Hogan Lovells

ELTEMATE

Digital Transformation & Law Summit 2025

Insights

Impulses for the Digital Future

Key Takeaways from the Digital Transformation & Law Summit

The Digital Transformation & Law Summit 2025 in Düsseldorf made one thing clear:

Digital transformation presents new opportunities and challenges for companies, technology providers, and legal advisors alike. During our summit, we joined you in discussing key developments at the European regulatory level, the strategic use of AI and data, and the growing demands for security and compliance. What flexibility remains in the face of ever-expanding regulation of digital technologies? Will the European Commission need to revisit and adapt its current regulatory framework? What guardrails must be observed in doing so? And how can we meaningfully promote our digital future?

One thing became evident: success in the digital age requires a close interplay between technology, strategy, and law.

With this follow-up document, we would like to provide you with a concise overview of the most important takeaways and insights from the presentations and discussions. It offers a compact summary of best practices, key questions, and legal guardrails that companies should keep in mind – both now and in the future.

We hope these insights will provide valuable guidance as you continue to shape and implement your digitalization strategies.

Thank you for your participation, your contributions, and the open exchange – we look forward to continuing this dialogue with you!

Your Hogan Lovells Team

Dr. Marcus Schreibauer
Hogan Lovells

Dr. Leopold von Gerlach
Hogan Lovells

Keynote

Emerging & Frontier Technologies

Ever-evolving forms of intelligent systems, robotics, and quantum technologies are fundamentally transforming the economy – and posing new challenges for Europe's regulatory framework and the legal landscape as a whole. The ongoing development of these technologies calls for a proactive and forward-looking approach from both companies and legal professionals.

Key innovations include multimodal AI models that integrate various data types – such as text, images, and audio – to support better decision-making across sectors like manufacturing, retail, and automotive. Retrieval-Augmented Generation combines AI language models with external knowledge databases, enabling high-precision applications in areas such as legal advice and healthcare. AI agents allow for autonomous decision-making processes and are revolutionizing financial advisory services and logistics management. Spatial and physical AI leverages sensors and 3D mapping for real-time interaction with physical environments, with use cases in real estate and manufacturing. Robotics and autonomous systems automate complex processes in industry and healthcare, while quantum technologies have the potential to exponentially increase computing power and transform secure communication.

It is essential to continuously monitor and understand these developments – particularly for legal professionals who must play an active role in shaping the legal framework at an early stage and advise companies on the responsible use of innovative technologies.

Dr. Leopold von Gerlach
Hogan Lovells

Digital Transformation & Law Summit 2025

Insights I Table of Content

1

Digital Transformation at a Glance: Developments in the EU

Data: Data Act, Data Governance Act

Digitalization and the use of new technologies enable new forms of data utilization. From a legal perspective, there has been a shift from “data protection laws” to comprehensive “data laws.” With the implementation of proper data governance, companies can meet these new legal challenges while improving the quality, availability, protection, and usability of data for internal business processes.

Data Governance Act
The key topics of the Data Governance Act include the re-use of protected data held by public bodies, requirements for data intermediation services, and the voluntary registration of data altruism organizations. While the Act identifies potential sources of data through relevant registers, it does not establish a legal right to access such data.

Data Act
The Data Act focuses on improving access to certain types of data and facilitating switching between data processing services.

At the Digital Transformation & Law Summit, the focus was placed on the new opportunities and legal requirements concerning access to data generated by connected products or related services. In this respect, the Data Act aims to give users control over their data. In general, manufacturers of connected products and providers of related services are required to design their products and services in such a way that data is, where relevant and technically feasible, directly accessible to users.

Additionally, data holders are obliged to provide data to the user—or to a third party at the user’s request. The disclosure of trade secrets cannot be refused outright, although companies are permitted to implement and contractually enforce certain protective measures.

For personal data, the requirements of data protection law apply in addition to those under the Data Act. Moreover, data holders will only be allowed to use certain non-personal data for their own purposes based on a contractual agreement with the respective users.

1

Digital Transformation at a Glance: Developments in the EU

Data: Data Act, Data Governance Act

To support agreements related to the provision of data to users or third parties, the European Commission has developed voluntary model contract clauses for various contractual relationships.

The Data Act will largely apply as of 12 September 2025. Recommended actions include:

- Taking inventory of connected products and related services
- Conducting a gap and risk analysis
- Establishing a data governance framework
- Developing strategies for data provision and data use, including the creation of appropriate information notices and contractual documentation
- Until 12 September 2026: Implementing development and design strategies for connected products and related services

Sarah-Lena Kreutzmann
Hogan Lovells

Dr. Martin Pflüger
Hogan Lovells

2

Digital Transformation at a Glance: Developments in the EU

The AI Act: A New Legal Framework for Artificial Intelligence

The AI Act has been in force since 2 August 2024. Since 2 February 2025, the first key obligations for companies have become applicable – including the prohibition of certain AI systems posing unacceptable risks and the requirement to ensure adequate AI literacy within the organization.

Further provisions and obligations will come into effect successively after 12 months (by 2 August 2025), 24 months (by 2 August 2026), and 36 months (by 2 August 2027). The AI Act follows a risk-based approach, determining the extent of obligations based on the potential risks AI poses to the health, safety, and fundamental rights of individuals. Violations of these obligations can result in significant fines of up to EUR 35 million or 7% of global annual turnover.

Companies will need to address and prepare for a range of new obligations, regardless of their role in the AI value chain – whether as a provider, deployer, importer, or distributor of AI systems.

Providers of high-risk AI systems must, for example, ensure lawful use of training and validation data during development and design, create technical documentation and user instructions for safe operation, and undergo a conformity assessment procedure.

Deployers of high-risk AI systems must ensure proper and intended use of the system, as well as human oversight. In addition, information and transparency obligations apply also to certain AI systems with limited risk.

In this context, implementing adequate AI governance is an essential requirement – not only to comply with the AI Act but also as part of a company's broader corporate governance duty to manage potential business risks within the organization. Appropriate AI governance helps minimize risks and enables the responsible use of AI in line with legal, ethical, and societal expectations.

By establishing the right organizational structure, policies, standards, processes, and controls, companies can ensure accountability, promote the effective and responsible use of AI, and ultimately benefit sustainably from this transformative technology.

Sarah-Lena Kreutzmann
Hogan Lovells

Dr. Martin Pflüger
Hogan Lovells

3

Digital Transformation at a Glance: Developments in the EU

New Legal Requirements for Cybersecurity

Regulatory requirements for cybersecurity are becoming increasingly stringent and affect companies across all industries. In particular, the NIS 2 Directive, the Digital Operational Resilience Act (DORA), the Cyber Resilience Act, the Radio Equipment Directive (Delegated Act), and the AI Act set out extensive new obligations for companies. These obligations include both company-related and product-related requirements.

Company-related requirements:
The NIS 2 Directive, which still needs to be implemented in Germany, applies to companies from a wide range of industries. Under DORA, banks and insurance companies in particular are subject to obligations. The new regulations require companies, among other things, to implement risk management measures and report security incidents. Particular focus is placed on the responsibilities of company management, who are accountable for implementing risk management measures within the organization and must, among other things, undergo regular training.

Product-related requirements:
The Cyber Resilience Act defines comprehensive security requirements for connected products with digital elements, covering all phases from design and development through to post-market support. Companies must ensure vulnerability management and security updates for at least five years after the product is placed on the market. A new requirement is that such products must undergo a cybersecurity conformity assessment procedure.

The Radio Equipment Directive (Delegated Act) sets security requirements for connected radio equipment, overlapping with the scope of the Cyber Resilience Act, while the AI Act contains specific provisions for AI systems.

Sanctions & liability:
Violations may result in fines as well as further sanctions, such as compensation claims, product recalls, and product liability. Additionally, there is a risk of personal liability for company executives.

Conclusion:
Cybersecurity is a core management responsibility. Companies should act early to meet regulatory requirements and minimize liability risks.

Dr. Marcus Schreibauer
Hogan Lovells

Dr. Michael Thiesen
Hogan Lovells

4

Digital Transformation at a Glance: Developments in the EU

The EU Perspective on Antitrust Implications of Digital Transformation

Digital transformation is reshaping business models and value chains—posing new challenges for both competition law and companies alike.

Merger control is becoming increasingly complex. More and more often, scenarios beyond traditional mergers and acquisitions are gaining relevance, such as the purchase of intellectual property, know-how, or entire development teams (so-called acquihires). Even loosely structured partnerships are coming under scrutiny. At the same time, the thresholds for merger notification are becoming more diverse. In addition to traditional turnover-based thresholds, transaction value thresholds (as in Germany and Austria) and so-called call-in powers – which allow authorities to review mergers even below notification thresholds – are becoming increasingly important. Key takeaway for companies: Assess potential merger control implications at an early stage and integrate them into transaction planning and documentation.

At its core, digital transformation is about connectivity – and that makes access to digital infrastructure like platforms, interfaces, and data all the more crucial. Under the abuse of dominance rules in Sections 19, 20 of the German Act against Restraints of Competition and Article 102 TFEU, companies have strong antitrust claims. Refusals to grant access can be abusive, particularly when applied in a discriminatory manner or when they hinder value creation in downstream markets. Key takeaway for companies: Examine potential claims – enforcement prospects are improving.

Companies today are no longer isolated silos but part of broad value creation ecosystems. As such, the antitrust-compliant structuring of cooperation is becoming a key focus – particularly in areas such as data sharing, standardization, or AI projects. When competitors are involved, understanding the antitrust boundaries is essential – without letting competition law become a deal-breaker. Key takeaway for companies: Early legal guidance can accelerate processes and minimize risks.

Dr. Julian Urban
Hogan Lovells

5

Digital Transformation at a Glance: Practical Applications in Business

AI in HR: External and Internal Regulation

The integration of artificial intelligence (AI) into business processes offers immense potential – but also presents companies with new legal challenges. In particular, the EU AI Act sets clear boundaries for the use of AI. AI applications used in the HR context are frequently classified as high-risk systems.

As part of effective AI governance, it is advisable to establish internal rules for employees' use of AI (an AI policy) and to implement appropriate monitoring mechanisms for AI systems. These mechanisms typically include appointing an “AI Officer” or, in cases of more extensive use, setting up a dedicated “AI Team.” While the law does not currently mandate such a role, centralizing responsibilities in this way can help ensure compliance with all regulatory requirements and promote the responsible use of AI.

It is also important to consider the co-determination rights of the works council – not only when introducing an AI policy or defining the AI Officer’s role, but also whenever AI applications are deployed in the workplace. While each AI implementation must independently comply with co-determination rights, it is advisable to adopt a framework agreement. Such a framework can streamline the approval process and accelerate individual implementations. For example, the company and works council can agree on different procedures depending on the risk level of the AI system in question.

Dr. Tim Gero Joppich
Hogan Lovells

6

Digital Transformation at a Glance: Practical Applications in Business

AI and IP Protection: A Strategic Perspective

The growing use of artificial intelligence (AI) into business operations poses significant risks for the protection of intellectual property (IP). The two case studies below illustrate common challenges and how companies can mitigate them effectively.

Case Study #1: Deploying Generative AI Internally
Using generative AI tools within a company environment can lead to several IP-risks: Sensitive business information may be inadvertently shared with AI providers; liability may arise from including third-party content in prompts, and the output produced by AI is typically not protected under current IP law. Moreover, the generated content may imitate existing works, potentially infringing third-party rights.

To counter these risks, companies should adopt a Generative AI Use Policy including guidance on using non-identifiable inputs, refraining from entering confidential data, disabling history tracking, and reviewing generated outputs. The aim is to raise company-wide awareness. IP-training can further reinforce this mindset. Internally, clear post-processing guidelines should be in place; externally, contracts with service providers should mandate similar safeguards.

Case Study #2: Developing AI Systems
Risks increase when companies develop AI systems using third-party databases—particularly in retrieval-augmented generation (RAG) models. IP infringements may result from the use of protected content during processing, or from integrating publicly available material that remains under copyright. Company's data used as training input may also be exposed, particularly through reverse engineering.

To mitigate these risks, businesses should implement an AI Developer Guideline that categorizes internal IP, sets usage rules, and includes output monitoring. License agreements—especially for RAG systems—should be reviewed for AI compatibility. Appointing an AI Officer to oversee compliance and safeguard the company's IP throughout the development process is also a strong recommendation.

Dr. Jasper Siems
Hogan Lovells

7

Digital Transformation at a Glance: Practical Applications in Business

Litigation in the age of digital transformation: Liability risks everywhere?

The digital transformation entails numerous new liability risks. It is leading to a fundamental reshaping of the market. Large traditional companies that do not adapt to the new circumstances in time will perish. Dynamic companies that have adapted to the new circumstances will thrive. The disruption this causes in itself triggers numerous disputes.

In addition, there are new liability risks associated with the digital transformation. Technological developments such as deepfakes are constantly creating new forms of threat, while making existing forms of attack, such as cyberattacks and CEO fraud, increasingly dangerous. Furthermore, in the digital world, everything is connected to everything else. Due to this interconnectivity, when damage occurs, there are usually further consequences.

All this requires new rules. And – as trivial as it may sound – every rule leads to new obligations. Due to the peculiarities of German manager liability, this leads to a considerable restriction of discretionary decision-making. Where there are legal obligations, the principle of legality applies – and the business judgement rule is suppressed.

Lawmakers are facing major challenges. Regulating liability risks in times of digital transformation is no easy undertaking. Many technical developments – especially artificial intelligence (AI) – are leading to a situation in which there is no longer any attributable human action. The conventional categories of the legal system follow the traditional liability scheme of a – human – action that has a (mono-) causal consequence. These categories are now becoming blurred. The law must be rethought.

And even the comparatively simple conversion to digital documents still leads to considerable liability risks. It is true that the German legal system now provides for regulations that are intended to provide legal certainty for digital documents. Nevertheless, the model of the German Civil Code (BGB) and the Code of Civil Procedure (ZPO) is still the (paper) document, not the digitalized document. The legal system is still full of liability risks when using digital documents in the absence of an original (paper) document.

Dr. Kim Lars Mehrbrey
Hogan Lovells

8

Digital Transformation at a Glance: Practical Applications in Business

Compliance in the Age of Digital Transformation

As generative AI reaches the peak of its hype cycle, legal tech providers must deliver on their promises. User expectations are steadily rising, and offering merely generic solutions is no longer sufficient. Instead, legal tech providers must demonstrate how their products can effectively solve real-life problems. This can be achieved through the automation of routine tasks (like NDA drafting or translation of documents), the optimization of legal workflows (like the regular identification of new relevant regulations), and the enhancement of document management through AI based automated classification and sorting of information.

At the same time, expectations from regulators are also increasing. For instance, the U.S. Department of Justice, in its recent guidelines, addresses the need to avoid an imbalance between the technological resources available to compliance departments and the technology applications used to identify and capture market opportunities.

A crucial aspect of successfully integrating AI in the legal field lies in the careful selection of suitable use cases. While highly complex legal processes and unique contractual agreements are less suited for AI deployment, there are already numerous opportunities to integrate AI into the daily work of legal teams. For example, there are opportunities for automation through generative AI in confidentiality agreements, employment contracts, and other recurring contract types. Legal departments can also deploy chatbots to efficiently handle initial inquiries from employees.

In monitoring for regulatory updates, over 90% of irrelevant information can be filtered out using so-called AI classifiers. Simultaneously, the use of AI in processing large datasets for disputes or internal investigations can save up to 80% of the time. It is expected that with continuous advancements of AI and the continuous increase of data volumes, the application of AI in the legal sector will continue to grow.

Dr. Sebastian Gräler
Hogan Lovells

Marcus Busch
ELTEMATE

hoganlovells.com