THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-912228-62-1

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 11

GERMANY

Olga Stepanova[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 even 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 in order to meet the requirements of a society in which data processing grew more important. Especially, digitalisation raised a lot of questions, which needed to be handled. Keeping this in mind, among others 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, since data protection law and telemedia law got 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). The GDPR entered into force on 25 May 2018 as scheduled. The ePrivacy Regulation is still subject to tripartite negotiations and will probably be applicable in 2020. For this reason, the following text provides an overview of the current legal situation in Germany, presenting the changes and the challenges of a new era of data protection in connection with digitalisation.

II THE YEAR IN REVIEW

The past year was marked by the upcoming adoption of Regulation (EU) 2016/679, the GDPR, which replaced the German data protection laws to a large extent.

1 Olga Stepanova is an associate at Winheller Rechtsanwaltsgesellschaft mbH.

As a regulation, the new framework does not have to be transposed into the different national laws of the European countries but is directly applicable in all EU Member States. However, as a specialty of the GDPR, the regulation also contains 'opening clauses' that provide Member States with the discretion to introduce additional national provisions to concretise and further specify the application of the GDPR for specific issues (e.g., in connection with employees). To that end, the German parliament passed a new version of the BDSG in April 2017. This new set of rules, the GDPR and the new German BDSG, both became effective in May 2018.

It was interesting to see how the GDPR became popular in mass media, which happens with very few laws, so even tabloid newspapers were reporting about upcoming changes every day. Due to the fact that the GDPR has always been mentioned in connection with the high penalties stipulated in Article 83 GDPR, a kind of public fear grew, which led to a high level of insecurity, even among customers who used messaging services, email services and social media.

Although the GDPR maintains the main concepts of data protection as we knew them before, or amends details of them (e.g., data processing is still prohibited if not explicitly permitted by the data subject or a law, the legal bases for the transfer of personal data into non-EU countries or the obligation to designate a data protection officer), the new rules also bring some important changes. Small companies and non-profit organisations, in particular, are unsure about how to implement the GDPR.

First and foremost, the GDPR extended its territorial scope, which means that non-European companies may also fall within its scope, making it the first worldwide data protection law due to globalisation. It applies to (1) all companies worldwide that target European markets and in this context process the personal data of European Union citizens (irrespective of where the processing takes place) and (2) those that process the data of European citizens in the context of their European establishments. The GDPR tightens the rules for obtaining valid consent to process personal information. Still, valid consent is one of the two possibilities to justify data processing, the other option is legal justification. Companies will therefore have to assess their processes to make sure they process personal data lawfully, and to review whether it is advisable to refrain from seeking consent but to switch to legal justification with fewer prerequisites and no possibility of being revoked at any time.

As a consequence, upon request of data protection authorities, companies have to provide prove that they fulfil their obligations under the GDPR. The authorities do not need to investigate and prove the infringements by themselves anymore. The GDPR also introduced mandatory privacy impact assessments (PIAs). It requires data controllers to conduct PIAs where privacy breach risks are high to minimise risks to data subjects. This means that before organisations can begin projects involving special categories of personal data, such as health, they will have to conduct a PIA and work with the data protection offices to ensure they are in compliance with data protection laws as projects progress.

Additionally, the GDPR expanded liability beyond the data controllers. In the past, only data controllers were considered responsible for data processing activities, but the GDPR extended liability to all organisations that process personal data. The GDPR also covers any organisation that provides data processing services to the data controller, which means that even organisations that are purely service providers that work with personal data will need to comply with rules such as data minimisation.

The enforcement of the GDPR is backed by significant fines of up to €20 million or 4 per cent of annual global turnover, whichever is higher.

To sum it up, the increase of obligations and fines are also likely to force previously idle organisations to rethink their positions.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The GDPR defines personal data as 'any information relating to an identified or identifiable natural person'. This definition applies to all personal data handled by electronic information and communication (telemedia) service providers.

However, all of these data are now subject to the GDPR, as the German Data Protection Conference presented a paper on 26 April 2018, which states that Article 95 GDPR has to be interpreted in a way that the provisions of TMA governing the data protection shall not be applicable anymore. Following this opinion, there is no privileged handling for data collection via telemedia anymore, so the controllers must obey the strict rules prescribed by the GDPR from now on.

ii General obligations for data handlers

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. Telemedia service providers as data collectors may collect and use personal data only to the extent that the law specifically permits, or if the data subject has given his or her consent, Article 6 GDPR. Moreover, to the extent that the law permits the collection of data for specified purposes, these data may not be used for other purposes, unless the data subject has consented to other uses.

According to Articles 13 and 14 GDPR, the controller must, *inter alia*, inform the user of the extent and purpose of the processing of personal data for any consent to be valid. Consent 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 revoke consent at 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. Consent, however, is not always required. Former, many statutory exceptions allow for the use of data without consent, for various business-related purposes. Though, following the aforementioned paper, controllers cannot make use of them since 25 May 2018. Therefore, controllers are now forced to find new ways to guarantee lawful processing while collecting data through websites, apps and by electronic communication. This also goes along with a proper assessment of previous data-processing procedures and can lead to increased shifts of service providers that are not able or not willing to comply with the high standards of GDPR.

iii Technological innovation and privacy law

Cookies

Under data protection law, the use of cookies is only relevant if the information stored in the cookie is considered personal data. A cookie is a piece of text stored on a user's computer by his or her web browser. It may be used for authentication, storing site preferences, the identifier

for a server-based session, shopping cart contents or anything else that may be accomplished through the storage of text data. The cookie is considered to be personal data if it contains data that allow the controller to identify the data subject. However, before the GDPR entered into force, and as long as the relevant part of TMA was still applicable, cookies could have been placed in Germany as long as the user had the option to object (opt out). Now, there is no such privileged treatment anymore as the general requirements regarding a lawful data processing are applicable for cookies too. The only question not answered so far by the European Court of Justice (ECJ) is whether the use of cookies must inevitably be based on the data subject's consent (Article 6(1)(a) GDPR) or is it sufficient when the controller states that this use is necessary for the purposes of his legitimate interest (Article 6(1)(f) GDPR). In any case, according to the German Data Protection Conference, prior consent is required for the use of tracking mechanisms, which pursue the behaviour of affected persons on the internet and create user profiles. That means, that informed consent within the meaning of the GDPR is required in the form of a declaration or other clearly confirmatory action taken prior to data processing (i.e., before cookies are placed on the user's device).[2]

The reason for this discussion and the legal uncertainty is derived from the fact that the ePrivacy Regulation did not enter into force on time and has not even been passed. So far, it may be advisable to fulfil the requirements of the GDPR in its whole scope, which means that consent has to be sought before tracking the user.

Social media

Social media becomes more popular each day as the number of users grows. The same applies to the opportunities and smart solutions offered by using these media. Most social media platforms are free of charge. Users pay with their personal data, even though many of them are not even aware of this fact. That is why the European legislator stipulated in the principles of processing in Article 5 GDPR *inter alia* that processing has to be transparent and the processor shall be responsible for obeying this principle. Therefore, one can find a lot of other regulations realising the legislator's will by creating a sharp sword against Big Data companies, which are often suspected of processing data in an unlawful way.

The first decision against Facebook was ruled by the ECJ just 11 days after the GDPR became effective (ECJ, 5 June 2018 – C-210/16). Admittedly, the original case dates back seven years. At that time, the German Schleswig-Holstein State Centre for Data Protection had asked the Academy of Economics to delete its fansite on Facebook and issue a ban order. The background to this was the fact that neither Facebook nor the Business Academy informed visitors about the data they had collected. After several instances, the case finally ended up before the German Federal Administrative Court, which referred the question of the responsibility for the data collection of the fansite operators to the ECJ, because the fansite operator only had very limited access to the data records of the individual fansite visitors collected by Facebook.

For many, the ECJ's relatively harsh verdict against fansite operators was surprising. Although the main responsibility for data collection lies with Facebook, it is theoretically possible for the page operators to place cookies on the visitor's device, even if the visitor does not have a Facebook account. According to the ECJ, this in addition to the fact that

2 https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf.

fansite operators receive the visitor's user data (even if only anonymised) and can use these for parameterisation lead to joint responsibility of the site operators. This is particularly because of the fact that the collection of this data cannot (yet) be deactivated. Until Facebook grants this option to its users, the common fansite operator remains jointly responsible for the collection of user data. Even the ECJ takes account of the significant imbalance in the use of data between Facebook and the operators of the respective fan page insofar as the degree of responsibility can be assessed differently in individual cases, however, in the court's opinion Facebook and the fansite operators are still joint controllers. In the end, Facebook will have to react to implementing mechanisms like cookie banners or others to give the user access to information. However, this decision and the German Federal Court's decision regarding the obligation of Facebook to provide heirs with access to the digital postbox of the decedent (BGH, 12 July 2018 – III ZR 183/17), clearly show that social media is now being regulated more strictly.

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 'appropriateness decision' that these countries ensure an adequate 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.

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 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, Guernsey, the Isle of Man, Canada (limited), the Faroe Islands, Israel (limited), Guernsey, Jersey, New Zealand, Switzerland and Uruguay. Any transfer of personal data to these countries will only have to satisfy the requirements of domestic data transfers.

Uncertainty currently surrounds data transfers to the United States. After the European Court of Justice declared the Safe Harbour principles of the Commission invalid, the Commission enacted the EU–US Privacy Shield. Under the protection of the new principles

of the Privacy Shield the United States is found to have an adequate level of data protection. But the Privacy Shield itself is again the target of a great deal of criticism. There are currently several complaints pending against the Privacy Shield at the European Court of Justice.

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.

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.

V PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Germany has a Federal Data Protection Agency and 16 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 charged with supervising the data privacy compliance of state entities, as well as all non-public entities whose principal place of business is established in the 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

One of the most discussed amendments specified by the GDPR and the new BDSG is the dramatic increase of the framework for fines. Before, the fines for data protection breaches were up to €300,000 per breach. Now, fines are up to €20 million or, in the case of an undertaking, up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher. This massive increase is directly addressed to Big Data companies. Especially the dynamic and the dependency on the turnover aims to achieve a deterrent effect even on the most be wealthiest companies worldwide. However, no fine has been imposed so far, thus everyone highly awaits the supervising authorities' first fines to estimate the further development and risks. However, the reasons for data protection breaches have not changed. Mostly they are caused by 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.

iii Private litigation

The GDPR imposes duties of notification on the data controller (see Articles 13 and 14 GDPR). He or she must notify the data subject among others, 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 the legal basis, the source of the data, where applicable, to whom they are disclosed, the duration of processing and the retention policy, etc. Additionally, the data subject has to be informed regarding all his or her rights granted by the GDPR. In detail, this notification has to 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 enumeration clearly shows that on the one hand the data subject is getting a lot of rights, on the other hands the controller will have invest more effort to satisfy the requests in a proper way, which is a question of time and expenses. 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. Especially, damages for pain and suffering from data protection violations can be claimed under civil law.

In Germany, the data protection authorities are not necessarily involved in enforcing the rights of individual data subjects. Instead, complaints against domestic controllers must 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 in.

VI CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As data protection gradually becomes a questions of technical measures, especially cybersecurity, Article 32 GDPR determines that pseudonymisation and encryption has to be applied to lower the risk of damaging the data subject in case of data breaches.

The implementation of such and similar technical 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. These measures became even more important with GDPR, as one can easily notice that the legal situation demands a higher ability to act. 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 have to 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.

VII OUTLOOK

The GDPR is still an unknown and often only can be understood by a teleological interpretation. In Germany, there are 16 data protection authorities that follow different interpretations of the GDPR text. This complicates advising in privacy matters. Therefore, it will be interesting to see how the new laws will be interpreted by German and European courts. Furthermore, we are looking forward to seeing what impact the GDPR will have on companies, especially social media operators.

Appendix 1

ABOUT THE AUTHORS

OLGA STEPANOVA

Winheller Rechtsanwaltsgesellschaft mbH

Olga Stepanova heads the IP/IT department at Winheller Attorneys at Law & Tax Advisors, where she advises German and international companies and non-profit organisations on issues of data protection, IT law and intellectual property. She also provides legal counsel in German and international copyright, trademark and media law matters. As member of Winheller's Russian desk, she advises her Russian clients in their mother tongue.

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

Tower 185
Friedrich-Ebert-Anlage 35–37
60327 Frankfurt
Germany
Tel: +49 69 76 75 77 80
Fax: +49 69 76 75 77 810
info@winheller.com
www.winheller.com

ISBN 978-1-912228-62-1