

Data Compliance Compass

Navigating safely through the data landscape

September 2024

Data Compliance Compass

In today's data-driven world, it is essential for companies of all sizes to keep to European and national rules regarding the movement of data. Failing to comply can lead to significant fines, reputational damage and even legal action.

Our **Data Compliance Compass** is designed to give you a overview of particularly relevant legislative acts and to point out the most important obligations arising from them.

Contents

| | |
|--|-----------|
| Data Compliance Compass | 1 |
| European legislative acts | 3 |
| Introduction | 3 |
| Overview of the most important European legislative acts | 4 |
| The European rules and regulations in detail | 5 |
| Key | 5 |
| Digital Markets Act | 6 |
| Data Act | 8 |
| General Data Protection Regulation | 10 |
| Data Governance Act | 12 |
| Digital Services Act | 14 |
| AI Act | 16 |
| Open Data Directive | 18 |
| ePrivacy Regulation | 19 |
| Free Flow of Data Regulation | 20 |
| German legislation | 21 |
| Introduction | 21 |
| Overview of the most important German legislative acts | 21 |
| The German legislation in detail | 21 |
| German Act on the Protection of Trade Secrets | 22 |
| German Competition Act | 24 |
| German Federal Data Protection Act | 26 |
| German Digital Services Act | 27 |
| German Act on Data Protection and the Protection of Privacy in Telecommunications and Digital Services | 29 |
| German Act on Copyright and Related Rights | 31 |
| German Act on the Copyright Liability of Online Content-Sharing Service Providers | 32 |
| German Telecommunications Act | 33 |
| German Criminal Code | 35 |

European legislative acts

Introduction

In recent years, the European legislator has taken steps to actively promote regulation of the data and digital economy in response to the enormous changes within society brought about by digital advances. On 19 February 2020, the European Commission published a “European data strategy” which aims to make the European Union (“EU”) a leader in a data-driven society.

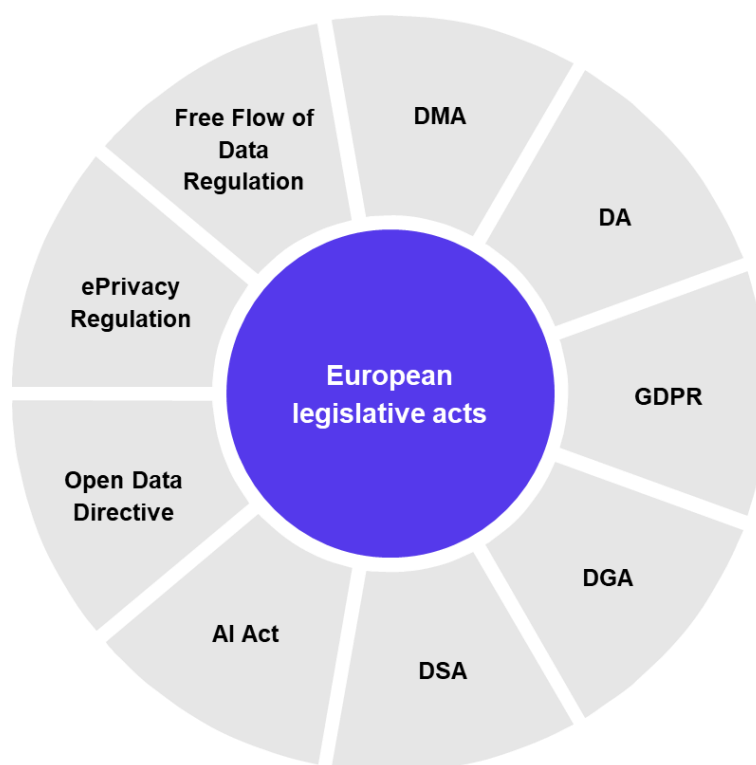
The motivation is to use the opportunities created by the data economy as effectively as possible by removing national barriers and promoting the availability, transparency and interoperability of data. These plans are being driven forward, among other things, by the enactment of the Data Act (“DA”), Data Governance Act (“DGA”) and Open Data Directive.

At the same time, the EU legislator has taken into account the risks to society in terms of the (systemic) threat to fundamental freedoms, above all in the area of personal data. In response to this, it passed the General Data Protection Regulation (“GDPR”), Digital Services Act (“DSA”) and AI Act.

In addition, the Digital Markets Act (DMA) and the application of antitrust and competition regulations are intended to check the power of the big players in the market (gatekeepers). Alongside the DMA, the antitrust and competition regulations of European primary law and national law are also highly relevant in this respect.

Although the new legislation – most recently especially the DSA – presents many challenges in terms of data compliance, we would like to use our [Data Compliance Compass](#) to show you the opportunities and key obligations which come with the creation of a legal framework for the data and digital economy.






Overview of the most important European legislative acts



- **DMA:** contains antitrust-like provisions limiting the market power of “gatekeepers” in the digital economy.
- **DA:** promotes the added value of data through data access rights, including contract law for data and likewise public-law provisions on data access.
- **GDPR:** protects personal data.
- **DGA:** promotes the availability of data, above all by promoting the sharing of protected public data, e.g. for research.
- **DSA:** protects fundamental rights (and freedoms) on the internet by combating illegal content.
- **AI Act:** protects against risks posed by AI to the fundamental rights of individuals.
- **Open Data Directive:** provides that data which is already in the public domain and is held by public-sector bodies should be made available as easily and as freely as possible.
- **ePrivacy Regulation:** based on the GDPR, this Regulation intends to improve the protection of personal data in the field of electronic communications.
- **Free Flow of Data Regulation:** removes obstacles to movement of data, in particular by prohibiting national data localisation requirements.

The European rules and regulations in detail

Key

| | |
|---|--|
|  | Legislative act relates to non-personal data |
|  | Legislative act relates to personal data |
|  | Legislative act is in force |
|  | Legislative act has been adopted but is not yet in force |
|  | Legislative act is in the process of being enacted |

Digital Markets Act



Brief outline:

The Digital Markets Act (DMA) lays down rules for the conduct of certain large digital companies (known as “gatekeepers”) who offer platform services in the digital economy and provide important gateways for business users to reach end users due to their position. To be identified as a gatekeeper, undertakings must also have a significant impact on the internal market and have an “entrenched and durable position” in their activities or foreseeably enjoy such a position in the near future. A presumption of this status applies if quantitative thresholds are exceeded (in terms of annual turnover/market capitalisation and user numbers).

The DMA is intended to ensure the contestability and fairness of markets in the digital sector by imposing extensive rules of conduct on gatekeepers (including regarding data).

Duties/requirements/risks in relation to data:

What is its relationship to other statutes?

The DMA applies in principle parallel to existing antitrust and competition provisions at national and EU levels (Article 1(6) DMA), while at the same time prohibiting the fragmentation of rules in relation to gatekeepers (Article 1(5) DMA).

What obligations are imposed with regard to data?

- Contains a comprehensive, directly applicable list of obligations in Articles 5 and 6 DMA, derived from antitrust decision-making practices from the last 20 years, including: prohibitions on self-preferencing, rules on data use and data interoperability, prohibitions on discrimination, obligations to disclose information, prohibitions on data combination, and (data) access claims.
- Article 7 DMA sets out an obligation to ensure interoperability for number-independent interpersonal communication services (e.g. WhatsApp).
- Article 14(1) of the DMA requires gatekeepers to notify the European Commission about planned concentrations within the meaning of Article 3 of the Merger Regulation under certain conditions. However, there is no obligation to obtain a clearance.

Primary (data protection) addressees of the legislation:

The addressees of the DMA are operators of “core platform services” who provide business users a gateway to reach end users. Core platform services include for example online intermediation services, online search engines, social networks, operating systems, web browsers, etc. The DMA applies to them **if and to the extent** that the operators are identified by the European Commission as gatekeepers.

All services offered in the EU are covered. It is irrelevant where the company’s registered office is based.

Data-related rules of conduct include bans on certain use of data, obligations to establish interoperability and claims by business users, end users and third parties for access to data against gatekeepers, etc.

- Article 20 onwards of the DMA grants the European Commission powers of investigation customary in antitrust law: opening of proceedings, information requirements, inspections at companies and imposition of remedies.
- Third parties are also called on to monitor the gatekeepers' compliance with the DMA, for example by filing complaints with the European Commission (also using the whistleblowing tool), and by private enforcement before national courts.

What are the penalties for breach of duty (risk)?

For infringements: fines of up to 10% of the company's worldwide annual turnover, and up to 20% in the event of a recurrence (from Article 30 DMA), as well as structural remedies in the event of systematic non-compliance.

Practical tips:

The scope of application of the DMA is relatively small, especially due to the high quantitative thresholds for the presumption of gatekeeper status (Article 3(2) DMA). Up to now, only seven gatekeepers have been designated (Alphabet, Amazon, Apple, Booking, ByteDance, Meta and Microsoft). If the thresholds are exceeded and an undertaking is designated as a gatekeeper by the European Commission, compliance with the DMA's rules of conduct (including data-related obligations) must be established within six months of designation (Article 3(10) DMA) and, among other things, demonstrated in a compliance report (Article 8(1) DMA).

Companies which do not qualify as gatekeepers themselves are advised to examine their own options for action under the DMA. This applies in particular to rights to access data and data access already granted by gatekeepers that may be useful for companies' own business models. The gatekeepers' compliance with the DMA should also be monitored on an ongoing basis in order to be able to take action against behaviour that is detrimental to one's own company.

Even if the provisions of the DMA do not apply (for instance because a company is not a gatekeeper), the antitrust and competition law provisions of European primary law (TFEU) or national law (in Germany the German Competition Act (*Gesetz gegen Wettbewerbsbeschränkungen, GWB*)) may be relevant. Data access rights, for example, may also arise from these provisions.

Data Act



Brief outline:

In the Data Act (“DA”), the EU aims to ensure fairness in the allocation of value from data, which has largely been untapped up to now.

The DA is intended to remove the legal, economic and technological obstacles that have so far prevented data from being used to its full potential, thereby promoting greater data utilisation and a flourishing data economy in the EU by redefining the legal framework for data access and its promotion.

While previous legislation on data was primarily aimed at protecting data, the Data Act takes a diametrical approach and is aimed at the commercial usability of data.

Among other things, it is designed to establish access rights to data for the private and public sectors.

Effective date: 11 January 2024

Obligations/requirements/risks in relation to data:

What legal aspects of data are covered?

The DA covers five key areas of regulation for access to and use of data in the EU:

- The right of users of IoT devices and related services to access and use user-generated data (both B2B and B2C data sharing) (Articles 3 to 5 DA)
- Prohibition of unfair contractual clauses in standardised data licence agreements to prevent abuse of contractual imbalances in contracts with companies (Article 13 DA) – a kind of B2B review of general terms and conditions
- Right of public-sector authorities to access and use data (B2G) (Articles 14 to 22 DA)
- Facilitation of switching between one data processing service and another (in particular cloud and edge providers), putting in place safeguards against unlawful data transfers (Articles 23 to 26 DA)
- Requirements for interoperability of data processing services and for international data transfer, protection from access by third states (Articles 27 to 32 DA)

Primary (data protection) addressees of the legislation:

Article 1(3) of the DA sets out the addressees of the DA: almost every company active in the EU that collects or processes data, uses it in its products or offers related services is potentially affected.

For example: providers of IoT products (Articles 3 to 5 DA), including product manufacturers and cloud providers, and all types of data holders.

All services active in the EU are covered, regardless of where the company’s registered office is based, and the Regulation applies across all sectors and industries.

Small and micro enterprises are given special treatment by being exempt from the obligations of Chapter II (obligations on sharing of data).

What other rights and obligations are established in relation to data?

- IoT devices must be designed and manufactured, and related services must be designed and provided, in such a manner that product and service data is available to the user by default in a simple, secure, free and comprehensive machine-readable format (Article 3(1) DA) = “accessibility by design”.
- Contains pre-contractual information requirements regarding the scope, storage and options for accessing generated data of an IoT device and the related service (Article 3(2),(3) DA).
- Users have to be able to access data free of charge (Article 4 DA).
- If the user requests that data is made available to third parties, the third party may only use it to meet its obligation towards the user and has to delete it afterwards (Article 6 DA).
- Any compensation that the data holder receives for providing its data to data recipients must be reasonable and non-discriminatory in the case of data licence agreements between enterprises (Article 9(1) DA).
- A provider of an application in which smart contracts are used must fulfil the essential requirements of Article 36 of the DA.

What are the penalties for breach of duty (risk)?

To be determined by the EU Member States. Penalties of up to €20 million or 4% of total worldwide annual turnover are possible.

Practical tips:

During a project to implement the DA, it should first be determined whether the company sells IoT products (and related services) that fall within the scope of the DA – for the definition, see Article 2(5) of the DA. The next step is to evaluate where the most urgent need for action exists and how the obligations of the DA can be implemented on the basis of a holistic approach. The focus should initially be on obligations that have an impact on development and product design (e.g. “access by design”).

The DA strategy to be developed must also cover processes with regard to requests to release data. It is important to know that business secrets do not have to be disclosed under certain, albeit high, conditions (Article 4(6) to (9) DA). According to recital 116 of the DA, the limits of data sharing under antitrust and competition law must also be observed (antitrust prohibition on sharing of information under section 1 of the German Competition Act and Article 101 of the Treaty on the Functioning of the European Union (TFEU)).

It is also recommended that technical protection measures be taken to prevent unauthorised use of data when providing data to third parties (Article 5 DA), which is generally allowed under data licence agreements (Article 11 DA).

General Data Protection Regulation



Brief outline:

The General Data Protection Regulation (“GDPR”) harmonises the legal requirements for the processing of personal data in the EU. In this Regulation, the EU aims to harmonise data protection in the EU in order to avoid a patchwork of different rules in the various EU countries. Instead, a uniform level of data protection has applied throughout the EU since 2018. The only areas excluded from full harmonisation are those in which the various EU countries can issue different rules and regulations on the basis of “opening clauses” in the GDPR. This is the case, for example, in employment law and for the processing of health data.

The stated objective is to protect natural persons with regard to the processing of personal data, while at the same time ensuring the free movement of such data (Article 1(1) GDPR).

The aim of this is to protect the fundamental rights of individuals.

Primary (data protection) addressees of the legislation:

The primary addressees of the GDPR are “controllers”, that is natural or legal persons, authorities or other bodies which, alone or jointly with others, determine the processing of personal data (Article 4(7) GDPR). In addition, the activities of processors who process data on behalf of a controller are also covered (Article 4(8) GDPR).

If the addressee has its headquarters and/or one or more establishments in the EU, the GDPR applies according to the principle of establishment, regardless of whether the processing takes place within the EU or not (Article 3(1) GDPR).

If the addressee has its headquarters outside the EU and does not have an establishment in the EU, the GDPR still applies to the processing of personal data in accordance with the market place principle, provided that the controller offers its goods or services to citizens in the EU or processes data of EU citizens (Article 3(2) GDPR).

Obligations/requirements/risks in relation to data:

What legal aspects of data are covered?

- Prohibition subject to permission: the processing of personal data is generally prohibited and only permitted in exceptional cases if the conditions of one of the authorisation provisions of the GDPR apply (Article 6(1) GDPR)
- Principles in Article 5 GDPR for the processing of personal data: lawfulness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, confidentiality and accountability
- Ensuring the rights of data subjects in Chapter III, key provisions for the obligations of controllers in Chapter IV and on the transfer of data to third countries in Chapter V

What obligations are imposed with regard to data?

- Duty to inform when personal data is collected from the data subject (Article 13 GDPR) and when the data is not collected from the data subjects themselves and originates from other sources (Article 14 GDPR)
- Ensuring appropriate technical and organisational measures to ensure data protection and data security (Articles 24, 25 and 32 GDPR)

- Requirements for the processing of data on behalf of a controller (Article 28 GDPR)
- Keeping a record of processing activities (Article 30 GDPR)
- Reporting personal data breaches to the supervisory authority and notifying the data subjects (Articles 33 and 34 GDPR)
- Conducting a data protection impact assessment and prior consultation of the supervisory authorities (Articles 35 and 36 GDPR)
- Designating a data protection officer (Articles 37 to 39 GDPR)
- Before transferring data to third countries outside the EEA, standard contractual clauses must generally be concluded with the importer and a transfer impact assessment must be carried out (from Article 44 GDPR).

Concept of risk adequacy: the more likely or severe the risk posed by the data processing, the more extensive and higher the obligations of the controller.

What are the penalties for breach of duty (risk)?

- For the particularly serious infringements listed in Article 83(5) GDPR, fines of up to €20 million or up to 4% of total annual worldwide turnover are provided for (Article 83 GDPR).
- In addition, there may be a threat of civil claims for damages under Article 82 GDPR (known as “private enforcement”).

Practical tips:

It is essential to bear in mind the principle of prohibition in Article 6 GDPR – as a rule, consent must be obtained for the processing of personal data. Compliance with the duty to provide information in Article 13 GDPR and the duty to provide access in Article 15 GDPR, and likewise the right to erasure in Article 17 GDPR, is also central.

A data protection officer must be appointed (Article 37 to 39 GDPR).

The adoption of appropriate security measures in accordance with Article 32 GDPR is also relevant. In the past, very high fines have been imposed on several occasions due to insufficient data security and the associated data leaks.

Data Governance Act



Brief outline:

The Data Governance Act (“DGA”) creates processes, structures and a legal framework for the joint use of personal and non-personal data. This is intended to ensure neutral access to data and interoperability, as well as to avoid lock-in effects.

The aim of the DGA is to increase the availability of data for commercial use, joint use and research purposes, in order to give the European market a competitive advantage in data-based innovations.

Primary (data protection) addressees of the legislation:

The DGA applies to public-sector bodies, data intermediaries and altruism organisations established in the EU or offering their services in the EU. In the latter case, a representative must be appointed.

Obligations/requirements/risks in relation to data:

What legal aspects of data are covered?

The DGA covers three central topics:

- Promotion of the re-use of certain categories of protected data held by public-sector authorities (provision of public-sector data, Articles 3 to 9 of the DGA). Example: the Finnish social and health authority Findata, where applications for access to data sources such as social insurance agencies or population registers can be made.
- The concept of data use and sharing through data intermediation services (Articles 10 to 15 DGA). Although these are still of little relevance in today’s data economy, the EU hopes to increase their importance by creating a legal framework. This is comparable to a commission agent in commission transactions under section 383 of the German Commercial Code (*Handelsgesetzbuch, HGB*). Example: Data Intelligence Hub of Deutsche Telekom AG for monetising data.
- Increasing data availability through voluntary data donations based on data altruism (Articles 16 to 25 DGA). Registration as an altruism organisation is only possible for independent, non-commercial activities.

What obligations are imposed with regard to data?

- Prohibition of exclusive arrangements for data held by public-sector bodies (Article 4 DGA) and other obligations regarding the design of data licence agreements between public-sector bodies and private parties (Articles 5 to 6 DGA)
- Obligation to register data intermediation services (Article 11 DGA)
- Obligation to charge fair prices for data intermediation services (Article 12(1)(f) DGA)
- Registration requirement for data altruism organisations (Article 18 DGA)

- Extensive transparency requirements and reporting obligations for data altruism organisations (Article 20 DGA)
- Comprehensive information requirements towards data subjects when personal data is processed by data altruism organisations (purpose, place of processing, etc.) (Article 21(1) DGA)

What are the penalties for breach of duty (risk)?

The penalties for infringements are to be determined by the EU Member States. In this context, the national authority responsible for ensuring compliance with the DGA is authorised to impose fines or to suspend the provision of the data intermediation service, for example (Article 34 DGA).

Digital Services Act



Brief outline:

The Digital Services Act (“DSA”) aims to create a safer and more responsible online environment. The purpose of the Act is to provide a uniform, common set of rules for the entire EU, protecting the fundamental rights of users and providing legal certainty for companies in the digital economy throughout the single market. This is also intended to promote innovation, growth and competitiveness in the EU single market.

The rules on online marketplaces are also intended to protect consumers.

The DSA essentially replaces the German Network Enforcement Act (*Netzwerkdurchsetzungsgesetz, NetzDG*).

Primary (data protection) addressees of the legislation:

The DSA applies to all intermediary services offered to users that have their place of establishment or are located in the EU, irrespective of whether the provider of those intermediary services is established in the EU or outside it (Article 2(1) DSA).

The list of obligations is differentiated, with each successive level of service imposing more obligations (very broad scope of application).

A distinction is made between (1) pure intermediary services, (2) hosting services, (3) online platforms, (4) online marketplaces and (5) very large online platforms. Pure intermediary services have the fewest obligations to fulfil, and very large online platforms the most.

Obligations/requirements/risks in relation to data:

How is a service classified (scope of application)?

- There must **always** be an information society service. Physically provided services, telephone and fax services, and television are, in particular, excluded.
- Intermediary services operate as a mere conduit (definitive legal list: caching, hosting, search engines), without having any active knowledge, role or control over the data.
- Hosting services, as a case of intermediary services, store user data on behalf of the user.
- Online platforms store user data on behalf of the user and also disseminate it publicly. Exception: the public dissemination is an insignificant, purely ancillary function of a hosting service or other services.
- Online marketplaces are online platforms where distance contracts are concluded between consumers and traders (B2C).
- Very large online platforms must exceed the threshold of 45 million users (unique visitors) in the EU and be designated as such by decision of the European Commission by decision.

What obligations and requirements (differentiated according to scope of application) are imposed in relation to data?

- The central point of reference for a large number of obligations is the handling of illegal content = all information that is not in compliance with EU law or the law of an EU Member State (Article 3(h) DSA).
- For pure intermediary services, (1) Articles 4 to 6 of the DSA set out reduced liability based on the nature of intermediary services, (2) Articles 9 to 10 of the DSA set out information requirements regarding deletion and disclosure orders from authorities, (3) Article 11 of the DSA sets out the designation of a central electronic communication point for communication with national authorities, and (4) Article 14 onwards of the DSA contains provisions regarding the design of general terms and conditions and transparency obligations.
- For hosting service providers, the following additional provisions are set out: (1) the obligation to set up a notice-and-action system for reporting illegal content (Article 16 DSA), (2) the obligation to provide users with reasons for the deletion of potentially illegal content (Article 17 DSA) and (3) an obligation on the part of providers to report suspicions of certain criminal offences (Article 18 DSA).
- For online platforms, the following additional provisions are set out: (1) a significantly more demanding complaints management and dispute resolution system (from Article 21 DSA), (2) requirements to disable access after issuing a warning, including for users who frequently post illegal content (Article 23 DSA), (3) a ban on “dark patterns” (Article 25(1) DSA), (4) further transparency obligations (Articles 24 and 27 DSA) and (5) the adoption of measures to protect minors (Article 28 DSA).
- For online marketplaces, additional consumer protection provisions apply in Articles 30 to 32 of the DSA, with an exception for SMEs.
- For very large online platforms and online search engines, Article 34 onwards of the DSA contains significantly stricter versions of the rules already applying to them as well as elements of third-party regulation and self-regulation to contain systemic risks (e.g. the obligation to carry out risk assessments, for example with regard to the dissemination of illegal content and negative effects on fundamental rights, and to take measures).

What are the penalties for breach of duty (risk)?

Infringements of the DSA can be punished by fines of up to 6% of annual worldwide turnover in the preceding financial year (see Article 52(3) and Article 74(1) DSA).

Practical tips:

The DSA is proving to be the most challenging new law in terms of compliance. Even the question of which category a service should be classified in is difficult to answer in individual cases. Meeting obligations can potentially take up a lot of resources, and therefore the service should not be classified in a higher category just to make sure. Once the classification has been made, the detailed compliance obligations must be observed and the service and the company’s organisational structures must be designed in such a way that they can be complied with as smoothly as possible (“compliance by design”).

AI Act



Brief outline:

The objective of the AI Act is to lay down rules for the use of artificial intelligence. Particular emphasis is placed on ensuring that AI is trustworthy, secure, technically robust, transparent, ethical, impartial and controllable by humans.

The AI Act is a preventive, cross-sectoral prohibitory law that prohibits the use of AI in numerous application scenarios or makes it dependent on technical, organisational and legal requirements.

The main purpose is to protect the fundamental rights of natural persons and copyright.

In the trilogue on 2 February 2024, many provisions were tightened even further compared to previous drafts.

In addition, an AI Office is being created to act as a market surveillance authority for GPAI models (such as ChatGPT).

Primary (data protection) addressees of the legislation:

The AI Act primarily targets providers (manufacturers) and operators of AI systems, but in special cases it also covers distributors, authorised representatives and end users, for example.

An AI system is defined as “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments” (Article 3(1) AI Act).

According to the market place principle, the AI Act applies to providers who place AI systems on the market or operate them in the EU, users of AI systems who are located in the EU, and providers and users of AI systems from third countries whose system results are used in the EU.

Obligations/requirements/risks in relation to data:

What important transparency obligations are imposed on AI systems that interact with individuals?

- Providers of AI systems (Article 3(3) AI Act) must inform natural persons (individuals) that they are interacting with an AI system when an AI system is used (Article 50 AI Act).
- Providers of AI systems (Article 3(3) AI Act) that generate synthetic audio, image, video or text content have to ensure that the output of the AI system is recognisably marked as such in a machine-readable format (e.g. using watermarks, metadata, cryptographic methods, digital fingerprints, etc.).
- Deployers of AI systems (Article 3(4) AI Act) must inform the natural person exposed thereto about the use of emotion recognition software and biometric categorisation systems.
- Deployers of an AI system (Article 3(4) AI Act) that generates or manipulates image, audio or video content constituting a deep fake must disclose that the content has been artificially generated or manipulated.

What are the important additional obligations for GPAI models such as ChatGPT?

- GPAI models = general-purpose AI systems as defined in Article 3(66) of the AI Act, i.e. an AI model that has “*the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems*”
- Obligations under Article 53 AI Act: including documenting the model; providing documentation to providers of AI systems who wish to integrate the GPAI model into their AI systems; publishing the content used to train the AI model
- Additional requirements for providers of models with systemic risks (see Article 3(65) AI Act regarding this term) under Article 55 AI Act: including conducting and documenting adversarial testing, risk assessment and risk mitigation, ensuring an appropriate level of cybersecurity)

What kinds of AI systems are prohibited?

- Social scoring systems (Article 5(c) AI Act), profiling in law enforcement (Article 5(d) AI Act), database AI systems for facial recognition (Article 5(e) AI Act), emotion recognition systems in schools and workplaces (Article 5(f) AI Act)
- AI systems that exploit manipulative techniques or personal weaknesses to induce harmful behaviour (Article 5(a), (b) AI Act)

What are the important obligations for high-risk AI systems?

- Classification as a high-risk AI system is based on (1) the type of product, including the use of AI in machinery, toys, medical devices and/or (2) high-risk areas such as biometric data, critical infrastructure, employment/human resources management, law enforcement, the administration of justice, democratic processes, etc.
- High-risk AI systems must establish, implement, document and maintain a risk management system (Article 9 AI Act). The high-risk AI system must allow for the automatic logging of events over the lifetime of the system (Article 12 AI Act).
- Strict requirements regarding training data: data must be relevant, sufficiently representative, and to the best extent possible free of errors and complete in view of the intended purpose of the AI system (Article 10 AI Act).
- Users must be enabled to interpret the output (Article 13 AI Act). Central technical challenge, since nowadays most AI systems are still a “black box”; thus they are not able to explain their output.
- Human deployer must be in a position to oversee the system (Article 14 AI Act); conformity assessment before system is placed on the market (Article 19, 44 AI Act).

What are the penalties for breach of duty (risk)?

- For infringements due to non-compliance with the prohibition of the AI practices referred to in Article 5, there is a threat of fines of up to €35 million or up to 7% of annual worldwide turnover.
- For general-purposes AI models, there is a threat of fines of up to €15 million or 3% of annual worldwide turnover.

Open Data Directive



Brief outline:

The Open Data Directive aims to increase the availability and flow of data held by public-sector bodies for commercial and non-commercial purposes. It seeks to improve access by harmonising the different conditions and procedures in the EU Member States for the use of public-sector information resources.

Primary (data protection) addressees of the legislation:

The addressees are public-sector bodies within the EU and also universities, for example, in relation to research data.

Cultural institutions such as museums and public broadcasting are, however, exempt.

It should be noted that only data that has already been declared publicly available on the basis of other legislative acts is covered by the scope of application, and that data concerning the intellectual property of third parties is excluded. Sensitive data (including security-relevant data) is also excluded.

The primary aim of the Open Data Directive is therefore to simplify the “how” in relation to the availability of data from public bodies, not the “whether”.

Obligations/requirements in relation to data:

- Public-sector bodies that previously had “sui generis” rights in relation to databases or similar may no longer invoke these after the Directive comes into force.
- Article 4 Open Data Directive sets out the arrangements for the provision of data: these include time limits for the provision of data to the public-sector body and the obligation to provide reasons and information on means of redress in the event of a negative decision.
- Article 5 Open Data Directive obliges public-sector bodies to make data available in a manner that is as accessible as possible, as far as possible over the internet.
- Article 6 Open Data Directive sets out arrangements in relation to charges, including the specification that only necessary expenses for sharing data may be charged. There are exceptions for entities such as libraries and bodies that finance their activities through charges.
- No additional conditions for use of data may be imposed (Article 8 Open Data Directive) and no exclusive arrangements may be entered into (Article 12 Open Data Directive).

ePrivacy Regulation



Brief outline:

The draft ePrivacy Regulation is a draft statute concerning the respect for private life and the protection of personal data in electronic communications. The main focus of the Regulation is on the confidentiality of communications (telecommunications secrecy) and the processing of communications data.

Its objective is to implement specific rules in the field of electronic communications which the GDPR, with its technology-neutral approach, cannot fulfil.

As of June 2024, the ePrivacy Regulation has still not been adopted and it is unclear how things will go forward. However, if it enters into force, it will (like the GDPR) impose wide-ranging obligations on platform operators.

Primary (data protection) addressees of the legislation:

Companies in the digital economy, especially website and software providers.

Obligations/requirements/risks in relation to data:

- Providers are to be obliged to use state-of-the-art technology to store data and protect it from unauthorised access.
- Trading in data through “backdoors” is to be prohibited.
- Geographical tracking by programs that are not actively used (unwitting creation of movement profiles) is to be prohibited.
- No data should be processed without the user’s consent. This obligation is to be extended by the Regulation to include providers of online communications, and no processing should take place without consent to storage.
- The more privacy-friendly option should be set as the default in all software and device settings (privacy by default).
- Protection of private life: displaying of phone numbers, end-user directories, direct marketing by means of electronic communications and supervision
- References to the provisions on fines in the GDPR planned (Article 23 draft e-Privacy Regulation)

Free Flow of Data Regulation



Brief outline:

The objective of the Free Flow of Data Regulation is to remove obstacles to the free movement of non-personal data within the EU in order to create a competitive data economy in the digital single market.

This is intended to protect the freedom of establishment and the freedom to provide services (TFEU) for data processing services, which could previously have been affected by possible national or regional requirements.

The Regulation also aims to reduce private-law restrictions.

Primary (data protection) addressees of the legislation:

The addressees of the Regulation are service providers who process electronic data (other than personal data) for users within the EU and natural and legal persons who process data for their own needs.

The aim is first and foremost to improve the processing and transfer of non-personal data across national borders.

Obligations/requirements/risks in relation to data:

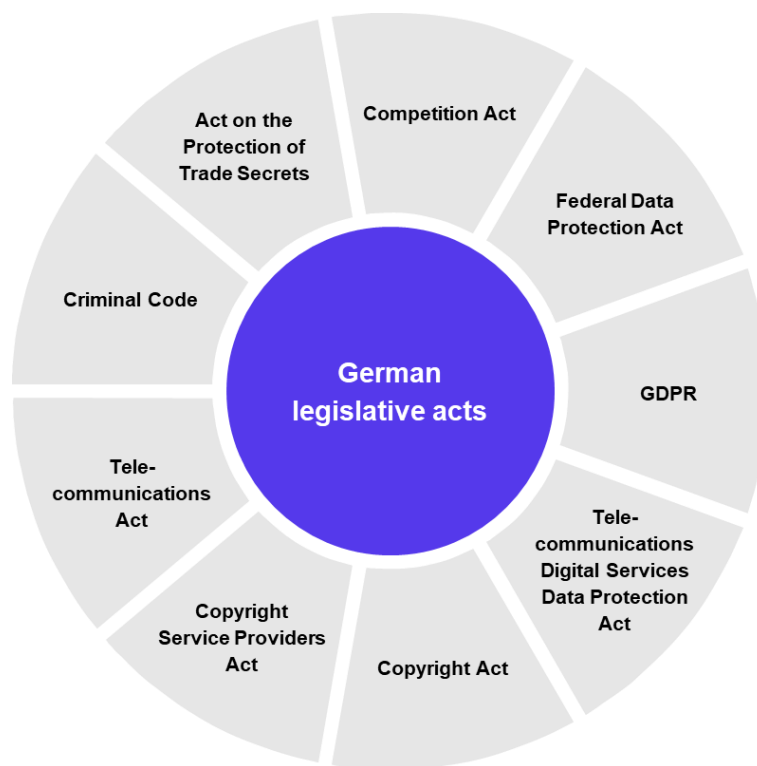
- Prohibition of national data localisation requirements, unless justified on grounds of public security in compliance with the principle of proportionality (Article 4(1) Free Flow of Data Regulation)
- Data availability for competent authorities so that national administrative and judicial authorities are able to access the data, even if it is located in another Member State (Article 5(1) Free Flow of Data Regulation)
- Easier possibilities to switch cloud service providers for professional users (“data portability”), since the location and offering of services can no longer be restricted to Member States
- Companies to draw up codes of conduct that ensure the principles of transparency and interoperability (Article 6 Free Flow of Data Regulation)

German legislation

Introduction




It is not only at European level that rules relating to data as an economic asset must be observed. Certain laws relating to the data economy must also be taken into account at a German level. These can vary considerably in terms of their requirements and focus, or may only contain fragmented rules and regulations on data.

Overview of the most important German legislative acts



The German legislation in detail

Key

| | |
|---|---------------------------------------|
|  | Act/code relates to non-personal data |
|  | Act/code relates to personal data |
|  | Date the law came into force |

German Act on the Protection of Trade Secrets



Brief outline:

The German Act on the Protection of Trade Secrets (*Gesetz zum Schutz von Geschäftsgeheimnissen, GeschGehG*) is based on European legislation. Its aim is to ensure standardised minimum protection for trade secrets under civil law.

The background to this is that companies are increasingly facing unfair practices aimed at the unlawful acquisition of trade secrets (industrial espionage, theft, unauthorised copying, breach of confidentiality obligations, etc.) due to factors such as globalisation, more outsourcing and greater use of IT systems.

Primary (data protection) addressees of the legislation:

Serves to protect owners of trade secrets: any natural or legal person lawfully controlling a trade secret (section 2(2) of the Act).

Intended to penalise infringers of trade secrets through civil action and criminal law provisions.

According to section 2(1) of the Act, “trade secret” means information

- a) that is not, as a whole or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question and is thus of economic value and
- b) that has been subject to reasonable steps under the circumstances, by its lawful holder, to maintain secrecy and
- c) concerning which there is a legitimate interest in maintaining secrecy.

Duties/requirements/risks in relation to data:

What types of data are considered to be trade secrets?

- The term “information” is to be interpreted very broadly – it covers any know-how such as manufacturing processes, customer and supplier lists, information on costs, business strategies, company data, market analysis, prototypes, formulae and recipes.
- The information must have economic value because it is not publicly known. Irrelevant information is excluded, even if it is secret in itself.
- Appropriate confidentiality measures must be taken. Active steps are required (obligation).

When is a trade secret infringed and what rights and penalties exist?

- Infringer: any natural or legal person who obtains, uses or discloses a trade secret contrary to the prohibitions on action in section 4 of the Act (including unauthorised access, copying). **Exceptions** to this are laid down in section 5 of the Act (known as the whistleblower section)
- Sections 6 to 8 of the Act: right to information, removal and injunctive relief. Fault is not a prerequisite, but according to section 9 of the Act there is a defence of disproportionality.
- Section 10 of the Act: claim for financial compensation (in the event of culpability)
- Section 13 of the Act: claim under the provisions of the German Civil Code on unjust enrichment
- Section 23 of the Act: facts constituting a criminal offence

Practical tips:

The first step is to identify what information is worthy of protection from an economic point of view. The information requiring protection should then be classified according to its need for protection. Following this, a protection plan must be developed and implemented in the company, and its effectiveness must be reviewed on a regular basis.

Protective measures that can be considered include

- Need-to-know principle: only providing each employer with the information they need to fulfil their tasks
- Insisting on confidentiality agreements
- Prohibiting the use of personal electronic devices and removal of work documents
- Operating a secure IT infrastructure
- Logging access to physical and electronic data

It is **important** that protective measures be taken, as otherwise any claims asserted could be refused. The intensity of the measures taken depends on the confidentiality of the specific trade secrets. The proportionality of the measures taken also plays a role: if the need-to-know principle cannot be implemented to ensure the economic viability of the company, the company is generally not expected to implement it.

German Competition Act



Brief outline:

The German Act Against Restraints of Competition (“German Competition Act”) (*Gesetz gegen Wettbewerbsbeschränkungen, GWB*) is the legal basis of German antitrust and competition law. The aim of the Act is to protect functioning markets and prevent distortions of competition.

While central provisions in the form of the ban on anti-competitive agreements and practices (section 1 of the Act) and the prohibition of abuse of a dominant market position (section 19 of the Act) are largely harmonised with European antitrust and competition law (Articles 101 and 102 TFEU), the Act also contains a number of special provisions, some of which are data-related. These include provisions on the abuse of a position with paramount significance for competition across markets (section 19a of the Act) and the abuse of relative market power (section 20 of the Act).

Increasingly, the market position of companies in German antitrust and competition law is also being assessed on the basis of access to competition-relevant data (section 18(3)(3), section 19a(1)(4) and section 20(1a) of the Act).

Duties/requirements in relation to data:

- In certain circumstances, rights to access data may arise against companies with a dominant market position, relative market power or paramount significance for competition across markets.
- In addition, certain uses of data by these companies may infringe the prohibitions of the Act.

What are the consequences for infringements?

- Competition authorities can impose fines of up to 10% of the total turnover in the previous financial year (from section 81 of the Act). The competition authorities can also issue cease-and-desist orders against companies.
- In addition, aggrieved companies can sue for injunctive relief/rectification and damages (from section 33 of the Act).

Primary (data protection) addressees of the legislation:

Data-related obligations concern in particular companies with a dominant market position, relative market power or paramount significance for competition across markets. Under certain circumstances, data access rights may apply to these companies.

In addition, the German Federal Cartel Office (*Bundeskartellamt*) can prohibit certain data processing activities, particularly in relation to companies of paramount significance for competition across markets (currently Alphabet, Amazon, Apple and Meta).

Practical tips:

The provisions of the Act represent both opportunities and risks for companies:

- If one of the aforementioned special market positions exists, companies must observe their obligations when handling data. As the provisions are sometimes formulated in very abstract terms, particular caution is required in respect of the collection, use and granting of access to competition-relevant data. This is the only way to ensure proactive compliance with antitrust and competition law.
- If, on the other hand, a company depends on access to competition-relevant data for its business activities in markets, the requirements for a right to access data under the Act should be examined and, if necessary, enforced.

German Federal Data Protection Act



Brief outline:

The basic structure of the German Federal Data Protection Act (*Bundesdatenschutzgesetz, BDSG*) is based on the GDPR and is intended to supplement it. It implements the regulatory tasks of the GDPR for the EU Member States.

It is intended to apply in particular to the processing of personal data in the context of the activities of federal public bodies that lie outside the scope of EU law.

The Act also lays down obligations for non-public bodies, in particular with regard to the processing of special categories of personal data and for special processing situations where the GDPR contains opening clauses in favour of national law.

Primary (data protection) addressees of the legislation:

The Act primarily addresses public bodies of the federal government and the federal states to the extent that they implement federal law.

The Act applies to non-public bodies if the controller or processor processes personal data in Germany or if the processing takes place in a domestic branch. The Act also applies to non-public bodies without an establishment in an EU Member State or a contracting state of the EEA provided that they fall within the scope of the GDPR. The processing must be fully or partially automated or not automated if the data is stored or is to be stored in a file system. An exception exists in the case of processing by natural persons for the performance of exclusively personal or family activities.

Duties/requirements in relation to data for non-public bodies:

- Video surveillance of publicly accessible areas only permitted under the conditions specified in section 4 of the Act; please note: GDPR has priority in its scope of application
- Special requirements for data processing in employment relationships (section 26 of the Act: including special requirements for employees' consent to the processing of their personal data)
- Compliance with the requirements of section 31 of the Act in the case of scoring

What are the consequences for infringements?

- Claims for damages/compensation in accordance with section 83 of the Act
- Fines (section 43 of the Act) and criminal penalties (section 42 of the Act)

Practical tips:

In the context of the Act, particular attention will have to be paid to the special requirements of section 26(2) of the Act in the context of employee consent and to the requirements of section 31 of the Act in the case of scoring.

German Digital Services Act



Brief outline:

The German Digital Services Act (*Digitale-Dienste-Gesetz, DDG*) replaces the German Telemedia Act (*Telemediengesetz, TMG*), implements the regulatory mandates of the EU's Digital Services Act Regulation and adapts the national legal framework for the effective implementation of the Digital Services Act Regulation accordingly.

The German Digital Services Act designates the Federal Network Agency (*Bundesnetzagentur*) as the body responsible for enforcing the EU's Digital Services Act Regulation and lays down rules for the consequences of breaching the EU's Digital Services Act. In all other respects, the provisions of the German Telemedia Act, which also contain rules relevant to data law, are largely adopted identically.

Primary (data protection) addressees of the legislation:

The primary addressees of the data protection statute are providers of digital services, which are to be understood as an information society service, i.e. any service that is generally provided electronically at a distance for a fee and at the individual request of a recipient.

The scope of application includes service providers established in Germany, even if they provide their services in another Member State of the European Union, unless the DSA applies directly in this case.

Duties/requirements in relation to data:

- Obligation to display legal notices on websites according to section 5 of the German Digital Services Act
- Special transparency obligations with regard to advertising in accordance with section 6 of the German Digital Services Act, including the recognisability of offers for sales promotion, discounts, bonuses and gifts as such; competitions or prize draws of an advertising nature must be clearly recognisable as such
- Right of holders of intellectual property rights to block the use of information in the event of an infringement (section 8 of the German Digital Services Act)
- Obligations for video-sharing platform providers (see section 1(4)(9) of the German Digital Services Act regarding the term) pursuant to section 11 of the German Digital Services Act: in particular, agreeing contractual usage bans with users that they may not disseminate any unauthorised advertising on a video-sharing platform, e.g. in relation to tobacco products or prescription drugs

What are the consequences for infringements?

Fines according to section 33 of the German Digital Services Act

Practical tips:

It is important to amend the legal notices on company websites so that they mention the German Digital Services Act instead of the German Telemedia Act. Providers of audiovisual media services should state which EU Member State their registered office is in or is deemed to be in, as well as the competent

regulatory and supervisory authorities. The German Digital Services Act does not result in any other changes to the obligation to include legal notices.

With regard to the transparency requirements under section 6 of the German Digital Services Act, there are no far-reaching changes compared to the legal situation under the German Telemedia Act. Only special provisions for video-sharing platform providers have been introduced in sections 3 and 4.

A right comparable to that in section 8 of the German Digital Services Act has not been included in the German Telemedia Act up to now, which is why the relevant conditions must be put in place.

The obligations for video-sharing platform providers under section 11 of the German Digital Services Act have been largely reintroduced.

German Act on Data Protection and the Protection of Privacy in Telecommunications and Digital Services



Brief outline:

In the German Act on Data Protection and Privacy in Telecommunications and Digital Services (“Telecommunications Digital Services Data Protection Act”) (*Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten, TDDDG*) (formerly *Telekommunikation-Telemedien-Datenschutzgesetz, TTDSG*), the data protection provisions of the German Telemedia Act (now German Digital Services Act) and German Telecommunications Act, including the provisions on the protection of telecommunications secrecy, were adapted to the GDPR and merged. In addition, the provisions on the protection of privacy on terminal devices under the EU ePrivacy Directive were transposed into German law.

The statute relates to data protection for telecommunications and digital services. They include privacy requirements in relation to incoming calls, caller ID withholding, caller ID display and automatic call forwarding as well as the protection of the privacy of terminal devices.

Duties/requirements in relation to data:

- Only the traffic data specified in section 9(1) to (5) of the Act may be collected from providers of publicly accessible telecommunications services and from natural persons and legal entities involved in the provision of such services, to the extent that this is necessary to establish and maintain telecommunications, for billing purposes or to establish further connections.
- Obligations with regard to location data in accordance with section 13 of the Act
- Rules on displaying and withholding caller numbers in accordance with section 15 of the Act: providers of voice communication services must offer end users the option of withholding their number free of charge; at the same time, end users who are called should have the option of rejecting incoming calls with a withheld number; the number is not permitted to be withheld on advertising calls.

Primary (data protection) addressees of the legislation:

The primary addressees of the German Act on Data Protection and Privacy in Telecommunications and Digital Services are providers of digital services (section 2(2)(1) of the Act) and telecommunications service providers who have a branch in Germany or who provide services, participate in the provision of services or make goods available on the market.

- Data protection obligations for digital services: including technical and organisational precautions, such as the option of using and paying for digital services anonymously or under a pseudonym (section 19 of the Act); processing of the personal data of minors (section 20 of the Act); rules on information about inventory data (sections 21, 22 of the Act)
- Data protection obligations for terminal equipment (section 2(2)(6) of the Act) in accordance with sections 25 and 16 of the Act: these include a consent requirement for cookies and similar technologies

German Act on Copyright and Related Rights



Brief outline:

The German Copyright and Related Rights Act (*Gesetz über Urheberrecht und verwandte Schutzrechte, UrhG*) primarily governs the rights of creators of literary, academic or artistic works. It is therefore not primarily a set of data law provision, although the Act does contain some relevant obligations.

Of particular note are the provisions on database producers granting them a property right in favour of the entire database or a substantial part of the database in terms of type or scope.

Primary (data protection) addressees of the legislation:

All natural and legal persons under private and public law are obliged to comply with the protective provisions in favour of database producers.

German nationals and nationals of another EU Member State are protected. In addition, legal entities that were founded in Germany or another EU Member State, or whose head office or principal place of business is located in one of the Member States, are covered by the scope of protection. Furthermore, legal entities whose registered office is located in the territory of one of these EU Member States and whose activities have an actual connection to the German economy or the economy of one of these Member States are also covered.

Duties/requirements in relation to data:

No infringement of the database creator's intellectual property rights (see section 87a of the Act regarding this term)

What penalties are foreseen for infringing property rights?

- Claim for injunction/removal/damages
- Penalties under criminal law and fines

German Act on the Copyright Liability of Online Content-Sharing Service Providers



Brief outline:

The German Act on the Copyright Liability of Online Content-Sharing Service Providers (“Copyright Service Providers Act”) (*Gesetz über die urheberrechtliche Verantwortlichkeit von Diensteanbietern für das Teilen von Online-Inhalten, UrhDaG*) governs the liability of service providers (section 2 of the Act) which publicly reproduce works by providing the public with access to copyright-protected works uploaded by users of the service.

If a service provider takes the measures specified in the Act, it is not liable under copyright law for the public reproduction of the protected work.

Primary (data protection) addressees of the legislation:

The primary addressees of the obligations are service providers (section 2 of the Act). These are providers of information society services, i.e. any service that is generally provided electronically at a distance for a fee and at the individual request of a recipient which also meets the requirements of section 2(1) to (4) of the Act.

The territorial scope of the provision is limited to Germany.

Duties/requirements for service providers in relation to data:

- Obligation to use best endeavours to acquire contractual rights of use for public dissemination of copyrighted works (section 4 of the Act)
- Obligation to block content (sections 7 to 11 of the Act)
- Obligation to pay remuneration pursuant to section 12(1) of the Act to the creator in the case of presumed uses pursuant to sections 9 to 11 of the Act
- Provision of an effective, free and speedy complaints procedure regarding the blocking and public dissemination of protected works (section 14 of the Act)

What are the consequences for infringements?

Service provider has full liability under copyright law for the unauthorised public dissemination of copyrighted works.

German Telecommunications Act



Brief outline:

The German Telecommunications Act (*Telekommunikationsgesetz, TKG*) is intended to promote competition in the telecommunications sector and lead to the development of efficient telecommunications infrastructures in order to guarantee adequate and sufficient services nationwide.

It sets out clear requirements and obligations for providers of publicly accessible telecommunications services to ensure the security and protection of personal data.

Primary (data protection) addressees of the legislation:

The primary addressees of the statute are all companies or persons who operate telecommunications networks or telecommunications systems or provide telecommunications services in Germany.

Duties/requirements in relation to data for operators of public telecommunications networks (section 3(7) and (42) of the Act):

- Notification obligation under section 5 of the Act for operators of commercial public telecommunications networks
- Obligation to prepare an annual financial report for companies covered by section 6(1) of the Act
- Interface descriptions in accordance with section 74 of the Act

Duties/requirements in relation to data for companies with significant market power:

- The Federal Network Agency (*Bundesnetzagentur*) can impose obligations on companies with significant market power in accordance with sections 24 to 30, 38 or 49 of the Act.
- Prohibition of misuse against end users or other companies (sections 37 and 50 of the Act)

Duties/requirements in relation to data for providers of publicly accessible telecommunications services (section 3(1) and (44) of the Act):

- Information obligations for providers of internet access services and publicly accessible interpersonal telecommunications services (section 52 of the Act)
- Contract law requirements towards consumers (sections 54 to 57 of the Act): including information requirements, contract summary, cancellation after tacit contract renewal, contract amendments
- Obligation to rectify faults at the request of the consumer (section 58 of the Act)

- Requirements for the calculation of call charges in accordance with section 63 of the Act for providers of publicly accessible number-based interpersonal telecommunications services and providers of internet access services
- End users' right to itemised billing in accordance with section 65 of the Act in respect of providers of publicly accessible number-based interpersonal telecommunications services and providers of internet access services
- Obligation of providers of publicly accessible telecommunications services to notify the Federal Networks Agency in the event of a breach of personal data (section 169 of the Act)
- Obligation to store traffic data, to use the data and to ensure data security for providers of publicly accessible telecommunications services that are not number-independent interpersonal telecommunications services (sections 175 to 181 of the Act)

Data-related obligations for providers of publicly accessible telecommunications services and operators of public telecommunications networks:

- Prohibition of discrimination against end users; consideration of the interests of end users with disabilities (section 51 of the Act)
- Rules on changing providers and number portability (section 59 of the Act)

What are the consequences for infringements?

- Cease-and-desist claims and claims for damages according to section 69 of the Act
- Fines in accordance with section 228 of the Act

German Criminal Code



Brief outline:

The German Criminal Code (*Strafgesetzbuch, StGB*) also contains numerous data protection provisions.

Primary (data protection) addressees of the Code:

The German Criminal Code generally applies to offences committed in Germany (section 3 of the Code).

Relevant data protection provisions:

- Section 126a of the German Criminal Code: dangerous dissemination of personal data
- Section 202a of the German Criminal Code: data espionage
- Section 202b of the German Criminal Code: phishing (interception of data)
- Section 202c of the German Criminal Code: acts preparatory to data espionage and phishing
- Section 202d of the German Criminal Code: handling stolen data
- Section 238(1)(3) of the German Criminal Code: stalking by repeatedly and improperly using the other person's personal data for the purpose of a) placing orders for goods or services for that person or b) inducing third parties to make contact with that person
- Section 263a of the German Criminal Code: computer fraud
- Section 268 of the German Criminal Code: forgery of technical records
- Section 269 of the German Criminal Code: forgery of data of probative value
- Section 270 of the German Criminal Code: deception in relation to data processing in legal commerce
- Section 274(2)(2) of the German Criminal Code: suppression of documents; changing border markers
- Section 303a of the German Criminal Code: data manipulation
- Section 303b of the German Criminal Code: computer sabotage

What are the consequences for infringements?

Fine or imprisonment for up to 5 years

Contacts



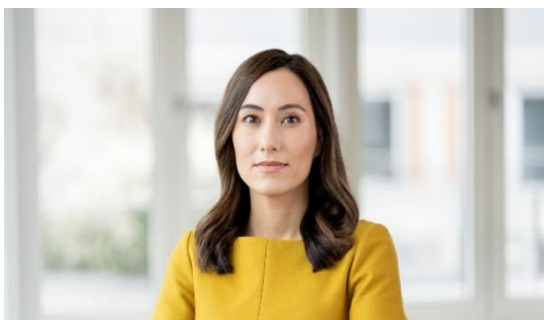
Daniel Rücker, LL. M. (University of New South Wales, Sydney)

Rechtsanwalt (Lawyer)

Partner

T +49 89 28628457

daniel.ruecker@noerr.com



Sarah Blazek, E.MA (European Inter-University Centre, Venedig)

Rechtsanwältin (Lawyer)

Partner

T +49 89 28628513 | +32 2 2745593

sarah.blazek@noerr.com



Sebastian Dienst

Rechtsanwalt (Lawyer)

Associated Partner

T +49 89 28628457

sebastian.dienst@noerr.com



Marieke Merkle

Rechtsanwältin (Lawyer)

Associated Partner

T +49 89 28628227

marieke.merkle@noerr.com

