Legal 500
Country Comparative Guides 2025

Germany
Data Protection & Cybersecurity

Contributor

White & Case

Erasmus Hoffmann

Partner | erasmus.hoffmann@whitecase.com

Markus Langen

Partner | markus.langen@whitecase.com

Dr. Sylvia Lorenz

Partner | sylvia.lorenz@whitecase.com

Dr. Constantin Teetzmann

Local Partner | constantin.teetzmann@whitecase.com

Alissa Arms

Associate | alissa.arms@whitecase.com

Swantje Behm

Associate | swantje.behm@whitecase.com

Friederike Kirch

Associate | friederike.kirch@whitecase.com

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

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

Germany: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

In Germany, data protection is primarily regulated by the EU General Data Protection Regulation (*GDPR*) and subsequent local laws, such as the Federal Data Protection Act (*BDSG*) and the Telecommunications and Media Data Protection Act (*TTDSG*). In addition, other sector-specific data protection laws apply, such as the Directive (*EU*) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, which was transferred into several German laws, such as the German Code of Criminal Procedure (*StPO*), the Act on the Federal Constitutional Court (*BVerfGG*) and the Code of Civil Procedure (*ZPO*).

As regards cybersecurity, the Act on the Federal Office for Information Security (*BSI Act*) mandates cybersecurity standards and incident reporting for operators of critical infrastructure in sectors such as energy, health, transport, and telecommunications. In addition, certain sector-specific rulebooks contain provisions relating to cybersecurity, such as the German Banking Act (*KWG*) *and the Energy Industry Act (EnWG).*

Enforcement is carried out by several authorities, including the Federal Commissioner for Data Protection and Freedom of Information and data protection authorities of the German federal states that oversee data protection compliance; the Federal Office for Information Security (*BSI*) oversees compliance with certain cybersecurity requirements, and the Federal Network Agency (*BNetzA*) monitors telecommunications infrastructure.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

Germany's data protection, privacy, and cybersecurity landscape is set to undergo significant changes in the coming years.

This includes several developments in relation to EU laws. Among these is the EU Artificial Intelligence Act, which begins phased enforcement in 2025, introducing obligations on providers of high-risk and general-purpose AI systems. Discussions on potential changes to the EU Artificial Intelligence Act are pending. In cybersecurity, the NIS2 Directive—expanding the scope of cybersecurity requirements to more sectors—is expected to be transposed into German law in 2025. The EU Digital Operational Resilience Act (*DORA*) came into force in January 2025, imposing cybersecurity and risk management standards on financial institutions. Additionally, the EU Cyber Resilience Act (*CRA*) will require manufacturers of certain IT products to start reporting vulnerabilities and incidents. Discussions on changes to the GDPR are pending, including on aspects such as record keeping requirements for smaller companies and enforcement rules.

In addition, the new German Government aims to amend the German privacy enforcement framework, including by paving the way for binding data protection standards on the federal level.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

The German Federal Data Protection Act (*BDSG*) does not include licensing requirements for entities processing personal data.

In the cybersecurity domain, companies classified as operators of critical infrastructure under the BSI Act must register critical infrastructure with the Federal Office for Information Security (*BSI*). These companies are required

to implement IT security standards, report serious security incidents, and undergo regular audits. Non-compliance may trigger administrative fines.

4. How do the data protection laws in your jurisdiction define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

Germany applies the definition of Art. 4 (1) of the GDPR.

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

The principles governing the general processing of personal data in Germany follow from the GDPR. For example, the general requirements set out in Articles 5 and 6 of the GDPR apply, according to which processing must comply with the principles of lawfulness, transparency, purpose limitation, and accuracy. In addition, the principles of data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability must be observed. A legal basis for the processing of personal data is essential, as stipulated under Article 6 of the GDPR.

Germany made use of the opening clauses under the GDPR by enacting, for example specific regulations in areas such as video surveillance, data protection for employees, research, archiving, rights of data subjects, consumer credit, scoring, and the appointment of data protection officers.

6. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

The definition of "consent" under Article 4 (11) of the GDPR applies, i.e. consent must be "freely given, specific, informed and unambiguous". The controller must be able to demonstrate that the data subject has consented (*Article 7 (1) of the GDPR*) and if the consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is "clearly distinguishable from the other matters", in an "intelligible and easily accessible form, using clear and plain language" (*Article 7 (2) of the GDPR*). When assessing whether consent is "freely given", it needs to be considered whether, *inter alia*, the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (*Article 7 (4) of the GDPR*). With regard to special category of personal data (sensitive data), the consent must be "explicit" (*see Article 9 (2) (a) of the GDPR).* There are further sector-specific requirements. For example, in employment relationships, consent must be given in writing or electronically, unless special circumstances permit otherwise (*Section 26 (2) of the BDSG*). The sending of unsolicited communications via email, requires prior consent (*Article 13 (1) of the Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, e-Privacy Directive, in conjunction with Section 7 (2) no. 2 of the German Unfair Competition Act, UWG*), unless the exceptions stipulated in Section 7 (3) UWG apply (e.g. the sender has obtained the email address in the course of selling goods or services to the email holder). The placing of "Cookies" requires express consent as well, unless they are necessary for the functionality of the website (*Article 5 (3) of the e-Privacy Directive in conjunction with Section 25 Telecommunications Digital Services Data Protection Act, TDDSG*).

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

Article 9 of the GDPR and Section 22 BDSG apply, i.e. the processing of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) is prohibited, unless the exceptions under Article 9 (2) GDPR or Section 22 (1) of the BDSG apply. Such exceptions, include the data subject has given explicit consent (except where Union or Member State law does not allow that) or the processing is necessary for the purposes to protect vital interests of the data subject or another natural person where the data subject is physically or legally of giving consent. With regard to consent, please see the answer to question 6.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Because the GDPR is fully harmonising the data protection law in the EU, German data protection laws are mainly of clarifying nature making use of the opening clauses in the GDPR, such as in the field of employment law (*see Article 88 of the GDPR, Section 26 of the BDSG*). However, certain fields are not subject to the GDPR (*see Article 2 (2) GDPR*), where data protection laws other than the GDPR can apply, such as with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (*see Directive (EU) 2016/680 of 27 April 2016*, response to question one above).

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

Here, Article 35 of the GDPR applies. Article 35 (1) of the GDPR requires that where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Such data protection impact assessment referred to in shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data (*Article 9 (1) of the GDPR*), or of personal data relating to criminal convictions and offences (*Article 10 of the GDPR*); or (c) a systematic monitoring of a publicly accessible area on a large scale (*Article 35 (3) GDPR*).

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

N/A

11. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

There are no Germany-specific requirements here, rather, Article 30 of the GDPR applies. Organisations that are controllers are required to keep records of their data processing activities in writing (including in electronic form) that contains certain information, such as the purpose of the processing or the description of the categories of data subjects and of the categories of personal data (*Article 30 (1) and (3) of the GDPR*). There is a similar obligation if the organisation is a processor (*Article 30 (2) and (3) of the GDPR*). Organisations usually meet those requirements by using an electronic record keeping and management system.

12. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

There are no Germany-specific requirements.

13. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

There is no mandatory requirement under German data protection law for such consultation. However, Article 36 of the GDPR applies, according to which the controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 of the GDPR (see question 9 above) indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

Article 37 of the GDPR require the designation of a data protection officer if the processing is carried out by a public authority, involves regular and systematic monitoring of data subjects on a large scale, or involves processing on a large scale of special categories of personal data relating to criminal convictions and offences. A group of undertakings can appoint a single data protection officer if the data protection officer is accessible from each establishment. The data protection officer must have expert knowledge of data protection law and practices and can be a staff member or the controller or processor. The controller or processor must publish the data protection officers contact details and communicate them to the supervisory authority. In addition to Article 37 of the GDPR, Section 38 of the BDSG stipulates that those controller and processors who employ at least 20 persons constantly dealing with the automates processing of personal data shall designate a data protection officer. Sections 38 (2), 6 (3), and 6 (4) of the BDSG stipulate that a data protection officer may not be dismissed or penalised because of the performance of their tasks and may only be dismissed for good cause.

15. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

There are no Germany-specific requirements here. However, Article 24 (1) of the GDPR requires controllers to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing of is performed in accordance with the provisions of the GDPR.

16. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

There are no Germany-specific requirements here, however, there are several information obligations under the GDPR (*see Article13, Article 14 of the GDPR*) which are further specified in the Federal Data Protection Act (*see Sections 32 and 33 of the BDSG*). Also, the controller is required to communicate a personal data breach to the data subject if the data breach is likely to result in a high risk to the rights and freedoms of the data subject (*Article 34 (1) of the GDPR), unless certain exceptions apply (Article 34 (3) of the GDPR*).

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

There are no Germany-specific requirements.

18. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

There are no Germany-specific requirements regarding automated decision-making, which includes profiling, Article 22 of the GDPR applies. “Profiling” is defined in Article 4 (4) of the GDPR and means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. Automatic decision making is not defined in the GDPR. According to Article 22 of the GDPR, a data subject shall have the right not to be the subject to a decision based solely on automated processing, including profiling, which produces legal

effects concerning him or her or similarly significantly affects him or her. Section 4 of the BDSG contains specific requirements for video surveillance in publicly accessible areas. Such video surveillance is permitted only under certain circumstances, such as far as it is necessary for public bodies to perform their tasks, to exercise the right to determine who shall be allowed or denied access or to safeguard legitimate interests for specifically defined purposes. Notably, it is controversially discussed to what extend Section 4 BDSG is covered by the opening clause of Article (6) (1) (e), (2) and (3) of the GDPR.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

There is no legal definition of targeted advertisement or behavioural advertisement in Germany. To the extent personal data is used, the general principles apply, e.g. a legal basis is required (*Article 6 (1) GDPR*). If the processing of personal data is based on consent (*Article 6 (1) (a) GDPR*) and/or "Cookies", please see the response to question 5. See also the further requirements as described under question 22 in case the advertisement is provided via automated calling systems without human intervention, fax or email for the purposes of direct marketing or phone calls.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

N/A

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

The requirements for unsolicited communication via automated calling systems without human intervention, fax or email for the purposes of direct marketing follow from Article 13 of the e-Privacy directive and Section 7 (2) No. of the German Unfair Competition Act (*UWG*). Such communication requires prior consent unless certain exceptions apply, such as that the recipient provided the contact details to the sender as customer in the context of the sale of a product or a service (*Section 7 (3) UWG*). In case of phone calls (by humans) to consumers, prior explicit consent is required (*Section 7 (2) no. 1 UWG*).

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

There are no Germany-specific requirements. The definition of "biometric data" under Article 4 (14) of the GDPR applies according to which "biometric data" means "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*". Article 9 of the GDPR and Section 22 of the BDSG apply with regard to the processing of such data.

23. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

N/A

24. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

There are no Germany specific requirements as regards such transfer of personal data, however, given that the GDPR applies directly in Germany, the provisions set out therein as regards transfers of personal data to a third country must be complied with. Thus, under the GDPR, a transfer of personal data to a third country may take place, *inter alia,* where the European Commission has decided that the third country ensures an adequate level of protection by means of an adequacy decision (*see Art. 45(1) and (3) GDPR*). In the absence of such adequacy decision, personal data may only be transferred to a third country subject to appropriate safeguards, which may be provided for by, *inter alia*, binding corporate rules (*see Art. 46(2)(b) and 47 GDPR)* or standard data protection clauses adopted by the European Commission (*see Art. 46(2)(c) GDPR*). In the absence of an adequacy decision or appropriate safeguards, personal data may only be transferred to a third country if the requirements of Art. 49 GDPR are met (which provides derogations for specific situations). Specific requirements for cross-border

processing of data are established for bookkeeping and tax accounts as well as auditor and tax consultants' data in the Fiscal Code (*AO*) and the Public Accountant Act (*WPO*) and the Tax Advisors Act (*StBerG*), banking data in the Banking Act (*KWG*), social data in the Social Code Book (*SGB*) and telecommunications traffic data in the telecommunications act (*TKG*).

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

In Germany, the Federal Data Protection Act (*BDSG*) contains only a limited number of specific obligations for processors. The majority of obligations are derived from the provisions of Regulation (*EU*) 2016/679 (*GDPR*). The main obligations in data processing include, in particular, ensuring appropriate technical and organisational measures to guarantee data protection and data security, Articles 24, 25, and 32 GDPR. Art. 33 GDPR stipulates reporting obligations to the supervisory authority in connection with personal data breaches. Art. 35 and 36 GDPR require the controller to conduct an impact assessment for high-risk processing operations.

In addition to general data protection law, there are also various sector-specific laws that impose data security requirements. For example, the Telecommunications Digital Services Data Protection Act (*TDDDG*) requires providers of digital services to take technical and organisational precautions.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

Article 33 GDPR stipulates a reporting obligation in the case of a personal data breach. A "personal data breach" is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed (*Art. 4 no. 12 GDPR*). Both the European Data Protection Board and the German data protection authorities have issued guidelines in relation to data breach notifications. In addition, notification requirements may also follow from further rulebooks, including for operators of German critical infrastructure under German laws on critical infrastructure.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

Since the GDPR, as a principle, fully harmonises data protection law in the EU, the specific rights for individuals (data subjects) are laid down in Chapter III GDPR. They include, *inter alia*, the right of access (*Art. 15 GDPR*), the right to erasure (*Art. 17 GDPR*) and the right not to be subject to automated individual decision-making (*Art. 22 GDPR*). The modalities for the exercise of the data subject rights are laid down in Art. 12 GDPR. Thus, e.g. Art. 12(1) GDPR provides that the controller shall take appropriate measures to provide any information referred to in Chapter III GDPR relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plan language. In addition, the German legislator made use of opening clauses contained in the GDPR and introduced specific exceptions from some of the GDPR's data subject rights in national law. As an example, Sec. 34 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz – BDSG*) lays down exceptions from the right of access (*Art. 15 GDPR*) under specific conditions.

28. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

In Germany, affected individuals have the right to file complaints with a supervisory authority and can take legal action if their concerns are not addressed (*Art 78 of the GDPR*). Notwithstanding this, the GDPR provides for the right of action against controllers and processors if an individual believes that their rights under the GDPR have been infringed as a result of processing of their personal data (*Art. 79 of the GDPR*). Substantively, such actions often rely on the right to compensation set out in Article 82 of the GDPR.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been

sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

In Germany, affected individuals are entitled to monetary compensation for data breaches. According to Article 82 of the GDPR, both material and immaterial damages can be claimed. Therefore, no actual material damage is required, and even non-material damage in the form of a loss of control or specific, individual fear is also sufficient for compensation. In practice, this leads to a large number of plaintiffs asserting claims for non-material damages. The decisive factor is whether the affected individual can present specific circumstances that plausibly indicate such an impairment. General concerns or abstract worries are typically not enough to meet this threshold.

30. How are data protection laws in your jurisdiction typically enforced?

In Germany, individuals have the right to file complaints with the competent data protection authority and to take legal action to privately enforce their data protection rights, which occurs frequently in the context of mass litigation. Qualified entities, as well as competitors, may also take legal action for violating data protection laws. In addition, data protection is primarily monitored by the data protection authorities, which are specifically responsible for investigating the filed complaints, conducting investigations and imposing fines or penalties when necessary.

31. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

In Germany, violations of data protection laws can lead to significant sanctions, including fines of up to EUR 20 million or 4% of the annual global turnover for serious violations. Less severe violations can result in fines up to EUR 10 million or 2% of the annual global turnover. In addition to fines, authorities can impose other orders, such as a temporary or permanent restriction or ban on data processing. In extreme cases, criminal sanctions, including imprisonment, may also be imposed.

32. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

In Germany, the calculation of fines for data protection violations is guided by Article 83 of the GDPR and further clarified by the guidelines of the European Data Protection Board. Fines are based on factors such as severity, duration of the violation, whether the violation was intentional, as well as the company's actions to mitigate harm. Also, factors like previous violations and the financial situation of the company are considered. The overall goal is to ensure that fines are proportional, effective, and dissuasive, promoting compliance with data protection laws.

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

In Germany, enforcement decisions are open to appeal. If a company disagrees with a sanction imposed by a data protection authority, it can challenge the decision in court. The appeal process typically involves filing a legal action with the administrative court (in the case of criminal sanctions before the criminal court). The decision can be appealed to higher courts if there are legal grounds. In certain cases, if there is a conflict of interpretation regarding EU law (*e.g. the GDPR*), the case could be referred to the European Court of Justice.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

In Germany, there is a growing focus on enforcing data protection regulations in the digital economy, particularly regarding large tech companies and data-driven business models. Another key trend is a focus on cross-border data transfers and ensuring compliance with GDPR's international data protection requirements.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

In Germany, only a limited number of regulations prescribe specific cybersecurity risk management measures. These regulations are primarily sector-specific and mostly concern critical infrastructures which are regulated under the BSI Act. Section 8a (1) BSI Act stipulates that operators of critical infrastructures are

obliged to take appropriate organisational and technical precautions to avoid disruptions to the availability, integrity, authenticity and confidentiality of their IT systems, components, and processes. The German implementation of the Directive (*EU*) 2022/2555 (*NIS2 Directive*) is pending and expected in 2025.

There are further sector-specific rules. For example, the German Banking Act (KWG) stipulates that a duly organised business must include appropriate and effective risk management measures, including appropriate technical and organisational resources, as well as an emergency management system for IT systems (*Section 25a (1) KWG*). In addition, Regulation (EU) 2022/2554 (*DORA*) includes several risk management related requirements for financial entities. Specific cybersecurity requirements may also apply for operators in the energy sector (Section 11 of the German Energy Industry Act (*EnWG*)).

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

In Germany, the legal framework for cybersecurity related supply chain management is still evolving. Currently, relevant requirements can be derived primarily from the laws on data security (which only indirectly relates to cybersecurity), and other sector-specific laws (for example *Section 25b of the German Banking Act* (*KWG*)). The Directive (*EU*) 2022/2555 (NIS2 Directive) captures supply chain management. The German implementation of the NIS2 Directive is pending and expected in 2025. Cybersecurity risk management measures are expected to consider the security of the supply chain as a whole, including aspects related to the security of interactions with direct suppliers and service providers. The German Government has also implemented additional arrangements to ensure that certain IT hardware from specific Asian suppliers is not used for German critical infrastructure.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

In Germany, operators of critical infrastructure have an obligation to report significant cybersecurity incidents to the Federal Office for Information Security (*BSI*) under the BSI Act. Companies in the special public interest may be subject to the same requirement under the BSI Act. In addition, information sharing requirements may follow from the GDPR and sector-specific rules.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

In Germany, operators of critical infrastructure are obliged under Section 8b (3) of the BSI Act to designate a central point of contact at the Federal Office for Information Security (*BSI*) and to ensure that they can be reached at all times through this point of contact. The BSI provides information on cybersecurity issues to this point of contact. Any incidents must also be reported to the BSI via this point of contact in accordance with Section 8b (4) BSI Act. Further sector-specific requirements apply. For example, operators of critical infrastructures that belong to the same sector may appoint a common higher-level point of contact for the exchange of information between the points of contact and the BSI. The same obligations also arise for energy operators (some of whom are also critical infrastructure operators) under Section 11 of the Energy Industry Act (*EnWG*). Operators of publicly available telecommunications networks as well as providers of publicly available electronic communication services must appoint a security officer according to Section 166 of the Telecommunications Act. The security officer is tasked with coordination and control of the security concept, and they are the contact person for the Federal Network Agency (*BNetzA*).

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

In Germany, there are specific cybersecurity requirements for operators of critical infrastructures in the sectors energy, information technology and telecommunication, transport and traffic, health, water, food, finance and insurance, and waste disposal under the BSI Act. Section 8a (1) BSI Act requires that operators of critical infrastructure take the necessary measures to ensure availability, integrity, authenticity and confidentiality of their information technology systems. This includes the deployment of detection systems (*Section 8a (1a) BSI Act*). Operators must prove compliance every other year, Section 8a (3) BSI Act, and they must report incidents immediately, Section 8b (4) BSI Act.

In addition, comparable requirements are laid down in further sector-specific rulebooks, e.g. in Sections 164ff. of the Telecommunications Act (*TKG*), Section 11 of the Energy Industry Act (*EnWG*) and Section 25a (1) German Banking Act (*KWG*).

Companies of special public interest must also report incidents regarding availability, integrity, authenticity or confidentiality of their information technology systems, Section 8f (7) and (8) BSI Act. Directive (*EU*) 2022/2555 (*NIS2*) extended the scope of "critical infrastructure". This directive has yet to be implemented into German law.

In addition, several specific requirements apply for public entities, including with respect to classified information.

40. What impact do international cybersecurity standards have on local laws and regulations?

European standards such as the EU Cybersecurity Act (*Regulation (EU) 2019/881*) and the NIS2 Directive (*Directive (EU) 2022/2555*) greatly impact the cybersecurity practice in Germany, as it is the duty of an EU Member State to implement EU directives into national law and to apply EU regulations. Standards such as ISO/IEC 27001, ISO/IEC 27701 and ISO 22301 provide relevant frameworks for managing information security and are also used by the Federal Office for Information Security as a benchmark for best practices.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

In Germany, there are cybersecurity-related reporting obligations in several specific laws. The reports must usually be made to the supervisory authority.

Operators of critical infrastructure and companies of special public interest are required to report incidents that are defined as disruptions to the availability, integrity, authenticity and confidentiality of the information technology systems the operator/provider uses, or components or processes that have led to or may lead to an outage or significant impairment of the functionality of the critical infrastructures they operate (Sections 8b (4) and 8f (7) and (8) BSI Act). In addition, providers of digital services must report security incidents that have a significant impact on the provision of a digital service they provide within the European Union, Section 8c (3) BSI Act.

There are further sector-specific rules. For example, operators of a public telecommunication network are required to report security incidents with significant impact on the operation of the networks or the provision of services, Section 168 (1) Telecommunications Act (*TKG*). Operators of energy supply networks (some of which have also been designated as critical infrastructure) must also report incidents regarding cybersecurity to the BSI (*Section 11 (1c) of the Energy Industry Act (EnWG)*).

42. How are cybersecurity laws in your jurisdiction typically enforced?

Cybersecurity laws in Germany are enforced through a combination of regulatory oversight, compliance requirements, public enforcement measures, such as fines and in some cases private enforcement. The Federal Office for Information Security (*BSI*) is the primary authority responsible for the enforcement of cybersecurity laws. In some specific sectors, the BSI's supervision is combined with the supervision of the competent authority for the respective sector. For example, in the banking sector, the Federal Financial Supervisory Authority (*BaFin*) is responsible for supervising compliance with the requirements of the German Banking Act (*KWG*), while in the energy industry sector the Federal Network Agency (*BNetzA*) monitors compliance with the provisions of the Energy Industry Act (*EnWG*). Enforcement measures include audits, inspections, monitoring, administrative orders, as well as fines and penalties.

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Under German cybersecurity law, regulators—primarily the Federal Office for Information Security (*BSI*)—have broad powers to inspect, audit, and oversee organisations, especially operators of critical infrastructure and companies of special public interest. The BSI can demand security audits, review documentation, conduct on-site inspections, and issue binding orders to fix security deficiencies under the BSI Act (*Sections 8a–8d*). Similar powers exist under the Telecommunications Act (*Section 166*), where the Federal Network Agency (*BNetzA*) can carry out audits and enforce compliance with a view to telecommunications

providers.

44. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction?

In Germany, cybersecurity and other regulatory rulebooks typically include rules on sanctions to ensure compliance with significant regulatory requirements. For example, failure to meet the cybersecurity requirements of the BSI Act is an administrative offense under Section 14 BSI Act. These administrative offenses can be punished with a fine of up to EUR 20 million Euros. In the energy industry, fines of up to EUR 100,000 Euros are possible (*Section 95 of the Energy Industry Act*), and in the banking industry, fines may reach up to EUR 50 million Euros (*Section 56 of the German Banking Act*). Section 228 of the Telecommunications-Act allows fines of up to EUR 300,000 Euros for failing to implement a security-concept. Fines can be higher in grave cases.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

For German cybersecurity-specific laws like the BSI Act or the Telecommunications Act (*TKG*), a specific range for the fine amount is typically set in the applicable legislation (e.g. up to EUR 20 million under the *BSI Act*). With respect to GDPR fines, the EDPB has published guidelines on fines. In practice, fines are imposed based on a case-by-case assessment, considering the risk posed by the violation and further factors.

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

In Germany, enforcement decisions can generally be challenged through an administrative or judicial remedy. These generally have a suspensive effect. In exceptional cases, appeals have no suspensive effect.

47. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

Cybersecurity enforcement efforts remain consistently growing, with a continued focus on critical infrastructures. Enforcement activity has mostly grown in response to ransomware attacks and supply chain vulnerabilities which have exponentially increased in recent years. To counter or optimally prevent breaches due to such attacks, authorities are prioritising rapid breach notification, risk-based security measures, and demonstrable compliance.

Contributors

Erasmus Hoffmann
Partner
erasmus.hoffmann@whitecase.com

Markus Langen
Partner
markus.langen@whitecase.com

Dr. Sylvia Lorenz
Partner
sylvia.lorenz@whitecase.com

Dr. Constantin Teetzmann
Local Partner
constantin.teetzmann@whitecase.com

Alissa Arms
Associate
alissa.arms@whitecase.com

Swantje Behm
Associate
swantje.behm@whitecase.com

Friederike Kirch
Associate
friederike.kirch@whitecase.com