The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INTERNATIONAL INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

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

ACKNOWLEDGEMENTS

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

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 7

GERMANY

Jens-Marwin Koch[1]

I OVERVIEW

Germany is Europe's economic engine and in this light, data protection law is becoming an ever more important 'location factor'. Consequently, enquiries for legal advice and counsel in the area of German data protection have increased noticeably in recent years. These enquiries are not only issued by large groups of companies with subsidiaries in Germany, but also by foreign lawyers, economical auditors, and universities. What these stakeholders share is that they often do not possess a proficient command of German, and if they do, they will find it difficult to command the vocabulary necessary to understand and implement advice and counsel in German. Therefore even the most elementary issues may fail simply because of the language barrier.

The German Federal Data Protection Act has separate provisions for data processing in the public and private sectors. In addition, Germany has special privacy provisions for electronic information and communication services ('telemedia') and yet another set of privacy rules for the providers of services that transmit electronic signals. All these laws apply to some extent to the providers of online services. Through these laws Germany transposed European Union (EU) Directives 95/46 and 2002/58, albeit in a very complex and differentiated manner. Some German experts find that this complexity interferes with the requirement of transparency in that it keeps consumers from being aware of their rights and from exercising them.

In Germany, data protection has constitutional dimensions that flow from the guarantees of human dignity and personhood. From these, the Federal Constitutional Court crafted the right of informational self-determination that permits the processing of personal data only if authorised by statute or by consent of the data subject. In 2008, the court expanded these principles by articulating a constitutional guarantee of the

1 Jens-Marwin Koch is a partner at Winheller Rechtsanwaltsgesellschaft mbH.

confidentiality and integrity of IT systems. In 2010, the Constitutional Court struck down a German transposition of the EU Data Retention Directive for violating the principle of proportionality and the individual's rights of personhood.

In keeping with the EU Directives, Germany generally prohibits the collection and use of personal data unless the law specifically permits this or the data subject has given his or her informed consent. German law also follows the Directives on issues relating to rights and remedies of data subjects, security requirements, restrictions on location data, minimisation of data, and safeguards against transmitting personal data to third countries with lesser standards of protection. The German provisions, however, often call for the balancing of competing interests and the application of the principle of proportionality. These provisions have resulted in an extensive and varied case law.

II THE YEAR IN REVIEW

During the past year, the developments were strongly influenced by the EU, namely by the legislative activities of the European Parliament on data protection and the current decision of the ECJ on the 'right to be forgotten'. At the national level, the law had to deal, *inter alia*, with various aspects of customer and employee data protection in the online and offline area.

On jurisdictional matters, Facebook won an important victory. Schleswig-Holstein's Data Protection Commissioner had ruled that Facebook's 'real names policy' (i.e., its policy against accounts held in pseudonymous names only) was unfair and unlawful. The German Administrative Court granted Facebook's application for the suspension of that order on the grounds that the issue should instead be considered by the Irish data protection authority, since Facebook is based in Dublin.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Legislative history

In the late 1960s, technical progress and the new opportunities with respect to automatic data processing created a rising sensibility towards risks related to technical products and computers. In addition, society's evolving awareness of civil liberties and the growing scepticism towards the government and its activities resulted in a need to limit the government's power to collect information about its citizens. As a reaction, the German state of Hesse enacted the world's first Data Protection Act on 30 September 1970. The other states soon followed and on 1 January 1978, the first federal Data Protection Act (BDSG) entered into force. These acts established basic principles of data protection law, such as the requirement of a legal permission or the data subject's consent for any processing of personal data (Section 4, Paragraph 1 BDSG). Thus, these early acts focused on the prevention of misuse of personal data by government, granting the data subject only a few individual rights. The present German understanding of the data subject having an all-embracing right of self-determination regarding the handling and disclosure of his or her personal data was non-existent at that time.

German data protection developed a new dimension in 1983, with the Census Decision of the German Federal Constitutional Court. In this decision, the court held that the individual has a constitutional right to 'informational self-determination', a fundamental right derived from Article 2, Paragraph 1 in connection with Article 1, Paragraph 1 of the German Constitution (i.e., the constitutional guarantees of human dignity and free development of one's personality). Responding to increasing risks that were created by electronic automatic data processing, the court developed the concept of an individual's right to independently determine the use and disclosure of his or her personal data and to decide at what time and to what extent information about his or her private life shall be revealed. More importantly, the Court held that any data collection and processing requires a legal permission and must be proportionate. The Court's approach already contains the basic principles that form the present day foundation of German and European data protection law, namely the principles of data reduction, data economy and strict limitation and adhesion of data use for specific purposes. In consequence, for any new law or regulation on the processing, collection, and use of personal data, the legislature must precisely stipulate the nature, extent and purpose of the personal data that is being collected, thereby allowing the data subject to exercise his or her informational self-determination.

In 1990, an amendment to the Federal Data Protection Act incorporated the requirements established by the Federal Constitutional Court. At the time, the BDSG aimed primarily at protecting against the abuse of data processing by the government, requiring data processing to be based on specific statutory enabling legislation. On the other hand, the consent of an individual is generally necessary to permit data processing in the private sector.

The courts of ordinary jurisdiction have also contributed to the interpretation of data protection law. They are often called upon to apply the principle of proportionality and to balance competing interests, such as privacy versus technical feasibility or freedom of expression. There is a flood of cases that limit the right to informational self-determination.

A decision of the Federal Court of Justice of 2009 explains that informational self-determination has to be balanced with other rights, in that case with freedom of speech. In May 2012, the Federal Court of Justice balanced the right to be forgotten with the public's right to know. The Court held that under the circumstances of the case, the public's right to know outweighed the interests of the complainants to be shielded from publicity.

Current law

The BDSG defines personal data as 'individual pieces of information about personal or factual circumstances about an identified or identifiable human being'. This definition applies to all the data handled by telemedia service providers irrespective of whether the data is governed by the BDSG or the Telemedia Act of 2007 (TMA). Different rules on consent requirements, however, apply to different categories of data.

Contract data, as defined in the TMA, is the data that is required to establish, develop, or change a contractual relationship with a telemedia service provider. Contract data is to be collected sparingly, to satisfy the principle of data minimisation. It may only be used for the intended contractual purpose and must be deleted once it is no

longer needed. This use is statutorily permitted. The data subject's specific consent, however, is required if the service provider wants to use the data for other purposes, such as advertising or market research. The provisions on contract data apply whenever a relationship is established by an online registration. They apply therefore, to Facebook and other social media.

Utilisation data is the personal data that a telemedia service provider may collect and use to facilitate use of the service and for accounting purposes. The service provider may use this data to create user profiles for market research and advertising, unless the user objects after having been duly informed. The thus-created profiles must be identified by a pseudonym, and the identity of the user may not be revealed.

Other data, particularly content data, falls under the consent requirements of Sections 28 through 30 of the BDSG if it is collected by online service providers. In their current form, these provisions were introduced through the 2009 reform of the BDSG, and their complexity is legendary. Generally, they allow certain commercial uses of data, including 'list-making' and 'scoring', albeit under numerous safeguards. Section 29 deals with data collection and storage for a controller's own business purpose and for the purpose of disclosure of the data to third parties, including for direct marketing. Such activities are permitted to some extent without the data subject's consent, yet the competing interests must be balanced and the data subject must be notified of the purpose of the processing.

There has been much discussion of whether IP addresses are personal data, and the majority opinion considers them to be always personal data when they are fixed IP addresses that identify a specific computer. If they are movable IP addresses that are assigned by the access provider every time the user logs in, then they are personal data only if the service provider has enough information to actually identify the user, which will usually be the case.

The BDSG defines sensitive data according to Directive 95/46 as that data relating to race, ethnicity, political opinions, religious or philosophical beliefs, or health or sex life. Consent must be expressed specifically in order to permit the collection and use of such data. Moreover, controllers of such data must undergo an examination of their operations as required by Directive 95/46.

ii General obligations for data handlers

The privacy provisions of the BDSG address data controllers, namely, entities that process personal data. The controllers are required to register with the pertinent state authority, and this also applies to telemedia service providers. Registration is required in particular for controllers who transfer data to others or conduct market research. They must always register even though other controllers can avoid registration if they appoint an internal data protection official (see below).

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

According to Section 13 TMA, the controller must 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 consent knowingly and unambiguously, the consent is recorded, the user may view his consent declaration at any time, and the user may revoke consent at any time with effect for the future. These principles conform with Section 4a BDSG, which requires consent to be based on the voluntary decision of the data subject. Consent, however, is not always required. Many statutory exceptions allow for the use of data without consent, for various business-related purposes.

According to Section 13, Paragraph 1 TMA, a telemedia service provider must inform the user at the beginning of the contractual relationship of the extent and purpose of data collection and use and of whether the data will be processed outside of the European Union. If the provider intends to use an automated process that will allow the identification of the user, then this information has to be provided when data collection commences, and the user must at any time have access to this instruction.

This provision of the TMA has been interpreted as applying only to contract and usage data, thus leaving content data under the governance of Section 4, Paragraph 3 BDSG. The latter provides that the controller must inform the data subject of the identity of the data controller, the purpose of the collection, processing, and use of the data, and the categories of intended recipients if this is not foreseeable for the data subject. This information must be provided when the data is first collected.

In addition to necessary imprint information, any service provider that collects, processes, or uses personal data on a website is obliged to publish a privacy policy on his or her website. The information provided in the privacy policy has to meet the requirements of Section 13 TMA. This means that the information has to be provided at the beginning of the session and in a generally comprehensible and understandable fashion. In addition, it needs to be accessible by the recipients at any given time.

The question of when a given act of processing must be notified to the supervisory authority depends on the act of processing itself and the structure of the responsible entity wishing to carry out such processing. This differentiation sets Germany apart from many of the EU Member States that require every act of processing to be formally notified to the supervisory authority before they can be implemented. However, with the exception of small corporations and insignificant acts of processing, the fact that there do exist certain carve-outs should not be taken to mean that the supervisory authorities will not take the notification duties seriously; they have the right to audit responsible entities regardless of whether these have notified them of any act of processing or not.

Section 4, Paragraphs 1 and 2 BDSG establish an obligation for private entities to notify the competent authority if any data is processed by automated means as well as setting out exceptions to that requirement. The duty to actively notify acts of processing to the supervisory authority does not exist where the responsible entity has appointed a data protection officer in accordance with Section 4f and 4g BDSG or if the respective entity deals with personal data for its own purposes and employs no more than nine people permanently in the automated processing of personal data.

iii Technological innovation and privacy law

Cookies

Under German data protection law, the use of cookies is only relevant if the information stored in the cookie is considered personal data. In such an event, the use of the cookie is only considered to be lawful if it is validated by the data subject's consent. A cookie is a piece of text stored on a user's computer by his web browser. A cookie 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 and when it contains data that allows the controller to identify the data subject. This might also be the case when the data subject cannot be identified by the cookie data itself, but only by means of other data that can be accessed by the controller and linked to the data contained in the cookie. With respect to website providers offering services that require an application, the consent for the use and processing of cookies containing personal data may be obtained during the application process. The use of cookies for the purposes of advertising, market research, or to organise the telemedia on the basis of need is lawful without consent to the extent permitted by Section 15, Paragraph 3 TMA.

Cloud computing

Cloud computing raises difficult data protection issues. Cloud computing relationships are technically complex and involve the transfer of data across multiple jurisdictions, as the physical location of data in the cloud is often not bound to a specific server in a specific country. Moreover, it is virtually impossible, at least for the data subject, to ascertain as to whether all servers used are effectively secure or to determine who has control over and insight into the data. According to German data protection law, the transfer processing of data to non-EU states is subject to strict regulations. The controller must ensure that his or her use of the cloud computing services is in compliance with the requirements outlined in Section IV, *infra* with respect to cross-border data transfer, processing and use. This is a highly complicated task. For instance, the controller will have to ensure that the cloud service provider observes an adequate data protection level at all times. As a result, the legality of cloud computing is highly disputed under current law.

Social media

The role of social media in the recruitment process is currently subject to intense scrutiny by the lawmakers and the supervisory authorities. There is a perceived need to protect potential and current employees, especially younger employees that are just starting their career from the adverse effects of publications they may have made about themselves and later regret.

Currently there exists no specific legislation that would govern how employers may be using data they have gathered from such social networks. It is, however, generally accepted that one may not obtain access to otherwise restricted data through improper means. Other than that, however, there are only the general rules of adequacy, and in many cases, most prominently in the case of Facebook, default settings adopted by users will cause much of their personal data to be publicly accessible in any event.

To countermand these perceived ill effects, the new employee data protection legislation will provide for a specific requirement: that an employer may only use data a prospective employee has published on telemedia services specifically designed as a platform to tender employment.

This proposed legislation has been met certain with criticism: the delineation between services such as LinkedIn and Xing on one hand and Facebook on the other continues to blur. Many employees today use Facebook as their sole resource for their online presentation and they expect it to be included in hiring or recruitment processes. Therefore, the question arises of how a service like Facebook should be categorised. Furthermore, if a prospective employee chooses to publicly disclose personal information without access restrictions, then the distinction between ordinary and job-related telemedia services becomes an artificial one.

Another main area of concern about the use of social networks is when social networks are used as part of a job.

If an employee chooses to use a standard social network like Facebook, the primary issue will be the protection of the personal data of the employee and of corporate data subject to non-disclosure requirements against improper disclosure. Corporations need to establish objective guidelines that instruct their employees as to the permissible extent of social network use, and the nature of information that can and cannot be disclosed on these social networks.

Several corporations, in some cases for several years, have established their own internal social networking sites and these internal networks offer the significant advantage of being hosted in a controlled environment, so that at least sensitive corporate information can be more freely shared than it would be on public social networks.

iv Specific regulation

Perhaps the most common cause for centralised collection, processing or use of personal data in an employment relationship, is the use of tools and lT infrastructure shared across multiple legal entities in groups of companies, and the use of shared services and shared functions, whereby individual centralised organisations take the place of hitherto decentralised staff functions. A good example are employee self-service helpdesks and centralised human resources departments supporting any number of legal entities in multiple countries and interfacing directly with the employees and their managerial structure.

The use of personal data in an employment relationship is associated with particular compliance requirements when such use is to be carried out by another legal entity within a group of companies that is not the legal employer of a given employee. The underlying reason for these issues is that Section 32, Paragraph l, sentence l BDSG includes a definitive justification for processing personal data where it is required to fulfil an employment relationship. This justification is limited to the employment relation between the employer and the employee only, and only the legal entity actually holding the employment contract, the 'legal employer', can draw upon the justification. Other legal entities in a group of companies that the legal employer is also a part of cannot rely on this justification, even though the employee may be interfacing with employees of such group members on a fairly regular basis.

This absence of group regulations is a major barrier to the free interchange of personal data in groups of companies; in effect, it causes each single legal entity in a group of companies to be considered separately and any intra-group transfer of data regarding an employee is treated no differently than if the other legal entity were not part of the group of companies at all. It is necessary to visualise this issue in order to appreciate the fact that centralised functions in a group of companies cannot generally rely upon the justification that their use of personal data satisfies the requirements of the fulfilment of the employment contract. To resolve this obstacle, the establishment of central processing structures of personal data in groups of companies by utilising the concept of commissioned data processing can be a viable option for corporations.

An *ad hoc* working group formed by the Düsseldorf Circle (an informal body made up of all the various German data protection authorities) published guidelines on the intra-group transfer of personal data designed to facilitate, as much as the current statutory framework permits, the internal workings of groups of companies. Apparently, the working group believes that there are certain high-level executive employees whose duties are related not just to their legal employers but also to the business of their organisations on a supranational level.

Corporations have adopted an approach that defines the management levels that shall have permission to access the personal data of individual employees that are required to fulfill their duties within the organisation. Thus, an approach that allows the direct manager or supervisor of an employee in another group entity to access that employee's personal data appears to be widely accepted.

IV INTERNATIONAL DATA TRANSFER

The international transfer of personal data is regulated within the framework of Sections 4b and 4c BDSG. There is a general distinction between the transfer within the EU/EEA or to a list of 'trusted countries', and the transfer to 'third countries' on the other. For an international data transfer to be lawful, it must not only comply with Sections 4b and 4c BDSG, but it must also be in compliance with the general provisions pertaining to the legality of processing operations involving personal data as described above.

i Data transfer within the EU or EEA area

Section 4b BDSG states that international transfer of personal data within the area of the EU or EEA is covered by the same rules as national data transfer within Germany. For such international data transfers, private entities merely require a legal permission under Sections 28 to 32 BDSG, or the data subject's consent.

ii Data transfer to countries outside of the EU or EEA area

If a private entity intends to transfer personal data internationally to another entity located outside of the area of the EU or EEA (a third country), Section 4b, Paragraph 2, sentence 2 BDSG stipulates additional requirements. 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 warranted in the country to which the data is transferred.

An adequate level of data protection exists in certain 'third countries' that have been identified by the European Commission. These are Argentina, Guernsey, the Isle of Man, Canada, Jersey and Switzerland. Any transfer of personal data to these countries will only have to satisfy the requirements of data transfers within the EU or EEA.

Data transfers to any other non-EU country, namely to the US, may only be justified by the derogation rules of Sections 4b and 4c BDSG. Under Section 4c, Paragraph 1 BDSG, 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 or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

e the transfer is necessary in order to protect the vital interests of the data subject; or

f 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 legitimate interest, to the extent that the conditions laid down in law are fulfilled in the particular case.

The most relevant grounds being that of (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 with data tranfers 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 is 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 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 Section 4c, Paragraph 2 BDSG. The primary safeguarding measures are the use of standard contractual clauses issued by the European Commission and the establishment of binding corporate rules.

V DISCOVERY AND DISCLOSURE

The 2009 amendments to the BDSG require companies to report an abuse or loss of sensitive data to the relevant German supervising authority as well as the affected person(s). The amendments also increased fines for serious data privacy breaches to

€300,000. In 2011, the German data protection authority issued a set of guidelines explaining the data-breach provisions of the amendments. In contrast to US discovery rules, German law generally does not require litigants to disclose documents to the other party. German authorities will nevertheless permit very limited discovery for pending US proceedings if the US court sends a letter of request for specific documents needed to resolve an issue.

Discovery of workplace e-mails in Germany is particularly challenging. The BDSG limits the use of nearly all employee personal data, which is defined to include most employee e-mails. If an employer permits employees to use their computers at work for private communication, then those communications are likely protected from discovery. The distinction between private and employment-related communication is sometimes difficult to make, and it is unclear how much of an employee's e-mails would ultimately be excluded from discovery for privacy reasons.

In 2012, Germany began to relax some of its strict control over access to public information such as tax and employment records, to meet the EU goal of achieving greater standardisation of data protection regulations across EU Member States.

Germany has at least one blocking statute, the Federal Maritime Shipping Act of 24 May 1965, which was enacted to frustrate attempts by the United States Federal Maritime Commission to gather information from shipping lines concerning allegations of anti-competitive practices.

VI 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 the consumer may 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 this data to profile the data subject for commercial purposes. Although German law prohibits these practices unless informed consent has been given and although German law applies to any collection of data on German soil, Germany cannot enforce these laws against global players.

The Federal Data Protection Agency is charged with supervising the data privacy compliance of federal entities, and well as certain non-public entities such as telecommunication service providers that are subject to specific supervision, as well as the application of the recently enacted federal Freedom of Information Act.

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 these (state or federal) parliaments.

The role and position of the supervisory authorities in Germany has, in particular just recently, become the subject of intense scrutiny, especially with respect to their own organisational compliance with the requirements of EU Directive 95/46/EC.

ii Recent enforcement cases

The relevant Sections 43 and 44 of the BDSG regarding administrative and criminal offences have been substantially enlarged by the last redraft of the BDSG that entered into force in 2009. It was introduced by the government as a consequence of a series of data protection scandals involving prominent German companies. Penalties were increased to €50,000 for failure to comply with formalities and €300,000 for other data protection breaches. Most of these data protection breaches were caused by internal compliance activities of the companies where the responsible management carelessly contravened the high standards of German data protection law (e.g., through video surveillance or screening bank account details). The main reason for wrongdoing was the false understanding that compliance activity by its nature is a justification for any use of personal data. This assumption turned out to be incorrect.

For instance, in October 2009 the Data Protection Authority of Berlin imposed a fine of €1.124 million on Deutsche Bahn AG for significant violations of data protection law. This is allegedly the highest administrative fine ever imposed in Germany for non-compliance with data protection law. Deutsche Bahn was fined for mass screenings of employee data, including names, addresses, telephone numbers and bank details, and for matching them with supplier data, supposedly to detect fraudulent activities, in particular employee-fronted shell companies.

In fact, there is no statutory law justifying use of personal data for compliance activities on a general level. This has to be decided on a case-by-case basis. Consequently, depending on the circumstances of the actual matter, the disclosure of personal data without consent of the data subject or explicit statutory right to do so may be subject to punishment according to Sections 43, 44 BDSG, with sanctions of imprisonment for up to two years or a fine.

iii Private litigation

The privacy rights and remedies of telemedia users are governed to a large extent by the BDSG. The Act imposes duties of notification on the data controller (see Sections 4, Paragraphs 3 and 33. He must notify the data subject on the types of data that are being collected, the source of the data, the purposes for which the data is collected, and to whom it are disclosed.

For the data subject, Section 34 of the Act grants rights of access and rights to effect correction, erasure, and blockage (Section 35). The right to demand erasure often becomes an issue when a user leaves a social networking medium. Users often waive the right of erasure in standardised terms of contract. It appears that this is currently permissible according to German law. Even if erasure were to be carried out, data is transmitted to third parties in many different ways in social media, so that erasure often does not fulfil its purpose.

Data subjects may enforce their rights through the judicial remedies provided in civil law. Injunctive relief as well as damages can be claimed. However, damages for pain and suffering are not available for data protection violations under private 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 (see Section IX.ii, *infra*).

VII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

In keeping with Article 4 of Directive 95/46, the law of the seat of the controller applies to data processing occurring in Germany if the controller resides in another Member State of the European Union. German law applies, however, if that EU-resident controller carries out data processing in Germany through a German subsidiary or establishment. German law also applies for any data processing occurring in Germany that is carried out by a controller who resides outside the European Union.

According to these principles, German law applies to an online search engine or social medium if it places a cookie on a German personal computer. Enforcement of German law, however, can rarely be achieved against foreign controllers.

The issue of applying German law to the collection of German data by controllers in third countries is addressed in the ongoing controversy over whether Facebook qualifies as an EU-domiciled controller because of its corporate address in Ireland. Many German experts are of the opinion that Facebook use in Germany, in particular the use of the 'Like' button, is subject to German law and therefore prohibited on the grounds that the data is ultimately transmitted to the United States, which does not have an EU-compatible data protection standard.

VIII CYBERSECURITY AND DATA BREACHES

Section 9 of the BDSG requires extensive technical organisational measures to ensure the overall integrity of IT systems that are being used for the processing of personal data, and these requirements live up to article 17 of Directive 95/46. The German provisions, as well as the Directive, call for a proportional interpretation of security requirements, by tailoring the need for security to the risk inherent in specific operations. Additional provisions on technical security are contained in Sections 107 and 109 of the Telecommunications Act.

Section 13 of the TMA requires controllers to install the necessary technical and organisational measures to ensure that:

a the user may terminate the relationship at any time;
b data will be automatically erased or blocked if required by law;
c the use of the service will not become known to third parties;
d data on the use of several telemedia by one user can be accessed separately, although they can be combined for accounting purposes; and
e data collected under a pseudonym cannot be combined with data personally identifying the user.

In August 2009, Germany introduced a security breach notification requirement that obliges controllers to notify the data subject if data was unlawfully transmitted or otherwise became known to third parties. This requirement was modelled after US law and is intended to increase consumer confidence in automated systems.

Anonymising data is a general principle of German data protection law, to be employed whenever feasible so as to minimise the proliferation of personal data. Data may also be placed under a pseudonym so as to preserve anonymity. These devices allow the data subject to retain control over his or her data while giving the controller greater possibilities for use and transmittal of the data. When data has been anonymised, it is no longer personal data and can therefore be freely used for market research. It becomes personal data again if the controller has the capacity to identify the data subject from that data. It appears that services are available in Germany that facilitate anonymity by allowing the user to communicate over an IP address that differs from his or her own.

Telemedia service providers are required to use pseudonyms for the collection of certain data. For example, for data concerning usage, the controller must employ pseudonyms to be allowed to create profiles for the purposes of market research. With regard to contract data, the telemedia service provider must make it possible for the data subject to use the service and pay for it under a pseudonym, and he or she must also inform the data subject of this option. The law provides, however, that the provider must make the use of pseudonyms possible only to the extent that it is technically feasible and can be reasonably expected. This is one of the many 'balancing and weighing' clauses that exist in German data protection law.

IX COMPANY POLICIES AND PRACTICES

i Compliance

Compliance with German data protection law will often require a number of agreements with different parties. In many instances, larger companies with an international approach or a German subsidiary will encounter the need for an agreement, for instance with the data subject for collecting his or her consent or with third parties to ensure a particular level of data protection and security. Therefore it may be useful for medium-sized or larger companies as well as NGOs or other international practising entities to have agreements, forms and directives adjusted to the particular situation but easily adaptable for the use with different clients, customers or situations. As far as external data protection and IT security is concerned, these agreements include those concerning data protection with third parties, as well as collection, processing or use of personal data on behalf of others, IT Security with third parties, granting a right to a data protection audit, or disclosure agreements with third parties. As far as internal data protection and IT security is concerned, agreements might encompass the appointment of internal or external data protection officers, data secrecy with employees, internal overview according to Section 4e BDSG, or deletion and disclosure agreements with employees.

ii Data privacy officer

Section 4f, Paragraph 1 BDSG sets forth a number of instances where private entities are obliged to appoint a data protection officer. According to this provision, certain medium-

sized and bigger companies have to appoint a data privacy officer (DPO). In particular, these are private entities dealing with personal data by automated means and, as a rule, employing more than nine people permanently in the automated processing of personal data. The same applies to private entities dealing with personal data by other means, and, as a rule, employing at least 20 persons for this purpose, as well as private entities carrying out automated processing of personal data in terms of Section 4f, Paragraph 1, sentence 6 BDSG. The DPO shall ensure compliance with the BDSG and other data protection provisions. His or her general duties are described in Section 4g BDSG. The obligation to appointment a DPO applies to almost every private business, since almost every business relies on the support of computer systems. Even if an entity is not obliged to appoint a DPO, it may be advisable to do so voluntarily because in that case the obligation to notify no longer applies. The German DPO is considered as a compliance function embedded in the organisation of public and private entities and somehow a surrogate supervisory authority and a figure of particular trust to guarantee data privacy compliance in a given entity. The person who shall be appointed as DPO must satisfy certain requirements set forth in Section 4f, Paragraph 2 to 5 BDSG.

X OUTLOOK

The fact that the German DPO model is a rather successful one can also be seen from current developments at the EU level. In both the Targeted Stakeholder Consultation and the High-Level Roundtable Discussion – both events orchestrated by the European Commission as part of the knowledge-gathering and consultation process in the course of the reform of the Directive 95/46/EC – multiple participants have commented that it would be desirable to relieve the responsible entity from the administrative burden of filing every single act of processing and system with the competent supervisory authority. The DPO, it was argued, is much more tightly implemented and embedded in the business processes of the responsible entity and he or she is therefore truly in a position to validate and assess the risks associated with a given act of processing – in contrast to the supervisory authorities that, when inundated with notifications, would hardly find time or knowledge to do much more than a cursory examination of the filing and would certainly then shelve the notification and only take a closer look once an issue arose, most prominently in the form of a complaint by a data subject. The concept of the DPO is therefore rightly regarded as a milestone in German data privacy and protection compliance, and a DPO is not only a valued administrative relief for the responsible entity but truly promotes and fosters data privacy and protection compliance. Consequently, the DPO model has also been integrated into the first proposal of the new EU General Data Protection Regulation. However, it is already subject to controversial discussions, in particular among those Member States that do not have any experience with the DPO concept yet. Addressed to those concerns it is fair to say that among the many disputed areas of German data protection law, the position of the DPO is one of the few that all relevant parties believe has proven itself.

As to the proposed EU Data Protection Regulation, many German experts are apparently in favour. Among them is the German Federal Data Protection Commissioner, who finds that the reform proposal has a chance of improving the current legal situation,

in particular in relation to service providers from non-EU Member States. Some Germans, however, oppose the proposed EU Regulation for violating the EU subsidiarity principle and for potentially lowering German data protection standards, as well as for surrendering constitutional sovereignty over the issue.

Appendix 1

ABOUT THE AUTHORS

JENS-MARWIN KOCH

Winheller Rechtsanwaltsgesellschaft mbH

Jens-Marwin Koch heads the IP/IT department at Winheller, where he advises German and international businesses and non-profit organisations on issues of data protection. He also provides legal counsel in US, German and international copyright, trademark, and media law matters. Before joining Winheller, he worked for many years at a law firm in Berlin, acted as head of the Berlin office of a Swiss law firm and worked for an IP boutique law firm in New York City. He is also admitted to practise as an attorney-at-law in New York.

Jens-Marwin Koch gained extensive experience in his fields of interest during his graduate studies at the University of Illinois at Urbana-Champaign (US) where he received his LLM degree. He also studied law at the Universities of Mannheim, Munich, Freiburg and Bielefeld and participated in the master of comparative law (MCL) programme at the Universities of Mannheim and Adelaide (Australia).

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

Europa-Allee 22
60327 Frankfurt am Main
Germany
Tel: +49 69 76 75 77 80
Fax: +49 69 76 75 77 810
j.koch@winheller.com
www.winheller.com