Photo by Fit Ztudio on Shutterstock

LEXOLOGY
Getting the Deal Through

Market Intelligence

DIGITAL TRANSFORMATION 2022

Global interview panel led by Kemp IT Law

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.

Government policy
Procurement best practice
Contractual negotiations
Cybersecurity & data protection

START READING

Photo by Monika Klenowska on Shutterstock

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 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 and regularly works with start-ups and technology companies developing new technological solutions for the healthcare sector.

Melanie Käser focuses on advising medium-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 that 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.

QUESTIONS

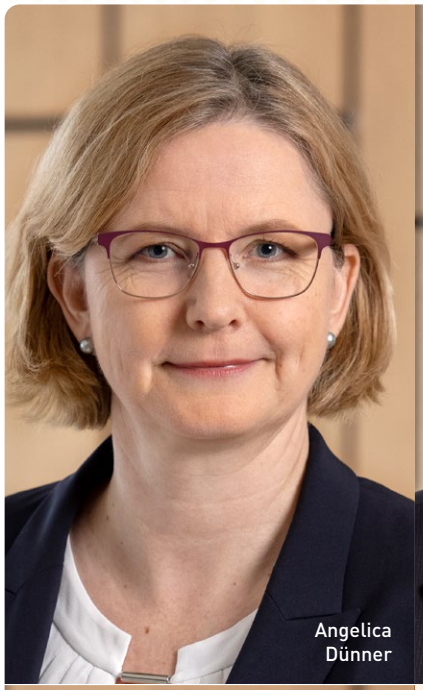
1 What are the key features of the main laws and regulations governing digital transformation in your jurisdiction?

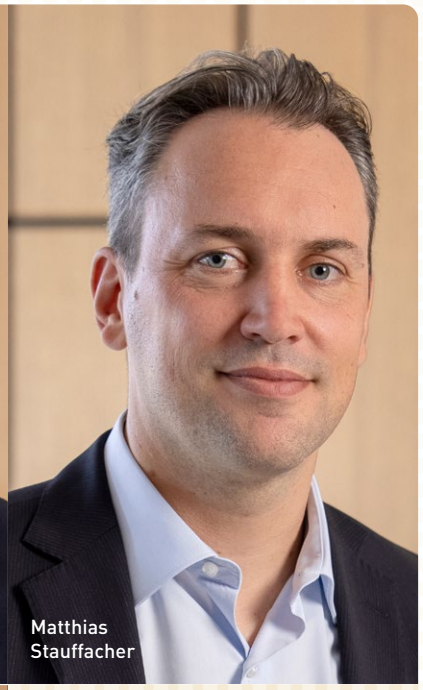
'Digital transformation' is understood here as referring to 'investment in technologies, people and processes that supports the development of an organisation's digital capabilities'. It primarily includes cloud migration; cybersecurity; data protection; DevOps and governance, with automation; big data;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

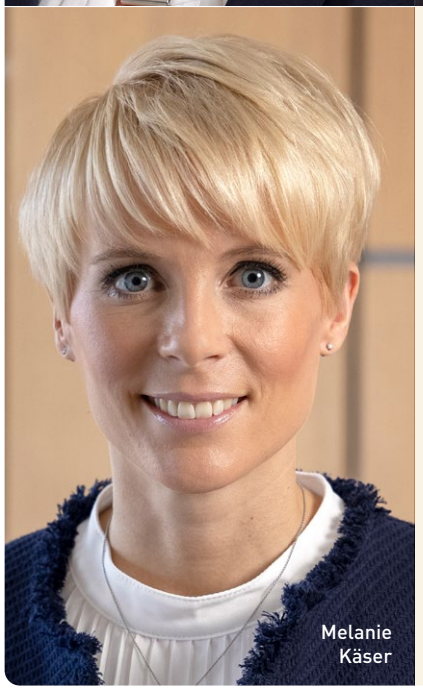
In Switzerland, the notable key feature is the absence of up-to-date meaningful or specific laws governing digital transformation. It is thus mainly regulated by secondary legislation. Depending on the industry in which the digital transformation is conducted, sector-specific laws may apply (eg, strict 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; data protection (DPA); surveillance of post and telecommunications; against unfair competition; technical trade barriers; certification services for electronic signatures and other applications of digital certificates; promotion of scientific research and innovation; and electronic patient files.

For businesses, one advantageous feature of Swiss legislation is its flexibility, specifically, the approach whereby laws regulating contracts only regulate 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 in detail how contractually to address key risks and requirements.


Angelica Dünner


Matthias Stauffacher


Melanie Käser

"Depending on the industry in which the digital transformation is conducted, sector-specific laws may apply."

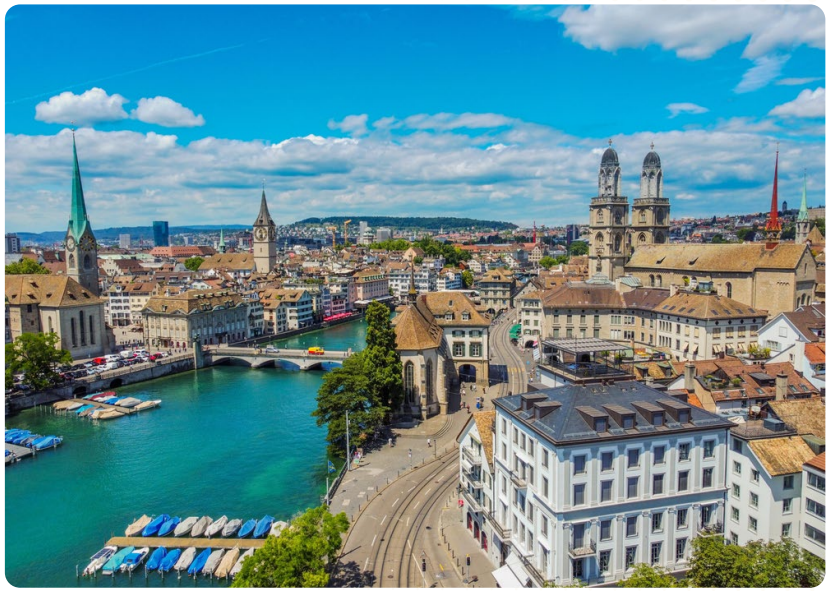


Photo by Iurii Dzivinskyi on Shutterstock

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.

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 2022 World Digital Competitiveness Ranking of the Institute for Management Development in Lausanne, Switzerland ranked as the fifth most competitive economy of the 63 economies evaluated, one up from 2021. 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 continued to constitute 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' was a must, and not optional anymore for a vast proportion of the labour population, schools, even kindergarteners and the elderly. Enterprises became painfully aware that availability of sufficiently sized, secure and stable IT infrastructure is not optional, but a must. Even after the end of the corona-measures, the demand for digital solutions to all questions and areas of life continues to develop rapidly, in the past few months near exponentially, specifically with Generative AI such as ChatGPT. Enterprises are well advised to conduct an indepth analysis on how they wish to internally regulate the use of new technologies, including Generative AI. This is specifically required, since there are hardly any regulations internationally or nationally setting borders on how Generative AI should and may be used.

The enterprises' focus therefore also needs to remain on keeping the human being as the central resource of the economy available and ready to work, even in changed circumstances and using digital solutions to enable this. The good news is that the (digital) transformation process forced to be started through corona still continues.

There are other noteworthy developments though, if not so striking. With its 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. In accordance with 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; the new Federal Act on Information Security) or updated (Federal Act on Data Protection, with an effective date of 1 September 2023 (nFDPA)).

Furthermore, 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 or AI regulation; consequences of the EU–US Privacy Shield invalidation by the EU Court of Justice and adoption of Privacy Shield 2.0; digital tax of the Organisation for Economic Co-operation and Development, etc).

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

"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."

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, for companies 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 continue to 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 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 good central breach or incident resolution organisation will organisations successfully mitigate risks.

From the legal perspective, in developing cloud and data centre strategies, understanding what data is being stored where, used by whom, and when, and what the legal terms around these services are, is crucial. 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. Also, they need to have a process to be able to fulfil such demands to be compliant.

Photo by Pedro Costa Simeao on Shutterstock

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?

Contracting for digital transformation services involving the cloud is typically complex, not least from a contractual perspective. The reason for this is that they are multiparty 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.

> "Service providers need to ensure that terms for hosting purchased are aligned with the terms agreed with the client."

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 project. Crucial questions that need to be answered during the multi-player negotiation are therefore, for example – who does what when; what happens when; for what fee; how to treat changes; how to cooperate; what is the agreed outcome; how to measure and react if something goes wrong and in this case, who talks to whom and when. Based on this only, lawyers can conduct a proper risk analysis and include the necessary protection in the contract, be it adequate consequences for service failure, 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 all parties' interests and restrictions into account. Thus, companies are well advised to include good terms around business continuity and disaster recovery upfront (keeping in mind lessons learned from the covid-19 pandemic), 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.

Thinking these clauses through is crucial: 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, need considering. All these elements are actually vital parts of a digital transformation journey.

Service providers need to ensure that terms for hosting purchased are aligned with the terms agreed with the client; that risks are clear and addressed in the contract and processes implemented in the project; 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 and continued to do so since, with having scalable, available and secure IT infrastructure no longer being one of the options, but the key option.

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 digital transformation projects fail, as a result of, for example, cost or timeline 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 structures that conspire 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. Rather, managing risks means defining the actual requirements

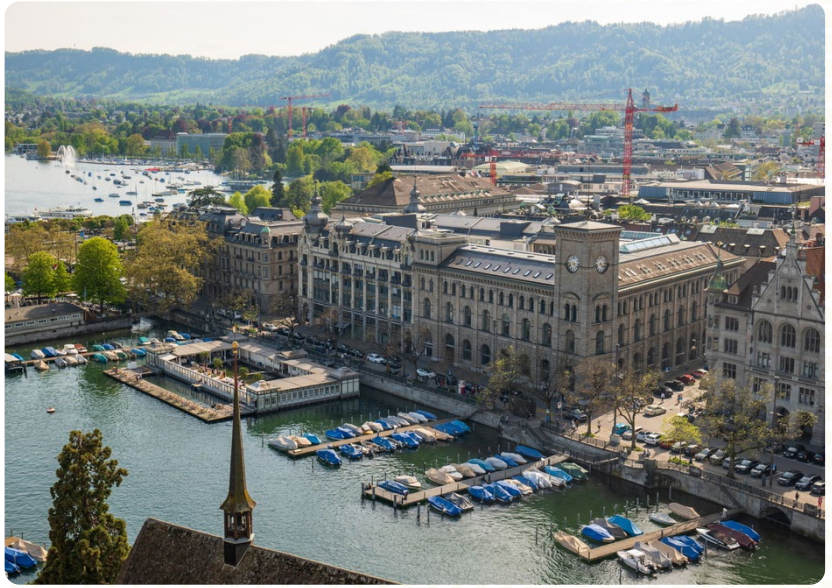


Photo by Octavian Lazar on Shutterstock

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.

"Organisations in Switzerland do not have to fear big hurdles on their digital transformation journey from Swiss cybersecurity laws."

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

Currently, Switzerland has no overarching law on cybersecurity. Various laws and ordinances contain regulations limited to certain areas of protection. There is, for example, an ordinance in place regarding cybersecurity in the federal government. As per 1 September 2023, two acts with certain additional regulation come into forces: (1) the new Swiss DPA and its ordinance; and (2) the federal act on information security, the latter of which regulates cybersecurity regarding critical or essential infrastructures of Switzerland. For most companies, the essential rules will again be in the new DPA and its ordinance, specifically with the new duty to notify in case of data breaches.

Due to the lack of overarching 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. Remember to align these DTAs along the cloud stack with each other. Appropriate measures include dedicated protection programs; encryption of sensitive personal 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 that affect every organisation on their digital transformation journey.

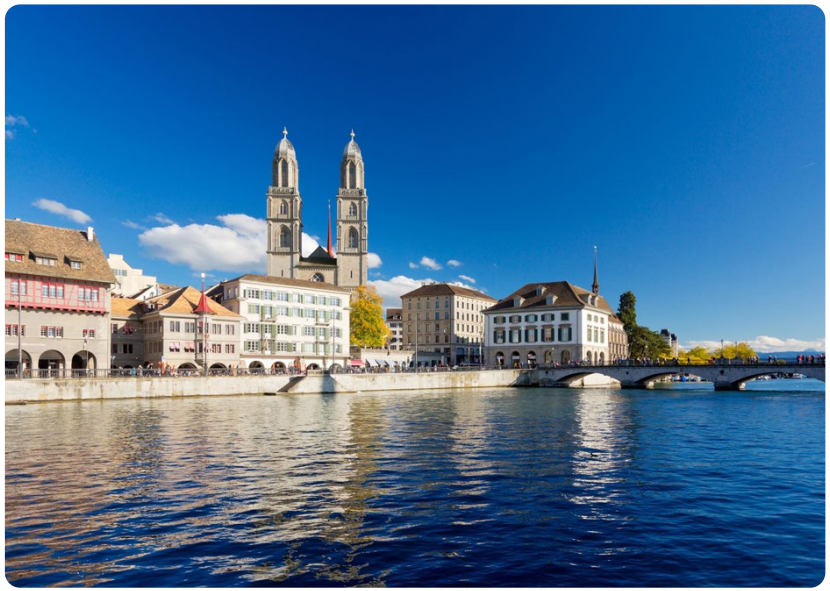


Photo by Sabine Klein on Shutterstock

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

Data protection laws are always a key point in the digital transformation journey of every organisation. Many organisations throughout Switzerland are currently evaluating their projects and structure for compliance with the nFDPA and its ordinance, with effective date of 1 September 2023. Several tools for evaluating partial aspects of compliance are available on the market, some of them free of charge. Organisations are well advised to regard the new requirements as a strategic chance in their digital transformation process, enabling them to have a holistic approach to integrate this topic into their firm culture – and seek required internal and external advice. The nFDPA has already brought protecting data as a vital asset of firms more clearly on the radar of the C-level in organisations. This not least because under the nFDPA, criminal prosecution directly of the actual natural persons violating the law within an organisation is foreseen. Furthermore, in particular in the healthcare sector, the Swiss criminal codes rules regarding professional or official secrecy needs to be respected and may add considerable complexity to projects for digital transformation.

Also organisations currently set up to comply with GDPR will need to review in detail which (additional or deviating) measures are required under the nFDPA which is not going to be the same as GDPR. Switzerland will, for example, not introduce the opt-in requirement, but continue to go with 'opt-out'. The nFDPA will however introduce the 'privacy by default and by design' principle, so that a key factor therefore will be that organisations need to be (much more) aware of what 'personal data' is and whether the data they process needs indeed to be 'personal data', and cannot, for example, be used in an anonymised or pseudonymised manner. The recent decision of the European General Court regarding pseudonymised data not being personal data for the recipient if the latter does not hold the key, certainly also clarifies for such use under Swiss law.

8 What do organisations in your jurisdiction need to do from a legal standpoint to move software development from waterfall through Agile to DevOps?

Given that Swiss law does not provide us with a fixed set of rules tailored to Agile or DevOps, from the legal standpoint, the key challenge for the parties is 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, how the parties continuously measure quality delivered and how they continuously communicate with each other to determine whether the project is still on track.

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

> "The need for information and interaction with our clients has evolved."

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 (Responsibility Assignment Matrix) 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

Streichenberg und Partner
Zurich
www.streichenberg.ch

Matthias Stauffacher
matthias.stauffacher@streichenberg.ch

Melanie Käser
melanie.kaeser@streichenberg.ch

Read more from this firm on Lexology

QUESTIONS

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 for 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.

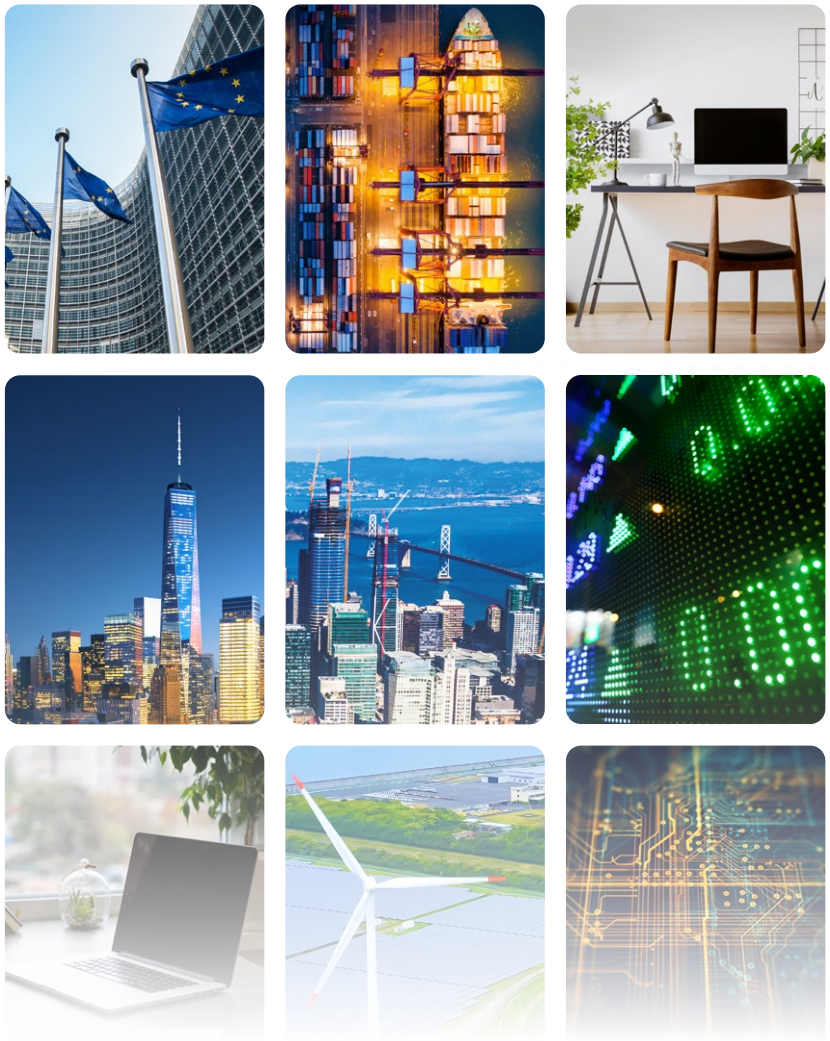
What challenges have you faced as a practitioner in this area and how have you navigated them?

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, who 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.



About Market Intelligence

Respected opinion, expert judgement

Lexology GTDT: Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes in major jurisdictions around the world. Through engaging, easily comparable interviews, the series provides the legal profession's thought leaders with a platform for sharing their views on current market conditions and developments in the law.

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 interesting cases and deals.

Click here for more Market Intelligence topics

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Matthew Bridgewater
matthew.bridgewater@lbresearch.com

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

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