IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 9

GERMANY

Michael R Kissler[1]

I OVERVIEW

Germany has been and still is the forerunner on privacy and data protection law. In 1970, the German state of Hesse enacted the world's first Data Protection Act. The other states soon followed, and on 1 January 1978, the first German Federal Data Protection Act (BDSG) entered into force. These acts established basic principles of data protection, such as the requirement of a legal permission or the data subject's consent for any processing of personal data. In 1983, the German Federal Constitutional Court held that the individual has a constitutional right to 'informational self-determination'. The background of this groundbreaking verdict was a census planned for the year 1983, which essentially focused on the census of the entire German population by the means of electronic data processing. The people of Germany were anything but pleased with this idea and – as a consequence – more than 1,600 complaints were filed at the Federal Constitutional Court against the census law that had been specifically adopted for the census by the German parliament. Finally, in December 1983, the German Federal Constitutional Court declared certain provisions of the Census Act to be unconstitutional.

Over time, the German Federal Data Protection Act was subsequently amended to meet the requirements of a society in which data processing has grown more important. Especially, digitalisation raised a lot of questions, which needed to be handled. Keeping this in mind, among other things the legislator passed the German Telemedia Act (TMA) in 2007, which stipulated the duty to safeguard data protection during the operation of telemedia services. However, when data protection law and telemedia law became increasingly intersected by the internet, it was planned by the European legislator that the ePrivacy Regulation replacing the TMA would also come into force at the same time as the General Data Protection Regulation (GDPR). Whereas the GDPR has been applicable from 25 May 2018, the ePrivacy Regulation is still subject to negotiations at the European level and is not expected to come into force before 2024. The German legislator intended to eliminate the legal uncertainty resulting from this by means of the new Telecommunications Telemedia Data Protection Act (TTDPA), which implements the requirements of the European ePrivacy Directive that should have already been transformed to German law years before. The TTDPA finally came into force in December 2021.

1 Michael R Kissler is a lawyer and of counsel at Winheller Attorneys at Law & Tax Advisors.

The following text provides an overview of the current legal situation in Germany and presents the changes and the challenges of a new era of data protection in connection with digitalisation.

II THE YEAR IN REVIEW

Over the past years, a shift in the jurisdiction has become apparent regarding non-material damage claims. More courts did not apply the substantiality threshold as strictly as it has been in previous years. The substantiality threshold requires an objectively comprehensible and noticeable impairment of the right of personality or a certain materiality of the losses. Whereas some courts apply this principle strictly,[2] others have a broad understanding and include also minor damages[3] or consider any breach of a provision of the GDPR, including the formal requirements, as sufficient for a non-material damage claim[4] under Article 82 GDPR. This development will continue within the next few years as the previous German case law, which awarded non-material damages only in the case of severe violations of personality rights are no longer applicable considering Article 82 GDPR. Since the GDPR has been in force, the term 'damage' is a concept under European law that does not acknowledge a substantiality threshold.[5] This inconsistency in the interpretation of the relevant damages standard of data protection law led to legal uncertainties for data subjects and data processing companies alike.

Finally, the European Court of Justice (ECJ) has made a landmark ruling on Article 82 GDPR on 4 May 2023 and made clear there is no materiality threshold, but damage must be proven.[6]

In this judgment, the ECJ points out that, according to the wording of Article 82(1) GDPR, not every breach of a provision of the GDPR automatically triggers a claim for damages. A systematic interpretation of the regulatory context of the provision, including its Paragraph 2, and the inclusion of Recitals 75, 85 and 146 of the GDPR also confirmed this result. According to the ECJ, the objective of the GDPR is to ensure a consistent and high level of protection of individuals with regard to the processing of personal data in the EU and to ensure a consistent and uniform application of data protection rules throughout the Union. A materiality threshold depending on the assessment by the competent courts would run counter to this, as this could vary depending on the court. This makes it clear that national courts can no longer reject claims for damages under Article 82 of the GDPR by referring to the damage to be compensated as trivial. However, the ECJ does not explain under which circumstances non-material damage should be present. Furthermore, the ECJ referred to the assessment of damages and stated that while the GDPR does not contain any provisions for the assessment of damages, further elaboration of the criteria for determining the extent of damages is the task of the national law of the individual Member States.

Another topic that has been of immense relevance over the past years is the topic of data transfers to non-EU countries, especially the United States. The legal uncertainties caused by the decision of the ECJ of 16 July 2020 (*Schrems II*) still exist, but there might be some

2 https://rewis.io/urteile/urteil/c9g-23-09-2021-6-o-19021/.

3 https://openjur.de/u/2352669.html.

4 BeckRS 2021, 32008; OLG Hamm, judgement of 20 January 2023 – 11 U 88/22.

5 https://openjur.de/u/2383407.html.

6 https://curia.europa.eu/juris/document/document.jsf?text=&docid=274772&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=474732.

movement in this matter. In this case, the ECJ declared the EU–US Privacy Shield invalid, so this adequacy decision could not serve as a transfer mechanism anymore. As the main argument against an adequate level of data protection in the US, the court stated the rights of US authorities to access the personal data of EU citizens secretly and without effective legal remedies. Although the court confirmed the European Commission's standard contractual clauses in its ruling, it also called for additional protective measures to ensure secure data transfer.[7] How exactly the additional protective measures must be designed depends on the specific individual case. Still, the European Data Protection Board passed guidelines on this topic.[8] Additionally, the European Commission introduced a new set of Standard Contractual Clauses which became mandatory by the end of 2022 at the latest and which already include a statutory obligation to perform a Transfer Impact Assessment (Clause 14).[9]

The assessment of whether secure data transfer to the United States can be guaranteed constitutes a big challenge for many companies. On the one hand, they are still busy with meeting the requirements of the GDPR and the corresponding new case law (e.g., obtaining the consent of data subjects when using tracking cookies for marketing and analysis purposes). On the other hand, they lack the possibility to check whether the requirements for a lawful data transfer are met, as there is often an absence of cooperation by the US service providers whose services they use. Smaller companies are simply overwhelmed because they do not know what to do. This became very apparent by the increased need for digital interaction as a result of the covid-19 pandemic; for example, when using videoconferencing tools. What is particularly problematic about this is that the companies themselves are responsible for compliance with the GDPR requirements.

They need to take this responsibility very seriously, as the German data protection authorities (DPAs) have started to check the lawfulness of third-country data transfers, especially to the United States. For this purpose, the DPAs send out questionnaires in which they ask companies to disclose such transfers and to comment on the necessary security measures. An additional aggravating factor is that the German DPAs do not shy away from imposing high fines for serious data protection violations. However, a potential resolution to this challenge appears to be on the horizon. Both the European Union and the United States are currently contemplating the creation of a Trans-Atlantic Data Privacy Framework, which aims to rejuvenate the data protection agreement and offer substantial relief to enterprises. Commencing in October 2022, the US government embarked on this journey by issuing an Executive Order along with complementary measures designed to address the concerns raised by the ECJ. This concerted effort paved the way for the EU Commission's adequacy decision from 10 July 2023 on the new EU–US Data Privacy Framework. The proposed measures include constraints on data access by US intelligence agencies, limited to necessary and proportionate actions for national security, alongside the establishment of a Data Protection Review Court tasked with adjudicating complaints from affected individuals.

However, while these developments may offer immediate solace to businesses, the final assurance remains somewhat premature. The measures outlined in the Executive Order are considered inadequate by privacy advocates and regulatory authorities alike. It is

7 http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18.

8 https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

9 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

highly probable that the new agreement will, in due course, come under scrutiny before the ECJ – the outcome of which remains uncertain. These advancements undoubtedly provide companies with a more streamlined process, as the newly proposed measures can be factored into the 'transfer impact assessment' to facilitate data transmission.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The data protection in the electronic information and communication sector (telemedia) has often been criticised regarding its lack of clarity since legal matters in this area had to be resolved by applying EU laws (GDPR, E-Privacy-Directive) and German laws (TMA[10] and TCA[11]) at the same time.

However, since the 1 December 2021 is the Telecommunications and Telemedia Data Protection Act (TTDPA) in force which repeals the TMA and TCA. Besides providing a greater clarity by uniting the relevant regulations of the TMA and TCA in law, the TTDPA states now in Section 25 that the website provider must gain an explicit consent from the user when applying tracking services and cookies.

There are two exceptions to this principle. No consent is required when using technically necessary cookies which are absolutely necessary for operating the website. Also, cookies that serve exclusively for the transmission of messages via a public telecommunications network might be applied without consent. Furthermore, the TTDPA lays in Section 26 the foundation to tackle the widespread cookie banner. It gives personal information management services (PIMS) a legal framework. These services ought to enhance the user's control over their personal data by enabling them to set the conditions they wish to give their consent or refusal to concerning the setting of cookies for certain websites.

ii General obligations for data controller

The privacy provisions of the GDPR address data controllers, namely entities that process personal data on their own behalf or commission others to do the same.

Whereas this definition of a controller seems to be unambiguous, there has been a controversial debate in the field of employee data protection law, whether the worker's council needs to be classified as a data controller separate from the employer. The legislator resolved this issue by stating in the new Section 79 of the Works Constitution Act that the employer remains responsible for all data processing within the company, including the data processing the worker's council concludes to fulfil the tasks within its competence. The consequence is that the employer is liable for damages the works council caused by infringing provisions of the GDPR.

Telemedia service providers, as data controllers, may collect and use personal data only to the extent that the law specifically permits pursuant to Article 6 GDPR.

One relevant legal basis is still the consent according to Article 6(1)(a) GDPR which may be given electronically, provided the data controller ensures that the user of the service declares his or her consent knowingly and unambiguously, the consent is recorded, the user may view his or her consent declaration at any time and the user may withdraw consent at

10 Telemedia Act.

11 Telecommunication Act.

any time with effect for the future. These principles accord with Article 7 GDPR, which requires consent to be based on the voluntary and informed decision of the data subject. The information obligations for data controllers are stipulated in Articles 13 and 14 GDPR, according to which they must inform the user, inter alia, about the scope and purpose of the processing of personal data.

Since the GDPR has tightened the requirements for obtaining valid consent to process personal information, in practice, the relevance of the consent as legal basis has decreased and shifted to the legitimate interest of the data controller pursuant to Article 6(1)(f) GDPR. For this, the data controller must perform a three-part test and identify the legitimate interest, explain the necessity of achieving it and balance the interest against the data subject's interests, rights and freedoms. As long as the data subject would reasonably expect the respective processing activities and they have a minimal impact on the individual's privacy, no consent is needed. However, similar to the consent, the data subject has the right to object to processing activities based on the legitimate interest at any time according to Article 21(1) GDPR. The important difference is that the data controller may continue its processing activities despite the data subject's objection when the data controller can demonstrate compelling legitimate grounds that override the individual's interests, rights and freedoms.

Moreover, personal data may only be collected for specified purposes the data controller has determined before the collection took place. They must not be used for secondary purposes that are incompatible with the collection purpose. When verifying the compatibility between the primary collection and the secondary processing purpose, the criteria named in Article 6(4) GDPR are of paramount importance.

For ensuring the transparency of data processing activities, the data controller is obliged according to Articles 13 and 14 GDPR, inter alia, to inform the user of the extent and purpose of the processing of personal data. Although the DPAs in Germany were hesitant in the beginning to allow a layered approach in providing the legally prescribed information, a change is emerging. Regarding video surveillance, the German Data Protection Conference permits the distribution into essential information that must be provided onsite and other information that can be looked at online.[12] Single DPAs follow the layered approach as suggested by the European Data Protection Board in general.[13]

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

The international transfer of personal data is regulated within the framework of Articles 44–50 GDPR. There is a general distinction between transfers within the EU and EEA or to one of the 'trusted countries' for which the European Commission has confirmed by means of an 'adequacy decision' that these countries ensure an appropriate level of data protection on the one hand and transfers to third countries on the other. For an international data transfer to be lawful, it must comply not only with the aforementioned articles, but must also be in compliance with the general provisions pertaining to the legality of processing operations involving personal data.

12 DSK, Kurzpapier Nr. 15, www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf.

13 LDA Bayer, 8. Tätigkeitsbericht, https://www.lda.bayern.de/media/baylda_report_08.pdf#page=45; EDPB, Working Paper 260, https://datenschutz-hamburg.de/assets/pdf/wp260rev01_en.pdf.

i Data transfer within the EU or EEA

In contrast to the former legal situation, the GDPR does not explicitly stipulate that there is no difference between transfers within Germany or within the EU or EEA. Therefore, the only distinction is made between domestic transfers (within the EU or EEA) and those outside the EU or EEA.

ii Data transfer to countries outside the EU or EEA

If a private entity intends to transfer personal data internationally to another entity located outside the area of the EU or EEA (a third country), Article 44 GDPR specifies the requirements for such a transfer. In this respect, personal data shall not be transferred when the data subject has a legitimate interest in being excluded from the transfer. A legitimate interest is assumed when an adequate level of data protection cannot be guaranteed in the country to which the data are transferred.

An adequate level of data protection exists in certain third countries that have been identified by the European Commission. These are Andorra, Argentina, the Isle of Man, Canada (limited), the Faroe Islands, Israel (limited), Guernsey, Jersey, New Zealand, Japan, Switzerland and Uruguay. Any transfer of personal data to these countries will only have to satisfy the requirements of domestic data transfers.

As mentioned above, uncertainty surrounds data transfers to the United States since the ECJ invalidated the EU–US Privacy Shield on 16 July 2020.[14] Also, the ECJ ruled that standard contractual clauses are only valid when the data exporter positively assesses that the data importer is in the position to obey the requirements stipulated in these clauses under the importer's national legislation. This requirement in particular may be problematic to fulfil if governmental organisations do not need a judicial order to access data.

Data transfers to any other non-EU country may be justified by the derogation rules of Article 49 GDPR. Accordingly, the international transfer of personal data is admissible if:

a the data subject has given his or her consent;

b the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;

c the transfer is necessary for the conclusion or performance of a contract that has been or is to be concluded in the interest of the data subject between the controller and a third party;

d the transfer is necessary for important reasons of public interest;

e the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

f the transfer is necessary to protect the vital interests of the data subject; or

g the transfer is made from a register that is intended to provide information to the public, and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law are fulfilled in the particular case.

14 http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18.

The most relevant grounds are those given in (b), namely if the transfer is necessary to perform a contract between the data subject and the controller. This includes international monetary transactions and distance-selling contracts as well as employment contracts. All transfers in this respect have to be essential for the purposes of the contract.

Any consent within the meaning of (a) will only be valid if the data subject was informed about the risks that are involved in data transfers to countries that do not have an adequate standard of data protection. In addition, the consent has to be based on the data subject's free will; this may be difficult if employee data are involved.

If none of the aforementioned exceptions applies, the transfer of personal data to third countries with an inadequate level of data protection is nonetheless possible if, among other requirements, the competent supervisory authority authorises the transfer. Such an authorisation will only be granted when the companies involved adduce adequate safeguarding measures to compensate for a generally inadequate standard of data protection, see Article 49(1)2 GDPR. However, the primary safeguarding measures are the use of standard contractual clauses issued by the European Commission and the establishment of binding corporate rules. This is indicated by the fact that the European Commission has released a new version of the standard contractual clauses. The new standard contractual clauses are adapted to the requirements of the GDPR and in line with *Schrems II* of the ECJ. Another novelty is that contractual clauses can be adapted according to modules. Companies must have replaced all previously concluded standard contractual clauses for data transfers to third countries with the new version by the end of 2022.

iii Brexit

By now, the United Kingdom has left the EU. The transitional period ended on 31 December 2020. Although the EU and the UK agreed on a Brexit deal just in time, no final solution was found regarding data protection. Therefore, a further grace period was agreed until 30 April 2021, which was later extended by two months.

After a resolution in the European Parliament failed in May 2021 because of concerns about data security regarding subsequent transfers from the UK to other third countries and the extensive surveillance rights of British secret agencies, an adequacy decision was eventually adopted by the EU on 28 June 2021. As a result, the UK is now considered a 'safe third country' in terms of the GDPR and has avoided the fate of an unsecure third country, as suffered by the United States. However, the adequacy decision does not apply to data transfers for immigration control purposes. In this regard, data controllers must comply with the requirements of Article 46 et seq. GDPR.

The adequacy decision is valid until June 2025, at which point the EU Commission must review whether the adequacy of the UK's level of data protection is still guaranteed.

V COMPANY POLICIES AND PRACTICES

Article 24 GDPR outlines the responsibility of data controllers to implement appropriate technical and organisational measures to ensure the ongoing security and protection of personal data. This includes the establishment of a data protection management system that encompasses policies, procedures, and controls aimed at safeguarding personal data and ensuring compliance with data protection laws. Furthermore, the BDSG, which is the national legislation implementing the GDPR in Germany, emphasises the need for companies to appoint a data protection officer (DPO) under certain circumstances. The DPO plays a

crucial role in overseeing the company's data protection activities and ensuring compliance with data protection laws. This role is closely tied to the data protection management system, as the DPO is responsible for its design and implementation. Failure to establish and maintain an effective data protection management system could result in regulatory fines and other legal consequences. Therefore, companies operating in Germany must adhere to these legal requirements and establish a robust data protection management system to ensure the privacy and rights of individuals whose data they process.

VI DISCOVERY AND DISCLOSURE

In Germany, the authorities can inspect the information of bank customers, particularly in the banking sector (Section 24c of the German Banking Act). This account retrieval procedure can consequently be carried out in certain proceedings to gather evidence. The purpose is to ensure equal, fair taxation of all citizens. In addition, the purpose of account retrieval is, among other things, to curb money laundering and terrorist financing as well as the abuse of social benefits and to support the enforcement of public law and private law claims. In principle, this is always a processing operation within the meaning of the GDPR, so that in Germany there are various legal regulations, particularly in the areas of anti-money laundering, tax law and banking law, in which personal data is allowed to be processed.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Germany has a Federal Data Protection Agency and 17 state data protection agencies. These often act in concert when making recommendations on how customers can navigate safely through the internet. In addition, German experts often discuss the data protection problems that arise from the widespread collection of data by search engines and social media, and the use of these data to profile the data subject for commercial purposes.

The state data protection agencies are authorised to supervise the data privacy compliance of state entities, as well as all non-public entities whose principal place of business is established in the particular state and that are not subject to the exclusive jurisdiction of the federal supervisory authority. In states that have enacted a freedom of information act, the state supervisory authorities are typically also charged with supervising the act's application by state entities.

The heads of the supervisory authorities are typically appointed by the federal and state parliaments, respectively, and are required to report to their respective parliaments.

ii Material enforcement cases

Before the GDPR went into force, the mass media often reported about the high fines DPAs are authorised to impose when infringements occur. In the case of serious data protection violations, DPAs can indeed impose fines of up to €20 million or 4 per cent of the annual global turnover, whichever is higher. Under the old law, the fines for data protection breaches were up to €300,000 per breach. This massive increase is directly addressed to Big Data companies, which are often suspected of processing data in an unlawful way and can be used as a sharp sword to ensure conformity with GDPR. In particular, the dynamic and the dependency on the turnover aims to achieve a deterrent effect even on the wealthiest companies worldwide.

The German DPAs agreed on a fining model – *Bußgeldmodell*[15] – which, inter alia, takes into account the violating company's yearly turnover and the level of severity. In line with this calculation, a German telecommunication provider was fined €9.55 million for insufficient technical and organisational measures, and a housing association had to pay €14.5 million for using an archiving system for the retention of personal data of tenants that did not provide for the possibility of deleting data that was no longer required. But the record holder is the fine of €35 million imposed on the well-known fashion chain H&M for unlawful surveillance of several hundred employees at a service centre in Nuremberg. These cases show that the initial excitement about the increase in the framework of fines was justified.

Mostly, infringements are caused by insufficient internal compliance activities of companies where the responsible management carelessly contravened the high standards of data protection law (e.g., through video surveillance or keylogging). Another source of data protection breaches is the lack of employee training, which shall ensure that everybody in the company has the necessary knowledge to handle personal data in a lawful way. This illustrates the importance of a comprehensive data protection management in companies, which is implemented both technically and organisationally and has been made clear to the employees.

iii Information obligations in the context of private litigation

The GDPR obliges the data controller to provide the data subject with certain information about the data processing (see Articles 13 and 14 GDPR). It must inform the data subject about the identity and the contact details of the controller, the contact details of the data protection officer, if applicable, the purposes of the processing and its legal basis, the source of the data, where applicable, to whom they are disclosed, the duration of processing and the retention policy. Additionally, the data subject must be informed regarding all his or her rights granted by the GDPR. In detail, this notification must contain information concerning the right to information, right to rectification, right to be forgotten, right to restriction of processing, right to data portability, right to object and the right to lodge a complaint with a supervisory authority. This clearly shows that the data subject is being given numerous rights, but also that the controller will have to invest more effort in satisfying the requests in a proper way, which is a question of time and expense.

The privacy rights and remedies of telemedia users are governed to a large extent by Article 77 GDPR (the right to lodge a complaint with a supervisory authority) and Article 82 GDPR (the right to compensation). Data subjects may enforce their rights through the judicial remedies provided in civil law. Injunctive relief as well as damages can be claimed. In particular, damages for pain and suffering from data protection violations can be claimed under civil law.

In Germany, the DPAs are not necessarily involved in enforcing the rights of individual data subjects. Instead, complaints against domestic controllers can first be lodged with the company's in-house data protection officer.

However, in the event of unsatisfactory contact with the company data protection officer, the supervisory authority and the civil courts can, of course, be called upon.

In addition, some market participants started to take legal action against their competitors for violating data protection laws. So far, the Federal Court of Germany has not

15 https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf.

ruled whether a breach of the GDPR or other data protection laws may constitute unfair conduct according to the German Unfair Competition Act. Recently, an increasing number of higher regional courts have confirmed the admissibility of the GDPR infringements under this Act. If a market participant fails to inform about the processing of personal data in accordance with Article 13 GDPR within the scope of its internet presence, they face the threat of being admonished by a competitor. Other courts believe that the GDPR and other data protection legislation cannot be understood as rules that protect fair competition as well. Thus, they declined claims under the Unfair Competition Act. That is why many companies and their advisers await the supreme decision before breathing out or starting to immediately check their policies and actions.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As data protection gradually becomes a question of technical measures, especially cybersecurity, Article 32 GDPR determines that pseudonymisation and encryption must be applied to lower the risk of damaging the data subject in the event of data breaches. Since 2019, a considerable number of fines in Europe were grounded on inappropriate technical measures. This was also the case with a German health insurance company, which was fined €1.24 million for accidentally sending advertisements to data subjects without having asked them for prior consent.

That is why it is always worth emphasising that the implementation of technical and organisational measures may safeguard the controller from notifying a data breach to the relevant authority as the risk to the rights and freedoms of natural persons had been reduced from the start. As Article 33(1) GDPR stipulates that data breaches, where feasible, shall be notified by the controller to the supervising authority within 72 hours. Therefore, controllers must implement an effective data protection management system to be able to meet the deadline. Otherwise, a violation of this provision alone can be punished with a fine of up to €10 million or in the case of an undertaking, up to 2 per cent of the total worldwide annual turnover of the preceding financial year.

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

In Germany, the topic of IT security is becoming increasingly important, not least due to the political developments surrounding Russia and China. For this reason, the German government adopted the 'Cybersecurity Strategy for Germany 2021' in September 2021, which sets out the strategic framework for the German government's actions in this area for the coming years.

The strategy describes the fundamental, long-term direction of the German government's cybersecurity policy in the form of guidelines, fields of action and strategic goals. This should enable all players to work together in a targeted and coordinated manner. To support federal cooperation between the federal Government and the individual German states, the cybersecurity strategy for Germany and the cybersecurity strategies of the individual states are closely interlinked. Embedded in the European Cybersecurity Strategy, it is also a contribution to shaping Europe's digital future.

Germany already has legal requirements, especially for critical infrastructure, in the form of the IT Security Act and the KRITIS Regulation. Nevertheless, the cybersecurity strategy is currently being further developed and defines four overarching guidelines:

a establishing cybersecurity as a joint task of state, economy, society and science;
b strengthening the digital sovereignty of the state, business, science and society;
c making digitisation secure; and
d making goals measurable and transparent.

ii Data breaches

In 2022, 21,170 data breaches were reported to the German supervisory authorities in accordance with Article 33 GDPR. A large proportion of the data mishaps were related to hacker attacks, data loss, incorrect dispatch of documents or technical defects.

Thus, the number of reported data breaches by companies in Germany decreased again. In addition to the increasing legal certainty regarding the GDPR, this can also be explained by the fact that many companies do not report data breaches and instead note internally in accordance with Article 33(1) Sentence 1 GDPR that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

X SOFTWARE DEVELOPMENT AND VULNERABILITIES

Software development in Germany is intricately connected to data protection law. By integrating data protection measures into the software development process, identifying and mitigating vulnerabilities, conducting privacy impact assessments and adhering to breach reporting requirements, developers contribute to the overall protection of personal data and ensure compliance with the GDPR and BDSG. In a digital landscape where software vulnerabilities can have far-reaching consequences, a proactive approach to data protection in software development is paramount. The GDPR places a significant emphasis on the concept of 'data protection by design and default'. This principle requires organisations, including software developers, to integrate data protection measures into their processes and systems from the outset. For software development, this entails implementing privacy-enhancing features and safeguards that minimise the risks to data subjects' privacy. When creating software solutions, developers must assess potential vulnerabilities that could compromise the security of personal data. These vulnerabilities could include inadequate encryption, weak authentication mechanisms and poor access controls. By proactively addressing these vulnerabilities during the software development life cycle, developers contribute to compliance with data protection requirements.

Thus, software developers in Germany are obliged to conduct thorough risk assessments to identify vulnerabilities that may impact the security and privacy of personal data. These assessments involve evaluating potential threats, assessing the impact of a breach and devising strategies to mitigate risks. Vulnerability scanning, penetration testing and code reviews are essential techniques to uncover weaknesses and ensure software robustness. Mitigating vulnerabilities requires a multi-faceted approach. Developers should implement encryption mechanisms to protect data in transit and at rest, employ strong authentication methods to prevent unauthorised access and establish strict access controls to limit data exposure. Regular updates and patches are crucial to addressing emerging vulnerabilities and maintaining the security of software systems. In cases where software development projects involve high risks to data subjects' rights and freedoms, a data protection impact assessment (DPIA) is

mandatory according to Article 35 GDPR. Developers must conduct DPIAs to assess the potential impact of their software on data protection and privacy. This assessment aids in identifying vulnerabilities and devising strategies to mitigate risks effectively.

XI DIGITAL GOVERNANCE AND CONVERGENCE WITH COMPETITION POLICY

Creating an attractive, secure and agile data economy is one of the German government's strategic priorities. The goal is to strengthen the internationally competitive industry and the strong medium-sized companies in Germany through the possibilities of digitisation, so that this ensures growth and sustainability as well as innovations, economic dynamism and future-proof jobs. It is the basis for future competitiveness and enables effective use of the potential of data to make life better for everyone. We need a comprehensive and open data ecosystem as a building block of a strong European single data market. The development of data infrastructure, such as data platforms and data spaces in all sectors, must be further advanced quickly. The availability and use of data must be strengthened across sectors, and serve as a basis for innovative AI applications. The EU Data Act is intended to promote innovation-oriented data law for fair data access and use in Europe, which sets incentives for collecting and sharing data and facilitates provider switching for cloud services. A German Data Act is intended to create the necessary legal basis for these measures at national level.

XII OUTLOOK

Even five years after its introduction, several aspects of the GDPR are still heavily discussed. The 18 data protection authorities in Germany follow different interpretations of the GDPR in many regards. Additionally, there is still little and incoherent interpretation of the GDPR by the German courts. This makes consultation in data protection matters in Germany difficult, and uncertainties in many aspects remain. Therefore, it will be interesting to see how the new laws are interpreted by German and European courts to bring consistency and legal certainty. The European Commission highlighted the successes of the GDPR, because it is open to new technologies and has proven its worth during the covid-19 pandemic. In the future, it will also constitute the basis for the European Artificial Intelligence and Data Strategy. The European Commission still foresees more efficient and coherent cooperation between national authorities. Thus, data protection remains a field that constantly changes and evolves, especially as digitalisation speeds up. We are also looking forward to watching the continuing impact of the GDPR on companies, especially on social media operators and technology companies, and how European and national legislation and case law will further develop European data protection standards.

ISBN 978-1-80449-214-7