GERMANY: PRIVACY

Philip Kempermann
Heuking Kühn Lüer Wojtek

Key statutes, regulations and adopted international standards

Data protection law in Germany has a long-established tradition. In 1977, the Hessian Data Protection Act was the first act on this topic worldwide. Today, the basis for the regulatory regime lies in the fundamental right of protection of personal data under article 8 of the Charter of Fundamental Rights of the European Union (CFR) and the German fundamental right to informational self-determination, as derived in the Census Act Judgment by the German Federal Constitutional Court (BVerfGE) in 1983. Finally, since 25 May 2018, the EU General Data Protection Regulation (GDPR) is directly applicable pursuant to article 288(2) sentence 2 of the Treaty on the Functioning of the European Union (TFEU). This means that, currently, data protection in Germany is primarily governed by the GDPR. However, the German legislator made use of a large amount of the numerous opening clauses in the GDPR to implement special national laws in the field of data protection. Since a vast number of acts in Germany deal with data protection in specific areas, it would go beyond the scope of this work to list all of them, so only the most important aspects will be dealt with in the following.

In Germany, the legislative competence for data protection is divided between the federal government and the federal states. This means that, in addition to the Federal Data Protection Act (BDSG), federal states may pass state-specific acts that apply to the public bodies of the states. To date, the federal states have not published any new state data protection laws other than drafts and reform intentions, so that, in general, the application of the new BDSG remains unchanged.

The new BDSG was published on 30 June 2017 as the first new data protection act enacted by an EU member state and came into force on 25 May 2018. The BDSG primarily serves to make use of the various opening clauses of the GDPR and contains rather fragmentary provisions on individual topic complexes, which refer back to the GDPR to a large extent. For that reason, the BDSG can only fully be applied in a conjunction with the GDPR.

For the applicability of the BDSG, there must not be any specific rules in the GDPR for the respective matter or an opening clause must exist. In addition, there must be no more specific federal laws that take priority. For example, there are a number of special provisions

for data protection in the social sector in the German Social Security Codes, with section 35(2) sentence 2 Social Security Code I stipulating the general applicability of the GDPR, supplemented by the corresponding special provisions (above all, section 35 Social Security Code I, sections 67 to 85a Social Security Code X).

The BDSG is applicable for both public and non-public bodies. This distinction, which is not recognised under the GDPR, is explained in section 2 BDSG: in principle, public bodies are authorities, organs and institutions under public law (at the federal and state level), whereas non-public bodies are defined negatively as natural and legal persons under private law that do not fall under public bodies.

For public bodies, the BDSG applies comprehensively and without exception, insofar as no state-specific data protection laws exist. In the case of non-public bodies, the BDSG shall apply if fully or partially automated processing, or non-automated processing but with storage in a file system, is carried out. An exception according to section 26(7) BDSG is the protection of employee data, which is comprehensively regulated by this act.

The third part of the BDSG (sections 45 to 84), deals with the areas of police and justice, which is not covered by the GDPR, but by the Directive (EU) 2016/680. As these only apply to the police and the justice sector, we refrain from going into detail.

Further important provisions dealing with data protection can be found in the German Telecommunications Act (TKG) and also in the provisions of the criminal law, in particular the punishment of breaches of confidentiality by certain professional groups including lawyers, in section 203 of the German Criminal Code.

As a result, there is a system of standards at various levels in which national data protection law is directly applicable in addition to the GDPR and there is also a division of data protection in Germany into federal law and state law standards. This makes finding the correct set of regulations burdensome work.

Regulatory bodies

In Germany, each federal state has its own data protection supervisory authority (DPA) and there is a federal data protection supervisory authority that is competent for federal public bodies pursuant to section 24(1) BDSG. In total, there are 17 authorities. The one-stop-shop principle of articles 55 and 56 GDPR was mirrored in Germany in sections 18, 19, 40(2) BDSG to the extent that the German authorities work together to implement the requirements of the GDPR and that in individual cases the supervisory authority of the federal states in which the main branch of the controller is established is responsible.

Section 40 BDSG supplements and specifies article 58(6) GDPR and regulates the responsibilities of the supervisory authorities in the individual federal states of Germany. Ultimately, section 40 corresponds to the GDPR; its significance is anchored in Germany's federal structure.

In addition, there is the German Data Protection Conference (DSK), a body in which the individual DPAs meet and publish joint opinions on controversial topics. The DSK itself is not a supervisory authority and it does not have the same competences as the European Data Protection Board. It is only a vehicle of collaboration and alignment between the DPAs.

Sanctions

Clarifications and additions to articles 83 and 84 GDPR on sanctions can be found in sections 41 to 43. Under German law, the procedure for applying fines is governed by the provisions of national administrative offences law and the Code of Criminal Procedure. Irrespective of the legal basis, it can be stated that the current practice of fines in Germany is more focused on advice on compliance with data protection law than on the imposition of fines. However, with the GDPR's official intention to have dissuasive fines and a new mechanism for determining fines discussed by the DSK, this is poised to change.

Section 43 extends the administrative fine provisions of the GDPR to cases of incorrect treatment of a request for information, more precisely a violation of the request for information by lenders regarding consumer credits (see section 30(1)) or if a consumer is not properly, not fully or not in time informed about the rejection of a consumer credit agreement (see section 30(2) sentence 1). Section 43 allows for a fine of up to €50,000.

According to section 42, a prison sentence of up to three years may be imposed, if the data controller (ie, the natural person responsible) acted intentionally and, in accordance with section 42(3), a complaint was made by the data subject, the controller itself or a DPA.

Communications and marketing

Telecommunications providers

The TKG applies to telecommunications services providers in Germany. The TKG also includes data protection provisions, which are predominantly found in sections 91 et seq. In principle, these provisions remain applicable because of the hierarchy stipulations of article 95 GDPR, since the sections 91 et seq TKG represent the German implementation of the ePrivacy Directive. However, the provisions of the TKG sometimes go beyond those of the ePrivacy Directive with the consequence that the GDPR supersedes these overreaching parts. Therefore, a very unclear regulatory complex has unfortunately arisen. A comprehensive description of all provisions on data protection in the TKG and their possible effects would go beyond the scope of this work, which is why only a few issues are highlighted in the following.

The scope of application of these provisions differs from that of the ePrivacy Directive. While sections 91 et seq TKG under section 91(1) also apply to persons who only participate in the operation of telecommunications services, article 3(1) of the Directive only applies to those who themselves are operators of such services. For this reason, participants (eg, in-house vicarious agents or external service providers) are not in the scope of the Directive. This overreaching scope of application of the TKG cannot be subsumed under article 95 GDPR, with the consequence that in the case of participants only the GDPR applies.

The TKG distinguishes between three types of data: data collected for the establishment, content, modification or termination of a contractual relationship relating to telecommunications services (user data); traffic data; and location data. Since the provisions on traffic data (sections 96 and 97 TKG) and location data (section 98 TKG) largely implement articles 6 and 9 of the ePrivacy Directive, they must still be applied. For example, section 96 TKG permits the collection of traffic data (eg, phone numbers, beginning and end of connections,

transmitted data volumes) solely for the purpose of establishing or maintaining a telecommunications connection. Section 98 TKG stipulates that location data may also be collected, but only if the data is anonymised or consent has been obtained. Additionally, the provider must inform the user when determining the location of his or her mobile device via a text message. Such a notification is not necessary if the location is only displayed on the mobile device whose location data was transmitted (see section 98(1) sentence 3 TKG). In addition, this only applies to mobile phone data, but not to other options for location monitoring, such as GPS.

User data, according to section 95 TKG, are foreign to the ePrivacy Directive. That means that section 95 TKG is an overarching regulation, which is superseded by the GDPR. The same applies to the information obligations under section 93(1) TKG, which are superseded by articles 13 and 14 of the GDPR, and to the consent regulation under section 94 TKG, which is also superseded completely by article 7 GDPR.

The employer as telecommunications provider?

A much discussed question is whether the telecommunications secrecy of section 88 TKG – which is an implementation of article 5 of the ePrivacy Directive and, therefore, continues to apply – also applies to employers if they allow their employees to use the provided internet access and company email accounts for private purposes. The dispute depends on the question of whether in this case employees are 'third parties' in the sense of section 3 No. 5 TKG in relation to the employer. If the internet and email may only be used for business purposes, the employee only works for the employer's purposes and can never be a third party. The prevailing view by the DPAs in the past was that employees must be classified as third parties if they are permitted to use the internet and email account for private purposes. The consequence would be that the secrecy of telecommunications also applied to employers. According to this, all types of telecommunications, including all content data and connection data, are protected insofar as they could somehow provide information about the parties involved. This would prohibit even simple tasks such as accessing another employee's emails for the purpose of substituting in the case of illness as access would only be possible in a few exceptional cases specifically laid out in law.

Since this is practically complicated and presumably not intended by the legislator, the Berlin-Brandenburg Regional Labour Court (LArgbG Berlin-Brandenburg) decided otherwise and did not regard employees as third parties within the meaning of section 3 No. 5 TKG. The ECJ ruling on *Gmail* leads in the same direction, as it established that Google cannot be classified as a telecommunications provider for its free Gmail service. If Google, which provides the mail service as part of its business to true third parties, is not to be classified as a telecommunications provider, as for Gmail it does not primarily transmit telecommunications signals, the same must apply for company email.

The role of the data protection officer

Sections 5 to 7 as well as section 38 extend the duties of data controllers and processors with regard to the appointment, position and tasks of data protection officers (DPOs). The sections are based on the opening clauses of article 37(4) sentence 1 and 38(5) GDPR and thereby extend the articles 37 to 39 GDPR. Sections 5 to 7 are valid for the public sector and sections 38, 39 for the private sector.

Sections 5 to 7 correspond basically with the wording of the GDPR with the peculiarity that section 5 also extends the appointment obligation to courts, which are excluded under article 37(1)(a) GDPR.

For the private sector, section 38 adds several criteria as reasons to appoint a DPO. Article 37(1) GDPR requires an appointment if the controller's core activities include regular and systematic monitoring of data subjects or processing of special categories of data on a large scale. Within the scope of application of the BDSG, there is an additional obligation to appoint a DPO if at least 20 persons are permanently engaged in the automated processing of personal data. 'Permanent' means that the employees work with IT systems with a certain continuity. This is the case if the processing activity is carried out for a longer or indefinite period of time, but it does not need to be on a daily basis.

A further obligation to appoint a DPO exists if processing operations are carried out that are subject to a Data Protection Impact Assessment according to article 35 GDPR. Finally the appointment is also obligatory if controllers process data for the purpose of carrying out as their business (anonymous) transmission of data or processing data for purposes of market or opinion research.

The protection against dismissal for DPOs under article 38(3) sentence 2 GDPR is significantly extended by section 6(4) – which is also applicable in the private sector via section 38(2). Accordingly, dismissal is only permissible for important reasons, that is, if facts exist on the basis of which a continuation as DPO is not reasonable for the controller after weighing the individual case. Standards similar to those for termination of employment relationships are applied. Thus, a DPO is protected against any kind of ordinary termination. In addition, section 6(4) extends this protection against termination to the duration of the year after the DPO has resigned its position as DPO but is still an employee.

It is unclear and not yet decided whether this protection against dismissal (and termination) only applies to DPOs appointed in accordance with the BDSG. The wording, which only refers to an appointment pursuant to section 5, seems to suggest this. If, however, voluntarily appointed DPOs or other DPOs appointed only under the GDPR did not fall under this protection against dismissal, this would be an unequal treatment that could hardly be justified.

Surveillance laws

German data protection law historically addressed video surveillance. This carried over into Section 4, which governs video surveillance of publicly accessible rooms. This should only be permissible if it is necessary to fulfil the tasks of public authorities, exercise domestic rights or safeguard legitimate interests for specific predetermined purposes and if there are no indications that the interests of the data subjects worthy of protection prevail. Although

the GDPR does not contain any special provisions on video surveillance, it is questionable whether the German legislator had any regulatory competence at all. In contrast to the public sector, where a corresponding opening clause can be found in article 6(1) sentence 1(e) in conjunction with (3) sentence 1(b) GDPR, there is no corresponding regulation for the private sector. A recent ruling of the Federal Administrative Court addressed the old legal situation before the GDPR came into force, but the court also took a stand on video surveillance under the GDPR: for private video surveillance, only article 6(1)(f) GDPR and not section 4 can be considered as a permission of processing the data.

In the context of legitimate interests, earlier decisions handed down by the court have to be taken into account when determining necessity and the balancing of interests. That means that the reason for the video surveillance should be based on sufficient, documented facts and that no equally effective, but less intervening measures are available. Owing to the data minimisation principle,[1] the controller also needs to consider what is recorded by the cameras. In addition, the recordings should be deleted after a very brief period of typically only a few days and the transparency principles of article 5(1)(a) GDPR should be met, for example by showing corresponding signs.

Employment data protection

Of particular importance is section 26 being the basis for permission to process employee data for the establishment, execution and termination of an employment relationship and, in addition, their processing for the investigation of criminal offences in employment contexts. Thus, section 26 makes use of the possibility provided by article 88 GDPR to introduce Member State law on the protection of employee data. It remains unclear and controversial whether article 88 GDPR merely sets minimum standards to be complied with or whether the creation of stricter rules by the individual member states is prohibited. This is relevant for section 26, among other things, because it introduces a principle of proportionality foreign to the GDPR and it also applies to manual data processing, even if there is no storage in a file system.[2]

Consent is specifically regulated in this context, since according to section 26(2), the existing dependence of the employed person on the employer must be taken into account for the necessary voluntariness and is, therefore, subject to more detailed examination. However, section 26(2) also makes clear that consent is a viable option even in the employment context.

Section 26(3) allows for the processing of special categories of data for purposes of social security and social protection as well as for legal obligations under labour law.

1 Article 5(1)(c) GDPR.

2 See section 26(7).

Photo and video recordings

Another data protection issue that can play a role not only but also in the context of employment is the creation and forwarding or publication of photo and video recordings. This may be relevant, for example, if the employer wants to create ID cards with the photo of the respective employee or if it wants to place recordings of a company event on the intranet. For the production of the pictures the GDPR applies. For forwarding or publishing photos sections 22, 23 of the German Art Copyright Act (KUG) applied in the past. Under the KUG, forwarding of photographs is generally lawful, provided that the data subject consented. Consent under the KUG could be declared implicitly or agreed to in general terms and conditions. If the data subject is merely an 'accessory' in the photograph, that is, if it is not in the foreground, then according to section 23(1) No. 2 KUG, no consent is required at all.

Here, however, the question arises whether the KUG still applies. In this respect, the Cologne Higher Regional Court recently confirmed that the KUG is a regulation within the meaning of article 85(2) GDPR insofar as it relates to the publication of images for journalistic, scientific, artistic or literary purposes. However, the court did not answer the question of whether the KUG remains applicable to portraits that pursue neither journalistic, artistic nor literary purposes. The Federal Ministry of the Interior affirmed the comprehensive application of it even after the GDPR had entered into force and referred to article 85(1) of the GDPR without further explanation. However, this classification by the ministry is not binding.

The DSK takes a different position and urges the legislator to clarify. The dominating opinion in Germany supports the OLG Cologne and wants to continue applying the KUG to media and press related cases and refers to the opening clause of the article 85 GDPR. For all other circumstances (as photos in an employment context or for marketing) the GDPR supersedes the KUG. Consequently all picture activities must be reviewed under article 6 GDPR. Within the scope of the balance of interests the requirements of section 23 KUG are to be considered nonetheless. Under section 23 KUG pictures may be published without consent if: they have a value for contemporary history; persons appear only as accessories beside a landscape or similar; persons appear only on pictures of assemblies or similar events; and the photos serve a higher interest of art.

Special processing situations

In addition to section 26 regarding employment contexts, sections 27 to 31 BDSG also describe special processing situations, whereby section 27 refers to scientific or historical research purposes and statistical purposes, section 28 to archive purposes in the public interest and section 31 to the protection of commercial law with regard to scoring and creditworthiness information. The first two make use of the opening clauses of article 9(2)(j), article 89(2) respectively (3) GDPR. In the context of section 31, the opening clause is not clear, some details are controversial and it seems as if it concerns less a data protection, but a consumer-protecting regulation.

Restriction of access rights

Section 29 deals with data subjects' rights and supervisory authority powers in the case of confidentiality obligations. Thereby section 29(1), sentence 2 restricts the right of access according to article 15 GPDR as far as the information would reveal information that has to be kept secret according to a legal regulation or its nature, in particular because of the predominant legitimate interests of a third party. The State Labour Court of Baden-Wuerttemberg (LArbG Baden-Württemberg) recently handed down a decision concerning the scope of this restriction. The background was a wrongful termination case in which the plaintiff requested access and involved the right to obtain a copy.[3] The employer refused by simply mentioning predominant interests of third parties worthy of protection. The LArbG Baden-Wuerttemberg saw this differently and decided the copy would have to be provided to the plaintiff.

If a controller wants to refer to the restrictions of article 15 GDPR, section 29(1) sentence 2, several requirements must be considered, which mean considerably more work for the controller. In each individual case the concrete interest of the data subject to access the information must be determined and weighed properly against the interests of the controller in the refusal of the disclosure. To this end, it must be specifically stated which information must be kept secret and to what extent the interest in secrecy actually prevails. Consequently, controllers must check very precisely and in detail to what extent they can assert their confidentiality interests at all. A blanket statement concerning interests of third parties, as it was made by the employer in the case before the LArbG, is certainly not sufficient. In case of doubt, information must then be provided. It can be redacted if necessary.

Further modifications to the rights of data subjects

Chapter 2, Part 2 of the BDSG (sections 32 to 37) contains modifications to the rights of data subjects and is based on the opening clause of article 23 GDPR. Again, there are strong doubts about their conformity with European law.

The right to information of the data subjects under article 13 GDPR can be restricted. Such a restriction – albeit only for when the purpose changes and with the consequence that, concerning the initial processing, the GDPR is exclusively applicable – is found in section 32. For further processing for other than the initial purposes, the information duty can be restricted if: the further processing concerns only analogously stored data; the proper fulfilment of the responsibilities of public bodies according to article 23(1)(a) to (e) GDPR is endangered; public safety or public order is endangered; the assertion, exercise or defence of legal claims is endangered; or if the confidential transmission to public bodies is endangered.

Section 33 extends the exceptions under article 14(5) and thus refers to information obligations if the personal data was not collected from the data subject. The use cases are similar to those in section 32.

3 See article 15(3) GDPR.

Additional restrictions on the right of access pursuant to article 15 GDPR are covered by section 34, which consequently stipulates that there is no right of access if there is no obligation to provide information pursuant to sections 32 and 33.

Instead of the deletion of data, in certain cases, the processing should be restricted in accordance with section 35. According to section 35(1), which refers to non-automated data processing only, this should be the case if the deletion is not possible or only possible at a disproportionately high expense owing to the special type of storage and the interest of the data subjects in the deletion is to be classified as low.

The right to object under article 21(1) GDPR is restricted in favour of public authorities by section 36 if there is an overriding public interest in the processing that outweighs the interests of the data subject, or a legal provision obliging the processing.

Finally, section 37 refers to automated decisions in individual cases, including profiling, but is limited to insurance-specific circumstances. The provision restricts the right under article 22(1) GDPR if the request of the data subject has been granted or if the decision is based on the application of binding regulations on fees for medical treatment.

Philip Kempermann
Heuking Kühn Lüer Wojtek

Philip Kempermann focuses on IT and data protection. He is a member of Heuking Kühn Lüer Wojtek'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 Kempermann assists start-ups with getting their products to the market. He has extensive experience with complex international IT projects, helping various companies to bring such negotiations to a successful ending. Also, he advises suppliers and OEM in the connected car sphere on questions of cybersecurity and privacy. Philip Kempermann has also assisted several international organisations with their GDPR compliance and advised on product design under the privacy by default and by design principles.

Philip Kempermann is also an active member of the International Technology Law Association (ITechLaw) as well as the German Association of Law and Informatics (DGRI). He regularly speaks and publishes on IT and data protection topics.

HEUKING KÜHN LÜER WOJTEK

Heuking Kühn Lüer Wojtek is a large independent German commercial law firm. National and international clients trust the expertise and experience of our lawyers, tax consultants, and notaries. We represent the interests of medium-sized and large companies in the areas of industry, trade, and the provision of services. Also organisations, public corporations and sophisticated private clients make use of our knowledge in the most diverse fields of law.

Heuking Kühn Lüer Wojtek is represented with offices in all major business regions in Germany as well as in Brussels and Zurich. We maintain close contact with international law offices in all the important markets in the world. Thus, a worldwide expertise network of lawyers is available to you depending on the transaction or mandate. Our international advisory activity is aligned with international standards.

On an international level, we have built up a network of law firms with which we cooperate on a 'good friends' basis without being tied to exclusivity agreements.

Additionally, we maintain close contacts with international law firms in all key markets around the world. Over the years, our clients have come to focus on certain territories, which are represented by our Country Desks for China, France, India, Japan & Turkey.

Georg-Glock-Str. 4
40474 Düsseldorf
Germany
Tel: +49 211 600 55-166
Fax: +49 211 600 55-160
www.heuking.de

Philip Kempermann
p.kempermann@heuking.de