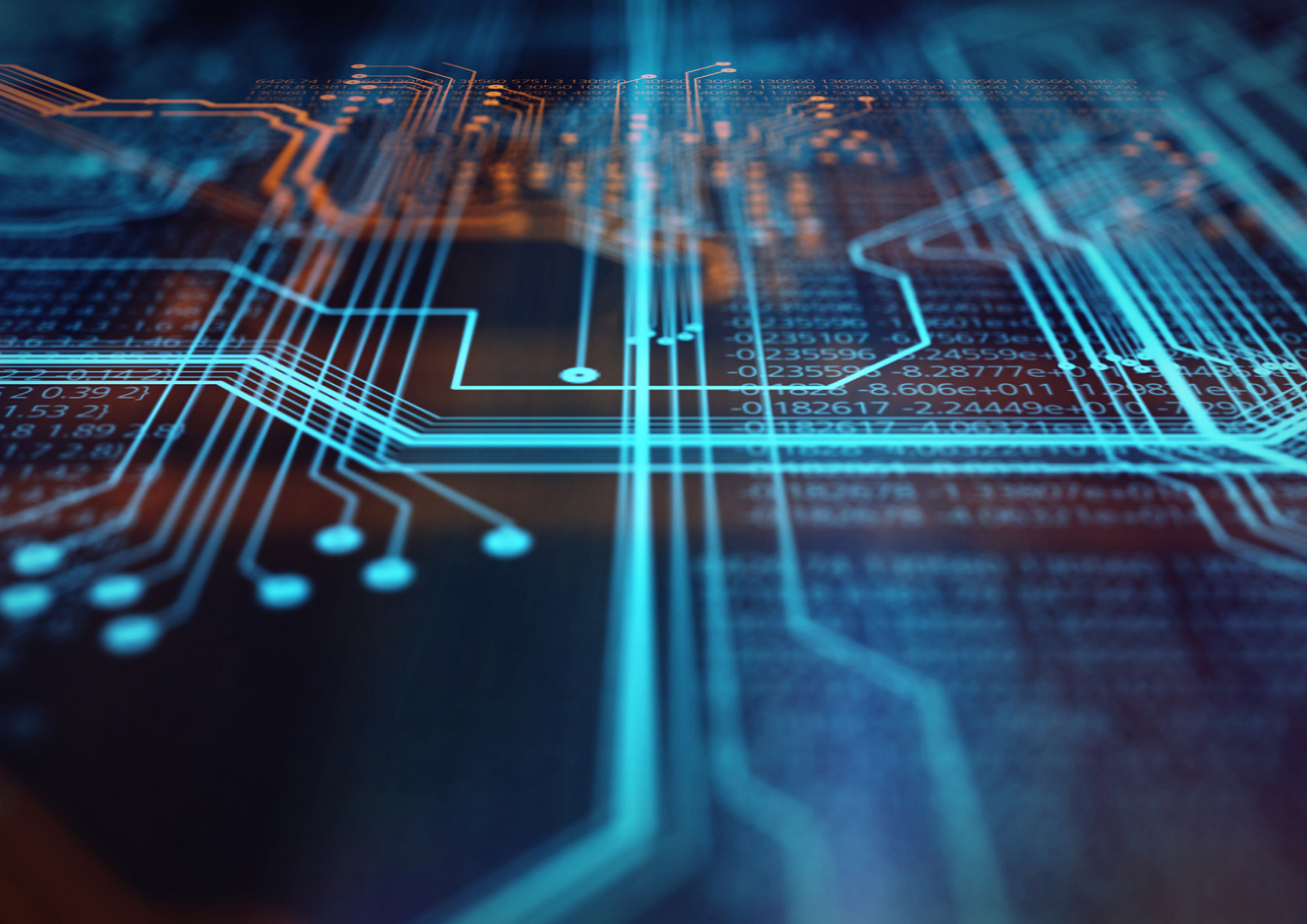
大成 DENTONS

MARKET INSIGHTS

DIGITAL TRANSFORMATION AND THE DIGITAL CONSUMER

CONTENTS



WELCOME

Online activities such as chatting, shopping, watching movies, and listening to music have become standard in todays' society. Standard perhaps, but not straightforward for businesses which are forced to adjust to new consumer behaviors, new competitors and new business models. Banks simply can't turn away young customers, who prefer Internet banking or mobile express loan apps to offline interactions, which often entail waiting in line. Tour operators can no longer count on customers to go window shopping in search of new travel deals. Television broadcasters have realized that the good times are over for old-style linear free to air TV.

The first wave of Digital Transformation (DT), which hit the Technology-Media-Telecommunications sector first, has already run its course. But the signs are telling us that this process is not over - it is just the end of the beginning. Other more traditional sectors will soon be face-to-face with change every bit as far-reaching as the revolution in the mass media, telecom and FMCG industries. The new wave could well wipe some businesses out (remember encyclopedia publishers?) and profoundly transform others, as was the case with music companies.

It is only natural that some 'analogue' businesses are reluctant to change. Many have adopted a wait-and-see policy, to understand what the competition will do before making their move. The reluctant approach taken by many European enterprises - fed understandably by concerns such as data protection, security and labor law - looks set to end shortly. The European economy is undoubtedly on the verge of a new technological revolution and companies will have no choice but to transform in order to grasp the vast opportunities offered by digital transformation.

WHAT IS DIGITAL TRANSFORMATION?

The digital revolution will change how 'analogue' companies do business. This means adopting new technological solutions and learning new skills, such as the ability to handle vast volumes of data generated by social media and the emerging Internet of Things.

Management will have to partner smartly with the new generation of digital clients, to offer new digital apps and services and solve new legal problems. Selecting and procuring technology is just the start of business digitization. No less important is changing the culture of the organization, which is often much harder to achieve.

Looking past the buzzwords, what is Digital Transformation?

DT can broadly be summarized as change triggered by digital technology which (1) creates new marketing and communication channels and tools, (2) increases the efficiency of the operational processes of a company, (3) enhances customer experience and/or (4) leads to the development of new business models.

Where are we today?

Most businesses are aware that DT is a necessity and research clearly demonstrates that digital transformation is well worth the effort. A 2017 Enterprise Strategy Group study, commissioned by Dell EMC,[1] found that 71 percent of respondents agreed that IT infrastructure transformation is essential to ongoing business competitiveness. However, only five percent of businesses were segmented into the IT maturity stage termed 'Transformed' (i.e. top users of IT resources to accelerate the development of innovative products, automate processes and transform IT departments into profit centers). The research revealed that 96 percent of companies in the Transformed group had exceeded their revenue targets.

The 2018 IDC forecast shows that making money out of data and increasing profits from digitization will be top priorities for as many as 75 percent of CIOs.

The initial challenge businesses usually face is how to manage change within the company. In a recent study[2], Bain & Company notes that an effective digital strategy must combine a wave of no-regret, short-term initiatives with a bold vision of how innovation might transform the whole industry.

You're not alone

The legal market is not immune to this change. We at Dentons not only understand the challenges businesses face but are also implementing them in our own business. We realize that our clients' expectations of legal services in the digital age are different to what we were used to in the twentieth century.

INNOVATING THE PRACTICE OF LAW THROUGH NEXTLAW LABS AND NEXTLAW VENTURES

The business of law has not yet benefited from technology as much as other professional services industries. Dentons is changing that through its Nextlaw Labs and Nextlaw Ventures businesses.

Nextlaw Labs, the first legal technology venture created by a law firm, was launched by Dentons in 2015 to reinvent the business and practice of law via technology and to own and shape the disruption that is transforming the legal industry. Leveraging unique insight and tangible output, and with the world's largest law firm as its testing ground and supporter, Nextlaw Labs is uniquely positioned to serve as a global intelligence hub for the legal innovation vertical.

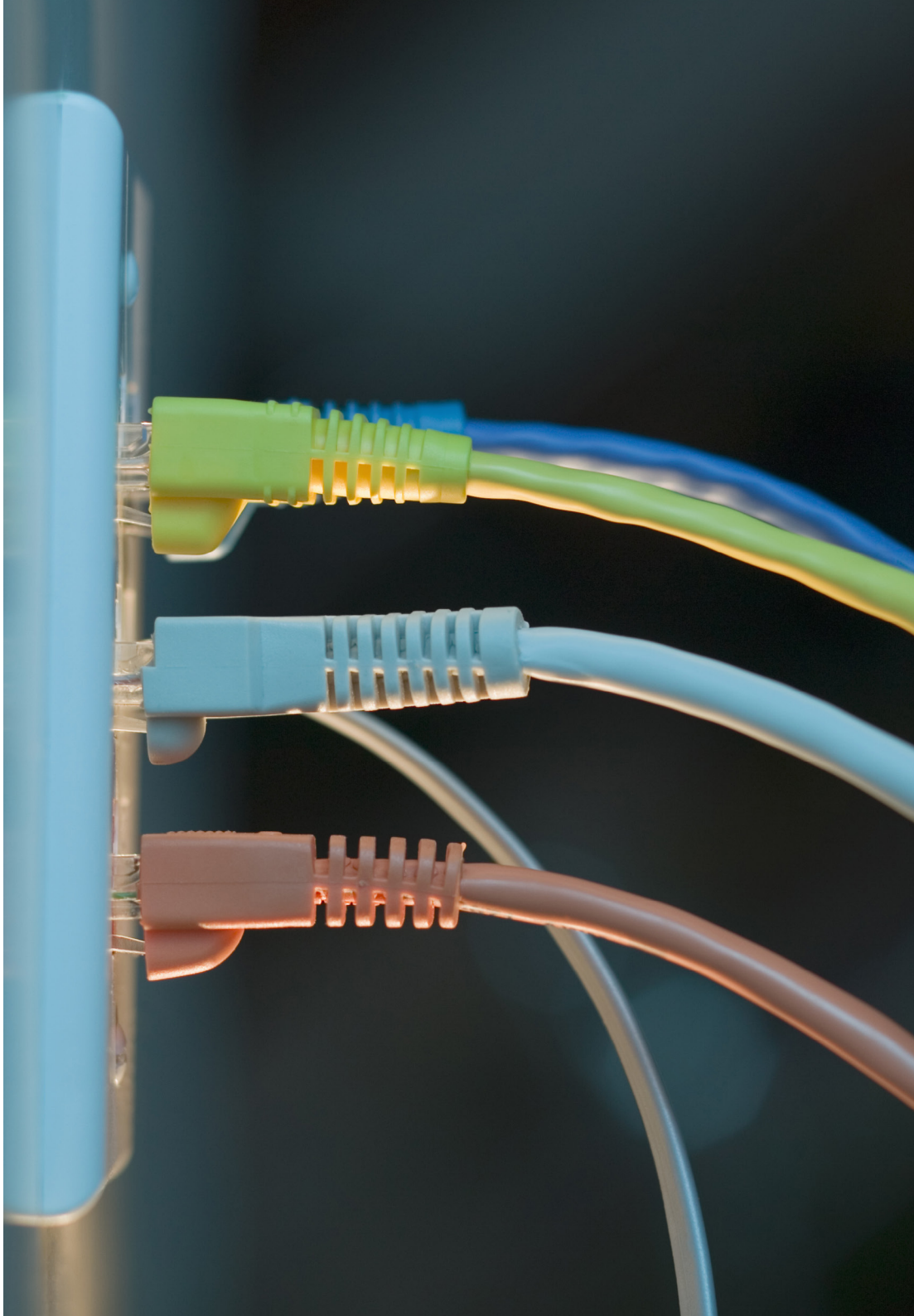
Solution-oriented and customer-centric, Nextlaw Labs accelerates and pilots leading-edge technology solutions and incubates innovative ideas to develop products and processes that transform legal services delivery. It delivers "innovation as a service" consulting for Dentons and its ecosystem, providing a safe sandbox to experiment, engage and collaborate.

Nextlaw Ventures is a globally active early stage venture investor that focuses exclusively on legal technology. Its current portfolio consists of ten innovative legal tech companies. Nextlaw Ventures helps grow the companies it invests in by tapping into Dentons' legal talent, unmatched global reach and extensive client base.

Staying safe

First and foremost we understand that digitizing your company means you have to acquire a whole array of goods, services and licenses for the products you are going to use. You need to address how you're going to stay safe in legal terms if any of the solutions implemented fail. Additionally, you should also bear in mind that digital consumers are far more likely to react to any breach of their rights while your employees will need to understand what the change entails.

These issues are addressed in detail, in the chapters of this Market Insight publication. The following is an introduction to the topics discussed.



1 https://www.emc.com/collateral/analyst-reports/esg-dellemc-it-transformation-maturity-report.pdf

2 http://www.bain.com/publications/articles/digital-strategy-for-a-b2b-world.aspx

CATCHING UP WITH THE DIGITAL CONSUMER

IGOR OSTROWSKI, WARSAW

The customer is king

One thing is absolutely certain: digitization has marked the dawn of a new era in client focus. Customers have access to a wide range of information on products and services from social media, online reviews, blogs, chat rooms and task specific apps. The upshot is they generally know what they want.

However, not every digital client can be easily pigeonholed. Some customers have greater awareness, while others have a rather limited perspective (for example they may appreciate being able to make quick purchases from their mobile device). Finally, there are people who still feel unsure in the digital world, as they do not know how to navigate safely and effectively or how to identify trustworthy, honest suppliers and service providers. These customer types frequently overlap and many clients present characteristics from each grouping. We should bear this in mind when building client relationships in the digital world.

Customer expectations are changing as digital technologies develop. Ericsson's 10 Hot Consumer Trends 2018 report shows that more than half of current users of intelligent voice assistants believe we will use body language, intonation, touch and gestures to interact with technology, just like we do with people. Two out of three believe it will happen within the next three years. In the study, as many as 30 percent of respondents say the new technologies require new skills. 46 percent say the Internet allows them to learn and forget skills faster than ever before.

E-consumer rights

In line with the above, many entrepreneurs see opportunities in e-commerce. This is hardly surprising given the explosion in online shopping, which continues to transform the retail market. Authorities have reacted by introducing measures to protect e-consumers, who are usually the weaker party in transactions.

EU member states must, for example, implement the Consumer Rights Directive (2011/83/EU) into their legal systems. For example, customers have a 14 day cooling-off period to back out of a remote contract, and when they return goods, the trader is responsible for the cost of delivery by means of the cheapest delivery method it offers.

Legislators are also looking to guarantee that before entering into a transaction, customers are aware of all the costs they have to pay. Sellers must clearly inform the customer of all costs arising from the contract and are prohibited from excessive additional charges for credit card payments and hotlines, and from automatically including additional services in the price of goods purchased. They also ban the use of misleading online offers which wrongly suggest that a product or service is free when, in fact, it is paid.

It is also the vendor's responsibility to clearly inform the customer of its identification data. The website of an e-store must display particulars such as the company's name and postal address, tax number and telephone number. It also has to provide customers with a cancellation form and instructions on how to rescind a contract. Chapters five and six take a more detailed look at consumer protection and contracting issues.

3 https://www.ericsson.com/en/trends-and-insights/consumerlab/consumer-insights/reports/10-hot-consumer-trends-2018

FinTech, the new frontier

With the evolution of technology in the financial services sector, FinTech is rapidly becoming the new frontier as governments grapple with digital developments in key market segments. As FinTech innovations continue to grow and evolve they continue to change the face of companies. In chapter seven we explore the development, growth and innovations in FinTech which sits at the crossroads between heavily regulated financial services and digital innovation.

Towards the Digital Single Market

Businesses operating in the European Union need to remember that Brussels is still working on the principles of the Digital Single Market, based on the rule of free access by consumers and businesses to goods, digital services and networks and the development of a digital economy and society. This will involve passing 35 legal acts of which several have already materialized. According to the European Commission, if a fully uniform digital market was up and running, the EU could profit to the tune of €415 billion a year. As things currently stand, progress is being blocked by obstacles such as complex VAT laws that vary between member states (approximately 80 different regulations) and copyright law.

A draft bill on the free flow of data is one imminent change. In order to fully benefit from a data-based EU economy, the Commission is also proposing a new set of regulations on the free flow of non-personal data. The Commission argues that member states cannot expect organizations to store or process data within their territory only. Potential restrictions may only be justified on legitimate grounds of public safety. Member states will be required to notify the Commission of any new or current requirements related to data location. The free flow of non-personal data will make it possible to carry out cross-border business operations more easily and cheaply, without having to duplicate IT systems or store the same data in various locations. It will be accompanied by the development of EU codes of good practice in order to remove obstacles when changing cloud service providers and storing or transferring data back to the user's own IT resources.

These changes aim to encourage businesses to use cloud services more readily and act with confidence when entering new markets or transferring their internal IT resources to cheaper locations. The Commission estimates that, in the final analysis, this will add an extra €8 billion per year in terms of the area's GDP. Chapter nine takes a more detailed look at big data issues.

Handle (data) with care

Appropriate management of digital data, and especially personal data, is a top priority when building relations with digital customers. The General Data Protection Regulation (GDPR) came into force in all member states on 25 May 2018. The regulation introduces a raft of major changes, including the need to consider data protection requirements when developing solutions and the need to guarantee that personal data will only be processed to the extent required to achieve the stated objective. The new regulations replace the personal data protection law previously in effect in all member states.

Previously, sanctions could only be applied by the regulator, but under the new system, a consumer may file claims against a company directly in court. This could

well become the course of action adopted by disgruntled clients, employees and competitors.

More stringent terms were applied as regards some of the legal bases used by organizations when processing personal data, such as for example the consent of data subjects. The GDPR provides individuals with wide-ranging powers, such as the right to be forgotten and the right of data portability. The list of what constitutes sensitive data was also expanded and now includes biometric and genetic data.

Consequently, companies and institutions have to be much more transparent in terms of how they process personal data. They are required to inform data subjects of details such as data retention periods, as well as the right to file complaints with a supervisory authority. Additionally, should any data protection breach occur, in some cases, data controllers are required to notify the relevant authorities and data subjects whose personal data was compromised within 72 hours of detection and all infringements of data protection must be duly documented so that checks can be made to ensure that they were duly reported and recorded. These issues are discussed in more detail in in our chapter on GDPR, chapter four.

The GDPR aside, work is also underway on the ePrivacy regulation to introduce more restrictive legal provisions on privacy on the Internet. The primary objective of the planned ePrivacy regulation is to guarantee the confidentiality of data originating from electronic communications. This involves, in particular, a ban on the illegal interference, eavesdropping, storing or intercepting of data. The new law expands the definition of e-marketing. In the new definition, B2C communications are aimed at individual users, while B2B communications are addressed to companies. With B2C communications, the sender will require the explicit consent of the recipient for the message to be delivered. The important question of whether direct marketing to employees qualifies as B2C communication or B2B communication is unfortunately not clearly answered and with room for member state derogation, there will likely continue to be divergence between the member states.

Many Internet advertising companies are anxious about the measures envisaged by the ePrivacy Regulations, such as the significantly expanded territorial scope: any company sending direct marketing to end-users in the EU or wanting to place cookies on end-users' devices will be covered by the ePrivacy Regulation. The legal aspects of using digital data are discussed at length in chapter four. At the time of publication of this guide, the e-Privacy regulation is still in a draft version and subject to change..

Cyber security

Cybersecurity is another challenge for businesses which rely increasingly on Internet channels and applications. Last year saw extensive coverage given to the WannaCry and Petya cyberattacks. WannaCry was the largest ransomware attack to date, blocking tens of thousands of devices and compromising the systems of Britain's National Health Service, the Russian Home Office, transport companies, telecoms, education centers and many others. Petya hit Ukraine first and spread to Russia and neighboring countries. It hit businesses in various sectors, such as energy, transport and the advertising industry.

Cyber criminals are expected to refine their techniques and increase the frequency of attacks. Set against this backdrop, Cisco coined a term for a new type of cyberattack: DeOS (Destruction of Service). Cisco warns that the new attacks will be much more destructive than the classic ransomware attacks, as they may completely deprive target companies of the ability to restore data or resume normal operations of their IT systems. DeOS use mechanisms that destroy backup systems and support networks. Along with the growing popularity of the Internet of Things (IoT) and online operations, the potential list of targets is growing and could result in an unprecedented escalation of attacks.

Check Point, a company from Israel, refers to such attacks as fifth generation cyberattacks, characterized mainly by large scale and rapid transfers between multiple environments. They involve sophisticated attacks on mobile networks, clouds and intranets that bypass conventional protection systems based on static detection.

This does not mean, though, that they cannot be prevented. To increase cyber security, Cisco recommends implementing updates to IT systems and apps so that cybercriminals are not able to exploit any known vulnerabilities, applying integrated protection measures and sustainable mechanisms to actively address security threats, and ensuring security training is appropriate to employees' roles. Cyber security should be a preoccupation of senior management from the early stages of system implementation projects. The key issue is to define clear methods for measuring and evaluating security levels and streamline cyber security practices.

Chapter two includes a summary of different legal challenges, including cybersecurity which need to be addressed before a successful DT project can be implemented.

In data centers we trust?

Cloud computing technology is on the rise. According to Huawei, by 2025 the entire IT infrastructure of businesses will be transferred to cloud and 85 percent of apps used by businesses will be based on cloud services versus 20 percent currently. Huawei claims there will be no company whose core business is not based on cloud computing technology and each business will be looking for tailored solutions that best suit their needs.

At present many companies, particularly in the financial sector, must operate in line with restrictive data protection requirements that greatly hamper the possible use of cloud technologies. Many businesses and institutions prefer to play it safe and shy away from storing the data of clients or business partners outside of their physical location. On the other hand, cloud service providers argue that they hold a certificate that guarantees secure and transparent data processing standards. They claim they can assure maximum security in data storage; communication; collaboration and document sharing; and website, app and service hosting.

The cloud operates through servers located in data centers. When signing a contract, you should verify the storage location of your data and select a service provider that guarantees a location in a given country so that you may rest assured that your data is protected in compliance with the law of that country.

It is also advisable to check the services offered at the data center. While you might wish to use only one or two cloud services initially, it is worth selecting a provider with a versatile portfolio that is constantly evolving. When, in time, your company's need change, it will be more convenient to use the services of a single data processing center. The more services you purchase from a single provider, the more negotiating power you have, and the more cost effective the arrangement is. The best scenario is where the provider is able to tailor its offer to meet the customer's needs - not the other way round. Chapter three takes a look at the key benefits and challenges relating to data centers.

Change of work standards

Digitization is not only profoundly changing client relationships, but it also affects the work standards of those employed. Owing to the IT solutions available, more and more individuals are working remotely instead of in the office. In the final chapter, we consider some of the key impacts of digitalization on employment law.

A recent report by Deloitte[4] indicates that employers will need to reinvent their organizational structures, talent management systems and HR strategies to keep up with the pace of technology. Companies can no longer consider their workforce to be made up of the employees on their balance sheet - they must include freelancers, seasonal workers, independent contractors and teleworkers. However, increased efficiency does not always go hand in hand with technological advancement. According to Deloitte, this derives from the fact that HR departments seldom keep up with changing trends - as few as 35 percent of HR specialists consider the efficiency of their units to be "good" or "excellent", and only 11 percent know how to create the organization of the future.

Meanwhile, a report by Hays, Kinnarps and Skanska[5] shows that the respondents believe flexibility will be the key driving factor on the labor market in the years ahead. Employees want the option of selecting the time, place and tools of their work. This is especially true of younger employees, accustomed to multi-tasking and frequent changes of delivery modes. Such a major change poses a challenge for employers that need to respond to the expectations of different generations.

As telework is new ground for many employers, they need to consider the new legal aspects related to this form of employment. For example, a telework contract should set out the rules of work, how to check the teleworker's presence at work (e.g. always when logging on) and the manner of sending work results.

Importantly, there are certain differences between home office and telework. Both refer to work performed remotely by an employee from home or elsewhere, but the difference is that telework is performed on a regular basis, while home office is only occasional, and the employee decides if and when to work remotely.

All those factors significantly affect the legal conditions of work time, which is an issue that we address in chapter 10. Questions might arise as to how an employee should treat an e-mail from a superior in the evening. Does it breach

4 https://www2.deloitte.com/content/dam/Deloitte/global/Documents/HumanCapital/hc-2017-global-human-capital-trends-gx.pdf

5 https://www.skanska.pl/4a29ca/siteassets/oferta/biura/raporty-i-standardy/raport-nie-boj-si-activity-based-working/nie-boj-si-activity-absed-working-raport-2017-ahys-kinnarps-skanska.pdf

the employee's right to a good rest? The Court of Justice of the European Union frequently notes that employees cannot have any obligations imposed on them during their leisure time.

Another general trend is the increasing number of employees willing to use their own portable devices at work, as smartphones and tablets become increasingly popular.

On the one hand, a company accepting BYOD (bring your own device) arrangements may boost productivity through better team collaboration and employee satisfaction. On the other hand, BYOD poses new challenges for businesses. The need to protect confidential data of the company and its employees against unauthorized access is a top priority. IT units need to provide technical support for a range of mobile platforms. Frequently, the most difficult part of the process is to make employees willing to accept security rules, which they may view as restrictive.

As a principle, companies allowing outside hardware to connect to their network should first develop a rational and functional safety policy. An updated list of devices using the intranet and their assigned users with access rights is a must. IT teams should also define data storage rules and specify whether data can be downloaded onto mobile devices, to be then carried outside the office. It is also worth developing procedures to follow in the event of data theft or termination of employment so that data can be cleaned or protected.

Attack of the robots

In chapter 11 we explore developments in Artificial Intelligence or AI, which has already fast become a part of everyday life. Employers and employees will likely soon be faced by challenges arising from the use of robots. A 2017 Deloitte report[6] revealed that 53 percent of respondents have already commenced implementing robots and automated processes and another 19 percent intend to do so within the next two years. According to the report, robots could ultimately replace one fifth of the full-time workforce and, at the same time, boost revenues. 64 percent of managers see Robotic Process Automation (RPA) as part of a wider, strategic corporate initiative, and most believe that investments in RPA are likely to break even in less than 12 months. As a result, future companies may seek employees with different competencies than they do today.

It is not yet possible to fully anticipate the effects of the digital revolution and the use of technologies such as artificial intelligence or virtual reality. In its artificial intelligence (AI) report prepared in collaboration with Dentons, Polityka Insight[7] emphasizes that technology boosts economic potential by automating routine and time-consuming processes, which in turn allows employees to perform more profitable tasks. Boosting the productiveness of irreplaceable employees, while also reducing the costs of capital, opens the way to increased investment in the economy. The latter mechanism is of the essence for countries with low savings reserves, as it increases the availability of state-of-the-art technologies for companies with no potential for developing specially tailored applications.

6 https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/strategy/deloitte-es-consulting-robots-are-ready.pdf

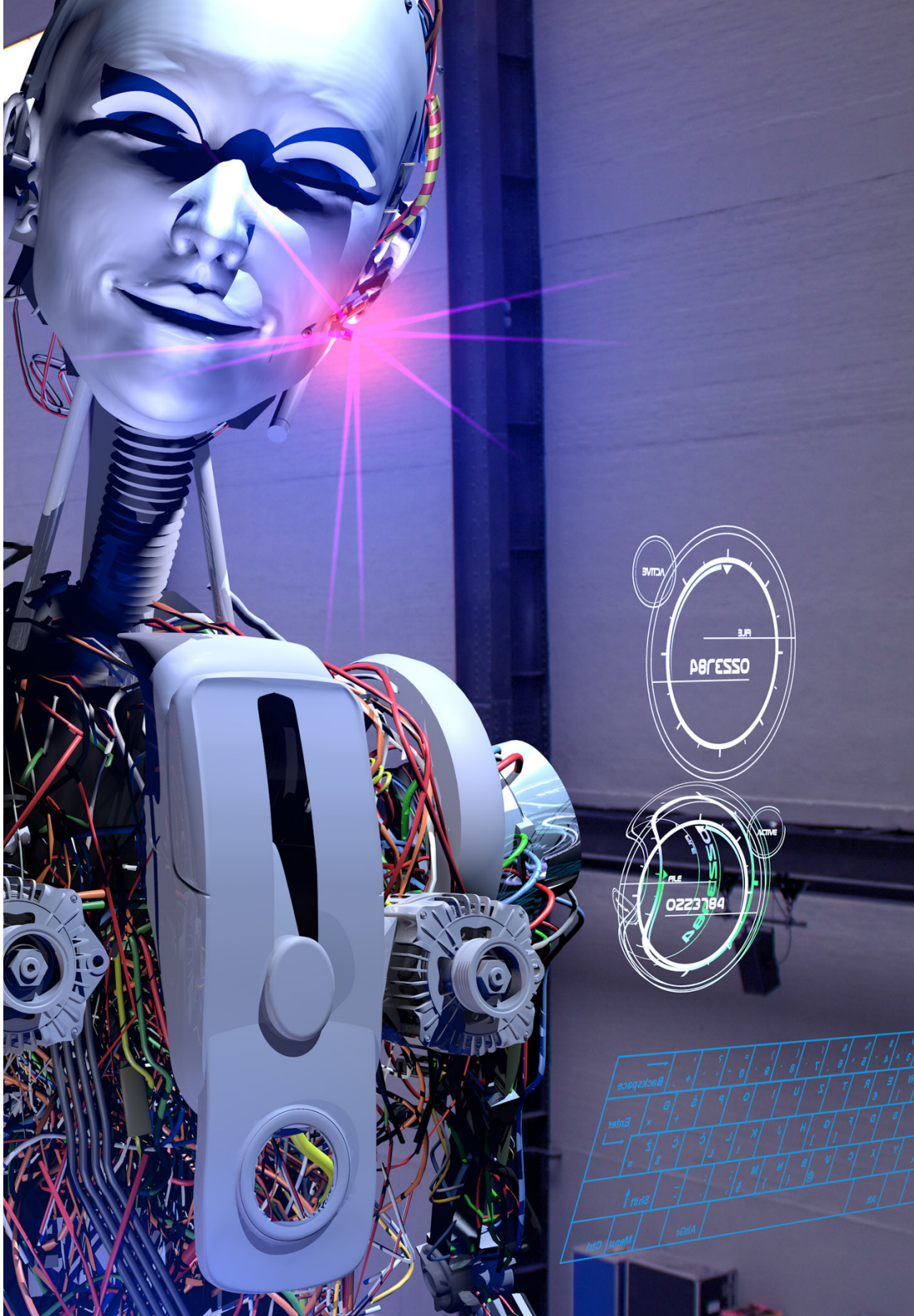
7 https://www.politykainsight.pl/en/_resource/multimedium/20145296.

8 https://www.sas.com/pl_pl/news/informacje-prasowe-pl/2018/sztuczna-inteligencja-nie-rozumie-ludzkich-emocji.html
https://www.sas.com/sas/offers/17/the-enterprise-ai-promise.html

However, according to recent research by SAS[8], 32 percent of responding EMEA companies said that the ethical problems related to the use of AI are one of the main challenges involved when using the technology. Respondents also pointed to the issue of liability (including legal liability), the inability of AI to make moral judgments regarding its actions, and the overestimated potential of AI as major challenges.

SAS experts emphasized that AI cannot learn creativity or innovation and lacks intuition or human understanding. Those human qualities allow us to distinguish between good and bad and read ambiguous signals. Without such skills, AI systems may be manipulated by someone intentionally providing false data and disrupting the cognitive process. In early 2017, the European Parliament adopted a resolution concerning legal liability for the operations of robots and artificial intelligence. MEPs called upon the European Commission to consider setting up an EU Agency for Robotics and Artificial Intelligence to support public authorities in the field of technology, ethics and the law.

We do indeed live in interesting times and can expect more changes to come in the near future, including regulations on AI. Hence the purpose of this insights publication is not to provide you with a comprehensive guide on digital transformation, but rather offer an open book where new themes are explored and fresh chapters added as the market evolves.



GETTING STARTED – CLEARING THE LEGAL HURDLES FOR YOUR TRANSFORMATION PROJECT

MARC ELSHOF, AMSTERDAM

To successfully implement and execute your digital transformation project, there are a number of legal challenges that you will need to address along your journey, including: legacy IT systems, contracting, data processing, cybersecurity, IP and regulation. Addressing these legal issues early on in the project can help avoid costly delays and prevent disruption of service to your customers.

Legacy IT systems

By definition, many digital transformation projects are designed to modernize legacy IT systems to better address the future needs of the company and its customers. This usually means procuring new hardware and software, which often consumes a significant part of the project budget. Usually digital transformation consists of combining the licensing of off-the-shelf software products with the development of bespoke software components.

Before embarking on a digital transformation project, it is important to review your existing license and maintenance contracts. Can the existing contracts be terminated and if so, what are the costs? Can you upgrade the existing license so that you may not need an entirely new product? Are there any exit-assistance arrangements in the contract?

It is also important to bear in mind that digital transformation products are often interconnected with other software and/or databases. Before embarking on your project, consider establishing an integration team to oversee the procurement, rollout, integration and of course the legal considerations at every stage of your planned transformation project.

Contracting with partners

If a digital transformation project is unsuccessful, the costly software you purchased is often of little or no use. Frequently, the various components of the project are split among multiple suppliers. This can give rise to a number of questions: Where does the company stand if one of these contracts (e.g. the development contract) fails, but the separately licensed standard software works properly? Are we obliged to continue using obsolete software? Are we allowed to continue using a particular piece of standard software if the development contract for the custom add-on is terminated?It is crucial to define at the outset what the impact will be on each contract if another contract is terminated.

There is often a high level of interconnectivity between software and database products, so it is crucial to ensure not only the interoperability of the technical components, but also the coordination and harmonization of the contractual framework. This means making clear contractual service level agreements, including the split of responsibility and liability without leaving gaps between those contracts. An overarching “digital integration” team, including a legal department representative, can be useful in overseeing and coordinating the various procurement activities within the project.

However, procuring standard software is not usually what causes the most headaches in legal departments. Rather, contracting for the development of bespoke software components usually carries the largest risk of failure.

Agile software development agreements are often set-up as service contracts and do not clearly stipulate the developer’s obligations, such as the deliverables,

timeframes, penalties, cooperation responsibilities and transfer of intellectual property rights. This approach can lead to significant delays or project failures with no enforceable options for the company. Therefore, development agreements should always be drafted with care and with a view to the specific situation and deliverables of the project.

Handling of data

A key component of many digital projects is the aggregation and combination of data. However, complex and divergent data protection regulations and data ownership issues may limit the company's right to perform these key functions. To successfully address the data processing challenge, you need a three-pronged approach:

- A clear understanding of relevant privacy and data protection frameworks
- An analysis of data streams and the legal framework
- The creation and subsequent implementation of legal, organizational and technical solutions (e.g. anonymization or pseudonymization).

With the implementation of the EU General Data Protection Regulation (GDPR), preparing for data breaches and how to respond to them will be a critical aspect of your digital transformation project. In chapter four, we look at the impact of GDPR in more detail, including the considerations for both EU and non-EU based businesses.

Cybersecurity

In today's economy, employees need instant access to data from different locations from multiple devices. Cloud-based solutions are increasingly used as a cost effective, safe and flexible form of data storage. In the next chapter we will take a closer look at data centers and cloud solutions, including the continued growth of the data center sector in Europe.

However, putting data online means a greater exposure to the risks of cyberattacks. These risks are significant and include potential damage to reputation, business interruption, litigation, loss of intellectual property and confidential information, as well as regulatory sanctions. Perhaps most importantly, since cyberattacks often target sensitive customer data, a security breach can damage - sometimes irreparably – customers' trust in your business.

To mitigate these cybersecurity risks, you need a proactive and integrated approach to prevent, prepare for, and respond to cyberattacks. This requires close collaboration across various disciplines within the company to understand, detect and respond to these advanced and evolving threats.

Intellectual property

Intellectual property (IP) is a key aspect of any digital transformation project. As we discuss in chapter eight, IP protection allows creators to benefit from their own work and owners to benefit from their investment in a creation. However, while IP law helps protect and promote originality, creativity and innovation, advancements in technology can facilitate the infringement of IP rights.

To begin with, you need to ensure that your company has the appropriate rights to use the software for the intended purposes. This may include arrangements on scaling licenses up and down.

Then, as part of your digital transformation project, you need to consider how best to protect your company's intellectual property. Digital technologies make it increasingly easy to share ideas and content, but it is not always clear where the intellectual property rights lie.

Intellectual property protection frameworks differ by jurisdiction and regulations are not always suitable for the digital world. This can lead to challenges for intellectual property rights management, in particular where technology or ideas are created in an open source environment or with input from various parties, and are commercialized at a later stage. In chapter eight, we explore how to respond and protect IP in the face of disruptive technologies.

Regulatory framework

In highly regulated areas such as banking, insurance, health care and public services, you need to closely monitor the applicable regulatory framework. This can be a challenge, as applicable rules change rapidly and are often scattered among different sources of law, both at a national and supranational level.

As new technologies emerge, regulatory frameworks evolve in order to address the new legal challenges they bring. Such regulations often seek to protect customers, who use those technologies, from potential threats. For example, the emergence of driverless cars poses a number of questions that lawmakers and regulators will have to answer. Who takes responsibility in case of a crash? Who is liable? The driver? The car manufacturer? The software developer?

As the legal framework evolves and new rules are put in place, you will need to continue to adapt your company's policies to stay current and compliant.

If your digital transformation strategy involves launching a new digital platform or technology, you should do a full risk assessment early on to identify and mitigate any potential threats or dangers that using the technology can bring to your customers. Such prudence will not only help you build and maintain trust with your customer base, it can also help you minimize additional regulatory burden once the product is launched.

In summary

Taking the time to consider and plan for these legal challenges early on in the project can help you avoid potential pitfalls and costly delays. To do this, it is important to assemble a digital integration team - comprising key individuals from across core disciplines, including legal, IT, risk management and procurement - to ensure your company is on the best possible footing before embarking on your digital transformation project.

DATA CENTERS – AT THE HEART OF THE EUROPEAN CLOUD AND CO-LOCATION MARKET

CHRISTOPH PAPENHEIM AND SVEN-OLIVER FRIEDRICH, FRANKFURT;
SHANE MERCER, TORONTO

Creating a data center is among the most common projects which companies undertake as part of their digital transformation strategies. Centralizing IT services into a state-of-the art data center or cloud solution offers a number of advantages, including cost savings, improved efficiency, reduced duplication and better IT security. For global businesses, by setting up regional data centers in strategic locations, companies can provide 24/7 IT support to their offices around the world – leading to better customer service.

As a result, Europe has seen rapid growth in the market of data center services, either in the form of data centers as a service (DCaaS) or Infrastructure as a service (IaaS). Frankfurt, London, Amsterdam and Paris are the most popular locations for data centers within Europe primarily due to their proximity to large financial markets. These locations also offer well developed infrastructure and direct access to leading internet exchanges, such as DE-CIX in Frankfurt, AMS-IX in Amsterdam, LINX in London and France-IX in Paris.

Build, outsource or buy?

When establishing a data center, there are three main strategies to choose from:

- **Build** your own data center
- **Outsource** to a traditional data center or cloud provider
- **Buy** an existing data center

The choice of strategy depends on the needs and competencies of your business. For example, a larger company might have the critical mass and IT know-how to operate its own data center economically, while a smaller business might be better off outsourcing. A company which is growing quickly may prefer the flexibility and scalability of a cloud-based solution. Certain companies, which hold very sensitive data on their customers, might prefer to operate a data center in-house so that they can directly control the location and processing of that data. Whatever strategy you choose, each has its own legal challenges, which you will need to address. These are examined in detail below.

Building a data center

Real estate

When thinking about building a data center, there are numerous considerations regarding location. Depending on the size and complexity of your business, you may consider leveraging space in existing premises to manage cost or reduce the complexity of introducing another property. There are many factors to consider when exploring your options, including cost, complexity, connectivity, power, jurisdiction, zoning, availability of talent, accessibility, stability, taxation, and outside risks or influences (for instance, risk of civil unrest, natural disaster).

If your business is located close to your data center, there may be opportunities to reduce some expenses such as connectivity, but you may find yourself paying a premium for space and utilities. On the other hand, locating your data center in a more remote location, you could save on these areas but increase your telecommunication or travel expenses. This can be a difficult decision with long-term impacts. Enlisting assistance to help with your assessment may prove beneficial, in particular when considering the potential zoning, tax, jurisdictional, and other legal implications.

Purchase and lease of equipment

Once you have decided where to locate your new data center, it is time to consider its build. Delivering a well-designed data center capability can be expensive and complex, involving numerous technologies to deliver robust security, flexible racking, redundant power (ups, generators), cooling and connectivity. When making the decision to purchase or lease the infrastructure required you should consider potential tax implications, potential changes to your requirements over time (due to evolving business needs or regulatory requirements) and the financial implications of each option. You may discover that aspects of your infrastructure are better aligned with one approach over another.

Security and privacy

The physical security of your data center is as important as the security of your systems. It is vital to clearly understand your legal and regulatory requirements, ensuring that you deliver capabilities to meet or exceed these requirements. Where appropriate, contractual agreements with third parties - such as maintenance providers or data center staff - should include appropriate clauses to address your responsibilities. The physical design of your space may also be influenced by these requirements, such as segmentation between areas within the data center, or the introduction of security systems and/or processes.

Staffing

When staffing your new data center you should consider a combination of internal staff and third party support. You will need to complete the appropriate background checks, put non-disclosure agreements in place, and ensure that everyone is operating under a set of policies clearly defining acceptable use. It's essential to ensure careful alignment of employment practices alongside local laws and the regulatory requirements specific to your business. When considering third party support, risk assessments should be completed and agreements should ensure adequate legal coverage that clearly define service levels, liability and other applicable legal considerations. These individuals may have access to some of your most sensitive digital assets and should be treated accordingly.

Outsourcing to a traditional data center or cloud provider

Data ownership

When a business is considering outsourcing custodianship over its data and systems, it is important to understand explicitly what access the provider will have to the information. In many outsourcing relationships, the provider may have no direct access to your systems and data. In other situations, the provider may be more directly responsible for the management of your systems, with access to the underlying information. In either case, it is important that you contractually reinforce your ownership and rights over your business data. Some cloud providers have established business models based on the monetization of information, so you need to ensure that no extended rights have been inadvertently granted to the provider for any other purposes.

Service Level Agreements

Depending on the outsourced provider, you may be in a position to negotiate service levels to meet your specific requirements, which typically comes at an increased expense. With other providers, service level agreements may not be negotiable as they are core to a provider's business model and shared by the entire customer base. With many providers, service levels are dependent on your understanding of the

platform's technical capabilities and whether you have designed your systems to deliver highly resilient services. In essence, if you do not setup your systems correctly according to the requirements, you void your warranty!

Data location

It is a common misconception that when a business outsources its datacenter to a "cloud" provider, its actual location is ambiguous. Not unlike a traditional data center provider, most cloud providers are able to explicitly detail where your information will be stored, or provide you with that direct control. When selecting a provider make sure to clearly understand how your systems and data are stored and what control you retain. When appropriate, you should also ensure that contractual restrictions are in place to ensure future changes on the provider's platforms do not negatively influence your business. Be careful to examine not only how production systems are stored, but also backup systems, including backed up data. These are commonly stored in separate physical locations, potentially in other countries.

Data protection and privacy

Regardless of the nature of your outsourcing arrangement, data protection and privacy is a shared responsibility between your business and the provider. By leveraging an outsourced provider, there is an opportunity to increase your security by leveraging capabilities the provider can deliver, but this will never absolve you from your responsibilities. Again, this is dependent on clearly understanding a provider's capability and designing your systems to take advantage of these. For instance, most providers today will encrypt your data while stored on their systems. However they could provide you the extended capability to encrypt your data using your own "keys". This extended capability could be the difference between meeting some regulatory requirements or not. You must ensure that perspective provider's capabilities align with your unique business requirements and that you take advantage of them.

In terms of data privacy, again, clearly understanding the nature of the relationship with a provider, and their access to your systems and data, is important to also understanding how your obligations extend to them. In terms of regulations such as GDPR, this understanding is critical. For instance, if your provider has access to your systems and the underlying data, they may be considered a data "processor". If they have no access, this may absolve them from these regulatory responsibilities. Any contractual agreements should factor in specific legal requirements related to data protection and privacy regulations.

Liability for service failures or security breaches

Service failures – worse yet – security breaches, are almost inevitable. Good planning and carefully selecting a provider who aligns with your requirements will reduce this risk and even mitigate the potential impact, but not eliminate it altogether. While negotiating with perspective providers, always ensure that you clearly define and understand limits of liability. You should obtain proof of insurance and update it regularly. With this understanding, you should also review your own business insurance to ensure adequate coverage.

Data portability and handover protocols

As with any business relationship, you should always have an exit strategy. This is no different with outsourced data centers or cloud providers. Your provider may be in possession of some of your most sensitive data, so you should ensure that you have contractually protected yourself in the event that the relationship breaks down, or you simply make the decision to move. Consider potential financial obligations,

time commitments and processes as these relate to transitioning your systems and data. Having these more difficult discussions up front, while the relationship is being established, and ensuring that they are documented contractually, can help to prevent a potentially sensitive situation in the future.

Buying a data center – M&A considerations

Asset or Share Deal

There are basically two ways of structuring a transaction: an asset deal or a share deal. In an asset deal, the purchaser acquires certain assets of a seller and assumes certain liabilities. In a share deal, the purchaser acquires a business via its shares or interests, comprising all its assets, liabilities, rights and obligations. While the choice of structure depends on the circumstances of the transaction, the decision is often driven by tax implications, complexity and the desire to avoid the assumption of certain liabilities. Data center transactions are typically structured as asset deals.

Preliminary Agreements

Preliminary agreements – such as non-disclosure agreements, letters of intent, memoranda of understanding, and term sheets - are entered into at an early stage in order to protect confidentiality and set out the key terms and timelines of the contemplated transaction. In addition, the purchaser may seek exclusivity for a certain period of time.

Due Diligence

To get a better understanding of the target business and identify any potential risks, a prudent purchaser will conduct due diligence, focusing on legal, financial, tax, environmental and commercial areas. In data center acquisitions, the focus of the legal due diligence will be on real estate, in particular compliance with public building law. It will also focus on contractual issues resulting from the target's relationships with its customers, suppliers and other business associates, as well as corporate, tax and financing issues. Due diligence should also examine compliance with data protection and security requirements.

Definitive Sale and Purchase Agreement

Once the parties have agreed on the legal and commercial terms of the transaction, they will enter into the definitive sale and purchase agreement. This contains such provisions as representations and warranties, indemnities, covenants and other obligations of the parties in connection with the sale. In some cases, the sale and purchase agreement may contain conditions, which must be fulfilled in order to close the transaction, such as governmental approvals (e.g. merger clearance), third party approvals (e.g. regarding the transfer of the contractual relationships), or waivers of change of control termination rights.

The legal remedy in case of a breach of the guarantees is damages. These are usually capped with a lower cap for the breach of operative guarantees (e.g. contracts, employees, assets) and a higher cap, typically amounting to the purchase price, for the breach of fundamental guarantees, (e.g. title to the assets or shares).

Tax considerations

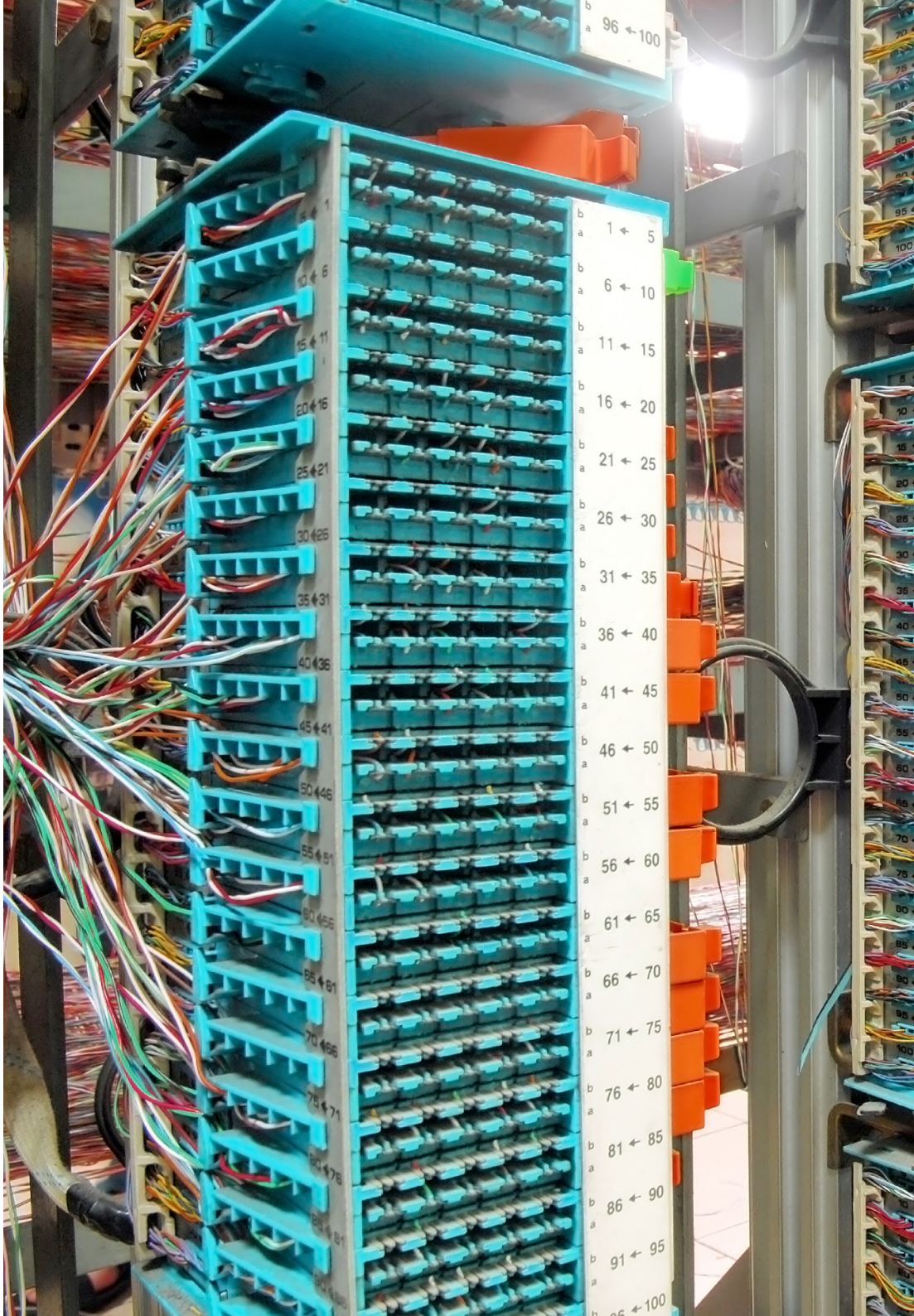
Tax structuring is a key consideration in an acquisition and a tax-efficient structure should be sought at the outset of the transaction. The transfer of real estate triggers real estate transfer tax. Share deals and asset deals are usually VAT-exempt, as long

as the latter relates to the sale of an entire business or a business unit, which is considered a going concern. Tax risks associated with the target and its business operations acquired are typically governed by the sale and purchase agreement in the form of specific indemnities and guarantees. In an asset deal, a prudent purchaser will exclude any types of tax liability attaching to the assets or the business from transferring and will seek indemnity from and against any tax liabilities.

Conclusion

Establishing a high quality data center – whether internally or outsourced – is a major investment and undertaking on behalf of your company. If done right, it can bring significant cost and efficiency benefits to your company, while ensuring consistent, stable and reliable service to your customers. On the other hand, if such a project goes wrong, it can be extremely expensive to your business and disruptive to your customers.

A successful data center project requires close collaboration between your IT, legal and risk management departments, as well as active input from your line departments as internal customers. There are multiple, IT, legal and risk management considerations which you need to take into account, and therefore we strongly recommend seeking legal and tax advice early on, and throughout the project.



ENGAGING WITH EVOLVING REGULATION – GDPR

VICTOR NAUMOV, ST. PETERSBURG

In today's convenience-based economy, more and more people are buying goods and services online. Every time you shop, you leave a digital footprint. Over time, these footprints accumulate in cyberspace and together, they can be used to establish your identity. In this context, the protection of personal data and privacy are integral guarantors of the protection of human rights in e-commerce.

Protecting personal data and the right to privacy

The main legislation governing data protection in the EU is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 General Data Protection Regulation (GDPR) which has applied across all EU Member States since May 25, 2018. The GDPR was adopted with the view of harmonizing data protection regulations across the EU. For any company involved in e-commerce, it is important to be familiar with these new obligations and to devote enough time to compliance.

According to the GDPR, personal data is understood as any information relating to an identifiable natural person (data subject). An identifiable natural person, or data subject, is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Does the GDPR reach beyond the EU?

In respect to e-commerce and personal data it is worth noting that GDPR outlines a set of progressive rules that consider specific aspects of personal data processing in the digital space. Article 3 specifies that the GPDR applies to the processing of personal data regardless of whether the processing takes place in the EU or not.

Beyond that, there are two situations in which the GDPR applies to processing by a controller or processor that is not based in the EU: first, if the controller or processor offers goods and services to individuals in the EU, and second, if it monitors individuals in the EU. Such entities must comply with the GDPR. For example, they will need to appoint a representative in the EU, who will represent the controller or processor with regard to their respective obligations under the GDPR.

These two cases of the extra-territorial effect of GDPR require further clarification. The controller or processor would be deemed as offering goods and services in the EU if it clearly intends to offer such services in one or more EU member states. Such an intention could be proved by the use of an EU-based language or currency on the e-commerce site, the possibility for EU-based customers to order goods and services, or the mentioning of customers or users who are based in the EU. Thus the accessibility of the controller's or processor's website, email address and other contact details in the EU alone are not sufficient to determine intent.

The definition of monitoring is also quite broad, but in the context of the GDPR, it could be interpreted as the use of various technical mechanisms to collect and analyze data to profile an individual. In light of the popularity of profiling, a large number of companies which do business online will thus fall within the scope of the GDPR.

Privacy and the impact on profiling

In order to recognize an activity as profiling three basic elements must be determined:

- It uses an automated form of processing;
- It includes the use of personal data;
- The aim of the activity is to evaluate certain personal aspects relating to a natural person, to analyze or predict aspects concerning that natural person's performance at work, health, personal preferences, interests, location or movements.

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or other significant effects concerning them. Individuals must also be informed about profiling activities and have the right not to be the subject of such activities.

Data portability

One more right of individuals that you should take into consideration is the right to data portability. It means that individuals have the right to receive their personal data that they previously provided in a commonly used and machine-readable format. However there is a limitation on this right, because it only applies if the processing of the personal data was based on consent or on a contract.

A compliance challenge

Data protection and privacy are among the most controversial and challenging issues of our time. For companies operating in the e-commerce sector – and indeed all companies operating in today's digital economy, compliance with the GDPR must be a top priority.

PERSONAL DATA PROTECTION IN RUSSIA

The regulation of personal data in Russia is similar to the GDPR in many aspects: Russian personal data legislation also applies to operators regardless of whether or not they have local representation in Russia if they have a website that targets a Russian audience. The 'localization amendment' is therefore rather impactful as it establishes an obligation on the localization of personal data of Russian citizens in Russia.

However Russian regulations use slightly different criteria for determining which foreign operators acting through a website comply with Russian personal data legislation. Foreign operators are determined as those who:

- Use a Russian-related domain name and/or a genuine Russian version of the website; or
- Include additional criteria which indicate "explicit evidence that the owner of the website intends to include the Russian market in its business strategy". This could be through the use of ruble payments, the delivery of goods to Russia, and/or the use of Russian advertising to lead to the website, etc.

CONSUMER PROTECTION AND ONLINE ADVERTISING

VICTOR NAUMOV AND YANA CHIRKO, ST. PETERSBURG; TÍMEA BANA AND TÜNDE GÖNCZÖL, BUDAPEST

The e-commerce industry is among the most dynamic sectors in today's economy, as the number of consumers purchasing goods and services over the Internet continues to skyrocket. While e-commerce offers customers many benefits – such as easy access, unlimited choice, competitive prices and convenient payment options – there are also risks, including payment fraud, misleading advertising and the misuse of personal data to name just a few. To mitigate these risks, a field of legislation has emerged to protect the rights of e-consumers.

Consumer protection

In today's global business environment, businesses should take into account the cross-border nature of e-commerce and consider the various regulations of the markets that they target. While this appears to be a daunting task, the key consumer rights and protection guarantees have already been harmonized through European Union Directives, and they are quite similar in countries outside the EU.

The Electronic Commerce Directive[7] directly regulates the e-commerce sector. In addition, consumer protection and consumers' rights are regulated by the EU's Consumer Rights Directive[8], the Unfair Commercial Practices Directive[9] and the Unfair Contract Terms Directive[10]. Most of the rules set out in these directives apply equally to offline and online transactions. Telecommunications companies must further comply with the rules of the Universal Service Directive[11] which includes certain user rights. Additionally, the European Commission is working on new rules which would further strengthen the protection of digital consumers.

1. Clear, transparent and easily accessible information

In terms of e-commerce, when a consumer is not able to see or test the goods, their right to information is vital. For this reason e-traders should disclose clear information to enable customers to make informed decisions regarding their transactions.

7 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)

8 DIRECTIVE 2011/83/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council

9 DIRECTIVE 2005/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')

10 COUNCIL DIRECTIVE 93/ 13/EEC of 5 April 1993 on unfair terms in consumer contracts

11 DIRECTIVE 2002/22/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) as amended by Directive 2009/136/EC

Businesses operating online must provide pre-contractual information to their customers. Pursuant to the Electronic Commerce Directive, online businesses must provide general information about the business, including the name of the company, its geographical location, as well as its contact details, including an email address for quick communication.

Additionally, businesses must provide details of the trade register, in which they are registered, along with their registration number. Where the operation of a company is subject to authorization, the details of the authority must be provided. With regards to regulated professions, the professional body, title, and Member State as well as the relevant professional rules should be available for review.

By virtue of the Consumer Rights Directive, businesses operating in the digital sphere are subject to further requirements. For instance, the principal features of the goods or services must be shown and prices should be transparent – including shipping fees, taxes and any other costs. If delivery fees cannot be calculated before concluding the contract, this should be mentioned to the customer. When relevant, the accepted payment methods must be specified along with the estimated deadline for delivery.

The Unfair Commercial Practices Directive (UCP Directive) sets out several additional requirements to ensure consumers receive complete and true information before purchasing. The most important requirement is to provide consumers with all the relevant information they need to make an informed purchase decision. This obligation also includes technical solutions on digital devices that make it possible for consumers to decide whether to use a digital service or not.

CASE STUDY: FINES IMPOSED ON APPLE IN HUNGARY

Apple introduced an innovation called WiFi assistant on its iPhones to detect the strength of WiFi signals used by iPhone users. If the WiFi assistant detects that the WiFi signal is not strong enough, it automatically switches the iPhone to the user's mobile network to get a seamless connection to the internet.

Users can switch off the WiFi assistant, however Apple did not provide specific information on this feature (apart from in the general terms and conditions), and users were not notified when the WiFi assistant switched their phone to the mobile network.

The Hungarian Competition Authority, which enforces the Hungarian legislation implementing the UCP Directive, found that Apple had omitted to provide important information to consumers when it: (i) did not provide sufficient information for consumers with regards to the WiFi assistant (most consumers were not even aware of its existence), and (ii) did not apply a solution which would have made it possible for consumers to decide whether they wanted to use the mobile network instead of the WiFi network (for example, a text notification with an option to accept or deny the switch).

Although the cost of switching to the mobile networks would not result in gains for Apple, the authority argued that this practice also benefitted Apple, as consumers attributed the seamless connection as a product feature of the iPhones. Therefore, the authority imposed fines of more than €300,000 on Apple.

Another important provision in the UCP Directive is that companies should outline the commercial intent behind their practices. For instance, advertising on social media platforms such as Instagram or Facebook must be indicated as such. Authorities are increasingly focused on social media "influencers" when enforcing the rules against unfair commercial practices. If their blogs or posts contain advertising, influencers must indicate this on the post.

Businesses must have a protocol for handling complaints which prospective customers can review before purchasing. Where relevant, the duration of the contract should be indicated as well as the conditions for termination. Furthermore, companies selling digital content should specify the relevant technical protection controls as well as the software/hardware which are compatible with their content.

Additionally, the directive prohibits the use of "pre-ticked boxes", which automatically add a product or service to the customer's shopping cart (for instance, the automatic addition of an insurance contract to the purchase of an airplane ticket).[12]

2. Clear and transparent terms

Businesses must comply with rules regarding the confirmation of the contract.[13] In accordance with the Directive on Unfair Terms in Consumer Contracts, contract terms should be communicated in plain and easily understood language. An "unfair" term is generally considered as one which creates an undue advantage for the seller over the buyer. Such terms are not binding for consumers. In the event that contract terms are found to be ambiguous, their interpretation will be in favor of the customer.

A company can't be held liable for a term that was negotiated with the buyer. However, if it claims that a seemingly standard term was negotiated, the burden of proof lies with the company.

3. Cancelling an online purchase

Businesses must be aware of the customer's right to cancel their online purchase, as set out in the Consumer Rights Directive. Customers have the right to terminate a contract with the seller within 14 days of the delivery of

12 DG JUSTICE GUIDANCE DOCUMENT concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council

13 https://europa.eu/youreurope/business/sell-abroad/on-line/index_en.htm#dop-consent-yes

the ordered good(s). Within this timeframe, the customer must notify the seller, which in turn must acknowledge the withdrawal request. This right entitles the consumer to a full refund (including shipping fees) within 14 days following his/her with-drawal request. Nevertheless, the customer bears the costs of returning the good(s) unless the seller has agreed to cover this expense or has omitted to specify otherwise.

Reimbursement must be made using the same payment means used for the initial purchase, unless the customer has agreed otherwise. However, in such cases, the buyer must not be subjected to additional fees. Additionally, companies are only expected to reimburse the costs associated with standard delivery and they may withhold payment until they receive the returned goods or proof of the return by the customer.

4. Delivery, cancellation and reimbursement

Under the EU Consumer Rights Directive,[14] companies must deliver ordered goods to their customers no later than 30 days following the purchase. This deadline can be extended if the consumer agrees. In the event that the seller is again unsuccessful at meeting this new deadline, the customer is fully entitled to cancel the contract and be reimbursed.

In case of goods for which the delivery date is essential (for instance, Christmas gifts), companies must grant the consumer the right to cancel the order and obtain reimbursement if the 30 day deadline is not met. The seller must reimburse the customer without undue delay. Furthermore, businesses are liable for any damaged or lost goods during the shipping period unless the customer has contracted their own carrier.

Secure payments

The digital economy provides consumers with a wide variety of online and offline payment options offered by different payment service providers, not limited solely to banks. In this regard, e-traders must ensure a minimum level of security and reliability of the payment systems used.

Not all transactions are protected equally (e.g. low value payments), so as to avoid disruption and because there are alternative authenticating mechanisms in place that are equally safe and secure. However, online traders planning to use a payment system provider should ensure that the payment system provider guarantees a sufficient level of security.

The aim of the first Payment Services Directive (PSD1), adopted in 2007, was to ensure safer and more innovative payment services across the EU. Because of subsequent technological advancements and a vast increase in online payment options, PSD2 was implemented at the start of 2018. The Directive guarantees a high level of security by ensuring that all payment service providers - including banks, payment institutions or third party providers (TPPs) - must prove that they have the appropriate security measures in place.

14 https://europa.eu/youreurope/business/sell-abroad/on-line/index_en.htm#dop-consent-yes

Payment service providers must assess the operational and security risks at stake, and any mitigation measures, on an annual basis. New strict security requirements for the initiation and processing of electronic payments reduce the risk of fraud and protect the confidentiality of users' financial data.

Strong customer authentication (SCA) provides an additional layer of security for consumers. SCA validates the user's identity when initiating a payment, by using two or more elements categorized as knowledge (e.g. PIN or password), possession (e.g. card), and inherence (e.g. fingerprints or voice recognition). As these elements are independent, the breach of one does not compromise the others.

Managing and resolving disputes

Effective protection of consumer's rights also implies the implementation of fair, effective, and transparent dispute resolution systems. Generally, consumers have the right to choose the trial court in case of a dispute. This means the consumer may file a claim at the court located in his/her jurisdiction of residence, or to the court of the state in which the e-trader is domiciled. This could lead to court proceedings being initiated by consumers across multiple states, which in turn could result in significant expenses for the e-trader.

Considering the global nature of e-commerce and different jurisdictions of the parties, it is important for businesses to develop alternative out-of-court dispute resolution mechanisms, which enable consumers and traders to resolve their disputes faster, easier and less expensively. Subject to applicable laws, the use of such mechanisms should not prevent consumers from applying to the competent authorities in administrative and judicial order.

Advertising

Nowadays blogs and social networks can be as effective in promotion, as TV and radio were in the past. The rise of social networking websites and blogs offers new ways to attract consumers to the brand. Consequently the online advertising sector is faced with legal challenges on a regular basis.

Misleading and false advertisements are probably the main legal issue that needs to be solved in the era of quick decision-making and purchasing. Photo retouching, misleading health claims, advertising of low-quality products and covert advertising are among the most common complaints.

Last but not least, the incredible number of profiles on the internet adds further complexity in getting to the bottom of misleading and false advertising. To combat this issue, many websites are developing terms of use or other instruments that are binding on website members. For example, Instagram now obliges bloggers to mark promotional posts with special tags and imposes fines for failure to do so.

As the regulation of the advertising sector is rapidly developing, participants must be agile in order to comply with Internet best practices and keep up to date with the changing legal environment.

Online contests

Some posts on social media platforms, which invite digital consumers to "like and win", could be defined as contests or lotteries, which are regulated both by legislation and the platform's terms of use. To ensure their promotion is not classified as an illegal lottery, marketers must comply with such regulations, including the obligation of mandatory disclosure of information about sponsors.

Advertising to children

Limited legal capacity makes children more vulnerable to advertising. For this reason governments of almost all countries specify additional requirements for information which is sensitive for children. For example, the GDPR requires the receipt of parental consent before collecting the personal data of children under the age of 16 (however, local legislation can differ from this rule and decrease the age limit to 13). Moreover, all online advertisements should be categorized and marked with a special rating. Special attention should be given to products that must not be marketed to minors - in these cases advertisers must apply a special tag in order to verify the age if the website user. In the case of advertising that targets children, such advertising must not include a direct incitement to children to buy the advertised products or indeed to persuade their parents or other adults to buy the advertised products for them. Such advertising is regarded as being unfair under the rules of the UCP Directive.

Direct marketing

Direct marketing - approaching potential clients via e-mail, messenger, door-to-door etc. - is the most vulnerable type of advertising. The obligation to comply with the GDPR places a significant burden on the advertiser. For example, organizations need to disclose what data is being collected, as well as where it is being transferred and stored; and users need to be offered a way of opting out.

The obligation to use direct marketing only with the user's "opt-in" permission makes this type of marketing unfavorable from the legal point of view.
In addition, the user should be informed about the way his or her data is transmitted, including cookies, which are in some cases the main source for marketing campaigns. The principle of informed consent requires websites to disclose the purposes of data collection and to inform the users, which means that they have the right to refuse privacy and cookie policies. The scope of these requirements will probably remove some of the more targeted advertising that occurs.

Metatags and search engines

When customers are searching the market for a product, they will usually use search engines such as Google, Yahoo, Bing, etc., which sort the results of each search on the basis of metatags that are embedded in a website's HTML code. Metatags are used to describe the website, however they sometimes contain other content, for example trademarks of famous competitors, to attract traffic. In such cases, the trademarks in the metatags can qualify as infringement and may lead to legal action.

UGC

User-generated content, or UGC, may hide content-related infringements and right violations. When does a brand have the right to publish and use a blogger's photo of the brand's product? Is the user liable for a negative review and if so, when? Should social media platforms moderate user-generated content? These questions have different answers depending on the rules of the website platform and the legislation of the country.

Steps protecting consumers continue to evolve

Increasing consumer protection for online transactions remains a priority for the European Commission. It has proposed a Directive relating to contracts for the supply of digital content.[15] A major innovation under the Digital Content Directive will be the granting of rights to consumers relating to contracts in which they've exchanged personal data for digital content. This is in contrast with the current regime, which only protects consumers that have paid a price to access such content. However, in the absence of a commercial use of the personal data by businesses, the Directive won't apply.

Two forms of remedy can be granted under the forthcoming directive:

- "Remedies for failure to supply": If purchased digital content is not provided successfully on the first try, a second attempt will be permitted, but a second failure warrants a right for the consumer to terminate the contract.

- "Remedies for lack of conformity": If content is supplied but does not meet the required legal standards or those agreed to with the consumer, the consumer will have the right to terminate the arrangement, to request a reduction in price or to request a repair of the defective digital product.

Consumers will also have the right to terminate long-term contracts in the event that companies make significant modifications to the content that they are providing.[16] Finally, the digital content supplier can be held liable for a minimum of two years following the conclusion of their contract with the consumer.

Keeping up with consumer protection legislation is very much in the interest of online businesses. Compliance will not only help you avoid fines or penalties, but more importantly it will enable you to protect client relationships and your brand. When an online review can make or break your business, building trust and treating customers with respect are keys to success.

15 Document 8672/15

16 Council of the European Union, Brussels, 1 June 2017 (OR. en), 9901/17

IDENTIFYING AND CONTRACTING WITH DIGITAL CONSUMERS

VICTOR NAUMOV AND GEORGY PCHELINTSEV, ST. PETERSBURG

In chapter four, we focused on the new GDPR legislation and its impact on the digital consumer and the wider e-commerce industry. Here we will spend some time focusing on the importance of electronic identification, as well as the evolution of e-contracts, both of which are essential to the smooth running of the digital marketplace.

Electronic identification – legal requirements

Although the remote identification of customers is important for any type of e-commerce business, some market players are subject to specific legal requirements relating to electronic identification. In particular, most countries require specific customer due diligence from financial institutions (banks, money transmitters, insurance companies, etc.). Subject to certain exceptions, these institutions must identify their customers prior to establishing business relationships with them.

Through these requirements, national legislators are in line with the international standards promoted by the Financial Action Task Force (FATF)[17] and the general legal framework adopted within the EU[18]. Thus, when structuring remote identification schemes, financial institutions have to assess not only the commercial effectiveness of the respective schemes, but also their compliance to applicable legal requirements.

Commonly adopted approaches to e-identification

As a general rule, the level of customer due diligence depends on the level of risk of a particular transaction. Nevertheless, according to the commonly adopted approach, verification of the customer's identity must be conducted on the basis of documents, data or information obtained from reliable and independent sources.

Under such circumstances, most jurisdictions do not consider popular mechanisms of electronic identification (e.g., obtaining a scan of the customer's ID) as sufficient for the purposes of anti-money laundering due diligence. In the absence of a trusted third party, such approaches do not ensure the reliability of the data provided by the customer. Accordingly, any remote identification scheme must be carefully analyzed prior to being implemented.

The benefits of harmonization

The EU is already moving towards the harmonization of regulation for electronic identification within the Single Market. In particular, the European Commission has introduced Regulations on electronic identification (eIDAS)[19] creating a legal framework for cross-border recognition of electronic identification for public and trust services across the EU. Electronic IDs issued in

17 FATF (2012-2017), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France.

18 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73–117.

19 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.

one EU country must be recognized in all others, provided they meet the regulation's requirements and have been reported to the Commission.

Additionally, this document sets forth a common legal framework for qualified and non-qualified trust services including the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, and certificates related to those services. Therefore, the eIDAS framework is one of the cornerstones of the European Single Market covering all elements of electronic identification and authentication.

The European Commission is particularly focused on FinTech trends and on enabling banks to identify customers digitally in the future. At the same time, it wants to ensure that modern tools for remote identification are and secure, do not pose new risks for consumers or systems, and comply with EU data protection laws.

In order to define methods of remote identification that meet these requirements, at the end of 2017 the Commission created an expert group for electronic identification and remote KYC processes.[20] The group is tasked with exploring issues relating to the use of remote identification schemes and whether or not they are notified under eIDAS. It is also looking into other innovative digital processes to comply with anti-money laundering rules. Where appropriate, the group will assist the Commission to prepare guidelines relating to digital identification.

The evolution of e-contracts

The concept of e-contracts is of paramount importance in driving and managing business in the digitally driven world of today. While e-contracts emerged in the 1980s, the widespread growth of the e-commerce sector began in the early 1990s. In response to this rapid growth, the European Union adopted the EU E-commerce Directive in 2000 to provide a legal framework to regulate the sector. The purpose of the Directive was to harmonize and clarify the rules applicable to internet business across the EU and safeguard consumer interests.

The current digital transformation - which is driven by more developed, more complex and wider reaching information technologies - represents a new legal challenge to both market participants and regulators. Therefore the EU is considering two special legislative proposals: a directive on contracts for online and distant sales of goods, and a directive on contracts for the supply of digital content. Both directives are presently at an advanced stage of consideration.

Legislating for the key issues

Historically, the key issues to be solved in relation to e-contracts were: identifying the contacting parties, proving a meeting of minds concerning a certain set of terms, and validating electronic signatures or other forms of acceptance. These have been settled with the development of both business and court practices.

In effort to harmonize the rules in this area, the EU recently adopted the Directive on Identification and Trust Services which took effect in July 2016. The Directive provides for three types of electronic signatures: basic, advanced and qualified electronic signatures, as well as electronic seals for legal entities.

Which laws apply?

Another major legal complication, which is inherent to Internet business, is determining what laws are applicable to a particular transaction and jurisdiction. Although this problem may be less acute within the EU than in other parts of the world due to the harmonization of legislation across member states, discrepancies between the laws of member states still exist, not to mention the lack of uniformity of the laws of other countries.

This complication requires e-businesses to pay special attention not only to the content of their website(s) or terms of sale and services, but also to the ways in which they advertise their business and organize their contracting infrastructure.

Next generation challenges and trends

With the digital transformation age, traditional e-commerce contract law is being challenged once again. Technologies such as SaaS, IoT, big data, cloud, AI, blockchain, augmented reality, and others are transforming both business and legal practice and require regulations to be adopted and adapted across a wide range of issues.

Not only is an e-contract different from the contract of a traditional business, but it could also be that a product or service that exists only in digital form, or indeed in blockchain, could have a contract performed and concluded without any human intervention. New forms of interaction such as Machine2Machine or Machine2Business were previously unheard of.

The latest trend of tokenizing assets and liabilities creates enormous opportunities to selling almost anything in digital form. However the creation and completion of digital contracts through automation requires more complex and instant document turnover involving advanced means of identification and signing, for example using smart phones and other devices.

Furthermore the automation of contracts brings to light the question of cybersecurity, adding a new dimension to such issues as contact interpretation and invalidity.

---

20 European Commission Decision of 14.12.2017 setting up the Commission expert group on electronic identification and remote Know- Your-Customer processes.

ECOMMERCE, THE EVOLUTION OF FINTECH AND THE GROWTH OF CRYPTOCURRENCIES

MATTHIAS EGGERT, MUNICH; NATALIA SELYAKOVA, KYIV

In the previous chapters, we looked at the growth of the digital marketplace and the challenges which this rapid growth has meant in terms of regulating e-commerce and protecting the digital consumer. Here we focus on the evolution of technology in the financial services sector and the legal challenges as governments grapple with digital developments in key market segments and the innovation of cryptocurrencies.

What is FinTech?

FinTech describes technology-based solutions to enable new, or facilitate existing, financial services. FinTech sits at the crossroads between heavily regulated financial services and digital innovation, and has resulted in new products and new business models coming to the market. Market participants include both startups as well as traditional and established market leaders.

Newly founded businesses may offer technology-based solutions or intermediary functions in the form of, for example an electronic platform or, they could simply offer financing. Mobile applications, data analytics, artificial intelligence, cloud computing, distributed ledger technology – all of these new technologies create opportunities for FinTech solutions.

The core segments in the FinTech sector include payment services, financing services, investment services and advisory and intermediary services. Each of these segments offers varied and evolving options for the digital consumer.

Development and growth

Founding activity for new FinTechs has been strong over the last few years. While some market commentators note that there has been a shift from B2C to B2B business models, others report that there is an even distribution. Recent FinTech investment and M&A activity in Europe has remained strong over the last decade, with spikes in both 2014 and 2015 followed by a low in 2016. Market reports indicate an increasing participation of established corporations in M&A activity.

Up to now, London has been the leading European center for FinTech based on reported investment and M&A activity in the sector, with France and Germany catching up. In a number of European countries, incubators have been established to foster the development of FinTech start-ups as well as facilitate co-operation between FinTechs and traditional market participants. While in the UK and France, such initiatives are centered in London and Paris, respectively, FinTech hubs have developed in a number of cities in Germany, namely Berlin, Munich, Frankfurt, Hamburg, Stuttgart and Cologne.

Future growth and regulation

During most of the current decade, European institutions have been looking at regulating individual elements of the FinTech industry. For example, the European Commission has been reviewing the area of crowdfunding, publishing a report in May 2016. The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) have been reviewing developments

in the automation of financial advice, also publishing a report in 2016. ESMA has analyzed the risks and benefits of distributed ledger technology applied to securities markets, publishing a report in February 2017.

More recently, European institutions have been taking a more holistic approach. In November 2016, the European Commission set up an internal task force on financial technology and conducted a public consultation on the role of FinTech. It published a summary of responses in 2017. The European Commission also issued a Consumer Financial Services Action Plan in March 2017.

Also in 2017, the EBA undertook a mapping exercise of FinTech businesses existing in the European Union as well as activities and business models of such businesses. The results were set out in EBA's discussion paper in August 2017, where the EBA stated: "The current growth of FinTech may also alter the scope and objectives of regulatory and supervisory authorities as they adjust to market developments and may result in the revision of risk appetite. It comes as little surprise therefore that public authorities in the EU and beyond have started to investigate the impact that FinTech is having on the financial system, and on the regulation and supervision thereof."

How is this progressing in Europe?

The Payment Services Directive (PSD) and the Payment Services Directive 2 (PSD2) are the European regulations, which have been triggered by developments in the FinTech industry so far. Other than that, it appears that European institutions continue to be in the fact-finding phase. At this stage, it appears likely that amendments will be made to existing legislation.

However, it is not yet clear as to whether entirely new pieces of legislation will be introduced. One potential field for new legislation is distributed ledger technology. Another concept that appeared in the EBA discussion paper in August 2017, and which might make its way into European legislation, is the concept of regulatory 'sandboxes', which enable validation and testing of business models for a limited period with the support of the relevant authority.

What this means for businesses and digital consumers in Europe

While FinTech businesses operating in Europe need to comply with generally applicable laws and regulations, with the exception of the PSD and PSD2, there is little specific FinTech regulation at this stage. In particular, the following areas as well as their impact on both businesses and consumers need to be considered:

Licensing

FinTechs need to determine at an early stage whether their business model requires a license. A significant number of the business models pursued by FinTechs are subject to licensing requirements. In a number of (but not necessarily all) EU member states, operating a business without the required license is subject to administrative fines. It may even constitute a criminal offence which could result in imprisonment and/or being banned from acting as director of a company delivering banking or financial services.

By way of example, the following activities are subject to licensing requirements in some (but not necessarily all) EU member states:

- B2C lending
- B2B lending
- Factoring
- Reverse factoring
- Loan brokerage
- Taking of deposits from the public
- Brokerage of financial instruments
- Asset management
- Payment services
- Collection services

When determining whether a license is required, FinTechs should consider the rules in the jurisdictions of each of the parties to the intended transactions. For example, in the case of lending, they need to consider the jurisdiction of both the lender and the borrower(s). In the case of factoring, it is mainly the jurisdiction of the seller(s) and the relevant purchaser(s) of receivables. In addition, the location of the debtors may also be relevant.

De minimis exemptions from licensing requirements are sometimes available. However, it should not be assumed that if a small number of transactions are intended, or if transactions are intended to have a low value, that an exemption will automatically be available. For example, as regards lending, the granting of the first loan may require a banking license depending on the circumstances.

If a license is required, requirements for obtaining the license generally involve the following:

- **Organizational form and minimum equity:** Some banking and financial services may only be provided by an entity established in a certain legal form and with a minimum statutory capital that could be higher than for the relevant organizational form under generally applicable company law.
- **Proof of reliability:** Some banking and financial services may only be provided if the entity's management includes one or more persons that can demonstrate thorough professional experience in the relevant field.
- **Business plan:** A number of banking and financial services require a sustainable business plan to be provided as a prerequisite for a license.
- **Regulatory capital:** A number of banking and financial services may be provided only subject to availability of regulatory equity capital which depends on the volume of the business in question (and is not correlated to the requirement for minimum statutory equity capital as set out above).

More recently, FinTechs have increasingly managed to equip themselves with sufficient means and personal resources to obtain required licenses. For example, some FinTechs are reported to have obtained full banking licenses in the UK and Germany. Alternatively, FinTechs may pursue one or both of the following strategies. First, they could modify their activities so that no license is required. Alternatively, or in tandem, they could cooperate with a licensed partner so that the activities requiring a license are performed by the licensed partner.

Fundraising

Fundraising from the public may in itself be subject to licensing and/or registration requirements. Moreover, a prospectus may be required. However, for seed and early stage funding, de minimis exemptions may be available.

Protecting digital consumers

As noted in chapter four, the GDPR entered into force on 25 May 2018. FinTechs operating B2C models will generally need to comply with GDPR, while FinTechs operating B2B models are only subject to the regulation if the businesses to which they offer services include natural persons.

Non-compliance with requirements of GDPR may result in administrative fines of up to 4% of the total worldwide annual turnover. Additional penalties may apply under legislation of EU Member States, which further enhance the GDPR.

Conclusion

As these new technology-based solutions are tested over time, they might themselves become (and in some cases even replace) traditional regulated financial services. In the meantime, the strong tendency in the financial sector for digital transformation and innovation brings with it a range of new legal risks to be assessed and addressed.

SPOTLIGHT: THE EVOLUTION OF CRYPTOCURRENCIES

As FinTech innovations continue to grow and evolve they continue to change the face of companies. An important FinTech innovation, and perhaps one of the most often debated, is blockchain. Using distributed ledger technologies, blockchain is a decentralized technology that enables both businesses and digital consumers to settle contracts and transactions quickly and efficiently, removing the need for intermediaries.

Since cryptocurrencies began to emerge in 2009, leveraging disruptive blockchain technology, the most widely known and used cryptocurrency in the world has been Bitcoin. Fueling the growth of cryptocurrencies like Bitcoin is the desire to increase efficiency and eliminate unnecessary costs, while having a currency that is readily adoptable across a variety of markets. A number of leading financial institutions have demonstrated an interest and willingness to experiment with blockchain technologies. Indeed some now have their own cryptocurrencies under development such as Citibank (Citicoin); UBS, Deutsche Bank, Santander and Bank of New York Mellon (Utility Settlement Coin); Goldman Sachs (SETLcoin); the Bank of England (RsCoin); and the Peoples Bank of China (RMBCoin).

While the appeal of cryptocurrencies continues to grow, in part fueled by their decentralization and anonymity, they have yet to be recognized by any state government as a preferred mode of currency. However many countries have been taking a strong interest in regulating

cryptocurrencies, especially as more and more mainstream companies, across a variety of industries, explore the benefit of cryptocurrencies and blockchain technologies. ECB president Mario Draghi recently indicated that the ECB does not have the authority to regulate cryptocurrencies, yet we have seen a number of European countries considering regulation of their own.

In Germany, the appropriate regulatory body is the German Federal Financial Supervisory Authority (BaFin). BaFin has qualified Bitcoin in particular and accordingly other comparable cryptocurrencies in general, as financial instruments in the form of accounting units. Considered intangible assets by the German Ministry of Finance, cryptocurrencies are generally subject to income tax and VAT – depending on the individual design of the ICO and the cryptocurrency.

While the stance of BaFin is officially neutral, in April 2017, it prohibited Onecoin (Dubai) and OneLife Network (Belize) from offering a publically accessible system on the internet for conducting transactions with OneCoins. BaFin's reasoning was that it considered the OneCoin business to be proprietary trading in terms of the German Banking Act (KWG) which would have required a license pursuant to s32 of KWG.

ENFORCING IP RIGHTS IN A DIGITAL ENVIRONMENT

DR. STEFAN DITTMER, BERLIN; DR. CONSTANTIN REHAAG, FRANKFURT;
AND HANNA KAROLINE HEIDKAMP, FRANKFURT

As noted in the second chapter, Intellectual Property (IP) is a key aspect of any digital transformation project. IP rights allow creators to benefit from their own scientific, technological, literary, or artistic work, and owners to benefit from their investment in a creation. Intellectual property law plays a very important role, not just in protecting companies from the misuse of their know-how, but in promoting originality, creativity and innovation within our society.

While advanced and disruptive technologies offer exciting possibilities for the creation of new works, ironically they also facilitate the infringement of IP rights. In the sharing economy, it is often difficult to protect content from being shared or to prove when an infringement has taken place.

Awareness of intellectual property rights and how to protect and commercialize them has become essential in today's digital environment. So any digital transformation project needs to take into consideration how to protect your own IP rights, while also making sure that you do not infringe on the rights of others.

Categories of intellectual property rights

When planning your digital transformation, you will need to keep in mind the five categories of intellectual property rights, as defined by the World Intellectual Property Organization (WIPO):

Copyright and related rights: Copyright laws grant authors, artists and other creators protection for their literary and artistic creations, in particular for the form of expression.

Patents: A patent is an exclusive right granted by a patent office for an invention – a product or process that provides a new way of doing something, or that offers a new technical solution to a problem. It provides owners with protection for their inventions for a limited period of time, generally 20 years.

Trademarks: A trademark is a distinctive sign that identifies certain goods or services produced or provided by an individual or a company. It may be one or a combination of words, letters and numerals. It may also consist of drawings, symbols or three-dimensional signs, such as the shape and packaging of goods.

Industrial design: An industrial design refers to the ornamental or aesthetic aspects of an article and is applied to a wide variety of industrial products and handcrafts including fashion items.

Geographical indication: A geographical indication is a sign used on goods that have a specific geographical origin and possess qualities or a reputation due to that place of origin. Most commonly, a geographical indication consists of the name of the place of origin of the goods. It is widely used for agricultural products, but can also be used to protect products that unique due to specific local skills and traditions.

Although not mentioned in that WIPO enumeration, trade secrets play an increasingly critical role in innovation and the digital and data economy. In the absence of specific rights protecting the ownership of data which is not part of a database protected by copyright, trade secrets protection is often the only way

to retain and commercialize the value of data. An area where the importance of trade secrets is obvious is encryption technology

What are the IP challenges in a digital world?

As noted above, advancements in technology can facilitate piracy, counterfeiting and other IP infringements. At the same time, as digital consumers, we are faced with the phenomena of user-created content online, mashups and access to digital culture. So how can we be best prepared to respond to the challenges of digital transformation from an IP perspective?

Firstly let's look at the challenges of piracy and the emergence of disruptive technologies. Infringements of IP rights occur when someone manufactures, sells or distributes protected items without the right holder's authorization. In addition to this measurable loss, intellectual property rights infringements have more severe impacts on the economy in the long run. These include adverse social and economic effects such as loss of jobs and reduced incentives for creativity and innovation.

In the digital age, the issue of piracy and counterfeiting is particularly important. Unauthorized data sharing, integration, utilization and public disclosure are the biggest areas of concern. The continuing development of technology and the global expansion of the Internet have made it easier to obtain information about products, including high-tech goods, like pharmaceuticals, computer chips, software etc.

What's more, new manufacturing technologies such as 3D-printing make the production of pirated goods easier than ever. These recent trends come on top of "classic" counterfeiting and product piracy practices which have not lost relevance, and which, according to Europol, make up to five percent or €85 billion of all imports into the EU.

The internet's anonymity and lack of borders create an ideal environment for IP infringement. This is particularly true of the Darknet, a network that can be accessed through special software or communication protocols, which has become a hotbed for shady activity. Worryingly, more and more infringements are committed by cross-border criminal groups, which use the internet for organization, distribution, customer care and online payment, thus making it extraordinarily difficult for rights owners to enforce their rights by turning to courts of law and initiating civil proceedings against infringers.

While trade has become more international, and regional economic integration has led to the dismantling of borders in order to ease trade flow, efforts to combat piracy and counterfeiting have been lagging behind.

The digital environment also presents legislative challenges in terms of IP enforcement, which have not yet been tackled in any global agreements. Infringements carried out over the internet pose very specific obstacles to effective enforcement such as the identification of the infringer, liability of service providers, enforcement of IP rights, the treatment of online rights protected abroad, and the question of court jurisdiction.

How do we respond to protect our IP?

No single actor - be it the government, business or consumer - and certainly no party acting only at a national level can win the fight against IP infringements on their own. In a globalized business environment, international cooperation is the key to protecting IP rights, with official players taking a vital role in the battle against piracy and counterfeiting including Europol, WIPO and BASCAP. In addition to these "official" players, many IP rights holders are approaching online marketplaces – which could be (unintentionally) used to sell pirated goods – to raise awareness of IP infringements and seek their collaboration in fighting IP crime. Many companies are developing security strategies that employ a suite of technologies and capabilities to combat intellectual property infringements:

- **Watermarking:** The biggest benefit of watermarking is its potential for deterring unauthorized uses of content. It is a piece of information added to content that establishes the identity and ownership of an individual piece of content.
- **Fingerprinting:** A digital fingerprint is an exclusive pattern of ones and zeros that identifies content.
- **Digital rights management (DRM) technologies:** Digital rights management technologies protect copyrights by identifying content, controlling access, protecting the integrity of the work and ensuring payment for access. Another way to protect digital content is through Technical Protection Measures (TPM).

Access to digital content

Despite IP challenges, digital disruption also has a positive impact by offering ever growing access to digital culture and user created content online.

The EU Commission recently announced initiatives to strike a better balance between rewarding the creator's investment and promoting the widest possible access to goods and services protected by IP rights.

For example, it is introducing legislation to allow the digitization and online availability of orphan works, for which the copyright holders are not known or cannot be located to obtain copyright permissions. It is also seeking to simplify the collective management of copyright in the EU, and create a European copyright code and "unitary" copyright title. The EU is also continuing to fight to reduce the sale of counterfeit goods over the internet.

The way forward

In today's digital world, the dizzying number of opportunities to distribute goods provides new and ever increasing challenges. The international IP legal framework provides consistent and flexible protection for owners of both traditional products and digital content. However, neither legal frameworks nor regulatory intervention will ever keep pace with the speed of technological advancement or with the pirates who seek to circumvent that technology.

When planning your digital transformation, it is important to bear in mind that IP protection is essential to encourage innovation and to preserve the diversity of creation, and to build such protective measures into your strategy. However, since the very concept of protecting intellectual property has come under attack in the sharing economy, policymakers and industry players alike should also think about new and innovative ways of remunerating creators in a way that discourages the infringement of rights.

BIG DATA AND EU COMPETITION LAW

JAMES VENIT, BRUSSELS

Before embarking on your digital transformation project, it is important to understand the state of play in the EU concerning the application of antitrust rules to big data, digital networks and digital platforms. To date, the European Commission has dealt with big data primarily in the context of two mergers – Facebook/WhatsApp (2014) and Microsoft Linked-In (2016). In both cases, despite all the hoopla, the Commission looked but did not touch.

In parallel, Germany and France have been active – indeed more active than the Commission – in identifying the analytic framework applicable to digital platforms and networks, including the possible link between data and market power. The French Competition Authority has brought two rather conventional dominance cases involving data, but not big data, while the German Federal Cartel office has brought a far less conventional case alleging that Facebook may have abused its dominant position by not complying with German data protection legislation.

The EU merger cases

Facebook/WhatsApp

The Commission examined three markets – (i) consumer communications services (ii) social networking services; (iii) on-line advertising services. There was a horizontal overlap for consumer communications services in which the merged entity would have a 30-40% share.

The Commission identified a number of factors that mitigated any negative network effects of the Facebook/WhatsApp merger, including (i) that consumer communications were a fast-moving sector with low switching costs and barriers to entry; (ii) the prevalence of multi-homing; i.e., the use of multiple communications apps by a single customer; (iii) the absence of customer lock-in since the parties did not control any essential parts of the network or any mobile operating system; and (iv) the absence of any status quo bias, since neither Facebook Messenger nor WhatsApp were pre-installed on a large base of handsets.

The Commission concluded that the merger was unlikely to strengthen network effects because integration between WhatsApp and Facebook posed technical difficulties (e.g. difficulties in matching user IDs and engineering hurdles to cross-platform communications). Even if some integration of WhatsApp with Facebook took place, it would be mitigated by the fact that there was already a significant overlap between the two networks.

The Commission also examined WhatsApp as a potential source of user data that had value for advertising purposes and the possibility that the merger would strengthen Facebook's online advertising position. Here it concluded that, aside from privacy issues and the risk that customers might switch to less intrusive communications apps, there would remain sufficient post-merger competition in online advertising services from rivals such as Google, Apple, Amazon, eBay, Microsoft, AOL, Yahoo, Twitter, LinkedIn, Adobe and Yelp even if the merged entity were to start collecting and using data from WhatsApp users. Together Facebook and WhatsApp accounted for only about 7.5% of data collected across the web, compared to 33% for Google and nearly 69% for all others.

Although the merger was strongly opposed by telecoms, which lose revenues to instant messaging, the market survey did not support the telecom's theories of harm.

In May 2017, the Commission imposed a fine of €110 million on Facebook for providing misleading information during the merger investigation. Facebook had told the Commission that it would be unable to establish reliable automated data matching with WhatsApp's user accounts, but in August 2016, WhatsApp announced the possible linking of WhatsApp user phone numbers with Facebook user identities. In Germany, the Hamburg Data Protection Agency said it would prevent WhatsApp from transmitting its user data to Facebook. The Commission's concern in this second case was purely procedural (provision of misleading information) and its decision to fine Facebook for providing misleading information did affect its conclusions concerning the absence of adverse effects on the market for consumer communication services.

Microsoft/Linked In

In Microsoft/LinkedIn, the Commission's review focused on three markets: (i) professional social network services; (ii) customer relationship management software solutions; and (iii) on-line advertising services.

The Commission had no concerns in respect of the horizontal overlap for online non-search advertising services, given the limited overlap and the parties' low combined shares of less than 10%. It did not raise concerns about the combination of the databases (consisting of job, career history, professional connections, email or other contacts, search behavior, etc.), but it did identify two potential antitrust concerns: (i) the creation or strengthening of market power for the provision of this data to advertisers; and (ii) the creation of barriers to entry/expansion impacting competitors which need data to be able to compete on the market for the supply of such data to advertisers.

The Commission noted any sharing of data between the parties might be limited or precluded by data protection rules. It also noted that, with limited exceptions, Microsoft and LinkedIn do not make their data available to third parties for advertising purposes and that the combination of their databases would not create barriers to entry because there are a large amount of internet user data valuable for advertising purposes that are outside Microsoft's control.

In relation to potential vertical issues, the Commission required Microsoft to enter into commitments to ensure that:

- PC manufacturers and distributors are free not to pre-install LinkedIn on Windows and users are free to remove pre-installed LinkedIn
- Competing professional social network service providers are allowed to maintain current levels of interoperability with Microsoft's office suite
- Competing professional social network service providers have access to Microsoft Graph which is used to build applications and services that can access personal data and emails stored in the Microsoft cloud

These commitments amount to standard vertical commitments unrelated to big data concerns, and the Commission had no concerns about Microsoft's acquisition of LinkedIn's database.

Activity at the national level

In contrast to the Commission, national competition authorities have been considerably more active as concerns big data and digital networks and platforms.

Joint Franco-German paper on digital platforms and networks

In May 2016, the German Federal Cartel Office (the "FCO") and the French Autorité de la Concurrence (the "AdC") published a joint paper on digital platforms and networks.[21] This paper provides a roadmap to competition issues involving digital platforms and networks and identifies the following possible antitrust harms:

- Data as a source of market power
- Potential price effects resulting from increased market transparency
- Data-related anti-competitive conduct including refusal to provide access; discriminatory access; exclusive dealing, tying and leveraging and price discrimination

FCO report on assessing the market power of digital platforms and networks

In June 2016, the German FCO published a report on the assessment of the market power of digital platforms and networks. As concerns big data, the report notes that access to data sources is a factor to be analyzed when assessing the market power of digital platforms and networks, but that control over data is not per se indicative of market power. Rather, the basis on which data are collected, their relevance for competition, whether they can be duplicated and the options for combining data from different sources all need to be assessed on a case-by-case basis. The FCO report identifies the following positive and negative factors that may give rise to or reduce the risk of market power.

21 Internet businesses are considered to be platforms if they provide intermediation services which allow for direct interaction between two or more user groups that are connected by indirect network effects. Internet businesses are considered to be networks if they provide intermediation services which allow for interaction between users of the same group which result in direct network effects. Of course, some business models combine platform and network elements: social networks (Facebook) are audience providing platforms that finance themselves through advertising.

Positive factors indicative of market power	Negative factors suggesting the absence of market power
(i) Strong self-reinforcing feedback loops which can lead to tipping (ii) Matching platforms have strong two-sided positive indirect network effects (iii) Strong network effects are a first indication of dominance if one platform has a clear lead over rival platforms (iv) Direct and indirect network effects which create barriers to entry (v) Economies of scale, which can either constitute an entry barrier in themselves or may strengthen the self-reinforcing positive feedback loop inherent in platforms.	(i) Multi-homing (ii) Platform differentiation (iii) Platform congestion[22]

The report notes that platform/network markets with high direct or indirect network effects tend to be highly concentrated, but also that market share may be less relevant in assessing market power because of the impact of network effects on competition. Nevertheless, a high user-based market share lead may be relevant for the risk of tipping as a result of indirect network effects.

22 Congestion refers to the technical/physical limitations of the platform which may make it impossible to accept more users. Virtual congestion refers to the decline in the usefulness of the platform if its user groups become too large.

The report has led the FCO to seek amendments to German competition law to facilitate its ability to take enforcement action against digital platforms and networks. These amendments would:

(i) Permit the definition of relevant antitrust markets for digital services such as search engines or price comparison websites – where no money exchanges hands;
(ii) Provide additional tools for assessing the market power of two-sided digital platforms by including factors such as network effects, efficiencies of scale, access to data and innovativeness;
(iii) Expand German merger review to cover concentrations whose transaction value exceeds €350 million even where the target achieves less than €5 million in turnover.

Cases brought by AdC

The French competition authority has been involved in two cases in which it has required firms to make their databases available to rivals.

GDF/Suez

In this case, the AdC imposed interim measures requiring GDF-Suez to make consumption data, obtained from its customers when it held a monopoly on the French energy market, available to rivals to facilitate their market entry.

Cegedim

The AdC required the leading provider of medical information databases in France to sell its main database to customers, who used the software of a competitor in the adjacent market for customer relationship management. Cedegim involved a classic case of tying in - Cegedim had linked access to its database to use of its customer relationship management software.

The UK Competition and Markets Authority (the "CMA")

Trod/GB eye - Use of price algorithms to facilitate horizontal price fixing

In the Trod/GEB eye case, both companies used automated re-pricing software to implement their agreement not to undercut each other's prices on Amazon's UK website. In addition to sanctioning the two protagonists for horizontal price fixing, the CMA warned software providers that they risk violating UK competition law if they help their clients use software to facilitate illegal price-fixing agreements.[23]

Regulatory concern about the use of pricing algorithms has been increasing, as their use becomes more prominent. David Currie, the head of the CMA has questioned whether regulators have the tools to keep up with price algorithms that learn without human agency, and Commissioner Vestager has indicated that higher fines may be imposed where cartelists rely on price algorithms to implement price fixing agreements.

23 In a recent Commission RPM investigation involving Asus, it appears that the use of algorithms has added a horizontal element to the vertical RPM. The pricing software permits alignment with highest prices so that RPM took on an horizontal dimension

Commissioner Vestager's warning and the Trod case involve situations where human actors agreed to fix prices and then used algorithms to implement their illegal agreement. Here traditional competition law has all the necessary tools to deal with the infringement. Mr. Currie's concern is different and relates to the use of artificial intelligence to coordinate prices without any agreement or human involvement. Given the lack of human agency, competition law may not be able to deal with this situation, although regulation prohibiting the use of such algorithms could.

Cases brought by the FCO

Of all the national authorities, the German FCO has been the most adventurous when it comes to data issues.

The FCO's abuse case against Facebook

In 2016, the FCO initiated a case alleging that Facebook's infringement of German data protection laws constitutes an abuse of its dominant position. According to the FCO, the failure to fully disclose to Facebook members how their data will be used and/or to protect the privacy of their data amounts to an exploitative abuse. It is far from clear that the FCO's approach is linked to any antitrust theory of harm. If digital platforms compete on the terms offered to users, privacy protection could be a competitive parameter. In that context, if dominant firms were under less pressure to provide such protection, the failure to do so might be an indication of market power.

It is less clear that failure to respect data protection laws should be treated as an infringement of competition law. Doing so may be an effective way of enforcing data protection laws, but it is hard to see how this conduct could amount to an antitrust violation, particularly in the absence of any causal link between market power and the failure to respect privacy laws.

The FCO's approach in its Facebook case diverges sharply from that of the Commission which, in 2006, took the position that issues relating to personal data are not a matter for competition law. The Commission reiterated this view in Facebook/WhatsApp when it stated that "Any privacy related concerns flowing from the increased concentration of data...as a result of the... [merger] do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules."

The FCO's investigation of Amazon

More recently, the FCO has indicated concerns about Amazon's dual role as a retailer and a marketing platform. The main concern is that Amazon may gain a competitive advantage as retailer as a result of its access to competitors' data in its role as a platform. Although dressed in digital clothing, the issue identified by the FCO may not go beyond the more traditional antitrust concern that arises when the same player operates on both upstream and downstream markets or where it distributes its own and rivals' products.

Conclusion

As the prior survey indicates, the Commission has so far not found any competition problems involving big data in the merger context in the two cases in which it has considered the combination of databases. None of the member state cases surveyed have addressed big data issues, although both the German and French competition authorities have produced studies setting out an analytic antitrust roadmap relating to big data and digital networks and platforms.

There has also been increased awareness and heightened concern at both the national level (in the UK) and at the Commission about the use of algorithms to facilitate cartel activity, although the concern here has been with run-of-the-mill cartel activity that falls short of the type of collusive interaction that some observers could result from the application of artificial intelligence to pricing.

The conflict between the digital and the old economy and the fascination with big data are unlikely to go away. It is therefore probably more a question of when, than of if, there will be future cases involving either big data or digital platforms and networks.

THE IMPACT OF DIGITAL TRANSFORMATION ON EMPLOYEES

FRANK LENZEN, FRANKFURT

While this guide focuses primarily on the digital customer, there is another key stakeholder group - your people - that must be front-of-mind in your digital transformation strategy. In today's knowledge-based economy, employees are among the most valuable resources for many companies. Furthermore, your people are on the front line in delivering a positive experience for your customers. Therefore, it is worth taking a look at some of the employment law aspects of digital transformation.

Advances in technology have revolutionized how people view work today. Through technology, we have gained much greater flexibility in terms where and when we work. We are more connected and can collaborate remotely with colleagues around the world. We can work from home, from the airport, or from our favorite cafe. And online job platforms have given rise to a "gig economy" where people can work independently and be engaged on aproject-by-project basis.

While most employees appreciate the increased flexibility, there are also potentially significant risks and legal challenges that need to be addressed. How do we protect employees as the boundaries between work and leisure time become more and more fluid and people are constantly available by email or smartphone? How do we offer flexible working hours, while ensuring real-time responses to customer requests?

Working hours

The EU's Working Time Directive (2003/88/EC) sets a minimum standard of employee protection across the EU (although some countries have implemented further measures beyond this minimum). According to the directive, employees must not work more than 48 hours per week on average, they must have minimum rest periods of 11 consecutive hours per day and 24 hours per week, and they must have paid leave of at least four weeks per year.

However, in today's digital era, the typical eight-hour working day is no longer the norm, and there is no rigid separation between working hours and leisure time as people are constantly reachable by smartphone. In particular, the periods of rest seem to be most vulnerable. For example, is the mandatory rest period interrupted if an employee checks his/her emails at home in the evening or over the weekend? This question often goes unasked and there is little clarity as to what constitutes an interruption during rest periods. According to the European Court of Justice, employees should not be restricted by any kind of obligations within their rest period to ensure that they can freely control their own wellbeing without interruption.

In practice, most employees simply accept the after-work interruptions by email as a tradeoff for greater flexibility. Legally, this is largely unregulated due to the fact that the burden of employees being constantly reachable by email is not comparable to being on call. However, in 2017, France introduced a new provision into labor law giving employees a "right to disconnect" by limiting after hours work related emails. Whether other markets follow suit remains to be seen.

Home Office, BYOD and employee surveillance

With mobile technology, home office is quickly gaining popularity. But what happens if the employee gets injured during while working from home? Having private accident insurance in place is indispensable in such cases.

With the home office model, employers need to trust their people more, as supervisors are less able to directly monitor their employees. This can give rise to greater risk of fraudulently recording working time or exceeding statutory working limits.

Generally the employer is not allowed to collect or use the private data of their employees, other than basic data needed for the purposes of employment. So there are legal implications to consider if you wish to monitor the IT equipment used by your employees. For example, mobile devices used for work continuously collect data. If the employer wishes to have access to this data, it is necessary to obtain a works council agreement or, where there is no works council, an individual agreement. Otherwise, there is the potential risk of non-compliance with data protection rules.

The line separating the private sphere and the working sphere is even further blurred by the approved use of business tools (e.g. mobile, laptop, email account) for personal communication, and "bring your own device" (BYOD) schemes, which allow the business use of private communication tools. This could result in a loss of control of data, raising a potential conflict with data protection laws. To avoid data protection violations, employees have to keep their private data separate from business related data.

The gig economy

Digital technology has given rise to a new and growing segment of the labor market – often refered to as the gig economy. This essentially refers to the engagement of freelance labor to work on short-term jobs, and is common in sectors such as media, advertising, construction, IT and delivery/transport services. The gig economy has emerged mainly as a result of new technology platforms – such as Uber, Deliveroo and others, which match freelancers with potential short-term job opportunities.

Such working arrangements are growing in popularity – both by businesses seeking short-term help and by workers, who prefer a more flexible and independent working schedule. However, they are also causing controversy, since employers pay no social premiums and wage taxes and workers receive no minimum wage, sick leave or protection from dismissal.

Since independent contractors often do similar jobs as regular employees under similar conditions and policies, many courts in Europe tend to interpret such arrangements as employment relationships. Therefore, companies employing freelancers are at risk of reassessment by the social security authorities, or of claims from the worker before the Labor Court to requalify their relationship as permanent employment.

As a result of this emerging trend, a number of countries, including France, the Netherlands and others, are enacting legislation to offer greater protection for self-employed or short term workers and to force employers to pay social security and/or insurance contributions on behalf of such workers.

Wearables at work

Wearables – mobile computer systems that are worn by the user, such as smart glasses or fitness bracelets – are an emerging trend in the digital world. When using such wearables in the workplace, personal information is generally collected, processed and used. Such wearables are typically connected to an individual user account so that information which is generated by the mobile computer system can be assigned to a specific employee. Generally, in such cases data protection provisions are applicable.

Problems may arise when using private wearables at the workplace. The employer is allowed to prohibit not only the use, but also the wearing of smart glasses in the workplace if employees handle sensitive business and company secrets. The risk that an employee could use the camera or recording function of his/her smart glasses to capture company and business secrets is sufficient to prohibit their use at the workplace.

However, the employer is not allowed to prohibit the use or wearing private wearables at work if the use of these wearables has no impact on the work performance of the employee and is comparable with the view on a private watch. On the other hand, the employer may prohibit such wearables during the working hours if they impact on working time or performance.

Professional use of messenger services

Currently, more than one billion digital consumers around the world use messenger services such as WhatsApp or Skype daily. Messenger services allow employers to quickly and easily reach their employees both during and outside working hours. They are also advantageous in terms of maintaining business contact with customers and business partners.

This trend has already been recognized by service providers. For example, according to media reports a business version of WhatsApp is soon to be developed. However the use of messenger services is only allowed if data protection, as well as protection against unauthorized access, is granted.

Contact lists in employee's mobile phones regularly include personal data about other employees, customers and other business contacts. From a data protection perspective, the employer is responsible for the protection of this information. The employer must ensure that the data on the business phones of his employees are processed in accordance with the applicable data protection laws. This is can be problematic with respect to the GDPR (which is dealt with in further detail in chapter four) as well as local data privacy legislation. In the worst case scenario, lawyers or other individuals with access to confidential information can be punished in case of ill-informed use of messenger services.

Private use of the messenger services on business mobiles can be permitted legally, provided that the employer ensures, through technical tools and instructions provided to the employee, that the instant messenger tools do not have access to business-related data.

Social media as cause for termination

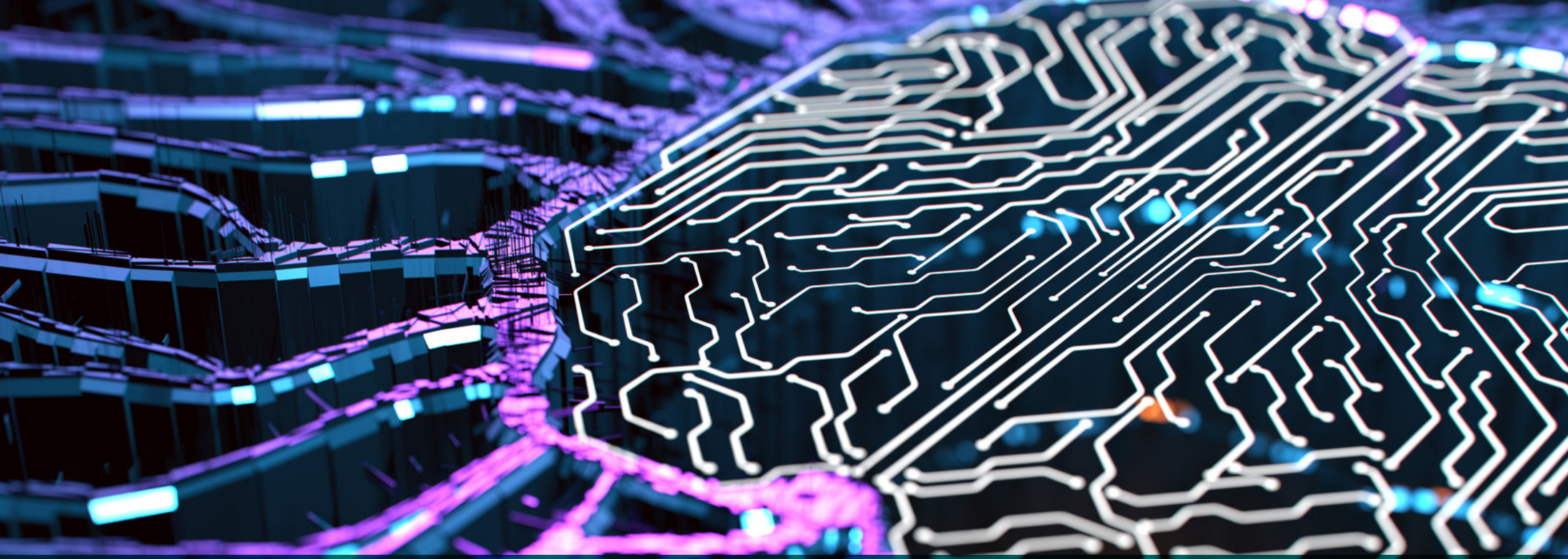
Generally, employees cannot be dismissed based on their activities outside the workplace. However, if employees post abusive, illegal or inappropriate political statements on social media, these are no longer covered by freedom of expression and can lead to a legal basis for a dismissal. In such situations, it is there needs to be a concrete connection to the employment relationship on social media, for example, if the employee indicates the name of his/her employer on their Facebook profile.

Data privacy in the cloud

Within just a few years, the use of the cloud has become a daily routine for many businesses. As part of their legal right to issue policies and directives, employers can generally select working equipment to be used and give instructions as to its use. The use of cloud solutions generally requires the co-determination of the works council in addition to the usual notification and consultation rights of the works council.

Conclusion

When it comes to technological progress, it is not a question of "if" but rather of "how" it will shape the working world of the digital age. Looking forward, the challenge will be to make effective use of the immense opportunities and advantages offered by new technologies, while at the same time preserving a high standard of employee protection for the future.



ARTIFICIAL INTELLIGENCE - THE NEXT EVOLUTION OF DIGITAL TRANSFORMATION

NICK GRAHAM AND MONIKA SOBIECKI, LONDON

Artificial intelligence, or AI, has already become a part of everyday life: from text and speech recognition – to targeted online advertising – to customer service "bots". It is predicted that 20% of all global business content this year will be authored by machines and that by 2020, AI bots will power 85% of all customer service interactions.[1] Thus it is an important area to consider when engaging with the digital consumer.

So what is artificial intelligence?

Artificial intelligence refers to systems exhibiting behaviors which are usually associated with human beings, rather than machines. We think of machines as only able to perform certain restricted tasks, as they were originally designed or programmed to do. AI, on the other hand, is able to learn from information received (such as data from the environment received through embedded sensors in the Internet of Things (IoT)) and to respond differently when it is given new data.

In headline terms, you could say that AI exhibits "intelligence", meaning that it has the ability to accomplish complex goals.[2] The global technology research and advisory company Gartner defines Artificial Intelligence as: ...technology that appears to emulate human performance typically by learning, coming to its own conclusions, appearing to understand complex content, engaging in natural dialogs with people, enhancing human cognitive performance (also known as cognitive computing) or replacing people on execution of nonroutine tasks.[3]

Machine learning

Machine learning is a popular type of AI. It involves the development of algorithms which are fed with input data. In supervised" learning, the data is labelled and the algorithms are effectively taught what the correct answer is. After a period of training the algorithm, it can then be deployed to make predictions based on the model which it has been taught. In unsupervised learning, the algorithms are not fed with labelled data and are left to their own devices to find patterns and build a model for themselves as to how they will process any new data received.

The European Commission noted recently[7] that AI can play a significant part in the digitalization of traditional analog businesses and has promoted, and contributed significant funding to a number of projects, including:

- **Manufacturing:** AI can predict maintenance and breakdowns in smart factories. SERENA uses AI techniques to predict maintenance needs of industrial equipment.
- **Agriculture:** AI can help achieve better productivity and minimize the use of expensive fertilizers, pesticides and irrigation, whilst reducing environmental impact. MARS is a mobile robot which plants seeds and workers can monitor the process remotely.
- **Transport:** AI can minimize wheel friction of a train against the track whilst maximizing speed and can enable autonomous driving. Transforming Transport is an initiative which will involve smart motorways and proactive rails, amongst other efficiencies.

1 Gartner, "Top 10 Strategic Predictions for 2017 and Beyond: The Storm Winds of Digital Disruption", October 2016.

2 Max Tegmark, Life 3.0 – Being Human In the Age of Artificial Intelligence, Allen Lane, 2017

3 Gartner IT Glossary, https://www.gartner.com/it-glossary/artificial-intelligence/

7 Digital Single Market: Artificial Intelligence for Europe, European Commission, 24 April 2018

SOLVING PROBLEMS, DRIVING EFFICIENCIES

AI has enabled companies to provide better decision making than would have been possible using human judgment alone, or to make the best use of limited available data. Some practical examples where we are seeing these evolutions and improvements in practice are:

- **Customer service:** Amazon has deployed neural networks to generate personalized product recommendations for customers, bridging the gap between their huge product catalog and sparse datasets for each individual customer, as a result of the small amount of products any individual typically purchases;[4]
- **Medical diagnostics:** A CNN, or deep convolutional neural networks - an AI system based on neural networks, is capable of classifying skin cancer with a level of competence allegedly comparable to dermatologists. It can be run on a smartphone, therefore potentially providing universal access to low-cost diagnostic advice.[5]
- **Cyber security:** AI², developed at MIT's Computer Science and Artificial Intelligence Laboratory, scans and reviews tens of millions of log lines each day and pinpoints anything suspicious to be escalated to a human being. AI² successfully identifies 86% of attacks whilst sparing analysts the time and effort of following up on false alarms.[6]

Big data and privacy

The European Political Strategy Centre has identified three ingredients that have led to the rapid advancement of AI in recent years – stronger computational power, more sophisticated algorithms and higher availability of vast amounts of data.[8]

Data is the fuel upon which AI runs, so it is crucial to ensure that the datasets available to AI systems are of high quality and are compliant with applicable privacy laws. Practical applications of AI engaging privacy laws may be psychometric testing services, employee recruitment and monitoring technologies and customer insights for retailers.

AI and the GDPR

As noted in chapter four, the GDPR governs the use of personal data. The use of AI, particularly when deployed on large, rapidly updating datasets which comprise different data sources – often referred to as Big Data – can create a number of challenges where these datasets contain personal data.[9]

Lawful processing under GDPR

One of these challenges is ensuring that processing is fair, lawful and transparent. Firstly, this means that its effects must be explained to the data subjects whose data is being processed by AI, particularly where there is automated decision making involved as a result of using the AI, including

4 https://aws.amazon.com/blogs/big-data/generating-recommendations-at-amazon-scale-with-apache-spark-and-amazon-dsstne/

5 https://www.nature.com/articles/nature21056

6 https://www.wired.com/2016/04/mits-teaching-ai-help-analysts-stop-cyberattacks/

8 The Age of Artificial Intelligence: Towards a European Strategy for Human-Centric Machines, European Political Strategy Centre, 27 March 2018

9 These issues are explored in more detail in the UK Information Commissioner's Office Paper on Big Data, Artificial Intelligence, Machine Learning and Data Protection, 2017

profiling. This requirement can be met in part by ensuring there is an appropriate privacy notice. However, fairness and transparency is broader than this and it will mean that any processing should be within the data subjects' reasonable expectations, based on what they have already been told.

Secondly, there must also be an appropriate lawful basis for carrying out processing by AI. Where relying on consent, the consent has to be freely given, specific, informed and unambiguous. This may prove a challenge where the use of the data by the AI is unclear, or if the data subject is insufficiently informed about the consequences of the processing. All of this goes back to the importance of taking innovative and creative approaches to producing an informative and well-drafted privacy notice and continuing to inform data subjects in an effective way.

Data controllers and AI

Data controllers are under an obligation to ensure that they comply with the Accountability Principle, meaning that they not only have to comply, but must show how they are complying with the GDPR. They must ensure, for example, that privacy is built into systems by design and default, that appropriate security measures have been implemented and that contractual relationships with any third parties processing data on their behalf (e.g. vendors providing AI technologies) contain the required mandatory clauses. Carrying out a Data Protection Impact Assessment before beginning the use of AI is an important step in helping to identify risks and implement safeguards.

Where the data is fully anonymized, it is no longer be personal data and therefore the GDPR does not apply. However, the act of anonymizing the data before storing in a data warehouse for use in training an algorithm can be a form of processing in itself and, in this case, the GDPR does apply. Companies will need to pay close attention to advances in technology around re-identification of datasets to ensure that any anonymization applied remains effective.

AI and other data laws

The use of data in AI technologies will be regulated by further legislation in the EU's Digital Single Market strategy, such as the forthcoming e-Privacy Regulation and the new proposed Regulation on free flow of non-personal data, which are aimed at removing obstacles to the free movement of non-personal data. The European Commission, the Council of the EU and the European Parliament reached a provisional political agreement on this Regulation on June 19, 2018.[10]

10 https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data

11 Categories are based on the Commission Staff Working Document – Liability for Emerging Technologies (SWD (2018) 137), 25 April 2018.

Regulating robots and artificial intelligence

The spread of robots and artificial intelligence creates numerous challenges for society and for the legal system. As robots begin to permeate all areas of life, we need to anticipate potential challenges and develop an approach to how the human-robot relationship will be regulated by law. Numerous proposals from around the world have sought to respond to this need, including the 23 Asilomar AI Principles, the European Charter on Robotics, and many others.

In 2016, Dentons was commissioned by Grishin Robotics to develop the concept of the first draft law on robotics in Russia. When developing the concept, the team not only looked to legal precedent, but also sought inspiration from science fiction, including Isaac Asimov's Laws of Robotics. The resulting document sparked debate about the regulation of this emerging field of technology.

The following year, the Dentons team decided to build on this experience and think bigger, by looking at the issue from a global perspective. The result was a draft for the first international convention on robotics, comprising 42 rules regulating people's relationships in connection with the active development of cyber-physical systems.

The convention consists of a single set of rules uniting all of the currently existing approaches to regulating AI and robotics, including the "black box" and the "red button" for robots, problems of security and confidentiality, and identification of robots. They also include new proposals to identify a category of higher-risk robots. Finally, the convention considers the regulation of AI and military robots, as well as issues of international cooperation in developing robotics in different countries.

The convention has been debated in business, academic and political circles, published in academic journals, and sent as a proposal to the United Nations.

Furthermore, in 2017 Dentons lawyers helped establish the Robopravo research center dedicated to the regulation of AI and robots. The center has developed several draft laws and publishes a journal on the regulation of new technologies.

Liability and safety

Liability can arise for AI-enabled products – for example, in the Internet of Things (IoT), AI-enabled robots or autonomous vehicles and systems. A practical example may be a smart home environment or a self-driving car. Liability could include:[11]

- **Contractual** - that is based on the contract between a consumer and a retailer.
- **Strict liability** – for example at EU level, based on the Product Liability Directive, as implemented in local Member States and which applies a strict liability regime to "producers" where a defective product causes damage to victims, such as personal injury, death or damage to property.
- **Fault-based liability** – for example under local law, such as the law of negligence in the UK.

The "EU safety framework" comprises a number of Directives such as the Machinery Directive, the Radio Equipment Directive, the Product Liability Directive and more detailed rules, for example around medical devices and toys. These should be considered in the context of any AI-enabled products which are developed or placed on the market. The Commission is currently assessing the EU safety framework in light of technological developments to determine whether further regulation will be needed.[12]

Intellectual property

In chapter eight, we examined the challenges of enforcing IP rights in a digital environment. Using AI to create works can also have implications on intellectual property rights such as on patentability, copyright and right ownership.[13] One issue which may arise is where AI has been used to create or enrich databases which the company wishes to protect, or where the AI has been trained using such databases.

12 Communication from the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions – Artificial Intelligence for Europe (COM (2018) 237), 25 April 2018.

13 Ibid, Footnote 52.

14 A Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems was published in March 2018.

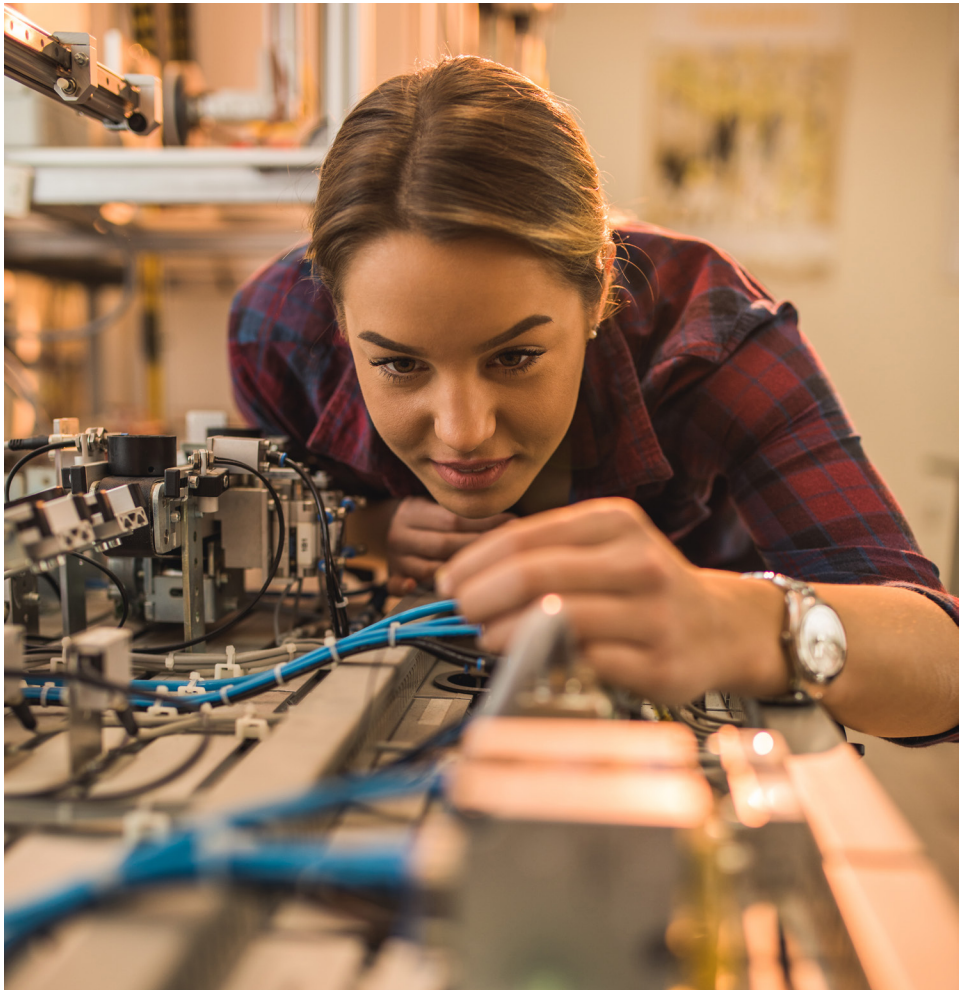
The future of AI regulation

The law on AI is still in a state of flux. Whilst regulatory frameworks exist around product safety and the protection of personal data, the development of AI systems themselves and the content of algorithms are not, at present, regulated.

However, there have been proposals at a European level to advance the development of ethical frameworks. Draft guidelines are anticipated by the end of 2018, in cooperation with the European group on Ethics in Science and Technologies, which has already started its work in this field.[14]

The next evolution of digital transformation

The use of AI and AI-enabled technologies presents unrivalled opportunities for businesses exploring the digital world to leverage their troves of data and create efficiencies internally (e.g. in employee engagement or maintenance of equipment). It can also present a new edge in interfacing with digital consumers, whether by making better judgment calls in terms of advertising, or offering a new and better AI-enabled product. Whichever way companies engage with AI, it is bound to transform the business world in ways in which we cannot even yet anticipate.



Contributors

Tímea Bana
Counsel, Budapest
T +36 1 488 5200
timea.bana@dentons.com

Yana Chirko
Of Counsel, St. Petersburg
T +7 812 325 8444
yana.chirko@dentons.com

Stefan Dittmer
Partner, Berlin
T +49 30 2 64 73 390
stefan.dittmer@dentons.com

Matthias Eggert
Partner, Munich
T +49 89 244408 487
matthias.eggert@dentons.com

Marc Elshof
Partner, Amsterdam
T +31 20 795 36 09
marc.elshof@dentons.com

Sven-Oliver Friedrich
Partner, Frankfurt
T +49 69 45 00 12 201
sven.friedrich@dentons.com

Tünde Gönczöl
Counsel, Budapest
T +36 1 488 5200
tunde.gonczol@dentons.com

Anastasia Gracheva
Paralegal, St. Petersburg
T +7 812 325 8444
anastasia.gracheva@dentons.com

Nick Graham
Partner, London
T +44 20 7320 6907
nick.graham@dentons.com

Hanna Karoline Heidkamp
Senior Associate, Frankfurt
T +49 69 45 00 12 148
karoline.heidkamp@dentons.com

Frank Lenzen
Partner, Frankfurt
T +49 69 45 00 12 284
frank.lenzen@dentons.com

Svetlana Lialkova
Associate, St. Petersburg
T +7 812 325 8444
svetlana.lialkova@dentons.com

Shane Mercer
Global Business Technology Director, Toronto
T +1 416 361 2313
shane.mercer@dentons.com

Igor Ostrowski
Partner, Warsaw
T +48 22 242 56 73
igor.ostrowski@denons.com

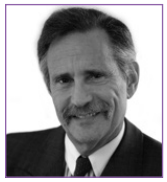
Christoph Papenheim
Partner, Frankfurt
T +49 69 45 00 12 201
christoph.papenheim@dentons.com

Georgy Pchelintsev
Partner, St. Petersburg
T +7 812 325 8444
georgy.pchelintsev@dentons.com

Constantin Rehaag
Partner, Frankfurt
T +49 69 45 00 12 248
constantin.rehaag@dentons.com

Kseniia Smirnova
Paralegal, St. Petersburg
T +7 812 325 8444
kseniia.smirnova@dentons.com

Monika Sobiecki
Associate, London
T +44 20 7320 6089
monika.sobiecki@dentons.com



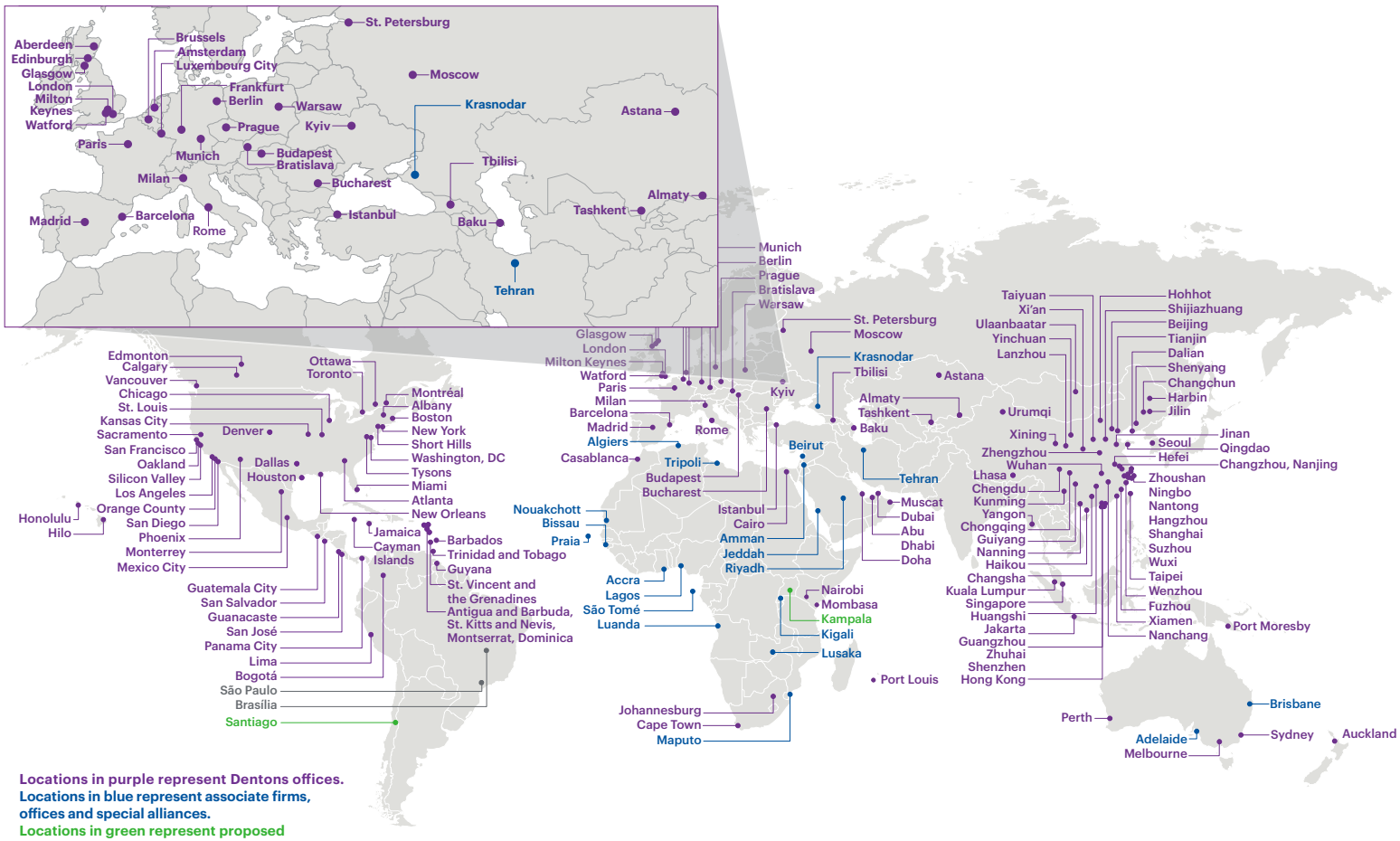
James Venit
Partner, Brussels
T +32 2 552 2941
James.venit@dentons.com

Natalia Selyakova
Partner, Kyiv
T +380 44 494 4774
natalia.selyakova@dentons.com

Victor Naumov
Partner, St. Petersburg
T +7 812 325 8444
victor.naumov@dentons.com

Technology, Media and Telecommunications in Europe

Dentons' Telecommunications, Media and Technology (TMT) practice provides full scope legal advice, ranging from general M&A and corporate advisory to more specialist areas such as regulatory issues, IP/IT licensing and distribution agreements and international spectrum allocations. With over 150 TMT lawyers in Europe and 450 around the world, you can rely on us to be a valuable extension of your team in virtually any key market in which you do business.



Locations in purple represent Dentons offices.
Locations in blue represent associate firms, offices and special alliances.
Locations in green represent proposed combinations that have not yet been formalized.
Locations in gray represent Brazil Strategic Alliance.

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.

dentons.com

CSBrand-9976-Digital-Transformation-Guide-Flipbook_10 — 26/10/2018