COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Germany

DATA PROTECTION & CYBERSECURITY

Contributor

Heuking Kühn Lüer Wojtek

Dr Hans Markus Wulf

Partner | m.wulf@heuking.de

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 by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

In Germany, the topic of cyber security is regulated mainly in the regulations on the protection of personal data, i.e. the EU General Data Protection Regulation (GDPR), the Federal Data Protection Act (BDSG) and the Telecommunications Telemedia Data Protection Act (TTDSG). Here, the focus is on Article 32 GDPR and Section 19 TTDSG, which stipulate that companies must take the necessary technical and organisational measures to ensure data protection. In addition, there are sector-specific regulations, for example for **critical infrastructures** according to Section 8a of the BSI Act (last amended at the end of May 2021 by the IT Security Act 2.0) as well as for the **banking industry** in the "*Banking Supervisory Requirements for IT (BAIT)*" of the Federal Financial Supervisory Authority (BaFin) as well as in Section 25a of the German Banking Act (KWG) with its specification in the "*Minimum Requirements for Risk Management (Ma-Risk)*" and Section 80 of the German Securities Trading Act (WpHG*)*. The above minimum requirements are legally to be qualified as administrative directives. Similar regulations exist for **insurance companies** with the "*Insurance Law Requirements for IT (VAIT)*" and the "*Minimum Requirements for the Rules of Procedure of Insurance Companies (MaGo)*", also issued by the Federal Financial Supervisory Authority. Additionally, the European Digital Operational Resilience Act (Regulation (EU) 2022/2554, DORA) contains further requirements for financial companies (including insurance of financial risks) and their service providers in the area of information and communication technology. Further, especially in the **automotive industry**, other special laws such as the Product Safety Act, the Intelligent Road Traffic Systems Act or the eCall Regulation (Regulation (EU) 2015/758) for the introduction of the Emergency Call contain specific requirements for IT security. In the **energy sector**, corresponding requirements are contained in § 11 of the Energy Industry Act, according to which energy network operators must ensure adequate protection against threats to telecommunications and electronic data processing systems. The area of **smart metering**, i.e. the operation of smart gas, water or electricity meters, is also regulated in Germany by a special law, the Metering Point Operation Act, which provides for minimum requirements for the smart meter gateway in § 22. With regard to possible **certifications** for IT security, the EU Cyber Security Regulation (Regulation (EU) 2019/881) also provides a framework in Germany for the EU-wide certification of information and communication technology products, services and processes.

Finally, German **criminal law** also contains corresponding regulations, according to which in particular data espionage, phishing, acts preparatory to data espionage and phishing, data manipulation, computer sabotage and computer fraud are punishable under certain conditions.

For **platform operators,** the new EU Digital Services Act will become important soon, especially regarding the obligation to ensure cyber security in Article 7.

2. Are there any expected changes in the data protection, privacy and cybersecurity landscape in 2023-2024 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

For critical infrastructures further requirements and an expansion of the scope of the term critical infrastructure itself is to be expected. The European NIS-2 directive must be transposed into national law until 17 October 2024, which is expected to result in an IT Security Act 3.0 in Germany. After a further transition period,

considerably more companies will have to implement the strict requirements for operators of critical infrastructures.

Further changes are expected because of the Artificial Intelligence Act (AI-Act) and the Cyber Resilience Act (CRA), which are currently going through the EU legislative process. The AI-Act is intended to regulate the use of artificial intelligence in high risk areas and provides, for example, transparency obligations, an authorisation requirement for the European market and a risk and quality management system. The CRA, on the other hand, will focus on protecting digital products from IT security gaps.

3. Are there any registration or licensing requirements for entities covered by these laws, and, if so, what are the requirements? Are there any exemptions?

Especially in the area of critical infrastructures, there is an obligation in Germany for the companies concerned to provide evidence of compliance with the necessary technical and organisational measures in accordance with § 8a of the BSI Act. Such proof must be provided every two years and can be provided through security audits, examinations or certifications by one of the recognised certification bodies. In addition, according to Section 8b of the BSI Act, there is an obligation to register and specify a contact point, and there is also an **obligation to report** IT malfunctions. Additionally, the obligation to report cyber security incidents in accordance with Art. 33 GDPR applies.

The **obligation to register** as a critical infrastructure operator exists as soon as a company falls under this term. According to Section 1 No. 2 of the **BSI Critical Infrastructure Ordinance**, a critical infrastructure operator is any natural or legal person who, taking into account the legal, economic and factual circumstances, exercises decisive influence over the nature and operation of a critical infrastructure facility or parts thereof. Whether such a facility is involved is regulated separately for each sector in the BSI Critical Infrastructure Ordinance. A bank, for example, falls under the definition of a critical infrastructure provider if it operates a system that processes more than 100 million account transactions per year for its customers.

4. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The definition of personal data is in accordance with the requirements of Art. 4 No.1 GDPR. The BDSG does not provide for a different definition. The same applies to the term sensitive personal data according to Art. 9 of the GDPR.

5. What are the principles related to the general processing of personal data or PII. For example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction, or must personal data or PII only be kept for a certain period? Please outline any such principles or “fair information practice principles” in detail.

In the area of general processing of personal data, German law does not contain any provisions that deviate from the GDPR. The general requirements in Art. 5 and Art. 6 of the GDPR apply, according to which processing must comply with the principles of lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability. Special regulations for companies (mostly specifications of the GDPR) were only made in Germany on the topics of video surveillance (§ 4), employee data protection (§ 26), research purposes (§ 27), archiving purposes (§ 28), data subject rights (§ 29, §§ 32-37), consumer credits (§ 30), scoring (§ 31) and the data protection officer (§ 38). Of particular importance in practice is the provision of § 26 BDSG, according to which personal data of **company employees** may only be processed if this is absolutely necessary for the performance of the employment contract. German companies are therefore subject to significantly higher requirements on this point than companies in other EU states, which can fall back on the general legal basis of Art. 6 para. 1 sentence 1 lit. f) GDPR.

6. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

The general requirements of Article 7 of the GDPR also apply to consent. In the area of **sensitive, personal data, the** condition applies in Germany that any processing requires the prior consent of the data subject, unless certain exceptions apply (Art. 9 GDPR, Section 22 BDSG). With regard to **employee data protection,** however, Section 26 (2) BDSG contains the additional

requirement that consent in the employment relationship should only be permissible in exceptional cases due to the lack of voluntariness, in particular if the employee in question receives a legal or economic advantage for giving consent to the processing of his or her data or if the employer and the employee pursue similar interests. The German legislator has thus explicitly increased the requirements for consent at this point. In the area of **direct marketing**, Section 7 of the Unfair Competition Act (UWG) expressly provides that sending e-mails to consumers for advertising purposes is only permissible with prior consent, unless the recipient is a customer and the other requirements of Section 7 (3) UWG are met.

7. 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 requirements of Art. 7 of the GDPR also apply to the form of consent, which can therefore also be given verbally. In the **employment relationship**, the special provisions of Section 26 BDSG apply. Paragraph 2 explicitly states that the employee's consent must be given in writing or electronically, unless another form is appropriate due to special circumstances. Overall, the German supervisory authorities require that consent be explicit, i.e. that it cannot be replaced by implied, tacit action. On the internet, therefore, an **opt-in** rather than an **opt-out** is necessary. This applies in particular to **cookies**, which, according to the provision of § 25 TDDSG, requires explicit consent unless the setting of the cookie is absolutely necessary for the function of the website. Declarations of consent must be **deleted** when they are no longer needed as evidence for the intended purpose, i.e. when a revocation takes place or the legal relationship in question expires for another reason. In most cases, the German supervisory authorities consider a further retention period of 3 months from the end of the intended purpose to be appropriate, unless there are statutory retention obligations (e.g. § 147 of the German Fiscal Code).

8. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection or disclosure?

The processing of sensitive personal data in Germany is also based on Article 9 of the GDPR. In addition, Section 22 of the German Federal Data Protection Act (BDSG) has been made more specific, according to which processing for purposes of preventive health care or medical diagnostics, for example, is expressly recognised as permissible under the conditions set out there.

AI Act prohibits the use certain AI tools, such as systems for social scoring or biometric real-time remote identification in publicly accessible spaces. The expected prohibition of these tools will result in a further restriction of the processing of sensitive personal data.

9. How do the laws in your jurisdiction address children's personal data?

With regard to the processing of personal data of minors, the German legislator has not adopted any independent regulations. The high requirements for the consent of minors according to Article 8 of the GDPR apply, according to which such consent is only permissible after the age of 16 and a special verification must take place within the framework of the proxy (Article 8 (2) of the GDPR). In addition, the Digital Services Act (DSA) requires the technical prevention of profiling and personalised advertising aimed at minors.

10. How do the laws in your jurisdiction address health data?

Also concerning health data, according to Article 9 of the GDPR and Section 22 of the BDSG the requirements regarding the processing of sensitive personal data are applicable (see above), including the exemptions for for purposes of preventive health care or medical diagnostics. For doctors or members of other professions who are subject to a duty of confidentiality, there are even stricter sanctions in case of disclosure of data (section 203 of the German Criminal Code). In some areas, the German legislator has exercised the possibility provided by Art. 9 (4) of the GDPR to create further restrictions in the area of health data. For example, consent to genetic examinations must be given in writing to the responsible doctor (Section 8 of the German Human Genetic Testing Act). Nevertheless, there are some laws that contain legal conditions under which the processing of health data is permissible, such as the German Infection Protection Act, the Transplantation Law, the Medical Devices Act, or the Insurance Contract Act.

11. Do the laws include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

The regulations in the BDSG are for the most part of a clarifying, concretising nature. With the exception of video surveillance and employee data protection, the provisions of the GDPR apply for the most part, partly supplemented by clarifying provisions in the BDSG (see above).

12. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

Data protection through technology design and data protection-friendly default settings is explicitly regulated in Article 25 of the GDPR and provides that every company must take the appropriate technical and organisational measures to comply with mandatory data protection principles of Article 5 of the GDPR, such as data minimisation. The German legislator has not adopted any specifications or supplements in this regard. The supervisory authorities also refer to the general provisions of the GDPR and do not impose any additional requirements.

13. Are owners/controllers or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

The requirement to keep a processing register is generally regulated in Article 30 of the GDPR. In Germany, no supplementary regulations have been made in this regard. In the employment relationship, the regulation in Section 26 (2) BDSG applies that consent from employees must be obtained in writing or electronically, unless another form is appropriate due to special circumstances. The corresponding consent must therefore be kept by the employer for the period of processing of the relevant personal data. In addition, tax law requirements apply, in particular from section 147 of the German Fiscal Code, according to which, for example, business letters must be kept for 6 years and accounting vouchers for 10 years. These legal retention requirements entitle the company to continue processing despite a possible cessation of the purpose of collection (see Art. 17 para. 3 lit. b GDPR).

14. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

There are no separate regulations in Germany on the obligation to delete data under data protection law. The general regulations in Art. 17 of the GDPR apply, according to which deletion must take place as soon as the purpose of the collection has subsequently ceased to exist, for example because the respective contract has been terminated. From the perspective of the German supervisory authorities, this (in conjunction with Art. 5 (2) GDPR) results in the obligation of every company to create and maintain a deletion concept in which the respective processing procedures are listed and provided with a respective deletion period.

15. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

In practice, advice from the supervisory authorities is only demanded in exceptional cases. The legal regulations in Germany do not impose any requirements of their own. As a rule, therefore, the obligation under Art. 36 GDPR remains, according to which every company must consult the competent supervisory authority before introducing new processing operations with a high risk to the rights and freedoms of natural persons, unless it can take measures to mitigate the risk. In accordance with Art. 17 DORA, serious incidents regarding information and communication technology in the financial sector must also be reported to the competent authority.

16. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

The performance of a risk assessment is explicitly required in some places of the GDPR, such as in the

analysis of technical and organisational measures under Art. 32 GDPR, in the **data protection impact assessment** under Art. 35 GDPR or in the question of the necessary notification of a **data protection incident** under Art. 33 GDPR. Furthermore, German law does not provide for any separate obligations for risk assessment in data protection. However, it is important to note that in 2020 the European Court of Justice (Schrems II) and subsequently the European Data Protection Board (Recommendation No. 01/2020) required a risk assessment to be carried out on international data transfers (**Data Transfer Risk Assessment**), assessing the legal provisions of the third country with regard to an impairment of the level of protection by official monitoring measures. These requirements were included in clause 14 of the new EU standard contractual clauses in June 2021. The risk assessment is carried out by each company in a different way. The supervisory authorities have partly published templates for such a risk assessment in German (www.lda.bayern.de/de/thema_dsfa.html).

17. Do the laws in your jurisdiction require appointment of a data protection officer or a chief information security officer (or other person to be in charge of privacy or data protection at the organization), and what are their legal responsibilities?

Article 37 of the GDPR provides for an opening clause in paragraph 4 on the requirements for the appointment of data protection officers. The German legislator has made use of this and provided in **Section 38 BDSG** that companies with **20 or more employees** must appoint a data protection officer if they are involved in the automated processing of personal data. The provisions of Sections 38 (2), 6 (3) and (4) of the BDSG stipulate that a data protection officer may not be dismissed or discriminated against because of the performance of his or her duties and may only be dismissed for good cause. As a rule, it is therefore not possible to dismiss the company data protection officer in Germany. However, many companies in Germany appoint external data protection officers, so that this protection against dismissal does not apply.

18. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

Pursuant to Article 24 of the GDPR, data controllers must take the necessary organisational measures to ensure that personal data are processed on the basis of the GDPR. In the view of the German supervisory authorities, this also includes the regular implementation of employee training, which also results explicitly from Art. 39 (1) (b) GDPR ("*...training of employees involved in the processing operations...*"). There are no special regulations on this in Germany.

19. Do the laws in your jurisdiction require businesses to provide notice to data subjects of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

The requirements for informing data subjects about the type and manner of processing when data is collected are derived from Art. 13 and Art. 14 GDPR. As a rule, such information is provided by means of data protection notices which are referred to in the context of the collection processes, for example by using data protection declarations on a website. In Germany, the legislator has adopted restrictive requirements for the fulfilment of the duty to inform through §§ 32 and 33 BDSG. In addition to the restrictions in Article 13 (4) of the GDPR, Section 32 of the BDSG, for example, does not require the data subject to be informed if a) analogue data is further processed, b) there are overriding public interests of a public body, c) there are overriding public interests in the event of a threat to public safety or order, or d) there is a risk of legal claims being impaired or e) there is a risk of confidential data being transferred to public bodies. Similar restrictions exist under Section 33 BDSG in the case of data collection from third parties.

20. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data, and, if so, what are they? (For example, are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

The processing of personal data on behalf of a service provider is regulated in detail in Art. 28 GDPR. According to this, the company must conclude a separate contract for data processing before commissioning a service provider, insofar as the service provider could have the possibility to access personal data of the company within the scope of the contract. If the service provider is based

in a country outside the European Union or the European Economic Area, the supplementary requirements of Article 44 et seq. GDPR must be observed. The German legislator has not adopted any supplementary regulations on the subject of data processing.

21. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII, or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

In Germany, apart from Art. 28 GDPR, no supplementary requirements for contracts with processors have been adopted. Nor are any such supplementary requirements demanded by the German supervisory authorities, with the exception of international data transfer (see point 14 above).

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

The monitoring of natural persons is subject to high data protection requirements in the GDPR. The supervisory authorities in Germany consider the requirements for a positive balance of interests pursuant to Art. 6 (1) sentence 1 lit. f) of the GDPR to be met in the case of monitoring measures only in a few cases, so that a detailed data protection review is recommended prior to the introduction of such measures. If **automated decision-making** is used, the requirements of Article 22 of the GDPR apply, according to which the consent of the data subject must be available as a rule. There will probably be further restrictions in the future resulting from the European AI-Act, since the current draft contains several obligations for high risk AI (e.g. biometric identification systems, critical infrastructures, or employee management), such as comprehensive transparency obligations, a licensing requirement for the European market or a risk and quality management system. The German legislator has made special national regulations, especially on employment data protection and the use of cookies. According to Section 26 BDSG, the processing of **employee data** (in particular for monitoring purposes) without prior consent is only permissible if this is absolutely necessary for the performance of the employment contract; a requirement that is only likely to be met in exceptional cases. The use of **cookies**, on the other hand, is only permissible without prior consent under section 25 of the TDDSG if it is necessary to carry out a transmission process or to use a telemedia service (e.g. a website). In case of doubt, prior consent must therefore be obtained in both cases.

23. Please describe any restrictions on targeted advertising and cross-contextual behavioral advertising. How are these terms or related terms defined?

Cross-contextual behavioural advertising combines the recognition of website content based on its context without collecting personal data with an anonymous collection of user behaviour on the website. In both cases, personal data of the users (such as the IP address) is not collected and used, so that a personal reference (at best) cannot be established. In Germany, this form of advertising has not yet become widespread; cookies are still predominantly collected on websites, with corresponding cookie banners being used. Specific legislation on the above form of advertising has not yet been passed. Most recently, in December 2021, there were new provisions on the use of cookies in Section 25 of the TTDSG (see point 22 above). Additionally, also the Digital Services Act requires online platforms to disclose who pays for advertisements and why they are shown to the user (Article 26 of the DSA).

24. Please describe any laws in your jurisdiction addressing the sale of personal data. How is “sale” or related terms defined, and what restrictions are imposed, if any?

The sale of personal data is not separately standardised in Germany. Therefore, the regular requirements of data protection and unfair competition law (UWG) apply. According to Art. 6 para. 1 sentence 1 lit. f) GDPR, the sale of personal data without prior consent of the data subject is only permissible if the data subject’s interests worthy of protection do not outweigh the legitimate interests of the selling company. This depends very significantly on the respective category of data. While the sale of personal privacy data usually outweighs the legitimate interest of the data subject, the sale of general personal information (IP address, general information on website use) can be considered in individual cases even without consent. In the case of e-mail addresses, the national specifics of Section 7 of the Unfair Competition Act must be observed (UWG, see point 6 above), according to which the sending of e-

mails for advertising purposes is only permissible if the prior, express consent of the data subject has been obtained. However, access to non-personal data by other market participants is expected to be governed in the future by the EU Data Act.

25. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

The requirements for direct marketing in Germany are regulated in Section 7 of the Unfair Competition Act (UWG, see above paragraphs 6 and 22). In detail, this is subdivided into advertising measures using the telephone, fax or e-mail or SMS. Advertising by **telephone calls** is not permitted without the prior, express consent of the data subject if the data subject is a consumer (natural person). If a commercially active data subject (not a consumer) is called, no explicit but also a so-called presumed consent is sufficient for this. In case of doubt, the caller must therefore provide arguments why he assumed that the data subject would agree to the call (e.g. because he had placed a corresponding advertisement). According to Section 7 UWG, advertising by **fax** is only permissible if prior, express consent has been given. Advertising by **e-mail/SMS** is also only possible after prior, express consent, which in case of doubt must be proven by the sender, otherwise there is a risk of injunctive relief and claims for damages. If consent is not given, however, an exception applies, Section 7 (3) UWG. According to this, consent is not required if a) the recipient is a customer of the sender and had received the e-mail/SMS address in this context, b) the e-mail/SMS address is used for own similar goods or services (proximity to the contractual relationship), c) the recipient had not previously objected to the sending of e-mail/SMS for advertising purposes and d) the recipient is informed with each message that he/she can object to further use of his/her e-mail/SMS address for advertising purposes at any time.

26. Please describe any laws in your jurisdiction addressing biometrics such as facial recognition. How are these terms defined, and what restrictions are imposed, if any?

The processing of biometric data (such as fingerprints, patterns of the iris, dentition imprint or measurements or proportions of the face) falls within the scope of Art. 9 GDPR. There is therefore the principle that such is only permissible after prior, explicit consent. The German legislator has not issued its own guidelines on this topic. In general, it is made clear by the supervisory authorities that high requirements are placed on the processing of biometric data, especially with regard to the use of raw data, decentralised storage of templates, cooperation with the data subjects and the protection of data from unauthorised access. The EU AI Act is expected to further restrict the processing of biometric data using artificial intelligence.

27. Is the transfer of personal data or PII outside the 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? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

The transfer of personal data is subject to the same requirements of the GDPR both **within Germany and the European Union (EU) or the European Economic Area (EEA)**. There are no special German regulations in this regard. Insofar as such a transfer to an independent company takes place, the requirements of Art. 6 para. 1 sentence 1 GDPR must generally be examined to determine whether such a data transfer can take place with a legal basis, e.g. on the basis of legitimate interests according to lit. f). If the recipient is a service provider who is dependent on instructions and is only to act as an “extended arm” of the company, however, data processing pursuant to Art. 28 GDPR comes into consideration, so that Art. 6 GDPR no longer needs to be resorted to. In this case, only a contract for data processing must be concluded. However, if the data recipient is located outside the EU/EEA, this is a third country transfer and the supplementary provisions of Art. 44 et seq. GDPR APPLY. As a rule, it is then necessary to conclude a further contract based on the EU standard contractual clauses pursuant to Art. 46 of the GDPR, unless Binding Corporate Rules or an adequacy decision of the EU Commission are available. In countries with legally legitimised data monitoring by government agencies (such as in the USA or China), the data protection authorities also require a risk assessment to be carried out (Data Transfer Impact Assessment, see point 16 above).

28. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

The obligations of companies to secure personal data are regulated in Art. 32 GDPR. The BDSG only provides for supplementary requirements for public bodies in Section 64, which, however, are largely covered by the generally required scope of services of Art. 32 GDPR. In addition, there are sector-specific special standards in Germany, such as for critical infrastructure operators under Section 8a of the BSI Act (see point 1 above). Further changes are to be expected when the NIS-2 Directive is incorporated into German law.

29. Do the data protection, privacy and cybersecurity laws in your jurisdiction address security breaches, and, if so, how does the law define “security breach”?

In the area of data protection, there are specific regulations on security breaches in Art. 33 of the GDPR. According to this, companies are obliged to inform the competent supervisory authority within 72 hours of becoming aware of a data protection incident. If there are high risks for the data subjects, they must also be informed separately in accordance with Article 34 of the GDPR. A data protection incident occurs as soon as there is a breach of the protection of personal data, for example through destruction, loss, unauthorised modification or unauthorised disclosure. In Germany, no supplementary national regulations have been adopted in the BDSG. In sector-specific terms, Section 8b of the BSI Act stipulates that operators of critical infrastructures must report certain disruptions to the competent federal office without delay. Corresponding requirements arise for energy network operators, for example, from Section 11 of the Energy Industry Act.

30. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

In Germany, operators of critical infrastructures are subject to special security requirements, which are primarily regulated in the BSI Act (see points 1 and 2 above). According to the BSI Critical Infrastructure Ordinance, the sectors of energy, water, information technology and telecommunications, health, finance and insurance as well as transport and traffic fall under the term critical infrastructure. However, the scope of the term will be extended by the NIS-2 directive.

Financial companies and their service providers in the area of information and communication technology (ICT) must also implement the requirements of the DORA on IT security such as compliance processes for the internal governance of ICT risks or uniform requirements for operational stability. Further requirements for the use of artificial intelligence are expected due to the EU AI Act.

31. Under what circumstances must a business report security breaches to regulators, to individuals or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator, and what is the typical custom or practice in your jurisdiction?

Notification obligations for security breaches exist in Germany for the area of data protection (Art. 33 GDPR, see point 27 above) as well as critical infrastructures (Section 8b BSI Act). The notification under the BSI Act is made to the Federal Office for Information Security (BSI), the notification under the GDPR is made to the supervisory authority responsible for the company (Article 51 et seq. GDPR). The German legislator has not made any special regulations for the notification of data protection violations, the GDPR therefore applies conclusively. However, it must be taken into account that in the event of a high risk for the data subjects (e.g. in the case of sensitive data or data relevant under criminal law), not only the supervisory authority must be informed, but also the respective data subjects pursuant to Article 34 of the GDPR.

32. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cybercrime, such as the payment of ransoms in ransomware attacks?

Specific legal regulations for dealing with cybercrime have not been enacted in Germany. However, the supervisory authorities regularly provide information on the current status of threats. For example, the data protection authority in the federal state of Bavaria recently published a special recommendation for preventive measures with regard to ransomware in 2021

(link: https://www.lda.bayern.de/media/pruefungen/Ransomware_Praevention_Handreichung.pdf).

33. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

In addition to the 16 state data protection authorities, which are specifically responsible for supervising compliance with data protection law, the **Federal Office for Information Security** (BSI) in particular is responsible for supervising compliance with IT security law in Germany. On the one hand, the BSI has the task to preventively promote cyber security in the state, economy and society, to create minimum standards as well as to protect the IT systems of the federal government, on the other hand, to certify security for IT systems and to supervise IT security for operators of critical infrastructures according to the BSI Act. Subordinate to the BSI is the National Cyber Defence Centre, which coordinates operational cooperation between the German federal authorities and develops and implements cyber defence strategies.

34. Do the laws in your jurisdiction provide individual data privacy rights such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

The data subject rights in data protection are regulated in Articles 15 et seq. GDPR. Accordingly, data subjects have the right to information, rectification, deletion, restriction of processing, data portability and the right to object to processing on the basis of legitimate interests. The rights of data subjects were concretised by the German legislator and partially restricted by the regulations in §§ 29 and 32 to 37 BDSG. For example, Section 29 of the BDSG explicitly states that information may be refused if it is intended to disclose information that by its nature must be kept secret, in particular because of the overriding interests of a third party.

35. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

Compliance with the legal requirements on data protection and thus also the rights of data subjects can – after filing a corresponding complaint – be enforced by the competent supervisory authorities, against which legal remedies are possible before the courts. In addition, according to Art. 82 GDPR, data subjects are entitled to claim damages in the event of a violation of their rights (see section 35 below).

36. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

According to German case law, companies can only assert data protection claims in exceptional cases. However, the question of private right of action was clarified by the European Court of Justice (Case C-319/20, 28 April 2022). According to the ECJ, a consumer protection association has the right to file a claim if the respective processing of data concerns identified or identifiable natural persons even without a separate mandate from a data subject.

37. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection, privacy and/or cybersecurity laws? Is actual damage required, or is injury of feelings sufficient?

According to Article 82 of the GDPR, data subjects can claim damages in the event of a violation of their data protection rights. The prerequisite is a breach by the responsible company of the provisions of the GDPR or other regulations on data protection, such as the BDSG or clarifying legal provisions of the member states. The burden of proof for the data protection breach lies with the data subject, but Art. 82 GDPR does not require fault on the part of the claimant. The latter therefore bears the burden of proving that it is not responsible for the data protection breach. German law does not provide for any special requirements for claims for damages under data protection law. According to recital 146 of the GDPR, the concept of damage is to be interpreted broadly. It is therefore possible to claim not only pecuniary damage, but also non-pecuniary damage (compensation for pain and suffering). Since the GDPR came into force, claims for damages for pain and suffering have been awarded in Germany in amounts between EUR 500 and EUR 5,000. Whether a so-called materiality threshold exists below which a claim for damages is to be excluded has not yet been clarified by the highest courts. This question was submitted to the European Court of Justice for a decision by the Supreme Court in Austria on 15.04.2021 (Ref. 6 Ob 35/21x). A decision is still pending at the time of publication of this article. The Advocate General's opinion on this matter, which says that not all non-material damage must be compensated regardless of its severity, could determine the general direction of the decision (Case C-300/21,

Opinion of Advocate General Campos Sánchez-Bordona, delivered on 6 October 2022).

38. How are data protection, privacy and cybersecurity laws enforced?

The control and enforcement of data protection regulations in Germany is the responsibility of the **16 state data protection authorities**. They are also responsible for the related administrative processes such as notifications or complaints from data subjects. Pursuant to Art. 58 of the GDPR, in addition to far-reaching investigative and remedial powers, they also have the possibility to impose fines. In addition, the state data protection commissioners have joined forces with the Federal Data Protection Commissioner to form a so-called **Data Protection Conference** (Datenschutzkonferenz**,** DSK), which discusses and coordinates current issues and problems in data protection in various working groups.

39. What is the range of sanctions (including fines and penalties) for violation of data protection, privacy and cybersecurity laws?

According to Art. 83 of the GDPR, violations of data protection regulations can be punished with fines of up to EUR 20 million or 4% of the annual worldwide turnover. According to this provision, the fine should be effective, proportionate and dissuasive. The German legislator has enacted supplementary provisions in § 43 BDSG. In addition, there are comprehensive further powers for sanctioning, such as an order to stop the violation, an instruction to adapt the data processing to the legal requirements or the pronouncement of a temporary or definitive ban on data processing. The German legislator has also made use of its right under Article 84 of the GDPR and created its own **criminal offence** with Section 42 of the BDSG. According to this, certain serious violations of data protection (commercial transmission or making available of unauthorised data to a large number of persons, unauthorised processing or obtaining data with the intention of enrichment) can also be punished with a prison sentence of up to 3 years. Infringements of the BSI Act can also be punished with fines of up to EUR 20 million (§ 14 (5) of the BSI Act).

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

In October 2019, the German Data Protection Conference (DSK), an association of the data protection commissioners of the federal states and the Federal Data Protection Commissioner, published a concept for the calculation of fines in proceedings against companies (https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf). The calculation of the fine is to be determined by taking into account the size and turnover of the company and the severity of the data protection violation. In application of this concept, the highest fine to date in Germany was imposed in 2021 in the amount of EUR 35 million on the company H&M for unlawful processing of sensitive employee data.

41. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Art. 78 GDPR provides that the addressees of sanction measures by the supervisory authorities have the right to appeal to the courts. In fine proceedings, the local courts or the regional courts (the latter from a fine of EUR 100,000) have jurisdiction pursuant to Section 41 BDSG and Section 68 of the Administrative Offences Act.

42. Are there any identifiable trends in enforcement activity in your jurisdiction?

Especially the GDPR continues to be enforced in Germany and a certain routine has now developed in the prosecution of violations by the data protection authorities. Also, very high fines are still only imposed in individual cases. Overall, there is currently a high level of enforcement, which can be well addressed through consistent implementation of all legal requirements.

43. Are there any proposals for reforming data protection, privacy and/or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

In Germany, the new **IT Security Act** only came into force in May 2021, which regulates comprehensive protection of critical infrastructures and, in § 8a BSI Act, for the first time provides for the obligation to introduce an attack detection system by 01.05.2023. At the EU level, the NIS-2 Directive was adopted in December 2022. Now the member states must transpose the requirements of the directive into national law by 17

October 2024 (see point 2 above). In addition, important regulations are being voted on at EU level, in particular the Cyber Resilience Act, the AI Act, the Data Act and the Data Governance Act. It is to be expected that these regulations will cause a considerable implementation effort for companies in practice.

Contributors

Dr Hans Markus Wulf
Partner

m.wulf@heuking.de