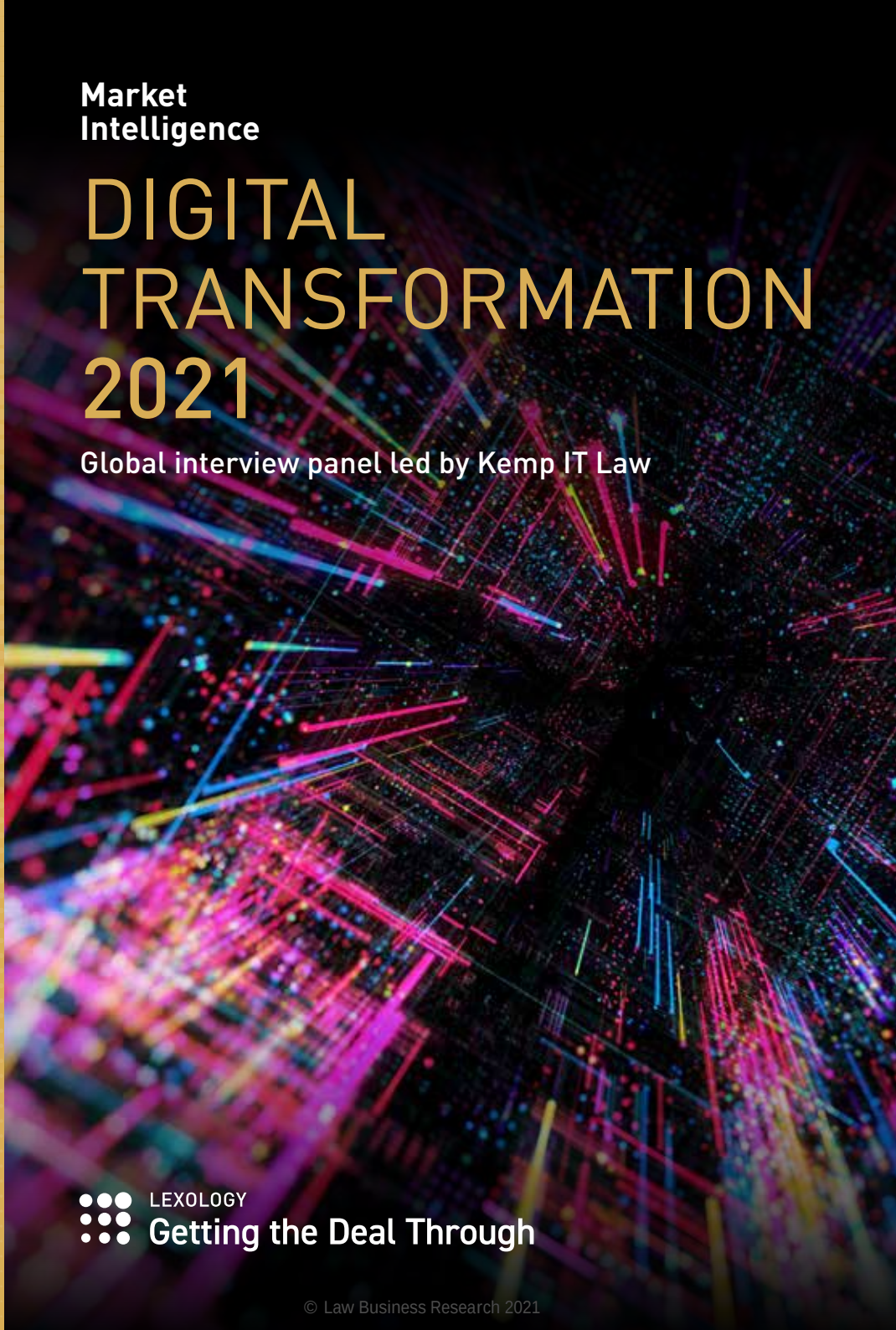
Market Intelligence

DIGITAL TRANSFORMATION 2021

Global interview panel led by Kemp IT Law



LEXOLOGY
Getting the Deal Through

LEXOLOGY
Getting the Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

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

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

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

Printed and distributed by Encompass Print Solutions

DIGITAL TRANSFORMATION 2021

Austria

Veronika Wolfbauer has been with Schoenherr's regulatory practice group and is a leading member in the firm's privacy and data protection team. In addition, Veronika is part of the Schoenherr's technology and digitalisation group, leads the technology regulation and audiovisual media law team and works in the field of IT and consumer protection law.

Veronika serves not only national but also international corporate clients, but also lectures in those areas. She has vast experience in giving strategic and legal advice, as well as leading administrative law proceedings before the Austrian regulatory authorities and 'appeal proceedings' at court, including addressing the Austrian Highest Administrative Court, the Austrian Constitutional Court and the European Court of Justice.

Peter Ocko has been an associate at Schoenherr in the technology and digitalisation group since 2020 and works mainly in the field of IT law. During his doctoral studies at the University of Vienna, he specialised in the legal aspects of digitalisation. In his doctoral thesis entitled 'The liability of the access-, hosting-, content-provider and the streaming service user for copyright infringements for streaming of films on on-demand streaming platforms', he dealt with, inter alia, the liability of YouTube, Facebook, A1 and Magenta.

Photo by Nok Lek on Shutterstock

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

GDPR / Austrian Data Protection Act

Regulation (EU) 216/679 (the General Data Protection Regulation, GDPR) is – also in Austria – the main legal framework for the protection of personal data (ie, information that relates to an identified or identifiable individual). The Austrian Data Protection Act (ADPA) supplements the GDPR. It contains the implementation of some (mandatory) opening clauses of the GDPR, but also some additional provisions specifying certain topics (eg, specific CCTV regulations). It also enshrines the fundamental right to data protection on a constitutional level.

The ADPA also serves to implement Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data. It also intends to implement Directive 2016/680/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

Austrian Distance Selling Act

The Austrian Distance Selling Act (ADSA) protects consumers in e-commerce (distance selling) contracts. Section 8(1) of the ADSA provides that the trader must draw the consumer's attention to the essential points of the contract before he or she makes his or her contractual declaration. According to section 8(2) of the ADSA, a web shop must be set up in such a way that the consumer expressly confirms when ordering that the order is associated with a payment obligation. Section 11 of the ADSA grants the consumer a right of withdrawal. This Act transposed the provisions of the Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights.

Austrian Law on Copyright

The Austrian Law on Copyright (ALC), particularly section 18a, regulates the right of making a work or image available to the public. This right is affected whenever a work or image is made available on the internet. Within this federal act the following directives have been implemented:

- Directive 96/9/EC of the European Parliament and the Council on the legal protection of databases;

- Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society; and
- Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights.

E-Commerce Act

The E-Commerce Act (ECA) regulates a legal framework for certain aspects of electronic commerce and legal transactions. It deals with the licensing of service providers; their information obligations; the conclusion of contracts; the responsibility of service providers; the country of origin principle; and the cooperation with other member states in electronic commerce and legal transactions. This federal act implements Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the internal market (directive on electronic commerce).

E-Government Act

The E-Government Act (EGA) was established to promote legally relevant electronic communication. Electronic communication with public authorities is to be facilitated taking into account the fundamental freedom of choice between the means of communication to be used for communications to these authorities.

Distance Financial Services Act

The Distance Financial Services Act (DFSA) imposes numerous information obligations (section 5 of the DFSA) on the service provider and gives the consumer the right to withdraw from the contract (section 8 of the DFSA). This Federal Act implements Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services.

Network and Information Systems Security Act

The Network and Information Systems Security Act (NISSA) aims to achieve a high level of security of network and information systems of essential service operators digital service providers and public administration institutions. Digital service providers are defined as providers of an online marketplace, an online search engine or a cloud computing service, provided that they are of a certain size. This Federal Act serves to implement Directive 2016/1148/EU concerning measures for a high common level of security of network and information systems across the Union.

Signature and Trust Services Act

The Signature and Trust Services Act (STSA) allows for the electronic signature of contracts despite Austrian law stipulating that an agreement has to be 'in writing' or 'in written form', which normally means handwritten signatures on paper. Article 25(1) eIDAS-VO (Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market) provides that an electronic signature has the same legal effect as a handwritten signature, and section 4(1) of the STSA provides that a qualified electronic signature meets the legal requirement of written form within the meaning of section 886 of the Austrian Civil Code (ACC). This Federal Act implements Regulation No. 910/2014/ EU on electronic identification and trust services for electronic transactions in the internal market.

Consumer Warranty Act

Austria has recently implemented the Digital Content Directive (DCD Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services and the Sale of Goods Directive (SGD, Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods). The changes will come

> "Deviation from the provisions of the CWA by means of contractual arrangements is only possible in favour of the consumer."

into force on 1 January 2022. For the implementation, the ACC and the Consumer Protection Act were amended and a new act, which is the centrepiece of the legislative reform, was issued: the Consumer Warranty Act (CWA). The CWA applies to contracts between consumers and entrepreneurs concluded for the purchase of movable tangible objects, including those that are yet to be manufactured (goods) and such who include digital elements (goods with digital elements), as well as for the provision of digital services against payment or handing over of personal data. However, the CWA does not apply, for example, to contracts for the purchase of living animals, electronic communication services, health services, gambling services or financial services.

Deviation from the provisions of the CWA by means of contractual arrangements is – as usual in consumer protection law – only possible in favour of the consumer. Although the focus of the legislative reform is on contracts between an entrepreneur and a consumer, certain changes also apply to contracts between entrepreneurs or contracts between consumers.

When it comes to digital transformation in Austria the most significant changes are the clarification that there is a right to warranty under Austrian law if data is provided as consideration and the introduction of an obligation to update.

Until now, it was unclear whether consumers were entitled to warranty claims if their consideration was not money but the provision of data. This is now clarified for contracts on the provision of digital services by explicitly including these contracts in the scope of application of the CWA.

This obligation to update is exceptionally also applicable to contracts between entrepreneurs (B2B). For digital services as well as goods with digital elements (eg, smart TV, smartwatch) an updating obligation is introduced that goes beyond the classic warranty concept (liability for defects existing at the time of handover) with the entry into force of the legislative reform. The entrepreneur has to provide the updates that are necessary to maintain the lack of defects during the update period. The obligation to update can be excluded by individual agreement.

This obligation to update exists in the case of the one-time (or several times single) provision of a digital service (eg, in the case of the provision of an e-book, movie, photo etc) as long as the consumer can reasonably expect this. In the case of continuous provision of the digital service (eg, a two-year contract for cloud storage, streaming services or an unlimited membership of a social media platform), the obligation to update exists for the duration of the obligation to provide the service. The obligation to update also applies to contracts between entrepreneurs (B2B) but does not apply to contracts between consumers (C2C).

Communications Platforms Act

As part of a regulatory package against hate speech on the internet, Austria established the Communications Platforms Act (ComPA). Simply put, these new act aims to quickly delete illegal content from platforms. The rules shall serve to promote responsible and transparent dealing of platforms (international and national platforms) with platform users' reports of 'hate speech' or similar specific content. Non-compliance can lead to significant penalties. However, the ComPA only applies to platforms with more than 100,000 registered users in Austria or revenues of more than €500,000 per year in Austria. Online marketplaces, non-profit online encyclopaedias (such as Wikipedia) and learning platforms, newspaper and television company platforms hosting their journalistic offerings, and apps used for individual communication are explicitly excluded from the scope of the ComPA. Whether the new rules comply with EU law is currently under debate.

Photo by creativemarc on Shutterstock

Draft Act of the Austrian Copyright Reform

On 3 September 2021, the ministerial draft concerning federal act amending the Copyright Act, the Collecting Societies Act 2016 and the KommAustria Act transposing EU Directives 2019/790 (DSM-Directive) was presented. When it comes to digital transformation the most significant changes are the new rules for the liability of online platforms. The draft law limits the liability regimes to 'providers of large online platforms' that play an important role for online content in the market and whose main purpose is to make profits by storing and making available to the public large amounts of works uploaded by users.

According to the draft law, by providing access to works uploaded by users, such online service providers interfere with the exercise of the transmission or making available rights of copyright holders. The liability privilege of the E-Commerce Act does not apply to such service providers.

The draft law limits the controversial regulations on the liability of such service providers to fault-based liability. The strict liability claims for injunctive relief, removal and appropriate damages remain unaffected. The liability regulations themselves – as well as the exceptions (eg, for parodies and caricatures) are

strongly oriented towards the requirements of the DSM-Directive, which is to be implemented in Austria by the draft law. According to this, service providers must prove that they have tried to obtain a licence and have made all possible efforts within the framework of the industry standard to ensure that certain works are not accessible in order to avoid liability, which means a reversal of the burden of proof compared to the classical Austrian liability regime. Here, one thinks first and foremost of the use of the highly controversial upload filters. Upon receipt of justified indications of infringement, such online service providers are also obliged to block access to the specific content. The liability of service providers who knowingly and intentionally cooperate to commit copyright infringement remains unchanged.

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 2020, the Austrian government announced that personal data and data sovereignty should be protected when using large amounts of data. The government wants to find a fair balance between the need for protection of people's data and the need for companies to use such data.

The Investment Subsidy Act has been in force since 25 July 2020. This Act is intended to counteract the current reluctance of Austrian companies to invest in fixed assets due to covid-19 and creates incentives for companies to invest in fixed assets during and after the covid-19 crisis. The funding will be granted for new tangible and intangible investments of depreciable fixed assets that are carried out in a permanent establishment in Austria. Explicitly excluded are, in particular, climate-damaging new investments; undeveloped land; financial assets; company takeovers; and own work capitalised. Funding is provided in the form of an investment grant amounting to 7 per cent of the eligible costs. The subsidy is doubled if the investment is related to digitalisation, greening or health and life sciences.

In 2021, the Austrian government announced its Digital Action Plan. The main points of this plan are as follows (Federal Ministry for Digitalisation and Economic Location, Digital Action Plan Austria).

Create space for the development of digital transformation

Austria will support the digital transformation of existing business models (eg, with e-commerce platforms for all Austrian entrepreneurs) and create space for the development of digital transformation. Furthermore, further training opportunities and information events for SMEs on the secure handling of data and digital data structures are to be expanded.

> "Company-relevant financial processes are to be digitalised and SMEs are to be able to complete their tax returns via intuitive online input masks."

Capital and digital public authority processes

A state-privately financed investment fund should be set up for the development of new business models, business processes and technologies. Financial incentives should be created for investments in SMEs and start-ups, innovative business models of SMEs or start-ups should themselves receive tax incentives and the framework conditions for innovative start-ups should be improved (eg, by easing tax and insolvency law and making it easier to set up a second company). Company-relevant financial processes are to be digitalised and SMEs are to be able to complete their tax returns via intuitive online input masks. Furthermore, business foundations via videoconferencing should be facilitated.

Infrastructure for innovation

With the Vienna Scientific Cluster and the MACH2 high-performance computer, Austria has a competitive basic high-performance computing capacity. Companies and corporations that need to manage computationally intensive processes should be able to easily use these capacities via digital innovation hubs. The standardisation and certification initiative 'Ö-Cloud' is intended to push the use of digital

cloud services among SMEs. In addition, the infrastructure for the digital transformation (especially the 5G mobile communications standard) and e-delivery should be expanded.

Interaction between business and research

Partnerships between private-sector research and development and science should be promoted by means of data hubs and digital innovation hubs, among other things, and cooperation between business and science is to be expanded in general. Technologies that play a key role in digital transformation (eg, 6G, AI Cloud, algorithm marketplace and cryptology) should be given priority in the Austrian Federal Ministry for Digitalisation and Economic Location's existing funding programmes.

Enable training and working conditions in the digital sector

Austria wants to promote digital talents, for example, with scholarships, career development models, support for start-ups and making study and training courses in the STEM sector more attractive, intensify digital training in all educational institutions (from in-company training to universities) and develop and support working time models and working models adapted to digitalisation.

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

When using cloud services, one should inevitably consider the GDPR and its accompanying national regulations, as personal data is passed on to third parties when using cloud services. Due to Schrems II (advanced data privacy software) and the troubles the Privacy Shield Concept is facing in the EU, data transfer to non-EU countries has become a serious legal issue.

But apart from data protection laws, further regulations may be applicable, depending on the sector in which the customer or user is active. Such regulations may, for example, be relevant for tele-medicine services or for financial institutions. Finally, sector relevant international bodies and authorities such as the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) have also enacted regulations relevant for cloud computing that need to be taken into account.

From an economic and organisational point of view, similar considerations have to be made as with outsourcing. The assessment of whether certain processes, functions and data should be entrusted to a third party outside the company (the provider) must be evaluated from all relevant perspectives. It should not be overlooked, however, that cloud computing differs significantly from outsourcing.

Assessment differs, depending on whether the service is software, platform or infrastructure.

From a risk perspective, it is often overlooked that perhaps working with a professional operator may be more secure than with a company's own data centre, but this does mean that the cloud customer is taking a new risk: further development of the cloud service used. The customer must therefore consider very carefully whether he or she can influence this or whether he or she is exposed to the development wishes of the provider.

The approach of standardisation, which is so strongly emphasised in cloud computing, must also be critically examined. Even if companies have had to painfully learn in the past that individual software developments often cannot keep pace with market developments and are not only very expensive to maintain, but also the exclusive use of largely standardised solutions is not always the panacea it appears to be, or sometimes may simply not be possible.

Photo by mRGB on Shutterstock

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?

In recent years, the way cloud contracts are negotiated has changed a lot. At the beginning of the 'cloud boom', the market was flooded with providers who rejected contract negotiations in the true sense of the word. With the argument that standardised services also require standardised contracts, customers experienced a 'take it or leave it' attitude. This has changed significantly in recent years, especially since large customers have made it clear that they are often unable to cope with 100 per cent standardised contracts, nor with 100 per cent standardised services, and so providers have been forced to be more flexible.

This flexibility is necessary on the one hand, on the technical and organisational side (eg, geolocations, interfaces, design of services, support models), and also on the legal side (warranty and liability issues, business continuity, etc, to name just a few).

On the Austrian market, internet as a service contracts are most comparable to classic IT outsourcing contracts, while software as a service contracts are often a mixture of 'lease contracts' with a certain service element.

Purchasing cloud services also differs significantly from purchasing outsourcing services. Whereas the classic outsourcing provider often adapts its services to the customer's wishes down to the smallest detail and the outsourcing contract is only negotiated after such a technical agreement has been reached, things are different with cloud computing. Despite the degree of standardisation already mentioned, most providers can now show a certain flexibility in their contracts, but this flexibility does have its limits. This means, however, that the actual cloud contract must necessarily be seen and evaluated as part of the provider's service in the purchasing process. It cannot usually be 'negotiated away'. The customer must thus check and recognise early on in the purchasing process whether there are red flags in the contract that he cannot accept and which the provider will not change.

In addition to the typical contract topics such as service description, remuneration (note: scalability should mean that the customer can also scale the service downwards), as well as warranty and liability, cloud-specific topics must not be forgotten. These include ensuring business continuity, disaster recovery and software update cycles and the resulting need for customer adaptation (often difficult and expensive from the customer's perspective).

If the use of the cloud service is preceded by a project, for example, to create

> "Purchasing cloud services also differs significantly from purchasing outsourcing services."

individual functions, migrate data, create interfaces, extensive configuration or parameterisation, it should be considered to conclude a separate contract for this. From the customer's point of view, Austrian contract law offers advantageous possibilities here, but these are not provided for in the typical cloud contract.

As to contracting techniques, for operations contracting management is not a pure administrative task anymore. This is especially true for cloud contracts where all relevant stakeholders need to be on board when structuring and negotiating the cloud deal.

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

The typical points of contention in negotiations about cloud contracts are the following.

Project

if a project precedes, the classic question is whether the provider owes a successful implementation (work contract) or 'only' an effort (service contract). The differences between these two concepts could not be greater from the perspective of Austrian contract law. It goes without saying that from the customer's point of view, a contract for work and services is preferable. It goes without saying that, from the customer's point of view, a work contract is preferable. And if the project is more extensive: should it be a classic waterfall or an Agile project?

Cloud service

There are a number of points of contention relating to cloud service, including:

- adaptation requests from the customer;
- commitment of the provider to further develop the service;
- commitment of the provider to implement any regulatory requirements for the service without additional costs;
- maintenance and support models;
- service levels (SLAs) and service credits;
- fee structure and scalability (up and down);
- warranty (commitment to fix bugs with agreed resolution times);
- liability;
- data protection;
- termination: notice periods and waivers of notice; and
- how to avoid vendor lock-in and exit scenarios.

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

The cybersecurity laws in Austria are chiefly the Network and Information System and Security Act (NISSA) and the ADPA but also the Telecommunication Act 2021 (especially section 44) and the Telecommunications Network Security Ordinance 2020.

The NISSA aims to achieve a high level of security of network and information systems of essential service operators, digital service providers and public administration institutions.

Section 2 of the NISSA defines the material scope of the act. This includes operators of essential services (section 3, No. 10 of the NISSA) in the sectors mentioned in Nos. 1–7 (key economic sectors), providers of digital services (section 3, No. 13 of the NISSA) and public administration institutions (section 3, No. 19 of the NISSA). Digital service providers are defined as providers of an online marketplace,

Photo by Rudy Balasko on Shutterstock

an online search engine or a cloud computing service, provided that they are of a certain size. In addition, they must also meet the following four general conditions for the definition of digital services: as a rule, the services must be provided for remuneration; the service must be provided at a distance; the services must be provided electronically; and individual availability is a prerequisite. Operators of essential services can be found in the following sectors: energy, transport, banking, financial market infrastructure, healthcare, drinking water supply and digital infrastructure. According to section 16 of the NISSA, the operators of essential services are identified in a two-stage procedure. The first step is the ordinance of the BKA (the Federal Chancellery) in agreement with the BMI (the Ministry of the Interior) to determine the essential services; the second step is the issue of an official decision.

Public administration offices include in addition to federal institutions also those of the federal provinces, whose protection is of great importance for the functioning of a (constitutional) administration and the provision of services of general interest.

The main points of the NISSA are: definition of tasks and responsibilities of authorities and powers to ensure a high level of security of network and information systems; definition of a national strategy for the security of network and information

systems; regulation of obligations for the identified operators of essential services, digital service providers and federal facilities (appropriate security measures for their network and information systems; reporting of security incidents to the competent authorities); verification of security measures and compliance with the obligation to report; establishment of computer emergency response teams, or computer security incident response teams, and definition of their tasks; regulation of structures and tasks in the event of a cyber-crisis (ie, one or more security incidents with a current and immediate threat to the maintenance of important societal functions and serious impact on the health, security or economic and social well-being of large sections of the population or the effective functioning of governmental institutions facilities); the establishment of sanctions in the case of non-compliance with the obligations of the NISSA.

Providers of digital services must take (preventive) appropriate and proportionate technical and organisational security measures with regard to the network and information systems they use to provide the digital service. The following must be taken into account: security of systems and installations, management of security incidents; business continuity management; monitoring; verification and testing; and compliance with international standards. Providers of digital services have to immediately report a security incident (ie, a disruption with significant impact affecting a digital service).

The legal provisions thus ensure a high level of security of network and information systems. As a result, it is easier for companies to trust in digital transformation projects.

Data Protection laws

The General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) stipulate that entrepreneurs must implement technical and organisational measures to ensure IT security, such as pseudonymisation and encryption (article 32 of the GDPR). Ultimately, however, companies decide what measures are actually taken. In principle, fines or penalties are directed at the company (article 83 of the GDPR; section 62 of the DPA), pursuant to section 9 of the Administrative Penal Act (APA) in conjunction with section 30 of the DPA, but can be imposed on the managing director instead of the company.

Other laws

Irrespective of the application of the aforementioned laws, liability may also arise in the event of a breach of organisational duties, including IT compliance. A managing director of a company with limited liability must exercise due managerial care in the performance of his or her duties (section 25 of the GmbHG (regulations for Austrian

> “The introduction of corresponding IT compliance, which also takes the risks of cybersecurity into account, is an absolute must.”

companies with limited liability)). If he or she violates this obligation, for example, by neglecting to introduce adequate IT compliance, he or she may be liable for damage.

In principle, a liability claim only arises in the case of unlawful and culpable damage,ie, the general conditions for damages under civil law must be fulfilled. Even in the case of slight negligence, damage resulting from successful cyberattacks can result in the managing director being liable to the company. In principle, the company must prove that it has suffered damage because of certain conduct (act or omission) by the managing director. However, if there is an objective violation of due diligence, fault is presumed to have been caused by it, meaning that the burden of proof shifts to the managing director. A comparable standard of due diligence is also provided, for example, for members of the executive board of a stock company (section 84 of the Stock Corporation Act).

Since even the most modern security measures do not offer absolute security against cyberattacks and the technical implementation of the legal requirements is at the discretion of the individual company, giving rise to a liability risk, the introduction of an appropriate IT compliance system also includes: technical standards, such as ISO standards, to guide the adequacy of technical and procedural

measures; cyber-insurance, for example, covering claims for damages due to a breach of data protection or confidentiality or claims for damages due to inadequate network security, limiting the economic impact of a claim; and contractual transfer of risks to counterparties (outsourcing providers). The introduction of corresponding IT compliance, which also takes the risks of cybersecurity into account, is an absolute must.

An amendment to the Administrative Penal Act (APC I 2018/57) provided some relief: since 1 January 2019, fault is no longer presumed by law if the administrative offence is subject to a fine of more than €50,000 (new section 5, paragraph 1a of the APA). This leads to a reversal of the burden of proof. The authority will have to prove the fault of the company or its managers. Furthermore, in accordance with section 371c of the Trade Ordinanace, the principle of 'consulting instead of punishment' is included in the APA (new section 33a of the APA). The authority will have to call for the establishment of the lawful condition if the fault; the significance of the legal interest protected under criminal law; and the intensity of the impairment of the legal interest protected by the offence, are low in each case.

Initial experience in connection with section 371c of the Trade Ordinanace, which came into force in July 2017, can be gained by the Tyrol Regional Administrative Court (LVwG Tirol, 23 August 2018, LVwG-2018/15/0903-6).

The Telecommunications Act 2021 and the Telecommunications Network Security Ordinance 2020 specify more detailed provisions to ensure network security in the telecommunications sector. At the same time, a large part of the EU catalogue of measures to increase cybersecurity is implemented in 5G networks.

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

Since the effective date of the GDPR (25 May 2018), organisations have been confronted with more harmonised but also more rigid data protection provisions. Even though the legal step between the pre-GDPR rules and those of the GDPR were not so big on paper, organisations affected frequently suffer under the legal uncertainty and under new concepts introduced by the GDPR. For example, taking privacy by design and privacy by default considerations into account during procurement processes will still take some time until organisations have more routine.

Also, international data transfers have become more and more complex, in particular taking the ECJ decision on the Privacy Shield and Standard Contractual Clauses (SCC) into account (Ref: C-311/18) and the European Commission's newly published SCC into account. By end of 2022, data controllers (ie, companies/organisations) must have implemented the new SCC to transfer personal data outside

"Since the effective date of the GDPR (25 May 2018), organisations have been confronted with more harmonised but also more rigid data protection provisions."

of the European Union. The implementation of those new SCC will take some time since the data controllers are obliged to conduct a data transfer risk assessment upfront. Given the fact, that some big players under cloud providers are located outside the EU, any transfer of personal data to those clouds has to be scrutinised in detail. Besides, Austria has few provisions regarding data localisation in place and – given the scope of the EU regulation on the 'free flow of non-personal data' (Regulation 2018/1807/EU) – it further aims at removing obstacles to the free movement of non-personal data across member states and IT systems in Europe.

According to article 1(2) of the GDPR this Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

According to article 35 of the GDPR, in the case of a solidly intended data processing, the controller has to make an independent forecast decision for the future, in which various factors have to be taken into account, such as, in particular, the type, scope, circumstances and the purpose of the planned data processing.

The GDPR provides for rules whereby the protection of data subjects may not be undermined by outsourcing data processing activities to subcontractors. A 'multi-dimensional responsibility' applies to the controller, by which he is not only liable for the selection fault, but also has a duty to guide and control the processor, thus ensuring a uniform data protection standard for the entire outsourcing process.

Articles 13 and 14 of the GDPR provide for various information obligations for the controller for processing personal data of data subjects.

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)?

The development of classic waterfall models to Agile projects and then to DevOps is one of the most difficult of all. The market shows that this still causes big problems. This starts with the IT teams, who are not used to Agile project work and remain embedded in old structures and procedures, and ends with the legal departments and lawyers, who have difficulties in meaningfully reflecting the requirements of modern project governance in contracts.

To make matters worse, agility is often prescribed by higher hierarchical levels without creating the necessary conditions in the organisation and without mapping and learning processes.

In Austria, contract design for Agile projects in large organisations typically faces the problem that the governance of the organisation requires budget security

"The development of classic waterfall models to Agile projects and then to DevOps is one of the most difficult of all."

(ideally in the sense of a lump sum payment) and liability assumption (ie, contract for work instead of service contract). Both are contractually not so easy to implement in Agile projects.

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

Larger organisations are generally experts in governance. However, they often have a blind spot when it comes to governing their digital presence. A lack of digital governance causes many of the same problems that a lack of association governance causes for an organisation: a lack of accountability, a lack of clarity about roles and responsibilities, and an inability to make good decisions in the face of change and uncertainty.

Successful digital transformation requires:

- a positive attitude towards digitisation;
- clear definition of goals with practical ranking;
- living an innovative corporate culture;
- entering into the right collaborations inside and outside the company; and
- creation of the required structures and processes (eg, Agile management; enabling trial and error; and integration of and transparency to stakeholders).

Veronika Wolfbauer
v.wolfbauer@schoenherr.eu

Peter Ocko
p.ocko@schoenherr.eu

Schönherr Rechtsanwälte GmbH
Vienna
www.schoenherr.eu

The Inside Track

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

We are enthusiastic about digital transformation, which allows people to be innovative and to focus on activities in the work environment that add value and are fun. We find it especially interesting to create an environment that supports such projects.

The mapping of such projects into contracts that promote innovation and at the same time provide security, the latter being an essential task of lawyers, is a great challenge.

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

The challenges of transformation projects are comparable to those of technology projects: different interests of stakeholders who hardly understand each other's language must be reduced to a common denominator. However, agility, flexibility and the space for innovation must not be lost.

Lawyers are often risk-averse and try to hedge all possible risks. Even if this is a legitimate goal in principle, the big picture must not be lost sight of. Old legal concepts do not always fit new topics. Lawyers must also be innovative in their solutions.

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

In our experience, it is especially important as lawyers to have a deep understanding of the client's organisational, economic and technical requirements. This is the only way to provide meaningful advice.

Risks must be recognised; but risk reduction must not lead to a loss of innovation opportunities.

Good lawyers are also 'translators' between the needs and languages of the different stakeholders.

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