well advanced.

On the practical side, two large IT associations (ICT Switzerland and Digital Switzerland) merged, jointly forming the new umbrella organisation, focusing on further strengthening Switzerland as a digital research and innovation location.

Lastly, our political system occasionally leads to delays in implementing national digital strategies. As an example, a sufficient number of Swiss citizens signed a referendum against the new federal act on electronic identifying services, and this new law will be voted on by the Swiss people at the beginning of March 2021, delaying or even inhibiting introduction.

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

The cloud is cited as 'the urgent business imperative'. Maximising its value and dividends while being compliant is, however, seen as the challenge. The consequences of the coronavirus pandemic on the economy leading to this urgent business imperative becoming omnipresent, are self-evident and inevitable.

Digitisation theoretically happened years ago, and many call the current times the 'post-digital era'.

Many smaller and even bigger firms are still struggling to recognise the value of data for their businesses, to move away from the 'silo' way of thinking (compartmentalisation of each department or person), and are far from even knowing what data they have or how they want to create value with the data.

From a practical perspective, in order for them to determine what to host where, for how long, which back-up, BC and DR solutions they need, and as a basis for determining the legal factors, we thus recommend a staged approach: first, analyse what data you have; second, where is that data located? (server, cloud, which provider?); third, determine the requirements for the use of data, including key factors around availability, risks involved, etc; fourth, conduct a proof of concept or trial phase; fifth, re-evaluate strategy based on results; and sixth, execute your new strategy. You should be aware, as an enterprise and as executives of a company, that addressing the issue of people within your organisation keeping data in various sorts of places is essential. An organisation will never be able to resolve this part technically or legally – only by introducing continuous education, training and being ready with a

"Organisations need to be aware of what 'personal data' is, and what data they have as their assets."

good central breach or incident resolution organisation will organisations successfully mitigate risks.

From the legal perspective, in developing cloud and data centre strategies, with the need to be compliant from a data protection perspective, understanding what data is being hosted where, processed by whom, and what the legal terms around these services are, is crucial.

The key factor is that organisations need to be aware of what 'personal data' is, and what data they have as their assets. Not all an organisation's data are kept in central databases as foreseen by company policy. In terms of data being generated 'on the go' via AI, (Google Research, for example), generating metadata, pictures, and video files is important. If companies are faced with demands from data subjects to be informed about data kept – or even more 'cumbersome', personal data having to be deleted, a company is well advised to know in the first place where to look for such data, and even more importantly (again), to have a process to be able to fulfil such demands in order to be compliant.

Overall, in contracting for digital transformation projects, an outcome-based thinking is key – and reflecting this in the contract, essential.

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?

Procuring digital transformation services involving the cloud is typically complex, not least from a contractual perspective. The reason for this is that they are multi-party rather than bilateral (client, service provider and hosting provider, other third parties of client or service provider). They very often involve multiple countries with various applicable laws. Assessing and adequately balancing these cross-party dependencies in the contract (and managing them in the project) is crucial for knowing and managing inherent risks of such deals.

Organisations have to be aware that in order to address risks in the contract, first and foremost a very good understanding of the purchaser's requirements on the one hand, and the offering on the other hand, are essential. Also understanding the high-level technical functionality of what an organisation purchases is the basis to assess involved risks; not only for the business, but also for the lawyer advising.

Given the complexity, involving an organisation's legal counsel from the outset can reduce project cost, risk awareness and allocation, enabling a coherent and consistent approach in managing the data as the crucial asset it constitutes in the value chain

Description of the processes in the project – what happens when; who does what when; for what fee; what happens if something goes wrong; what and how to measure and react if something goes wrong – are crucial questions that should be answered during negotiation. Based on this only, lawyers can conduct a proper risk analysis, and include the necessary protection in the contract, be it adequate liability, warranties, termination rights, etc. Again, these need to take into account, and be designed to address, consequences throughout the stack. Our advice is to find a balanced way for this. Given that we are looking at long time cooperation, it is advisable to take both parties' interests and restrictions into account. Thus, companies are well advised to include good terms around business continuity and disaster recovery upfront, but also addressing access to data in insolvency by, for example, including escrow terms or, maybe more practically, how they can access their data and files in a crisis.

In light of the recent covid-19 pandemic, including a good force majeure clause is important. Thinking these clauses through is criucial: knowing exactly how to access data; availability of data; how to retrieve data (direct access); whether the intra-town backup is adequate – think about government curfews, leading to your providers; personnel not being able to go to their work location in the data centre;

has the provider ensured that all their employees can work from home from day one and do they all have the necessary computer equipment at home; are systems sufficiently secured, employees adequately trained, and how many people share the room or space at the home from which the employee works? These, among other things, should be considered.

Service providers need to ensure that terms for hosting purchased are aligned with the terms agreed with the client; that risks are crystal clear; and any gaps are manageable for the provider. This does not only refer to the obvious terms such as service levels or availability, but rather also to warranties, liability, termination, business continuity, etc. Given that hosting is often in countries other than where your client contract resides, it is essential to have a good understanding of how the respective applicable laws are interpreted to assess whether there are additional inherent risks in the contract.

Over the past five years, the direction has been to continuously and increasingly more quickly move services to the cloud, to purchase more 'as a service'. The speed has multiplied during the pandemic, with having scalable, available and secure IT infrastructure no longer being one of the options, but the key option.

Photo by Maykova Galina on Shutterstock

"Digital transformation projects are cross-dependent, not only with the various parties involved, but also within the client's organisation."

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

Studies found that nearly 70 per cent of all IT projects fail, as a result of, for example, cost overrun, dissatisfied clients, etc. The main causes for this are unrealistic and mismatched expectations; conflicts of interest among customers, vendors and integrators; and corporate organisation structure that conspires towards failure. This is exactly what companies, businesses and lawyers should keep in mind for their transformation projects and contracts.

What we meet more and more often are client expectations that include having tailored solutions and contracts, but at the price of a multi-client offering, so seeking all the advantages of single ownership without the price tag.

Digital transformation projects are cross-dependent, not only with the various parties involved, but also within the client's organisation. Utilising a staged approach, by investing in analysing and defining what the actual service requirements are before the project is started, also by, for example conducting a proof of concept

or trial phase, helps recognise and address risks. Internal stakeholders buy-in is essential if transformation is to be successful.

In our view, good contracts identify, fairly allocate and manage risks as the basis for longer term relationships. Much too often, the parties spend ample time on warranties, liabilities, indemnities and pricing. For the contract, this means defining the actual requirements of the client, clearly describing expected outcomes (not in sales language, but actual commitments on what will be provided, when, at which quality, how quality and the outcome is measured); roles and contributions of each of the parties; designing the contract to be about change (ie, typically from day one of the project); setting up continuous governance; and which process to follow when discussions get stuck (escalation).

It goes without saying that defining what data is used, who does what with the data, and how data security is set up and audited, are also key.

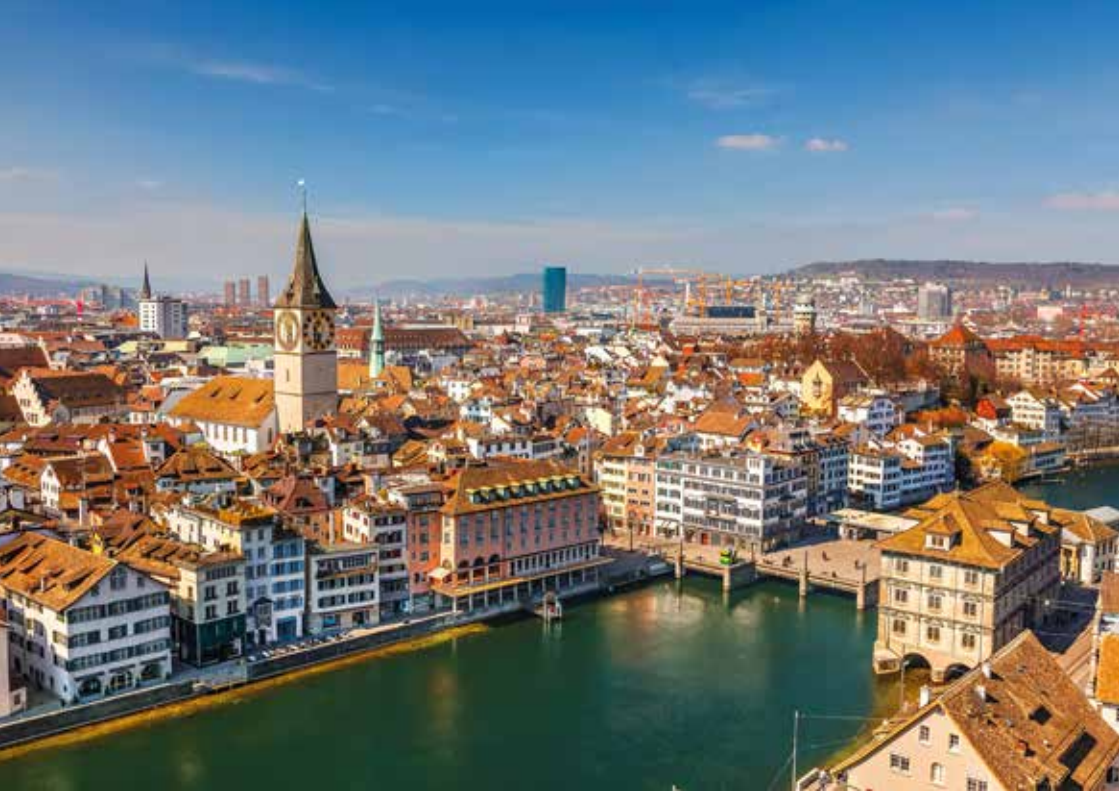
Last but not least, do not forget to 'live' the contract, in other words, apply rigorous contract management to ensure compliance with the contract. Never forget that scope creep and change orders will destroy a project budget and schedule.

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

In Switzerland, currently, only the 1992 DPA and the relevant ordinance outline certain basic principles for cybersecurity. There is, however, no federal law on cybersecurity (with the exception of one ordinance regulating cybersecurity in federal government). Thus, currently, there are, for example, no requirements to notify affected parties or the regulator of data security breaches. However, notifications under the GDPR may be required. In the future, notification will also be required under the DPA.

This lack of national rules means that every company, as well as contracting parties, is required to establish internal data security policies or adequate cybersecurity rules which govern all relevant aspects with regards to data security and data breaches. Furthermore, organisations are well advised to implement appropriate technical and organisational measures to protect themselves from cybercrime and issues. Due to the lack of specific Swiss cybersecurity laws, it is up to the organisation to regulate the necessary measures as well as internal policies in sufficient detail and granularity and keep these on the radar of the executives of the organisation to be on the safe side.

Such policies must be accompanied by the adequate and regular training of all employees involved in data processing. Where third parties (such as cloud providers) are processing data, entering into data processing agreements (DTAs)



is standard. Think again of aligning these DTAs along the cloud stack with each other. Appropriate measures include dedicated protection programs; encryption of sensitive data; regular software updates; multi-factor authentication; and the implementation of a data breach plan.

In summary, organisations in Switzerland do not have to fear big hurdles on their digital transformation journey from Swiss cybersecurity laws, but need to keep international laws and actual technological market requirements in mind which affect every organisation on their digital transformation journey.

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

As mentioned above, the current DPA dates from 1992, setting the framework for outsourcing data processing and data export, fairly generically, but basically consistent with practice also for the EU. Furthermore, in particular in the healthcare sector, the Swiss criminal code regarding professional or official secrecy needs must be respected and may add considerable complexity to projects for digital

Photo by S.Borisov on Shutterstock

transformation. Given that Switzerland is an export country and host to many European or even worldwide headquarters of groups of companies, many companies have set up data privacy to be compliant with GDPR by which they are also meeting Swiss legal requirements. This will enable them to even more easily be compliant with the new Swiss DPA, which becomes effective in 2022.

So, in short, the current DPA would give more flexibility than the GDPR, for example with no duty to inform on data breaches; however, due to the international setting in which companies act, most comply with even more strict rules like the GDPR and act according to these regulations when considering their digital transformation projects (given that these projects often involve the cloud hosted abroad).

Data protection laws are therefore always a key point in the digital transformation journey of every organisation.

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)?

Given that Swiss law does not provide us with a fixed set of rules tailored to DevOps, from the legal standpoint, the key challenge is for the parties to describe in the contract – apart from the expected outcome – the processes as to how the outcome is to be achieved, how change is handled and how the parties continuously measure quality delivered.

Think of tailoring the financial model to this form of delivery by including value-based elements or payment deductions for quality levels not achieved. In addition, set up and describe a good and stable governance process, ensuring that continuous communication actually does occur, and change is actively managed. Consider describing within your governance which topics are discussed at which level and how issues get escalated from one governance body to the next. Given that the parties do not really know the expected outcome or whether it will evolve continuously, resist the temptation of spending too much time on defining the last technical details for it, and in its place, define clearly each party's duties and contributions, for example, in a RACI chart.

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

We do not believe that there are Swiss specifics in this respect. First of all, each of the business partners needs to have a clear and internally aligned understanding

of its own goals with regards to digital transformation. Such strategy should be documented with regards to governance processes, project management, clear responsibilities of the parties involved, etc. Such a strategy needs to be reviewed regularly. From our point of view, it is also crucial that not only the IT department is involved in digital transformation, but also the business departments, internal or external legal as well as the leadership of the company.

Keep in mind that the need for information and interaction with our clients has evolved. Thus, we recommend to design and live processes to address this interaction of the parties as business partners rather than enemies. Build up change top down and bottom up and create more and more direct interaction with your client, that is, more external contact. Simple processes often prove to be more stable and easier to follow – so that they do not get forgotten but are actually enacted and contribute to project success.

Angelica Dünner
angelica.duenner@streichenberg.ch

Matthias Stauffacher
matthias.stauffacher@streichenberg.ch

Melanie Käser
melanie.kaeser@streichenberg.ch

Streichenberg und Partner
Zurich
www.streichenberg.ch

The Inside Track

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

Constant change is what fascinates us with digital transformation – strategic thinking and designing processes to address the future. We are moving away from purely technical thinking to the client being centre stage, tailoring offerings to their needs. Also, since digital transformation projects are cross-dependent, very often sporting international components and including new technology, finding the adequate solution is a creative process, the responsibility of which lays with the business team and the lawyers involved; we cannot just pull pre-existing contract wording for all challenges. New and up-to-date language must be included in the contract.

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

Understanding the actual deal, the technology involved and set-up is crucial. We ask our teams to explain these to us in quite some detail. This enables us to understand what is going to be delivered, to assess potential risks and develop appropriate terms in the contract to mitigate such risks. Also, we ask the teams to help us understand client needs, maybe cultural or language requirements, how the team envisages addressing these and what governance processes they are considering. We are proud when parties see contract negotiation as a first step into a working relationship with our contribution.

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

A good adviser for digital transformation projects is thus in our view and experience a person who likes to work with complex projects and contracts, who is able to listen to, manage and exchange with the client, provider and third party teams, has a good grasp of and fascination for technology and who is able to find solutions even if not available in law, jurisdiction or contract templates. Being interested in the interaction with human beings as internal or external representatives of the parties involved, and open, though focused on developing adequately tailored solutions, are key.

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