COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Germany

TMT

Contributor

Orrick, Herrington & Sutcliffe LLP

Christian Schröder

Partner | cschroeder@orrick.com

Tobias Lantwin

Scientific Assistant | tlantwin@orrick.com

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. What is the regulatory regime for technology?

In Germany, there is no regulatory regime that specifically regulates technology as such. Instead, a multitude of rules governing technology are scattered across a variety of legislative acts. The regulation of technology involves many different aspects (such as telecommunications, privacy, cybersecurity or e-commerce) and spans several areas of law. The following list outlines the most relevant legislation covering technology which are specific to Germany (there are also a number of wider European laws governing technology which are not discussed in this chapter).

- Electronic communications are regulated in the Telecommunications Act ('Telekommunikationsgesetz', '**TKG**') and Telemedia Act ('Telemediengesetz', '**TMG**') which are based, in part, on several EU Directives, among them the Directive (EU) 2018/1972 ('European Electronic Communications Code', '**EECC**'), the eCommerce Directive 2000/31/EC ('**eCommerce Directive**') and other former EU Directives that have in the meantime been replaced by the EECC.
- Data privacy aspects relating to technology are regulated by the General Data Protection Regulation ('**GDPR**'), the Federal Data Protection Act ('Bundesdatenschutzgesetz', '**BDSG**') and the Telecommunications-Telemedia Data Protection Act ('Telekommunikation-Telemedien-Datenschutzgesetz', '**TTDSG**'), the latter of which is in part based on the ePrivacy Directive 2002/58/EC ('**ePrivacy Directive**').
- Sector-specific cybersecurity requirements for operators of essential or digital services arise under the NIS Directive (EU) 2016/1148 which have been transposed into national law through the IT Security Act ('IT-Sicherheitsgesetz') that led to further changes in several laws, among which have been the TKG and TMG, as well as the Federal Office for Information Security Act ('BSI-Gesetz', 'BSIG').
- Protection of computer software and databases is provided via Copyright protection offered under the German Copyright Act ('Urheberrechtsgesetz', '**UrhG**').
- Consumer rights in relation to contracts for the supply of digital content and digital services are regulated in Directive (EU) 2019/770 which has been transposed into national law in provisions of the German Civil Code ('Bürgerliches Gesetzbuch', '**BGB**').

2. Are communications networks or services regulated?

Yes, communications networks and/or services are regulated by the Telecommunications Act (TKG). It provides the legal framework for the operation of telecommunications networks and facilities and for the provision of telecommunications services. 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 throughout Germany (Sec. 1(1) TKG).

3. If so, what activities are covered and what licences or authorisations are required?

Under German law, no license or authorisation is required for the commercial operation of telecommunications networks or for the provision of telecommunications services. Instead, electronic communications networks and services are subject only to a 'general authorisation' (as required in Article 12 EECC and formerly under Directive 2002/20/EC). This general authorisation covers, among others, the provision of electronic communications networks and services, usage of radio spectrum in relation to electronic communications networks and services and the right to have applications for the necessary rights to

install facilities and/or for the necessary rights of use for numbering resources considered.

Thus, a telecommunications operator or service provider is only required to notify the Federal Network Agency ('Bundesnetzagentur') without undue delay of any intended commencement, change or termination of the operator's/service provider's activity and of any changes to its name or company name, legal structure or address (Sec. 5(1) TKG).

4. Is there any specific regulator for the provisions of communications-related services?

The provision of communications-related services is subject to regulatory supervision by the Federal Network Agency ('Bundesnetzagentur', '**BNetzA**'). It is tasked with ensuring fair competition and transparency in, among others, the telecommunications sector. In addition, ensuring telecommunications and postal service providers' compliance with privacy obligations which is subject to regulatory supervision by the Federal Commissioner for Data Protection and Freedom of Information ('Bundesbeauftragter für den Datenschutz und die Informationsfreiheit', '**BfDI**').

5. Are they independent of the government control?

As an upper federal authority, the BNetzA is subject to regulatory supervision by the Federal Ministry for Economic Affairs. The BfDI, in contrast, is a supreme federal authority and thus independent from any regulatory supervision.

6. Are platform providers (social media, content sharing, information search engines) regulated?

In Germany, platform providers are regulated by a complex multitude of laws that constitute different degrees of content moderation obligations, depending on the respective kinds of platform providers.

Pursuant to the general principle of Sec. 7, 8-10 TMG (which are based on the eCommerce Directive), host and access providers are only responsible for their own contents and are generally not required to monitor third party information transmitted or hosted by them or to investigate circumstances that indicate illegal activities. However, once host providers have become aware of illegal activities or third party information, they are required to remove the information or to disable access to it without undue delay (so-called 'notice and takedown') and are henceforth liable for such information.

In addition, certain kinds of platforms are subject to a variety of content moderation obligations. These stem from, among others, the NetzDG ('Netzwerkdurchsetzungsgesetz') which aims at combatting hate crimes and other illegal conduct on social networks by requiring user reporting procedures. Other acts that contain content moderation obligations include the AVMSD (Directive (EU) 2018/1808) that obliges video sharing platforms to protect minors from harmful content and the general public from hate and violent messages as well as terrorist, racist and xenophobic material and child pornography. These rules have been transposed into national law across various laws, among them the TMG (Sec. 10a-10b), the Media State Treaty ('Medienstaatsvertrag', 'MStV') and the Youth Media Protection State Treaty ('Jugendmedienschutz-Staatsvertrag', 'JMStV'). Other child protection regulations (such as the Youth Protection Act) provide for similar obligations. Under Regulation (EU) 2021/784 ('TCO' Regulation), host providers are obliged to remove or disable access to terrorist contents within one hour. Finally, the new Digital Services Act ('DSA') will also include rules regarding platforms' content moderation practices once enacted.

In respect of copyright-infringing content, Article 17 of Directive (EU) 2019/790 ('DSM' Directive) stipulates certain content blocking obligations for powerful platforms that host and make available to the public large quantities of copyrighted materials.

Finally, online marketplaces are subject to newly introduced information and transparency obligations in the German Act against Unfair Competition ('Gesetz gegen den Unlauteren Wettbewerb', 'UWG') that concern product rankings and customer reviews.

7. If so, does the reach of the regulator extend outside your jurisdiction?

Of the regulations mentioned above, only the proposed DSA will have genuine extra-territorial reach. However, the NetzDG applies to online platforms regardless of where the platform is situated in cases where hate speech or other content that falls within the scope of the NetzDG may be uploaded or viewed by a German citizen. Rules stemming from the EU Regulations and Directives mentioned above are binding for all EU/EEA Member States.

8. Does a telecoms operator need to be domiciled in the country?

No, a telecoms operator does not need to be domiciled in Germany. However, an address of a general representative domiciled in Germany must be given that is authorised to receive correspondence from the BNetzA.

9. Are there any restrictions on foreign ownership of telecoms operators?

Currently, there are no restrictions on foreign ownership of telecommunications operators in place in Germany. Instead, Sec. 2(4) TKG provides that remaining obstacles to the investment in, and the provision of, electronic communications networks, electronic communications services, associated facilities and associated services throughout the Union shall be reduced.

10. Are there any regulations covering interconnection between operators?

Yes, there are rules on access and interconnection between operators in Sec. 20 et seq. TKG. To ensure users' communications, the provision of telecommunications services and their interoperability within the EU, operators of public telecommunications networks are permitted and, at the request of another undertaking, required to negotiate on an offer of access and interconnection.

The BNetzA can also require undertakings that control access to end-users to interconnect their telecommunications networks with those of other undertakings or impose further obligations if this is necessary to ensure end-to-end connectivity and the provision and interoperability of services.

11. If so are these different for operators with market power?

Undertakings with considerable market power are subject to additional, more specific rules set out in Sec. 24 et seq. TKG. The BNetzA can require undertakings with considerable market power to provide access to other undertakings, if it is otherwise to be expected that the development of a competitive retail market would be impeded and the interests of end-users would be adversely affected. In addition, they can be required by the BNetzA to adhere to transparency obligations and to provide that access agreements are non-discriminatory.

12. What are the principal consumer protection regulations that apply specifically to telecoms services?

General consumer protection regulations are set out in Sec. 51 et seq. TKG. These rules, inter alia, prohibit operators of public telecommunications networks and providers of publicly accessible telecommunications services from applying discriminatory conditions and requirements vis-à-vis end-users based on nationality, residence or location of an establishment. In addition, a consumer of such services must be provided with pre-contractual information in a clear and understandable form on a permanent data carrier. The consumer must also be provided with a clear and easy to read summary of the contract in accordance with the model in the Implementing Regulation (EU) 2019/2243. Certain requirements also apply to the content of invoices.

In addition, undertakings may not offer contracts with an initial term longer than 24 months and they are required to offer consumers a contract with an initial term of no more than twelve months prior to the conclusion of the contract. These rules are complemented by consumer protection rules in the German Civil Code (BGB) that limit automatic contract term extensions or renewals leading to such an extension (Sec. 309(9)(b) BGB).

Other obligations include a right to reduce the contractually agreed remuneration and a right to extraordinary termination in case of an improper performance of a contract with regard to certain quality parameters. In the event of a disruption, the consumer has a right to immediate troubleshooting and the payment of a contractual penalty in the event of delays. Other obligations include a right to a seamless change of provider and call number portability.

13. What legal protections are offered in relation to the creators of computer software?

Computer software can be protected as an original work pursuant to Sec. 69a et seq. German Copyright Act (UrhG). These provisions are based on Directive (EU) 2009/24/EC on the legal protection of computer programs. Pursuant to Sec. 69a(3) UrhG, a computer program can be protected as a literary work if it is original in the sense that it is the author's own intellectual creation. The protection for a computer program, as is the case with any other work protected by copyright, extends only to its expression in any form and not to the idea or the principles that underlie a computer program (Sec. 69a(2) UrhG). The copyright is held by the author(s) of the work, i.e., the software developer(s).

Although copyright is not transferable under German law, a license may be granted pursuant to Sec. 31 et seq. UrhG. In case of an employment or service relationship, Sec. 69b UrhG stipulates that the employer is exclusively entitled to exercise all proprietary rights to the computer program unless otherwise agreed. The copyright to a computer program grants the right holder the right to authorise or prohibit reproductions, adaptations, the distribution of reproductions including rental and wire or wireless public communication of the computer program.

So-called 'computer-implemented inventions' may also be eligible for patent protection under German patent law. However, patent protection does not extend to algorithms or computer programs.

14. Do you recognise specific intellectual property rights in respect of data/databases?

Data in itself, is not eligible for intellectual property protection. However, databases can be subject to copyright protection as a database work pursuant to Sec. 4(2) UrhG if the selection or arrangement of the database's contents constitute an author's own intellectual creation. The copyright protection for database works does not extend to a database's contents. Another form of protection is stipulated in Sec. 87a et seq. UrhG pursuant to which a qualitatively and/or quantitatively substantial investment of a maker of a database is protected via a related (or sui generis) right of the database maker. While database works are protected to a similar degree as computer programs are (see question 7), the related right granted for databases extends only to the right to reproduce and distribute the database as a whole or a qualitatively or quantitatively substantial part of the database and to make it available to the public. Both the protection for database works as well as the sui generis right for databases are based on Directive 96/9/EC on the legal protection of databases.

15. What key protections exist for personal data?

In Germany, the protection of personal data is primarily governed by the General Data Protection Regulation ('GDPR') and the Federal Data Protection Act ('BDSG'). The GDPR has introduced fundamental data protection principles (Article 5 GDPR), specific lawful bases for the processing of personal data (Article 6 et seq. GDPR) and a multitude of data subject rights (Article 12 et seq. GDPR), including, among others, information rights, a right of access and to be forgotten as well as restrictions to automated decision-making and profiling. The GDPR also introduced data breach notification obligations, some of which must be fulfilled within a narrow 72-hour timeframe (Article 33, 34 GDPR). These data protection rules can be enforced through significant fines or claims for immaterial damages in case of non-compliance (Article 82, 83 GDPR).

Special regulations on the protection of personal data relating to the use of telecommunications services and telemedia are provided in the Telecommunications Telemedia Data Protection Act ('TTDSG'). Sec. 3 TTDSG stipulates the secrecy of communications that, among others, telecommunications service providers and telecommunications networks operators are obliged to maintain. In addition, Sec. 25 TTDSG stipulates that the storing of information on the end user's terminal equipment or the accessing of information already stored on the terminal equipment shall only be permitted if the end-user has consented on the basis of clear and comprehensive information. This requirement is particularly relevant to the use of cookies. The conference of the German data protection supervisory authorities has released guidance on the TTDSG and the rules applicable to cookies on 20 December 2021 and implements the e-Privacy Directive.

16. Are there restrictions on the transfer of personal data overseas?

Extensive restrictions to transfers of personal data to third countries outside of the EU and the European Economic Area ('EEA') are stipulated in chapter V of the GDPR (Article 44 et seq.) to ensure that the level of protection guaranteed by the GDPR is not undermined. Chapter V provides for a multitude of different grounds for transfer. A transfer to a third country may take place on the basis of an adequacy decision by the European Commission (Article 45 GDPR) or, in the absence of such decision, on the basis of appropriate safeguards (Article 46 GDPR) or derogations set out in Article 49 GDPR. The derogations of Article 49 GDPR are, however, in the view of the European Data Protection Board only seldom applicable.

A transfer may take place without further specific authorisation on the basis of an adequacy decision in which the European Commission has decided that a specific third country, a territory or one or more specified sectors within that third country ensures an adequate and "essentially equivalent" level of protection. There are a handful of adequacy decisions currently in place, with countries such as Canada (only partial adequacy), Israel, Japan, South Korea, New Zealand, Argentina or Switzerland among them.

In the absence of an adequacy decision, any transfer must either be justifiable based on one of the derogations under Art. 49 GDPR or be based on appropriate safeguards that need to be provided by the controller or processor. Appropriate safeguards are, among others, Standard Contractual Clauses ('SCC') or Binding Corporate Rules ('BCR'). Most commonly, transfers rely on the implementation of SCC. In June 2021, the EU Commission released standard contractual clauses to overhaul and replace the existing three sets of SCC released under the Data Protection Directive 95/46/EC. The new SCC (Commission Implementing Decision (EU) 2021/914) contain four modules that cover different controller/processor transfer constellations. The old sets of SCC will be phased out until 27 December 2022. However, it is currently unclear how transfers to data importers who are themselves subject to the GDPR, can be justified as the SCC of June 2021 do not cover these data transfers. The EU Commission is currently preparing separate SCC for such kind of transfers.

The new SCC also take into consideration that, prior to any transfer, the laws and practices of the third country applicable to the processing must be analysed by the parties involved in the transfer. This 'transfer impact assessment' ('**TIA**') requires the parties to put in place supplementary safeguards such as technical, organisational and contractual measures to ensure compliance with GDPR transfer requirements and SCC clauses. These requirements were established in the CJEU's Schrems II judgment of 16 July 2020 (C-311/18).

17. What is the maximum fine that can be applied for breach of data protection laws?

Pursuant to Article 83(4)-(6) GDPR, the maximum fine ranges from EUR10m to EUR20m or, in the case of an undertaking, 2% to 4% of the total worldwide annual turnover of the preceding financial year, respectively, whichever is higher. The amount of an administrative fine is dependent on the circumstances of each individual case and shall be effective, proportionate and dissuasive (Article 83(1), (2) GDPR). The European Data Protection Board has issued Guidance on the calculation of fines in its Guidelines 04/2022 of 12 May 2022.

Pursuant to Sec. 28(2) TTDSG, the maximum fine amount possible for a breach of telecommunications and telemedia data protection rules is EUR300,000.

18. What additional protections have been implemented, over and above the GDPR requirements?

The GDPR contains opening clauses that give room for national legislation to regulate certain privacy-related aspects. Germany has made use of some of these opening clauses in the BDSG. Most importantly, Sec. 26 BDSG contains special rules with regard to the processing of employee data and the requirements for consent in employment relationships. Pursuant to Sec. 26(1) BDSG, employee personal data shall only be processed if this is necessary for purposes of entering into, performing or terminating an employment relationship or for the exercise or fulfilment of rights and obligations stemming from laws, collective agreements, service agreements or works agreements. In Sec. 42 BDSG, the German legislator has also set out penal provisions.

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

Under German law, the use of cloud-based services is generally lawful. Some restrictions arise from sector-specific regulations. For instance, there are specific requirements concerning outsourcing of activities and processes that may regularly apply to the use of certain cloud-based services in Sec. 25b Banking Act ('Kreditwesengesetz', 'KWG'), Sec. 5(3) Stock Exchange Act ('Börsengesetz', 'BörsG'), Sec. 80(6) Securities Trading Act ('Wertpapierhandelsgesetz', 'WpHG') and Sec. 32 Insurance Supervision Act ('Versicherungsaufsichtsgesetz', 'VAG').

In addition, extensive guidance on the use of cloud-based services and outsourcing has been issued by the conference of the German data protection supervisory authorities ('Orientierungshilfe – Cloud Computing' of 9 October 2014) and the Federal Financial Supervisory Authority ('BaFin') ('Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter of November 2018). Further, the Federal Security Agency (BSI) has issued a catalogue containing criteria for the secure use of clouds which has become a widely accepted standard and may also be required to be adhered to by many public entities ('Cloud Computing Compliance Criteria Catalogue – C5:2020 '). The European Data Protection Board is currently investigating into the use of cloud services and it is expected to get further guidance within the course of 2022. The various State data protection supervisor authorities also issue guidance on the use of specific cloud services.

20. Are there specific requirements for the validity of an electronic signature?

Requirements for the validity of an electronic signature are derived from the eIDAS Regulation (EU) 910/2014. In Germany, there are several provisions that concern electronic signatures and trust services. The requirements under the eIDAS regulation are governed by the Trust Services Act ('Vertrauensdienstegesetz', 'VDG'). It regulates electronic signatures, electronic seals and the validation of these methods of identification.

In addition, Sec. 126a of the German Civil Code ('BGB') sets out the formal requirements that need to be fulfilled when a written form required for certain legal acts is to be replaced by an electronic signature. However, the electronic form is seldom used as it requires a certified identification unit.

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

Under certain circumstances that have been outlined further by the Federal Labour Court ('BAG') (see, e.g., decision of 24 January 2013, 8 AZR 706/11), the outsourcing of IT services may be considered a "transfer of an undertaking" ('Betriebsübergang') (or of a part of an undertaking) pursuant to Sec. 613a BGB. This requires that the identity of the company be preserved. In this respect, relevant criteria for the assessment are, inter alia: the nature of the business in question, whether a transfer of tangible assets has taken place, the value of intangible assets at the time of the transfer, the takeover of the main workforce by the new owner, the transfer of customers and supplier relationships, the degree of similarity between the activities carried out before and after the transfer and the duration of any interruption of such activities.

In case an outsourcing is deemed a transfer of an undertaking, the employees, assets or third-party contracts would transfer automatically to the supplier.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

Questions around the liability of A.I.-related malfunctions are subject of lively debates in Germany. Some scholars argue that damages inflicted by a malfunctioning A.I. may be addressed through existing means of contract or tort law. Others argue that future legislation should provide for strict liability regimes for A.I. manufacturers or operators. Other proposals employ insurance solutions to the A.I. liability issues. In order to address the common lack of a suitable liability subject, some scholars also want to assign an own legal personality to A.I. systems (so-called "e-person").

Apart from the proposed A.I. Act, on a European level, the Commission also started an initiative to address liability issues as part of an overhaul of the Product Liability Directive 85/374/EEC.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

Cybersecurity obligations are scattered across different laws in Germany. Apart from Article 32 GDPR which addresses cybersecurity obligations for controllers and processor that process personal data there are several sector-specific obligations in other laws. In the telecommunications sector, Sec. 165 TKG stipulates several technical and organizational security measures for telecommunications operators and service providers. Telemedia providers are subject to security obligations under Sec. 19 TTDSG. Operators of critical infrastructures face a multitude of security obligations pursuant to Sec. 8a BSIG to ensure availability, integrity, authenticity and confidentiality of their IT systems, components or processes.

Hacking and DDoS can constitute several criminal offences under German penal law. Sec. 202a-202d of the German Criminal Code ('Strafgesetzbuch', 'StGB') penalise the spying and interception of data and the preparation of such acts, as well as the unauthorized receiving of data. In addition, Sec. 303a-303b StGB penalise the alteration of data and the manipulation of data processing operations. These offences are subject to punishment by imprisonment for up to two or three years or to a fine.

24. What technology development will create the most legal change in your jurisdiction?

The technological development most likely to create significant changes to the German legal landscape is the emergence of Artificial Intelligence. Given initiatives by the EU Commission, there will be changes to a variety of fields, including rules on liability, content moderation and data privacy.

25. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

The lack of clear guidance and the fairly restrictive views on privacy requirements when operating AI based systems put a significant burden on the operation of such systems, in particular, for smaller companies. The new EU laws on AI and the use and sharing of data are steps in the right direction to address these issues.

26. Do you believe your legal system specifically encourages or hinders digital services?

The German government and the EU have developed a better understanding on the needs for promoting digital services but a lot of changes will be needed to truly foster the development and use of digital services.

27. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

The changes will come on the EU level where we expect a new AI Regulation.

Contributors

Christian Schröder
Partner
cschroeder@orrick.com

Tobias Lantwin
Scientific Assistant
tlantwin@orrick.com