Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Data Protection & Privacy 2022

Germany: Law & Practice
Philip Kempermann and Thomas Jansen
Heuking Kühn Lüer Wojtek

practiceguides.chambers.com

GERMANY

Law and Practice

Contributed by:
Philip Kempermann and Thomas Jansen
Heuking Kühn Lüer Wojtek see p.19

CONTENTS

1. BASIC NATIONAL REGIME

1.1 Laws

As a member state of the European Union, Germany is subject to EU law. Therefore, the most important data protection regulation is EU Regulation 2016/679 (the General Data Protection Regulation, or GDPR). In addition to the GDPR, the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, or BDSG) is of importance. In Sections 1–44, the BDSG contains supplementary regulations on the GDPR putting data controllers' rights and responsibilities in more concrete terms. Sections 45–85 of the BDSG implement the provisions of EU Directive 2016/680. This Directive concerns the processing of personal data by authorities for the purposes of crime prevention and prosecution.

In addition to the BDSG, each federal state has its own data protection law. These state laws only affect public bodies.

Apart from the general data protection laws (GDPR, BDSG) there are various sector-specific data protection regulations; for example, in the areas of telecommunications, media or public health. However, so far there is no specific regulation for current hot topics such as AI or the metaverse.

Article 58 of the GDPR vests investigative and corrective powers in the supervisory authorities (see **1.2 Regulators** for details). As State authorities, they are bound by the general administrative law restrictions. With regard to fines, in addition to Article 83 of the GDPR, certain provisions of the German Law on Administrative Offences (*Ordnungswidrigkeitengesetz*, or OWiG) apply. Fines cannot be imposed on authorities (Section 43 (3), BDSG). Some state laws further stipulate exceptions to fines on public bodies.

1.2 Regulators

The federal structure of Germany is evident in the organisation of data protection supervision. The national supervisory authority, the Federal Commissioner for Data Protection and Freedom of Information, is responsible for federal authorities and telecommunications companies. The data protection authority of a particular state is responsible for the respective state authorities and for all the companies that have their main establishments in that federal state. Consequently, there are several supervisory bodies in Germany (18 in total) that sometimes have different views on the interpretation of the GDPR. For this reason, the supervisory authorities have formed a joint informal body to develop common positions on individual issues in order to ensure a uniform interpretation (*Datenschutzkonferenz*, or DSK). The DSK does not have any powers. However, if the DSK publishes opinions supported by all supervisory bodies, they cannot deviate from these opinions to the disadvantage of the controller due to administrative law restrictions.

All data protection authorities act independently. They are, in particular, not subject to any ministry's right of instruction. This independence of the supervisory authority is required by the GDPR (Article 52 (2)). It used to be one of most discussed topics in German data protection law before the GDPR came into force.

The authorities may investigate on the basis of their own initiative, a complaint by a citizen, a notification or other request from the controller or a request by another authority. According to Article 58 (1) (a) of the GDPR, every supervisory authority is entitled to conduct data protection audits. There is no requirement that a specific occasion must exist (however, see the restrictions described in **1.3 Administration and Enforcement Process**).

1.3 Administration and Enforcement Process

The authorities, like all state authorities, are bound by law. They may not proceed arbitrarily, must hear the person concerned before they act and may only act proportionately. For example, a fine is usually only proportionate if it is imposed in conjunction with another specific corrective measure that remedies the data protection breach.

In addition to these general restrictions, there are various specific restrictions that the supervisory authorities must observe: Section 29 (3) of the BDSG stipulates that no investigations may be carried out on persons subject to the obligations of professional secrecy (doctors, lawyers, etc) if this would be in violation of their confidentiality obligations. Apart from this, in the event of a search, the authority must only be granted access to the business premises during normal business hours (Section 16 (4), BDSG).

Fines

With regard to the level of fines imposed on companies, the DSK has developed a model to establish a uniform procedure for all German supervisory authorities. According to this model, fines are determined in five steps:

- assignment of the company to a size class;
- determination of the average annual turnover of the respective sub-group of the size class;
- determination of an economic basic value (*Tagessatz*);
- multiplication of the basic value by a factor dependent on the severity of the circumstances of the offence; and
- adjustment of the value determined on the basis of circumstances relating to the offender and other circumstances that were not yet taken into account.

This model is the subject of considerable controversy as it may lead to very high fines even for minor digressions. A first decision handed down by the Regional Court of Bonn (LG Bonn, judgement of 11 November 2020, case No 29 OWi 1/20), joined the critical voices. It explicitly stated that it is problematic to use the turnover of a company as a basis. Instead, according to the Court, the focus should be on the severity of the violation(s). In the specific case, the Federal Commissioner for Data Protection and Freedom of Information had originally imposed a fine of EUR9.55 million on the telecommunications company 1&1. The court reduced this fine to EUR900,000, as no serious violations were involved. While it is to be expected that the supervisory authorities in Germany will revise their model to meet the requirements set out by the Court this has not happened yet. Nevertheless, companies should by no means slacken in their data protection efforts. Fines can still be imposed, and still at a hefty level.

Another topic of current discussion is whether the violation of the GDPR needs to be attributable to a responsible person within the data controller. The regional court of Berlin said this was the case and annulled a EUR14.5 million fine because the supervisory authority failed to do so (LG Bonn, decision of 18 February 2021, case No (526 OWi LG) 212 Js-OWi 1/20). This decision has been appealed.

To provide effective legal protection, all actions of the supervisory authorities can be challenged before the administrative courts. This does not apply to fines. These must be challenged before the ordinary courts due to different procedural rules applying.

1.4 Multilateral and Subnational Issues

As mentioned in **1.1 Laws**, the GDPR applies in Germany. This also means that the German data protection authorities are part of the Euro-

pean Data Protection Board (EDPB), which aims at ensuring the consistent application of data protection rules throughout the European Union and at promoting co-operation between the national supervisory authorities. For example, under Article 70 (1) (k) of the GDPR, the EDPB can adopt guidelines on the imposition of fines by the supervisory authorities. This has not yet happened, but in the event that such EU-wide guidelines are adopted, the DSK has already announced that its own fine model (see **1.3 Administration and Enforcement Process**) would no longer be valid.

Data protection laws at state level apply, as already mentioned, only to public bodies. However, the state laws on administrative procedures can become relevant for private companies when challenging rulings by the data protection authorities (except those of the federal authority).

1.5 Major NGOs and Self-Regulatory Organisations

The German legislature has decided that some data protection rules are consumer protective (Section 2 (2) No 11, Law on Injunctions for Consumer Rights and other Infringements (*Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen*, or UKlaG)). As a result, consumer protection associations can take legal action against violations of data protection in certain cases.

Article 40 of the GDPR provides for the possibility of inter-branch organisations drawing up codes of conduct for their members. These codes can then be approved by the competent supervisory authority. This has the advantage that it is, subsequently, easier for a company to prove that it operates in conformity with data protection requirements. However, this possibility has only been used by a few associations so far.

1.6 System Characteristics

Germany is part of the EU data protection system, which is one of the most developed systems in the world. Even before the GDPR came into force, Germany already had a differentiated data protection regime. However, the GDPR has further increased acceptance and sensitivity around this topic. In addition, data protection authorities are increasingly enforcing the respective rules, particularly imposing fines. For these reasons, more and more companies are realising that data protection is an integral part of their compliance management. Accordingly, there is a high demand for consulting services. Apart from this, it is a political goal in Germany and the EU to establish data protection-compliant solutions as a trade mark.

1.7 Key Developments

The new standard contractual clauses (SCCs) implementing the ECJ's ruling on the EU-US Privacy Shield Agreement and standard contractual clauses (SCCs) (judgement of 16 July 2020, case No C-311/18 – "Schrems II") were adopted in summer 2021 and must be used for all new international data transfers that are based on SCCs. Existing international data transfers based on SCCs are grandfathered until 27 December 2022. By that time, the existing SCCs must be replaced by the new SCCs including, where necessary, putting in place transfer impact assessments (TIA) for each recipient. The question of the specific measures required after the TIA is still not fully clear and the various regulators in the DSK have so far not come to a unified position. (see **4.2 Mechanisms or Derogations that Apply to International Data Transfers** for details).

1.8 Significant Pending Changes, Hot Topics and Issues

The E-Privacy Regulation

The EU has still not passed the so-called E-Privacy Regulation. However, the German legisla-

ture replaced the data protection provisions of the Telecommunication Act (*Telekommunikationsgesetz*, or TKG) and the Telemedia Act (*Telemediengesetz*, or TMG) with the TTDSG (see below).

The TTDSG

The new Telecommunications Telemedia Data Protection Act (*Telekommunikations-Telemedien-Datenschutzgesetz*, or TTDSG) combines provisions on data protection for telemedia and in the telecommunications sector previously found in other laws. Among other things, it contains new rules for the use of cookies and other tracking tools. In principle, the user's consent is required before cookies can be set. This corresponds to already existing case law, but the legal situation had not previously been formulated so clearly. In addition, the responsibilities of the supervisory authorities are to be changed. The Federal Commissioner for Data Protection and Freedom of Information is to be uniformly responsible for data protection in telemedia (eg, for cookies). As an accompanying document, the DSK released guidelines for cookie management, consent, etc.

Right of Access and to Damages

The question of the scope of the right to access (see also **2.1 Omnibus Laws and General Requirements**) under Article 15 of the GDPR is still one of the most controversial issues in Germany. Several rulings have already been handed down on this issue, with varying implications. The Federal Labour Court (BAG) referred a case to the ECJ where the BAG is of the opinion that any violation of the GDPR indicates that a data subject suffers damages and that culpable behaviour on the part of the controller is not required to avoid damage (BAG, decision of 26 August 2021, case No 8 AZR 253/20). If the ECJ upholds the BAG's decision data subjects would be in a very strong position to enforce claims even for the most minor of GDPR violations.

2. FUNDAMENTAL LAWS

2.1 Omnibus Laws and General Requirements

As mentioned in **1.1 Laws**, the relevant data protection laws in Germany are the GDPR, the BDSG and some sector-specific regulations. These data protection laws all follow the same basic principle: the processing of personal data is prohibited if no permission has been granted (Article 6, GDPR). This can be a legal permission or the consent of the person concerned.

The scope of data protection laws is a crucial point. In order for the data protection rules to be applicable, the following conditions must be met. First, there must be personal data (Article 4 No 1, GDPR); secondly, this personal data must be processed (Article 4 No 2, GDPR). Thirdly, the processing must be carried out by means of an automatic system or, at least, the personal data must be stored in a filing system (Article 2, GDPR). Finally, the territorial applicability requirements must be met (Article 3, GDPR).

Personal Data

Generally speaking, personal data entails all information that can be linked to a natural person (eg, name, address and gender). According to the case law of the ECJ, even legal means that can be used against third parties to identify a person must be taken into account. One of the most important examples is an IP address. One can thereby identify a person if one claims information against the respective internet provider. Thus, an IP address is considered personal data.

Processing

The GDPR lists the following examples for processing: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction,

erasure or destruction. In general, any action concerning personal data constitutes processing in the meaning of the law.

Automatic System or Stored in a Filing System

An automatic or partially automatic system means all electronic means of processing personal data. Storage in a filing system refers, for example, to file folders that are sorted alphabetically.

Territorial Applicability

The GDPR is applicable if a controller or a processor is established in the EU. Apart from that, the GDPR is also applicable if the controller or processor is not established in the EU but their goods or services are offered to persons in the EU. Finally, the GDPR is also applicable if a company monitors the behaviour of persons in the EU.

Data Protection Officers (DPOs)

Whether a DPO must be appointed is determined by Article 37 of the GDPR. Authorities must always appoint a DPO. For private companies, the standard follows a risk-based approach: if the processing of personal data is one of the main activities of the data controller and if it is critical from the perspective of the data subjects, a DPO must be appointed. Whether the processing is critical depends on the nature, scope and/or purpose of the data processed. An example of critical processing in this sense are big data applications. Apart from this, there is an obligation to appoint a DPO if the controller or processor mainly processes special categories of personal data (Articles 9 and 10, GDPR). The German legislature has tried to specify these general requirements and stipulated in Section 38 of the BDSG that a DPO must be appointed in addition to the provisions of the GDPR if, as a rule, at least 20 persons in a company are permanently involved in the automated processing of personal data. If this threshold is met, the controller must appoint a DPO regardless of the other requirements.

The data protection officer is not subject to directives and enjoys special protection against dismissal. Their duties include working towards compliance with all provisions of data protection law. To this end, they shall advise the data controller and all employees and monitor compliance with the regulations. In addition, they act as a contact point for the supervisory authority.

Authorisation to Process (Legal Basis)

As mentioned, the legal permissions for processing personal data are listed in Article 6 of the GDPR. In detail, the possible permissions are:

- consent by the data subject; it is important to note that the consent must have been given voluntarily and can be withdrawn at any time;
- performance of a contract concluded with the data subject;
- compliance with a legal obligation;
- protection of vital interests;
- performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
- legitimate interests pursued by the controller or by a third party.

Another important legal permission is stated in Section 26 of the BDSG, which specifically applies in the employment context. Accordingly, personal data of employees may be processed for purposes of the employment. This concerns, among other things, recruitment, employment and termination of employment and also includes the processing of special categories of data. According to this provision, data processing in a company may also be carried out on the legal basis of a works agreement (see **2.2 Sectoral and Special Issues** (Employment Data) for details).

Data Protection by Design and by Default

It is the controller's obligation to implement appropriate technical and organisational measures to ensure that data protection principles are intact (Article 25 (1), GDPR). This must be taken into account when creating the procedure and during the actual processing. The relevant data protection principles are listed in Article 5 of the GDPR; eg, data minimisation. As a specific obligation, the controller has to ensure that, by default, only personal data that is necessary for each specific purpose of the processing is processed (Article 25 (2), GDPR). All these regulations implement data protection by design and by default as a legal obligation. A violation can be punished with a fine.

Impact Assessment

Under certain conditions, the responsible person is obliged to conduct a data protection impact assessment in advance of the processing; however, that and the Transfer Impact Assessment for international data transfers are the only mandatory impact assessments. So far no mandatory fairness or legitimacy assessments are required. At this point, the risk-based approach of the GDPR becomes evident: it is not necessary to carry out a prior impact assessment for every data processing operation. It is only necessary if the processing results in a high risk to the rights and freedoms of natural persons. The purpose of the assessment is to identify high-risk processing operations and to then take measures to minimise the associated risks. The DSK has drawn up a binding list for some processing operations where an impact assessment is or is not mandatory. This list is approved by the EDPB.

The assessment should be carried out in three steps: description of the processing operations, assessment of risks and definition of corrective actions. The impact assessment must be carried out for specific processing operations. Operations with similar risks may be grouped together.

Privacy Policies

There is no direct obligation to implement a data protection policy. However, there are numerous information obligations for certain processing situations (eg, Articles 13, 14 and 49 (1) (a), GDPR) and the general obligation to be able to prove compliance with the GDPR (Article 5 (2), GDPR). It is therefore recommended that a comprehensive data protection concept is developed and communicated to customers and/or employees. The information obligations are mandatory.

Furthermore, codes of conduct may exist in industry associations (see **1.5 Major NGOs and Self-Regulatory Organisations**). They can also become part of a company's private policy.

Data Subject Rights

It is one of the central goals of the GDPR to strengthen the rights of data subjects. For this reason, every data subject has the right of:

- access to data and information (Article 15, GDPR);
- rectification of inaccurate data (Article 16, GDPR);
- erasure of personal data (Article 17, GDPR);
- restriction of processing (Article 18, GDPR);
- portability of personal data (Article 20, GDPR); and
- objection to processing (Article 17, GDPR).

Apart from these rights, a data subject has the right to withdraw its consent at any time and without any reasons (Article 7, GDPR) and the right to lodge a complaint with a supervisory authority.

Some of these rights have certain preconditions that must be met before the affected person can exercise them. Nevertheless, it is the duty

of the controller to be able to comply with these rights in a timely and transparent manner (Article 12, GDPR). The data protection authorities can enforce these obligations (Article 58 (2) c), GDPR).

Anonymisation, De-identification, Pseudonymisation

Anonymisation, according to the GDPR, means that data can no longer be associated with a person. It is therefore no longer personal and is no longer subject to the provisions of the GDPR. However, it is important to note that data is only anonymous if it can no longer be traced back to a person under any circumstances. This is not the case with pseudonymisation. Here, the name of a person is replaced by a combination of different letters and figures. However, as long as it is possible for the controller to re-establish the connection to the name or to identify the person on the basis of the remaining personal information, the data continues to be personal in the meaning of the law. Nevertheless, pseudonymisation can be a useful technical protection measure (Article 25, GDPR), because it can, among other things, prevent unauthorised third parties from using the data.

Profiling, Automated Decision-Making, Big Data Analysis and AI

These ways of processing pose a higher risk to the rights and freedoms of data subjects than normal data processing. This does not mean that they are prohibited. However, following the GDPR's risk-based approach, these ways of processing personal data increase the obligations of the controller. For instance, as already mentioned, in the case of profiling, the controller has to conduct an impact assessment. Besides, Article 21 of the GDPR permits automated individual decision-making, which has legal effects, only in specific cases. In addition, the German legislature has created two further permits for automated decision-making in Section 37 of the BDSG. These requirements would also apply to microtargeting which has not been addressed specifically by regulatory requirements so far.

Injury or Harm

The GDPR provides, in Article 82, for a claim for damages for all immaterial and material damage resulting from a violation of data protection. Recital 85 of the GDPR gives the following examples of such damages: loss of control over personal data, restriction of rights, discrimination, identity theft or fraud, financial loss, unauthorised removal of pseudonymisation, damage to reputation, loss of confidentiality of data subject to professional secrecy, or other significant economic or social harm to the natural person concerned. The claim can be directed against the controller or the processor. The liability of the person responsible or the processor is presumed, but they may show that they are not responsible for the event giving rise to the damage and thereby evade liability. This provision is quite favourable to the data subject.

In addition, a so-called model declaratory action may be brought before a court. This is based on Sections 606 et seq of the Code of Civil Procedures (*Zivilprozessordnung*, or ZPO). This legal instrument allows certain consumer protection associations to bring such an action and thereby have it determined by a court whether consumers are entitled to damages. This can also refer to compensation for damages according to Article 82 of the GDPR. If the action is successful, the affected consumers themselves must, in a second lawsuit, seek legal action to obtain actual compensation based on the findings made in the class action.

The risk of representative actions in the case of data protection violations will increase in the future. The EU has adopted a new directive providing for the Europe-wide introduction of representative actions to protect consumer interests

(Directive 2020/1828). Breaches of the GDPR are explicitly mentioned as a basis for such lawsuits. What is special about these lawsuits is that qualified associations cannot only bring an action for a declaration of a breach, but directly for redress measures. Such measures include compensation, repair, replacement, price reduction, contract termination or reimbursement of the price paid (Article 9 (1) Directive 2020/1828). This possibility did not exist in this form in German law until now. However, the Directive is not yet applicable law. It must first be implemented into national law, at the latest by the end of 2022. The member states have some scope for implementation.

2.2 Sectoral and Special Issues

"Sensitive" Data

Different rules apply to the processing of special categories of data. According to Article 9 of the GDPR, these special categories of data are information relating to:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health; and
- data concerning a natural person's sex life or sexual orientation.

In all these cases, data cannot be processed on the legal basis of Article 6 of the GDPR. Instead, the permissions are listed in Article 9 (2) of the GDPR. However, the regulation contains some so-called opening clauses. These allow each EU member state to pass its own rules in a specific matter. The German legislature has used the opening clauses regarding special categories of data. For example, under Section 22 (1) No 1 of the BDSG, data may be processed in connection with social security and social protection law. This concerns, for example, pension and health insurance funds. However, it must be taken into account that sector-specific regulations – such as Sections 67 et seq of the Social Code (*Sozialgesetzbuch*, or SGB X) may also intervene. The processing of special categories of data of employees is regulated in Section 26 (3) of the BDSG. Accordingly, such special employee data may be processed, for example, if this is necessary for the fulfilment of legal obligations arising from labour law and if there is no reason to assume that the data subject's legitimate interest in the exclusion of the processing outweighs the employer's interests. Another special category of data concerns data on criminal convictions and offences (Article 10, GDPR). This data may in principle only be processed by public authorities. Private individuals or companies may do so only under certain conditions and to a very limited extent.

Children's Data

It is not generally prohibited to process the data of minors. However, there are some special rules and the obligations for the persons responsible, which are tightened. If the processing is based on the consent of the minor, Article 8 of the GDPR applies. If the minor concerned has reached the age of 16, they can give their own consent. If they are under 16 years of age, the persons having custody must give their consent. This only applies if the service offered is aimed at children. Due to another opening clause, EU member states can lower this age limit. Germany did not modify the EU law at this point. There are also special obligations for the controller processing children's data. For example, the controller has to ensure that the language used is suitable for children. It must be noted that in all balancing tests decisions, the protection of children's data has a particularly high priority. Apart from data protection law, national adver-

tising law also imposes special requirements on advertising aimed at minors.

Communication Data

The GDPR does not contain specific provisions on communication data. This should be done through the E-Privacy Regulation, which was originally intended to come into force at the same time as the GDPR. However, the legislative process has still not been completed. As a result, the processing of communications data is governed by Article 95 of the GDPR. Accordingly, the rules of the GDPR are applicable to communication data unless a more specific rule exists in the E-Privacy Directive. In Germany, this Directive was mainly implemented in the TTDSG.

Section 3 of the TTDSG prohibits the providers of telecommunications services from obtaining knowledge of the contents and circumstances of any communication. This concerns telephone calls as well as internet communication. The only exceptions concern acts necessary for the provision of the service or the protection of technical systems. In addition, only specific legal standards can justify the disclosure of data, such as the investigative powers of public authorities. Sections 9 and 10 of the TTDSG permit and at the same time limit the processing of traffic data and data necessary for determining charges.

The provisions of the TTDSG only apply if telecommunications services are provided. This classification may be difficult in individual cases. Internet service providers and telephone providers, for example, fall under the aforementioned provisions of the TTDSG. The decisive factor is whether a service provider transmits signals in a technical way. This is the case with internet and telephone connections. In regard to the email service, Gmail, on the other hand, the ECJ has ruled that this is not a telecommunications service, as there is a lack of sufficient signal transmission. SkypeOut, on the other hand, was classified as a service within the meaning of the TTDSG, since regular telephone numbers could also be called using the service.

Employment Data

The legal framework for handling employee data has long been a much-discussed topic in Germany. There have even been attempts to create a separate law for employee data. With the GDPR, the most important legal requirements are now Article 88 of the GDPR in conjunction with Section 26 of the BDSG. Accordingly, employee data may be processed by the employer if it is necessary for the establishment, performance or termination of the employment relationship. This also applies if the data processing is necessary to fulfil obligations arising from a law, a collective agreement or a works agreement. The latter represents a useful instrument for regulating internal company data protection policies.

In addition, employees can also give their consent to data processing. However, special care must be taken to ensure that consent is given voluntarily and that no direct or indirect pressure is exerted. For example, no pressure is exerted if consent is obtained to process data required for bonus payments.

Cookies

Regarding website cookies, the ECJ has ruled that pre-set consents in cookies are inadmissible. This does not mean that all cookies require consent, but where it is required, active action is necessary to meet the legal requirements for consent. In addition, the person concerned must be informed about the functioning and duration of the cookies. It should also be noted that consent under Article 7 (4) of the GDPR may be invalid if consent is given to data processing that is not at all necessary for the desired action. For a best practice design of website cookies, it is therefore recommended that a distinction is made between necessary and unnecessary

cookies and that the visitor has the opportunity to consent to the various categories. It should be noted that the legal basis was recently modified by the TTDSG (see **1.8 Significant Pending Changes, Hot Topics and Issues**).

Hate Speech, Disinformation, Terrorist Propaganda, Abusive Material, Political Manipulation, Bullying, Etc

With regard to hate speech, terrorist propaganda and abusive material on social networks, the German legislature has taken a special path and created a law specifically for this purpose: the Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*, or NetzDG). According to this law, operators of social networks are obliged to set up an effective complaint management system for certain illegal content, especially hate speech, terrorist propaganda and abusive material. Furthermore, they have to delete affected content if necessary and have to report on the complaints and deletions to the authorities. Currently, a change in the law is in progress that may lead to further obligations for the operators. For example, the possibility that the operators must report illegal content and information about the account holder directly to the police is being discussed. The dissemination of fake news has not yet been covered by this law or made into a punishable offence.

2.3 Online Marketing

The admissibility of advertising is governed by the Law against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb*, or UWG) and the data protection laws. In principle, the prior consent of the recipient must be obtained. This applies equally to advertising calls and advertising emails. The advertiser must be able to evidence the consent. While there is no mandatory procedure for this, the double opt-in with a registration and confirmation message has established itself as the de facto market standard. In addition, the sender must always be identifiable in advertising by email and there must be an opportunity to object to the advertising.

Section 7(3) of the UWG provides for an exception for advertising by email, in which no prior consent is required. The following conditions must be met:

- the customer has purchased goods and has therefore given their email address;
- only advertising for similar products – the term "similar" being interpreted very narrowly by the courts – is sent;
- the customer has not objected to the advertisement; and
- they are informed that they can object at any time.

When using web tracking tools and other analysis tools, care must be taken to ensure that the provisions of the GDPR are observed in the case of processing personal data. In the opinion of the ECJ, it is even possible for the website operator and the provider of the analysis tool to be regarded as joint controllers.

2.4 Workplace Privacy

Infection Prevention Measures

In the course of the fight against the COVID-19 pandemic, the federal government has developed and published a "Corona Warning App". In anonymised form, encounters between mobile devices are stored so that in the event of a positive test the person concerned can notify their contacts via the app. Employers should not require their employees to use the app. This is because it is based on the legal basis of voluntary consent. Consent cannot be given voluntarily if there is an instruction from the employer. The employer may recommend its use.

Similarly, mandatory temperature-taking before entering the workplace should be refrained from. This is sensitive health data (Article 9, GDPR)

that does not provide reliable information about a coronavirus infection and is therefore not necessary.

In fall of 2021, in the context of COVID-19 measures, the German legislature required employers to only admit employees to the premises that were fully vaccinated, cured from a previous infection or who can provide a negative test result. This applies for the time being (as of March 2022) and as long as that is the case the employer may record the employees' status.

A common response to the pandemic was the widespread introduction of home office. The German government has imposed an obligation on companies to offer employees the opportunity to work in a home office, provided there are no operational reasons to prevent it. In doing so, it must be ensured that adequate security measures (Article 32, GDPR) have been taken to protect data on the company network. These include a secure VPN connection, two-factor authentication and training. However, the exact measures always depend on the specific individual case.

Monitoring

When monitoring the email traffic and internet use of employees, it makes an important difference whether employees are allowed to use the company IT systems for private purposes or not. If private use is permitted, the employer may be considered a provider of telecommunications services within the meaning of the TKG (see **2.2 Sectoral and Special Issues**). If the employer were a telecommunications provider, surveillance would only be possible in very limited exceptional cases; for example, in the case of a justified suspicion of misuse. If private use is prohibited, the employer may monitor the use at least by random sampling. This does not apply to telephone conversations, which in both cases may not be recorded. Recording of telephone conversations requires a special legal basis or the consent of all participants. It is widely recognised that IT threat detection is permissible even if the employer is considered a telecommunications service provider.

Protection Measures

The employer may protect its technical systems by, for example, blocking access to websites or using a firewall. In some cases, there might also be a legal obligation to impose protection measures. As far as possible, these measures should be carried out without the processing of employees' personal data. Otherwise, a legal basis is required. In most of these cases, Article 6 litera c (legal obligation) or litera f (legitimate interest) of the GDPR will apply.

Works Councils

Apart from telecommunications law, the provisions of labour law have to be followed. The works council must approve all technical equipment that is suitable for monitoring the behaviour of employees (Section 87 (1) No 6, Works Constitution Act (*Betriebsverfassungsgesetz*, or BetrVG)). This applies to explicit monitoring equipment such as video cameras and internet log files, as well as to any equipment that allows conclusions to be drawn about work behaviour. This can be a photocopying machine that records the printouts on a personal basis or access equipment that records the personal identification of employees entering and leaving the building. Works councils further have a right to information concerning data protection according to Section 80 (1) No 1, (2) of the BetrVG, but specific questions of compliance are not subject to co-determination.

Whistle-Blowing

Under Section 4d of the Financial Services Supervision Act (*Finanzdienstleistungsaufsichtsgesetz*, or FinDAG), whistle-blowers can contact the Financial Supervisory Authority to

report legal violations in the financial sector. This can also be done anonymously. The German Act on the Protection of Business Secrets (*Geschäftsgeheimnisgesetz*, or GeschGehG) also provides that information on illegal conduct may be provided if this serves the public interest. In addition, the EU has issued a Directive on whistle-blowing. While this Directive provided for implementation by the member states by the end of 2021 the German legislature has not yet (as of March 2022) done so.

2.5 Enforcement and Litigation

Supervisory Authorities

The supervisory authorities must first investigate the facts of the case in order to be able to initiate any sanctions. Therefore, the competent authority may request information from the controller. The authority will then issue a formal decision stating that a breach of data protection has occurred and, if necessary, impose sanctions. In any case, the responsible person must be heard before any sanctions are imposed. In general, these sanctions must be dissuasive but also proportionate. It is important to note that fines are only one part of the set of sanctions available to the authorities. The others are:

- orders to provide information (Article 58 (1) litera a, GDPR) as well as to provide access to data and premises (Article 58 (1) literas e and f, GDPR);
- warnings or reprimands (Article 58 (2) literas a and b, GDPR);
- orders to the controller or processor to bring processing operations into compliance with the GDPR (Article 58 (2) litera c, GDPR); and
- the imposition of a temporary or definitive limitation, including a ban on processing (Article 58 (2) litera f, GDPR).

As regards fines, the model already mentioned in **1.3 Administration and Enforcement Process** is expected to be revised. Irrespective of this, the supervisory authorities have also imposed numerous fines in recent years. These include the following:

- Unauthorised employee surveillance occurred at the service centre of the fashion company H&M (in some cases, employees' living conditions were questioned and recorded in great detail without any legal basis); the responsible supervisory authority in Hamburg imposed a fine of over EUR35 million.
- Housing company Deutsche Wohnen was fined EUR14.5 million by the Berlin authority for not having a sufficient retention policy. This fine was annulled by the courts on procedural reasons (see **1.3 Administration and Enforcement Process**).
- Telecoms company 1&1 was fined close to EUR10 million for insufficient technical and organisational measures (TOMs) on the customer hotline. This fine was reduced to EUR 900.000 by a court who held the fine calculation scheme inapplicable (see **1.3 Administration and Enforcement Process**).

Once a data protection breach has been identified, the authority is also entitled to inform the data subjects and other authorities of the breach. Germany has also adopted further provisions in Sections 42 and 43 of the BDSG concerning criminal offences and administrative offences relating to the unlawful processing of personal data.

Private Litigation

In order to obtain damages, Article 80 of the GDPR requires the following: firstly, a breach of data protection rules; secondly, damage, resulting thirdly from the breach; and fourthly, liability for the breach. Under these conditions, the data subject may claim damages from the controller or the processor.

3. LAW ENFORCEMENT AND NATIONAL SECURITY ACCESS AND SURVEILLANCE

3.1 Laws and Standards for Access to Data for Serious Crimes

Law enforcement authorities may request information on personal data for the investigation of criminal offences. If there is a legitimate request for information, it must be complied with. It does not matter whether the crime is a serious offence. Judicial approval is not required. However, it is necessary for the requesting authority to specify the requested data, to give reasons as to why the data is relevant and to state the legal basis for the request for information. The transmission of the data to the authority can then be based on Article 6 litera c of the GDPR and Section 24 of the BDSG. In order to avoid violations of data protection, enquiries and information should be carefully documented.

It should be noted that special rules apply to requests for information on telecommunications data. In principle, this may only be requested in the case of serious crimes and only by court order (Section 100a ff of the Code of Criminal Procedure (*Strafprozessordnung*, or StPO)). In case of imminent danger – ie, in urgent cases – the public prosecutor's office can order the information to be provided. However, this must be approved by a court afterwards.

3.2 Laws and Standards for Access to Data for National Security Purposes

Very similar rules to those discussed in **3.1 Laws and Standards for Access to Data for Serious Crimes** apply in the field of national security. In these cases, the authorities can demand information if it is necessary for the prevention of imminent threats. These demands have to be followed if the data request is specific, states reasons for the relevance of the requested data and names a legal basis. Telecommunications data is again subject to increased requirements.

3.3 Invoking Foreign Government Obligations

A request for information from a court or authority of a non-EU country is only legitimate if the request is based on an international agreement, such as a mutual legal assistance treaty, that is in force between the requesting third country and the EU or a member state (Article 48, GDPR). The US Cloud Act, for example, does not meet the requirements of a mutual legal assistance treaty in the meaning of the law. It is contrary to the requirements of the GDPR and cannot be used as a legal basis for any transfer of data. Irrespective of Article 48 of the GDPR, other legal bases from Articles 44-50 of the GDPR may justify the transfer in individual cases (see **4.2 Mechanisms or Derogations that Apply to International Data Transfers**).

3.4 Key Privacy Issues, Conflicts and Public Debates

One of the most controversial issues from a legal and political point of view concerns so-called data retention. Telecommunications companies will be obliged to store connection data for a longer period in order for law enforcement and security authorities to access it under certain conditions. A first statutory regulation was declared invalid by the German Constitutional Court in 2010. In 2014, the ECJ also ruled that a corresponding EU directive was unconstitutional. In 2015, the German legislature nevertheless enacted a new law regulating data retention. However, since it is unclear whether this new law is compatible with the case law of the ECJ, the competent authority is currently not implementing the legal provisions. As a consequence, there is currently no obligation to retain data for telecommunications companies. However, the discussion is ongoing, as both the European

and the German legislatures are seeking new regulations.

4. INTERNATIONAL CONSIDERATIONS

4.1 Restrictions on International Data Issues

If personal data is transferred within the EU, the general rules apply (see **2.1 Omnibus Laws and General Requirements**). It is a key objective of the GDPR to create a single market for personal data in the EU. Since the same rules apply in all EU member states, no special rules need to be followed when transferring data to other EU countries.

If personal data is transferred in countries outside the EU, there are additional rules that need to be followed (Articles 44–50, GDPR). First of all, there has to be an additional legal basis. This can be an adequacy decision by the European Commission (Article 45, GDPR), appropriate safeguards (Article 46, GDPR) or specific exemptions; eg, consent (Article 49, GDPR). Apart from that, all other rules (general legal basis, rights of the data subject, etc) apply as well.

EU companies doing business in the UK should consider whether they are required to appoint a UK representative. This is required by UK law under certain circumstances, especially if the company does not have a branch in the UK.

4.2 Mechanisms or Derogations that Apply to International Data Transfers

The EU Commission can decide that a specific country has an adequate level of data protection (adequacy decision, Article 45, GDPR). If there is such a decision, it serves as legal basis for the transfer of personal data in this country. The Commission has so far approved Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, United Kingdom and Uruguay. Adequacy talks with South Korea are currently being held and close to successful completion.

In the absence of an adequacy decision, Article 46 of the GDPR lists various possibilities for adequate safeguards. In addition to these safeguards, enforceable data subject rights and effective legal remedies for data subjects have to be ensured. Appropriate safeguards are, for example, binding corporate rules, standard data protection clauses approved by the Commission or a supervisory authority, approved codes of conduct, certifications or approved individual contract clauses.

With regard to SCCs, the SCCs newly issued in 2021 must now be used and the requirements of the ECJ (see **1.7 Key Developments**) must still be observed. The court's requirements that any controller seeking to transfer data to a third country on the basis of checking the adequacy of the level of data protection in that third country in advance has been made part of the new SCCs. In particular, how much access government agencies have to the data in the destination country must be checked. If the controller concludes that the level of protection is not adequate, it must either terminate the transfer or take supplementary measures to ensure adequate protection of the data. The recommendation of the data protection authorities suggesting various contractual, organisational and technical measures that can be taken in such a situation should also be taken into account.

If there is neither an adequacy decision nor appropriate safeguards, Article 49 of the GDPR provides specific exemptions for transfer of data. These are, inter alia, the explicit consent by the data subject, the performance of a contract concluded with or in the interest of the data sub-

ject, the protection of vital interests or reasons of public interest.

4.3 Government Notifications and Approvals

Apart from the decision itself, transfers based on Article 45 of the GDPR do not require further government approval. The appropriate safeguards listed in Article 46 of the GDPR are all authorised by a public body at some point in time. Transfers based on Article 49 of the GDPR generally do not require government approval. However, if a transfer is based on Article 49 (1) subparagraph 2 of the GDPR (compelling legitimate interest), the controller has to inform the supervisory authority.

4.4 Data Localisation Requirements

There are no specific data localisation requirements under German law.

4.5 Sharing Technical Details

There are no obligations to share software code, algorithms or similar technical details with the government. Information regarding technical details might come to the attention of a data protection authority because of an investigation by that authority. However, it acts independently from other state bodies and is not allowed to share this information.

4.6 Limitations and Considerations

In the case of foreign government data requests, foreign litigation proceedings (eg, civil discovery) or internal investigations, the general rules about international data transfers (see **4.2 Mechanisms or Derogations that Apply to International Data Transfers**) and about foreign government requests (see **3.3 Invoking Foreign Government Obligations**) apply.

4.7 "Blocking" Statutes

The only blocking statute currently affecting German companies was passed by the EU and is intended to protect companies from US sanctions against Iran. The Blocking Statute nullifies any court rulings based on the sanctions and provides for the possibility of compensation.

5. EMERGING DIGITAL AND TECHNOLOGY ISSUES

5.1 Addressing Current Issues in Law

The topic of big data analysis is still being intensively discussed at the academic level. Specific laws on this topic have not yet been enacted. In principle, the GDPR does not prohibit comprehensive analyses of personal data. However, numerous questions arise, for example, with regard to identifiability, change of the purpose of the processing, data minimisation and effective rights management. In addition to data protection law, other legal areas are also affected. For example, there is the question of liability in the event of inadequate data quality.

The discussion is similar with regard to algorithms that regularly require large data collections. If these algorithms make decisions with legal effect, the question of liability for erroneous decisions or for an erroneous data basis arises again. In this context, there is a discussion about creating legal personality for algorithms and/or autonomous systems. In addition, there is the specific problem of non-discrimination; for example, when an algorithm decides on the hiring of persons and ends up perpetuating the discrimination that already existed in the data collection based on previous (human) hiring decisions.

The German legislature has made a first legal regulation in the area of liability for automated systems in the case of autonomous motor vehicles. In doing so, it has defined criteria that an automated car system must meet. Furthermore, the legislature has stipulated that the vehicle

driver is still liable even if permitted to transfer vehicle control to the system and to turn their attention away from the traffic. At the same time, however, the driver must remain on standby during the drive to take control of the vehicle again. This is, so far, the only example of specific liability rules regarding autonomous systems.

With regard to profiling and automated decisions, see **2.1 Omnibus Laws and General Requirements**.

5.2 "Digital Governance" or Fair Data Practice Review Boards

The Federal Ministry of the Interior has appointed an independent commission of experts to consider the ethical processing of data in the future (Data Ethics Commission, *Datenethikkommission*). The Commission has proposed a comprehensive catalogue of measures. Among other things, it recommends more specific regulation regarding big data analyses, effective supervision and an adaptation of liability law. With very few exceptions, the Commission considers the use of algorithms in government decisions as unjustifiable.

The federal government has announced that it intends to take the recommendations into account. So far, no specific regulatory proposals have been presented.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.

Please see **2.5 Enforcement and Litigation**.

5.4 Due Diligence

Data protection plays an important role in due diligence in two ways. From the buyer's point of view, there is interest in the question of whether the company to be purchased has acted in conformity with data protection regulations or whether financial risks exist in the form of fines or claims for damages due to data protection violations. In this respect, there must be an assessment as to whether the company has acted in conformity with data protection regulations. If the target runs a digital business, it is also important to establish whether the business model itself is data protection compliant as otherwise the target's value would be greatly reduced.

In addition, however, the due diligence itself is a data processing exercise, as personal data on employees and/or customers is often disclosed to potential buyers. There must be a review as to which legal basis applies. As a rule, the legitimate interest according to Article 6 litera f of the GDPR should be taken into account. Care must be taken to ensure that only data that is really necessary is disclosed and that this data is anonymised as far as possible.

5.5 Public Disclosure

There are no laws that require a public disclosure of an organisation's cybersecurity risk profile. The operators of facilities that constitute critical infrastructure (eg, energy suppliers) must submit their IT security plan to the competent authority. However, this does not constitute a public disclosure.

5.6 Other Significant Issues

The obligations of the GDPR depend on whether a company is to be regarded as a controller. The term is currently being further extended by the ECJ's case law (see **1.7 Key Developments**). In particular with co-operation models, it will still have to be shown here where exactly the border runs between controlling, processing and other auxiliary activities.

Heuking Kühn Lüer Wojtek is one of Germany's major commercial law firms, with more than 400 lawyers in nine offices across Germany and in Zurich offering service at the highest level. The lawyers in the firm's data protection, privacy and cybersecurity group are leaders in their fields and help clients develop global privacy and data security strategies for today's digital economy. They advise clients on, inter alia, data processing agreements, international data flows within groups of companies and binding corporate rules; development of compliance programmes (including GDPR compliance); technology-related data usage; the setting up and operation of customer relationship management, personnel or other databases involving personal identifiable information; as well as the setting up of whistle-blowing and other reporting schemes. Furthermore, they represent clients before administrative authorities and in legal disputes related to (alleged) data protection and data security breaches.

AUTHORS

Philip Kempermann is a managing partner at Heuking Kühn Lüer Wojtek based in Düsseldorf. He focuses on IT and data protection and is a member of the firm's IP, media and technology and antitrust practice groups. He advises and represents several large national and international corporations with their IT projects, operations and data protection matters. Additionally, Philip assists clients with IoT strategies and provides several international organisations with GDPR compliance advice. He is an active member of the International Technology Law Association (ITechLaw) as well as the German Association of Law and Informatics (DGRI).

Thomas Jansen is a partner at Heuking Kühn Lüer Wojtek's Munich office and a member of the IP, media and technology practice group. Thomas has over 25 years of experience as a technology transactions lawyer. He advises German and international corporate clients across diverse industries on all kinds of technology-related matters, with a focus on providing strategic guidance in the creation, acquisition, use and commercial exploitation of technology. He also counsels clients on the intellectual property aspects of mergers, acquisitions and financings, and advises clients on privacy and data protection and cybersecurity-related issues. Thomas is a frequent speaker, and is also the author of numerous articles, on technology and privacy-related topics.

Heuking Kühn Lüer Wojtek

Georg-Glock-Straße 4
40474 Düsseldorf
Germany

Tel: +49 211 600 55 166
Fax: +49 211 600 55 050
Email: p.kempermann@heuking.de
Web: www.heuking.de