Legal 500
Country Comparative Guides 2024

Germany
TMT

Contributor

Lindenpartners

Thomas Britz, LL.M (Berkeley)

Associated Partner | britz@lindenpartners.eu

Dr. Moritz Indenhuck

Partner | indenhuck@lindenpartners.eu

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Germany.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Germany: TMT

1. Is there a single regulatory regime that governs software?

No – there is no single regulatory regime in Germany that governs software. Instead, software regulation is covered by a variety of laws and regulations, depending on the specific context and use of the software.

Probably the most important of these are the provisions on the protection of intellectual property rights in software and databases under the Copyright Act (UrhG, in particular Sections 69a et seq.) as well as the Copyright Service Provider Act (UrhDAG), the Patent Act (PatG), and the Employee Inventions Act (ArbNErfG).

Here are some other key laws which typically play an important role in connection with software:

- General civil law: Legal provisions on the conclusion of the contracts (i.a. mandatory rules regarding warranties and T&Cs) as well as on the protection of consumers and competitors are typically of significance when providing or sourcing software and can be found in the German Civil Code (BGB), the German Commercial Code (HGB) and the Act Against Unfair Competition (UWG).
- Data law: Provisions regarding the protection of personal data and privacy are contained in the EU General Data Protection Regulation (GDPR), the Federal Data Protection Act (BDSG) and the Telecommunications Digital Services Data Protection Act (TDDDG).
- Digital services: Digital services are currently i.a. regulated in the German Digital Services Act (DDG) and the EU Digital Services Act (DSA). Furthermore, the EU Digital Markets Act (DMA) and the EU Regulation on Platform-to-Business Relations (P2B Regulation) regulate online platforms. New relevant EU Acts will become applicable in the near future, such as the EU NIS 2 Directive (2024), the Data Act (2025), the AI Act (2025) and the update of the EU Product Liability Directive (2026). There are also some advanced legislative initiatives in the area of product security/liability and software, such as the EU AI Liability Directive and the EU Cyber Resilience Act.

2. How are proprietary rights in software and associated materials protected?

In Germany, proprietary rights in software and associated materials are protected through several mechanisms:

- First and foremost, Computer programs (including drafts and preparatory design materials) are protected under the German Copyright Act (UrhG) if they constitute individual works in the sense that they are the result of their author's own intellectual creation. Ideas and principles underlying any element of the program, including its interfaces, are as such not eligible for protection (cf. Section 69a UrhG, which is based on Directive (EU) 2009/24/EC). As soon as new software that is eligible for copyright protection comes into existence, it is automatically (i.e. without any formal process to register the right) protected under the law.
- Computer programs "as such" are not eligible for patent protection, but inventions related to computer programs can potentially qualify for patent protection. Due to this high threshold, patent law in practice typically has rather limited impact on protecting computer programs.
- Software can also be protected under the German Employee Inventions Act, in particular if it's patentable,

3. In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

Under German law, the ownership of proprietary rights in software developed by a third party is not automatically vested in the customer. As software is typically classified as a creative work, the initial ownership of the copyright rests with the author(s). The customer may acquire exclusive rights of use regarding the program – but not the actual copyright itself.

In the absence of any contractual provision, it depends on

the context to what extent the customer automatically receives such rights of use. Here are two key rules:

- To allow employers to fully exploit programs created within an employment relationship, Section 69b of the German Copyright Act (UrhG) states that the employer alone is entitled to exercise all economic rights in the computer program that employed programmer have created in the performance of their duties or in accordance with their employer's instructions. This statutory rule however typically does not apply to programmers who work as freelancers.
- Section 31 (5) of the German Copyright Act (UrhG) is a pivotal regulation that interprets the extent of usage rights in the software granted to the customer based on the intended purpose of the contract when there are no clear contractual rules. It safeguards the author's interests by ensuring they retain as many rights of use as possible without frustrating the underlying goals of the contract.

4. Are there any specific laws that govern the harm / liability caused by Software / computer systems?

In Germany, the legal framework regarding harm/liability caused by software is currently primarily governed by two main laws:

- The German Civil Code (Bürgerliches Gesetzbuch - BGB) contains general rules about contractual and tortious liability, which can be applied if software causes damage.
- Additionally, claims for damages can also be made under the Product Liability Act (Produkthaftungsgesetz) when a defect in a product causes damage. To what extent software falls under this Act is often still disputed under the current regime. However, it will likely be updated within the next two years in order to implement the revision of the underlying EU Product Liability Directive. The update will clarify that software and AI may constitute a defective product and is generally intended to tighten the liability rules, i.a. by broadening the range of potentially liable actors as well as a lowering the burden of proof for claimants.

Furthermore, the EU's current draft of an AI Liability Directive aims to establish a uniform set of rules to address non-contractual civil liability for damages caused by AI systems. Whereas the Product Liability Directive regulates the manufacturer's liability for defective products independent of fault, the AI Liability Directive is supposed to cover liability claims which are based on intent or negligence. The timeline of this directive is however still unclear.

5. To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

Sections 69a-69g of the Copyright Act (UrhG) contain specific rules on restricted acts when using software. This includes for instance restrictions on modifications or the distribution of computer programs, but also certain special rights for the licensee concerning i.a.

- back-up copies,
- text and data mining, and
- decompiliaton.

Some of these rights cannot be circumvented by deviating contractual provisions (cf. Section 69g Copyright Act).

Sections 31 et seq. of the Copyright Act contain rules on how the rights of use regarding software IP are granted by the authors. These are important to observe, for example when drafting end user license agreements (EULA), as they might overrule contractual agreements between the parties to a certain extent. The copyright holder may i.a. grant exclusive or non-exclusive, revocable or irrevocable licenses and he may limit the right of use regarding time, place and subject matter.

Furthermore, the new Sections 327 et seq. of the German Civil Code (BGB), which implement the EU Directive 2019/770/EU, regulate the contractual aspects of providing digital content and services. They mainly apply to contracts between businesses and consumers (b2c), but may also allow for b2b recourse in contracts for digital products within the commercial supply chain.

Finally, there are several criminal offenses related to the misuse of software. For example, Section 303b of the Criminal Code (StGB) addresses computer sabotage. The criminal offenses of spying on data (Section 202a of the German Criminal Code), interception of data (Section 202b of the German Criminal Code) and computer fraud (Section 263a of the German Criminal Code) can also be relevant.

6. Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

There are no technology-specific laws that govern the provision of software between a vendor and customer. The civil law classification under German law usually depends on the type of contract. Depending on the use and creation of the software, the provisions of the purchase contract, work contract, services contract or leasing contract may be applicable. Different regulations govern customer warranties in the event of defects. In addition, some laws are applicable depending on the parties involved, such as Sections 327 et seq. BGB in the case of consumer contracts for the provision of digital content and services.

There are however some sector-specific regulations that govern the usage of cloud-based services, especially in the context of outsourcing (see question 11).

7. Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Under German law, there is generally limited flexibility concerning liability limitations due to strict regulations on standard terms and conditions outlined in the German Civil Code (Sections 307 et seq. BGB), even within business-to-business (B2B) transactions. Fixed caps in T&Cs might often be deemed unenforceable if they concern essential contractual obligations. Companies often strive to restrict their liability by excluding liability for regular (as opposed to gross) negligence in individually negotiated cap agreements. In the SaaS context, a typical individually negotiated cap would limit any damage claims against the provider arising in a specific year to the amount of remuneration paid to the provider in the respective year (or a multiple thereof).

8. Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

(a): Confidentiality breaches are sometimes excluded from cap agreements. As damages due to a breach of confidentiality are often difficult to prove, providers often additionally insist on fixed contractual penalties as a baseline for damages in case of a breach.

(b) and (c): Breaches concerning data protection and data security are often excluded from caps on damages as many companies have concerns about high damages due to GDPR enforcement.

(d), (e) and (f): IPR infringement claims, breaches of applicable law and regulatory fines are typically not as such specifically excluded from caps.

(g): Financial caps in case of willful and deliberate breaches are generally precluded under German contract law (Section 276 (3) of the German Civil Code (BGB)), which means unlimited liability is the mandated by law.

9. Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

In Germany, holding software source code in escrow for the benefit of the software licensee is rather the exception than a normal practice. Escrow providers are occasionally engaged for software source code for custom-build software, products developed by smaller firms or where the software is vital to the licensee's operations, such as in the case of Enterprise Resource Planning (ERP) software. In such instances, businesses commonly enlist the services of notaries or legal practitioners to oversee escrow arrangements of escrow providers. Professional escrow service providers are also available for cloud-based software.

10. Are there any export controls that apply to software transactions?

The export of software to other countries may require authorization from the Federal Office of Economics and Export Control (BAFA) under certain circumstances. Authorization is particularly required for the export of goods specifically designed or modified for military

purposes. Also, for items with dual civilian and military applications (known as “dual-use goods", cf. Regulation (EU) 2021/821), certain licenses can be necessary. Additionally, license requirements may arise in particular from the Foreign Trade Act (AWG), the Foreign Trade Regulation (AWV), Regulation (EU) No. 258/2012 (Firearms Regulation), Regulation (EU) 2019/125 (Anti-Torture Regulation) and various embargo regulations (such as Iran or Russia).

11. Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

IT outsourcing is typically governed in sector-specific laws, in particular regarding the financial sector. These regulations are delineated in various provisions such as Section 25b of the Banking Act (KWG), Section 26 of the Payment Services Supervision Act (ZAG), Section 80 (6) of the Securities Trading Act (WpHG) or Section 32 of the Insurance Supervision Act (VAG).

Regulators such as the Federal Financial Supervisory Authority (BaFin) and the Federal Office for Information Security (BSI) have issued detailed guidelines on how they interpreted statutory requirements regarding IT outsourcing, IT security and cloud services.

The provisions of the recently adopted EU Digital Operational Resilience Act (DORA), which governs IT security in the financial sector and will be applicable from 17th January 2025, will also likely also become relevant soon.

12. Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

German labor law imposes strict regulations on terminating employment contracts, which might occur in cases of outsourcing. If the Protection Against Dismissal Act (KSchG) applies, the employer may only terminate an employment contract if it is “socially justified”. This means the termination must be based on reasons related to the employee's conduct, personal circumstances, or compelling operational requirements that prevent the continued employment of the employee in the business. If the termination is due to operational reasons, such as business reorganization, the employer typically must apply correct “social” criteria to determine which employees to let go. Certain categories of employees, such as pregnant employees or members of the works council, enjoy enhanced protection against dismissal.

Individual staff members may also be protected by rights of a work council under the Works Constitution Act (BetrVG). For instance, the employer may have to inform the works council in full and in good time of any proposed “alterations” which may entail substantial disadvantages for the staff and consult the works council on the proposed alterations (Section 111 BetrVG).

Furthermore, outsourcing IT services might be considered a “transfer of operations " under Section 613a of the German Civil Code (BGB). In the event of a transfer of operations, the acquirer of the business enters into all existing employment relationships of the seller as a mandatory legal consequence. The termination of the employment relationship of an employee by the previous employer or by the new owner due to transfer of a business or a part of a business is ineffective (Section 613a (4) BGB).

13. Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

Telecommunications networks and services are mainly regulated in the Telecommunications Act (TKG). The purpose of the TKG is to promote competition in the telecommunications sector and efficient telecommunications infrastructures through technology-neutral regulation and to ensure adequate and sufficient services nationwide (Section 1 (1) TKG). The TKG contains regulations on market regulation, access regulation, fee regulation, abuse prevention, customer protection, information on infrastructure and network expansion, frequency regulation as well as public safety and emergency preparedness.

The Telecommunications Digital Services Data Protection Act (TDDDG) i.a. contains special provisions on the protection of personal data and privacy when using telecommunications services, in particular regarding confidentiality of telecommunications and the use of traffic or location data.

Supplementary to the aforementioned laws, a multitude of regulations exist that cover distinct elements of telecommunications. The overarching purpose of these regulatory instruments is to facilitate the efficient

functioning of telecommunications services, safeguard the rights of consumers and guarantee the security of information technology systems.

14. What are the principal standard development organisations governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

The Federal Network Agency (Bundesnetzagentur), Germany's main authority for infrastructure, promotes interoperability and standardization with respect to information and communication technology by collaborating with various SSOs at national, European and international level. The following key SSOs are currently mentioned by the Bundesnetzagentur for mobile communications and connected technologies:

- Mobile communications:

The 3rd Generation Partnership Project (3GPP) is a global cooperation between standardization bodies which includes the ETSI (European Telecommunications Standards Institute, a leading SSO in Europe). In 2019, 3GPP for instance published an initial package of 5G specifications.

Recently, global research activities on 6G have gained significant momentum. In the radio sector of the International Telecommunication Union (ITU-R), initial work on 6G was launched in March 2021, the results of which will be incorporated into 3GPP in the future.

- Connected technologies:

Machine-to-machine (M2M) communication refers to technologies that for instance enable automated exchange of data between devices. It encompasses various application areas such as e-health or automotive technology communication and plays a significant role in the Internet of Things (IoT). The standardization of M2M is handled by different committees that focus on specific fields of application. OneM2M, a global partnership for standardization of M2M, i.a. includes the European SSO ETSI.

Dedicated Short Range Communication (DSRC) is one of the technologies that can be used in vehicles for collision avoidance, congestion reporting or toll collection. Current standardization activities on this topic are taking place at ETSI and 3GPP, among others.

Intensive standardization work has been going on at ETSI for several years in the area of Reconfigurable Radio Systems (RRS), which are expected to offer the possibility to support the needs of our networked world – including the Internet of Things (IoT) – e.g. by sharing frequencies between different services.

For a comprehensive overview of other relevant SSOs in Germany, see the website of the Federal Network Agency (Bundesnetzagentur).

15. How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Technical standards facilitating interoperability between connected devices are crucial for the development of connected technologies. They play a vital role in ensuring seamless communication, fostering innovation, and driving market growth.

Key legal frameworks in Germany include the Telecommunications Act (TKG), the Act on Electromagnetic Compatibility of Equipment (EMVG), and the Radio Equipment Act (FuAG). These laws transpose EU directives into national legislation and provide the legal basis for technical standards and interoperability requirements.

For a comprehensive overview of relevant technical standards, the Federal Network Agency (Bundesnetzagentur) website serves as a valuable resource, offering information on standards, regulatory requirements, and developments in connected technologies and telecommunications.

16. When negotiating agreements which involve mobile communications or other connected technologies, are there any different considerations in respect of liabilities/warranties relating to standard essential patents (SEPs)?

SEP holders are typically required to license their patents on Fair, Reasonable, and Non-Discriminatory (FRAND) terms. This obligation stems from EU competition law and has been significantly clarified by the Federal Court of Justice (Bundesgerichtshof, BGH) in its landmark "FRAND-Einwand" decision (Case No. KZR 36/17, judgment of 5 May 2020).

The FRAND system relies on the principle that standard users and SEP holders reach an agreement on FRAND-

compliant licensing terms through bilateral contract negotiations.

While FRAND does not mandate uniform conditions, it allows differentiation based on objective factors such as market conditions, volume discounts, or risk allocation. Therefore, conditions may vary based on the licensee's position or technology use. However, any differentiation must be justifiable and non-discriminatory. SEP holders must demonstrate fair practices, potentially requiring disclosure of existing agreements under confidentiality.

17. Which body(ies), if any, is/are responsible for data protection regulation?

In Germany, data protection regulation is overseen by multiple bodies. Each of the 16 federal states has its own data protection authority, alongside a federal data protection authority. These authorities monitor compliance in both the public and private sectors. At the European level, the European Data Protection Board (EDPB) plays a crucial role. Established by the GDPR, the EDPB ensures consistent application of data protection rules across the EU. It comprises representatives from national data protection authorities of EU/EEA countries and the European Data Protection Supervisor. The European Commission participates without voting rights. The EDPB provides guidance on GDPR interpretation, advises on data protection matters and new legislation, and issues binding decisions in cross-border disputes. It is supported by a secretariat from the European Data Protection Supervisor.

18. Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

Data protection in Germany is primarily governed by the EU General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG). The Telecommunications Digital Services Data Protection Act (TDDDG) additionally regulates telecommunications secrecy and data protection for telecommunications and digital services.

The GDPR ensures that personal data is processed lawfully (see Article 6 GDPR), fairly and in a transparent manner for specified purposes and imposes various obligations on companies. They must maintain records of processing activities (Article 30 GDPR), providing a comprehensive overview of their data processing operations. In case of data breaches, controllers are required to notify the supervisory authority and, in certain cases, the affected individuals (Article 33, 34 GDPR). Companies must implement appropriate technical and organizational measures to ensure data security (Article 32 GDPR), which may include encryption, regular testing, and measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems. In many cases, organizations are required to appoint a data protection officer (Article 37 GDPR) to oversee compliance and act as a point of contact for data subjects and supervisory authorities. Transfers of personal data to third countries outside the EU/EEA are subject to strict requirements (Chapter V GDPR), often necessitating appropriate safeguards such as standard contractual clauses or binding corporate rules.

The GDPR also grants data subjects extensive rights, including the right to information, access, rectification, erasure, and data portability.

The BDSG complements the GDPR, providing specific local rules for data processing by public bodies and addressing particular processing situations. The TDDDG focuses on the protection of privacy in telecommunications and digital services, such as restrictions on storing information on user devices (Section 25 TDDDG).

19. What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

The maximum sanctions for data protection breaches are primarily set by the GDPR. For the most serious infringements, fines can reach up to EUR 20m or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83 (5) GDPR). Less severe breaches may incur fines up to EUR 10m or 2% of annual turnover (Article 83 (4) GDPR). The German Federal Data Protection Act (BDSG) also provides for criminal penalties in certain cases, including imprisonment up to three years (Section 42 BDSG). Additionally, the TDDDG allows for fines up to EUR 300,000 for specific telecommunications and digital services-related infringements (Section 28 (2) TDDDG).

20. Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

Usually, technology contracts in Germany include clauses that mandate compliance with applicable data privacy laws as cardinal obligations. Beyond such general

clauses, these contracts typically do not and should not include references to external data protection regimes, as the GDPR is directly applicable. It is uncommon for purely domestic contracts to reference external regimes like the CCPA. However, data processing agreements (as per Art. 28 GDPR) commonly contain more detailed references to specific data protection requirements, which may include mentions of other relevant data protection regimes when international aspects are involved.

21. Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

Currently, no single body in Germany is specifically responsible for AI regulation. As the EU AI Act is being implemented, Germany has 12 months to designate market surveillance authorities for AI systems. The Federal Network Agency (Bundesnetzagentur) is a strong candidate, with some suggesting its development into a comprehensive digital authority. The Data Protection Conference (DSK) has also positioned itself for this task. Sectoral authorities, like BaFin for finance, are expected to retain roles in specific areas. Other bodies, such as the Federal Office for Information Security (BSI) and Federal Cartel Office (Bundeskartellamt), are involved in AI security and competition aspects.

22. Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

The primary law governing AI in the EU, including Germany, is the new EU AI Act. This comprehensive framework addresses risks associated with AI applications while promoting innovation. It adopts a risk-based approach, categorizing AI systems into four risk levels: unacceptable (banned), high (strictly regulated), limited (transparency requirements), and minimal (freely usable). Key aspects include prohibiting unacceptable risk AI practices, setting stringent requirements for high-risk AI systems, establishing obligations for deployers and providers, requiring conformity assessments before market introduction, and enforcing compliance through European and national governance structures. High-risk AI systems must undergo risk assessments, use quality data sets, ensure traceability, provide documentation, implement human oversight, and maintain robust security. The AI Act is part of a broader EU initiative including the AI Innovation Package and the Coordinated Plan on AI, aiming to balance safety, fundamental rights protection, and AI innovation. While already adopted, its full implementation in Germany is still in progress, with national authorities working on aligning their regulatory frameworks with the Act's requirements.

23. Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI?

The EU AI Act introduces specific legal provisions for Large Language Models and generative AI, particularly under the category of general-purpose AI models (Articles 51-55). It establishes distinct regulations for these models, especially those with systemic risk (Article 51). Providers of general-purpose AI models must maintain technical documentation, provide information to AI system providers integrating their models, comply with copyright laws, and publish summaries of training data content (Article 53). For models with systemic risk, additional obligations apply, including performing model evaluations, assessing and mitigating systemic risks, reporting serious incidents, and ensuring cybersecurity protection (Article 55).

In addition to the AI Act, the deployment of generative AI solutions must comply with other relevant legal frameworks, such as works council co-determination rights and data protection regulations when processing personal data.

24. Do technology contracts in your jurisdiction typically contain either mandatory (e.g mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

The EU has introduced model contractual AI clauses for use in AI procurements, with two versions available: one for high-risk AI and one for non-high-risk AI. These standard contractual clauses are designed for public bodies procuring AI systems developed by external suppliers.

For the private sector, there is no established standard for addressing AI risks in B2B contracts, as European and national legal frameworks on AI liability are still under development. However, to adequately address risks in private contracts, parties may consider including provisions that address:

- Data quality and management, including data

protection and privacy compliance
- Transparency and explainability of AI decision-making processes
- Performance metrics and quality assurance measures
- Liability and indemnification for AI-related errors or harm
- Ethical AI use and compliance with relevant guidelines or standards
- Intellectual property rights related to AI systems and training data
- Cybersecurity measures and incident response protocols
- Regular auditing and monitoring of AI system performance
- Human oversight and intervention mechanisms
- Provisions for system updates, maintenance, and decommissioning

25. Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Software and technology contracts involving AI systems typically contain provisions regarding intellectual property rights and ownership of outputs. This is especially relevant for solutions in the field of generative AI, such as text or image generators. Contracts usually specify that users obtain extensive usage rights to the AI-generated content. This is typically the default position, but the scope of these rights can vary. Many contracts also allow for commercial use of AI-generated content, particularly in paid versions of the service. However, some providers may restrict commercial use in free versions.

When procuring AI solutions, companies should ensure that contracts clearly differentiate between the training phase, specifying which content can be used for training the AI model, and the application phase, defining ownership and usage rights of the AI-generated outputs.

26. What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

The European Union has taken a leading global role in establishing regulations for the application of distributed ledger and blockchain technology in the financial market. Key initiatives include the Regulation on Markets in Crypto-Assets (MiCAR), the Transfer of Funds Regulation (TFR), and the Regulation on the establishment of a DLT Pilot Regime. These legislative measures aim to establish a consistent, standardized legal framework across Europe for the lawful handling and further experimentation with DLT in the financial sector. Through this unified regulatory approach, the EU acknowledges the potential of distributed ledger technology and seeks to address various challenges it presents, including those related to financial stability, market integrity, and consumer protection. Ultimately, these efforts are expected to foster greater trust among market participants.

In Germany, the regulation of blockchain technology and digital assets is further governed by several key laws. The German Banking Act (Kreditwesengesetz – KWG) includes crypto-assets and crypto custody business as financial services, requiring authorization from BaFin. The German Electronic Securities Act (Gesetz über elektronische Wertpapiere – eWpG) allows for the issuance of electronic securities, including those based on blockchain. The Fund Jurisdiction Act (Fondsstandortgesetz – FoStoG) regulates investment funds that incorporate crypto-assets. Lastly, the German Crypto Asset Transfer Regulation (KryptoWTransferV) implements the FATF's "travel rule" to prevent money laundering through enhanced due diligence for crypto-asset transfers. These regulations aim to create a stable and trustworthy legal environment for the adoption and use of blockchain technologies and digital assets in Germany.

27. Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

Search engines and marketplaces are primarily regulated by two key EU legislations: the Digital Services Act (DSA) and the Digital Markets Act (DMA).

The DSA provides a unified set of rules to protect users and combat illegal online content. It regulates obligations and liability of intermediary services, including hosting providers, online platforms, marketplaces, and search engines (Article 2 DSA). Key provisions include:

- Content moderation obligations (Article 16 DSA)
- Transparency reporting requirements (Article

24 DSA)
- Internal complaint-handling and dispute-settlement mechanisms (Articles 17-18 DSA)
- Ban on deceptive practices like dark patterns (Article 25 DSA)
- Restrictions on ads targeting minors based on profiling (Article 28 DSA)
- Traceability requirements for traders on online marketplaces (Article 30 DSA)

Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) face additional obligations, including systemic risk assessments (Article 34 DSA), annual risk assessments (Article 35 DSA), and maintaining public repositories of displayed advertisements (Article 39 DSA).

The DMA targets "gatekeepers" (Article 3 DMA) – large digital platforms providing "core platform services" in at least three Member States. It aims to ensure fair and open digital markets by:

- Requiring interoperability with third-party services (Article 7 DMA)
- Allowing access to data generated on their platforms (Article 6(10) DMA)
- Prohibiting self-preferencing in rankings (Article 6(5) DMA)
- Ensuring users can connect with businesses outside the platform (Article 5(5) DMA)

In addition to these specific regulations, search engines and marketplaces must also comply with general data protection laws, particularly the General Data Protection Regulation (GDPR). Of particular importance in this context is the "right to be forgotten" (Article 17 GDPR), which allows individuals to request the deletion of personal data, including the removal of search results linking to such information.

28. Please summarise the principal laws (present or impending), if any, that govern social media, including a brief explanation of the general purpose of those laws?

In Germany, social media platforms operate within a complex regulatory framework that combines EU-wide regulations with national laws. The European Digital Services Act (DSA), forms a cornerstone of this framework, introducing comprehensive obligations for online platforms, with particularly stringent rules for very large platforms. It mandates content moderation procedures, transparency measures, and user protection mechanisms.

Complementing this at the national level is the German Digital Services Act (DDG), which i.a. contains provisions on dealing with violations of the law by users of digital services. The DDG replaced the Telemedia Act (TMG) and large parts of the Network Enforcement Act (NetzDG), which prior to the DSA required social media platforms to implement effective complaint management systems and promptly remove illegal content.

The Interstate Treaty on Media (Medienstaatsvertrag) further regulates media diversity and user protection across various online platforms, including social media. Additionally, child protection regulations such as the Youth Protection Act aims to safeguard minors from harmful content on social media and other online platforms. The regulatory landscape remains dynamic, with ongoing adjustments to address emerging challenges in the digital sphere, requiring social media companies operating in Germany to continuously adapt to ensure compliance while maintaining their services.

29. What are your top 3 predictions for significant developments in technology law in the next 3 years?

First, following the adoption of the AI Act, the primary focus will shift to its implementation and practical enforcement by supervisory authorities across EU member states, potentially leading to new regulatory guidance and case law clarifying its application. Second, substantial changes in internal compliance frameworks are expected due to the reform of the Product Liability Directive, the introduction of the new Product Safety Regulation, and the upcoming AI Liability Directive, which will reshape how companies approach risk management and product development in the tech sector. Third, the European Commission's initiative for a new Digital Networks Act aims to regulate digital infrastructure on a European scale. This controversial proposal could potentially reshape the internet landscape by introducing a "sender pays" model, where large content providers would be required to contribute to network costs.

30. Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Provisions addressing sustainability, net-zero obligations, and similar environmental commitments are not yet common in German technology contracts, but they are becoming more prevalent. While specific

sustainability clauses are still emerging, many companies, especially larger ones, are already incorporating broader Environmental, Social, and Governance (ESG) criteria into their compliance obligations. This trend is likely to continue, with environmental commitments expected to become more standard in technology contracts as awareness of sustainability issues grows and regulatory pressures increase.

Contributors

Thomas Britz, LL.M (Berkeley)
Associated Partner
britz@lindenpartners.eu

Dr. Moritz Indenhuck
Partner
indenhuck@lindenpartners.eu