04.17

PinG

Privacy in Germany

Datenschutz und Compliance

5. Jahrgang
Juli 2017
Seiten 129–164

www.PinGdigital.de

ESV ERICH SCHMIDT VERLAG

86118

Big Data im Gesundheitswesen

Big Data und E-Health

Herausgegeben von der **Stiftung Datenschutz**

Mit Beiträgen von Prof. Dr. Björn Bergh, Antje Brandner, Prof. Dr. Roland Eils, Prof. Dr. Ulrich M. Gassner, Björn Haferkamp, M.A., Prof. Dr. Dirk Heckmann, Dr. Oliver Heinze, Prof. Dr. Christof von Kalle, Christian Klose, Dr. Ulrike Kutscha, Klaus Müller, Anne Paschke, Bertram Raum, Peter Schaar, Dr. Christopher Schickhardt, Dr. Björn Schreiweis, Prof. Dr. Stefan Selke, Prof. Dr. Stefan Sorgner, Prof. Dr. Frank Ückert, Dr. Thilo Weichert, Prof. Dr. Eva Winkler

2017, 201 Seiten, fester Einband, € (D) 42,–
ISBN 978-3-503-17491-1
DatenDebatten, Band 2

Telemedizin, datenbasierte Gesundheitsanalysen, Health-Apps und mobile Geräte zur individuellen Gesundheitskontrolle – immer mehr Gesundheitsdienstleistungen werden mit Hilfe digitaler Dienste und Strukturen angeboten.

Chancen nutzen, Patientenrechte wahren

Die rasante Entwicklung verspricht nicht nur enorme Qualitätssteigerungen in der Gesundheitsversorgung und neue Märkte im Gesundheitssektor. Sie wirft auch viele Fragen mit weitreichender **Relevanz für den Datenschutz auf**:

- Wie sehen die wissenschaftlichen, aber auch die ökonomischen Perspektiven dieser Entwicklung aus?
- Wie zuverlässig sind digitale Lösungsansätze im Gesundheitsbereich?
- Wie entwickelt sich zukünftig das Arzt-Patienten-Verhältnis?
- Welche gesellschaftlichen Folgen könnte eine „Kultur der Selbstvermessung“ haben?
- Wie kann das Vertrauen der Patienten bzw. der Anwender in E-Health-Dienstleistungen nachhaltig gestärkt werden?

Auch als eBook erhältlich mit komplett verlinkten Inhalts- und Stichwortverzeichnissen.

www.ESV.info/17492

Weitere Informationen:

www.ESV.info/17491

ESV ERICH SCHMIDT VERLAG

Auf Wissen vertrauen

Bestellungen bitte an den Buchhandel oder: Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-265 · **Fax** (030) 25 00 85-275 · **ESV@ESVmedien.de** · **www.ESV.info**

PinG

Sehr geehrte Leserinnen, sehr geehrte Leser,

Anonymisierung und **Zweckbindung**: Zwei **Grundsatzthemen** prägen dieses Heft. *Johannes Eichenhofer* nimmt den Zweckbindungsgrundsatz kritisch unter die Lupe und kommt zu dem Ergebnis, dass die DSGVO und das neue BDSG im nicht-öffentlichen Bereich nicht allzu viel von dem ebenso hehren wie nebulösen Grundsatz übrig lassen. *Omer Tene* und *Gabriela Zanfir-Fortuna* befassen sich mit der Anonymisierung und zeigen auf, dass man sich von einem binären Schwarz-Weiß-Denken verabschieden sollte. Statt immer höhere Anforderungen an eine rechtlich anerkannte Anonymisierung zu stellen, sollte man anerkennen, dass jede schwache Anonymisierung vorzugswürdig gegenüber den „Klarnamen" ist. *Tene* und *Zanfir-Fortuna* öffnen den Blick auf ein veritables **„Spektrum der Identifizierbarkeit"**.

Datenschutz und **IT-Sicherheit** sind ein Geschwisterpaar. Mit dem neuen IT-Sicherheitsgesetz und der europäischen NIS-Richtlinie befassen sich *Simone Rosenthal* und *Frank Trautwein*.

Die **DSGVO** kommt auch in diesem Heft nicht zu kurz. *Max Mosing* befasst sich mit dem Entwurf eines österreichischen Datenschutz-Anpassungsgesetzes. *Daniela Gaub* und *Kay Uwe Berg* stellen den Leitfaden zur Anwendung und Umsetzung der DSGVO für das **Forderungsmanagement** vor. *Christian Volkmer* und *Ingo Kaiser* bereiten die Änderungen auf, die die DSGVO für die Anforderungen an **Verfahrensverzeichnisse** mit sich bringt, und analysieren die Voraussetzungen und Bedingungen einer **Datenschutz-Folgeabschätzung**.

Die **Bundestagswahl** steht vor der Tür. *Frederick Richter* wirft aus Sicht der **Stiftung Datenschutz** einen Blick in die Parteiprogramme und fasst zusammen, was die Parteien zum Datenschutz zu sagen haben.

Politisch brisant ist der gelegentliche Spagat zwischen gesetzlichen Offenbarungspflichten und Übermittlungsverboten, zu dem es in **transatlantischen Fällen** häufig kommt. *Kai-Uwe Plath* befasst sich mit dem **deutsch-amerikanischen Rechtshilfeabkommen** und dessen Bedeutung bei der Anwendung des Datenschutzrechts.

Das Heft wäre nicht rund ohne die **Schlaglichter**, die *Philipp Müller-Peltzer* zusammengestellt hat mit Anmerkungen zu aktuellen Entscheidungen und Entwicklungen.

Eine anregende Lektüre wünscht

Ihr Niko Härting
Für Redaktion und Verlag

PinGdigital:
Das eJournal der PinG

Wissenswertes zu Datenschutz und Compliance per Klick & Wisch

PinGdigital ist die digitale Seite der PinG: der Zeitschrift für Datenschutz und Compliance.

PinGdigital ist zeit- und ortsunabhängig online verfügbar auf Ihrem Rechner, Smartphone und Tablet.

PinGdigital erscheint wie die Zeitschrift 6x im Jahr und bietet Ihnen zahlreiche zusätzliche Vorteile und Extras, nämlich

- „Online First" – Ihr **Wissensvorsprung** durch ein **zeitlich früheres Erscheinen** als die Printausgabe,
- den **PinG-Blog** und den **PinG-Tweet**, die Sie mit News und Denkanstößen versorgen,
- die leistungsfähige **Volltextsuche** mit zahlreichen intelligenten Filtermöglichkeiten,
- das **Online-Archiv** mit allen bereits erschienenen Ausgaben und der übersichtlichen, separaten Darstellung aller Einzelbeiträge,
- den **Erinnerungsservice per E-Mail**, der Sie an jede neue Ausgabe der **PinG** erinnert.

www.PinGdigital.de

ESV ERICH SCHMIDT VERLAG

Auf Wissen vertrauen

Bestellungen bitte an den Buchhandel oder: Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-225 · **Fax** (030) 25 00 85-275 · **ESV@ESVmedien.de** · **www.ESV.info**

Privacy in Germany Datenschutz und Compliance

PinG 04.17 5. Jahrgang Seiten 129–164

Inhalt

Impressum

PinG Privacy in Germany
5. Jahrgang (2017)
Erscheinungsweise: 6 mal jährlich
www.PinGdigital.de

Herausgeber: RA Prof. Niko Härting
Redaktion: RA Prof. Niko Härting, RA Dr. Niclas Krohm, RA Dr. Carlo Piltz, RA Sebastian Schulz (Compliance)

Schriftleitung:
Dr. Niclas Krohm / Dr. Carlo Piltz
Schriftleitung PinG
Erich Schmidt Verlag GmbH & Co. KG
Genthiner Str. 30 G, 10785 Berlin
Telefax: 0 30/25 00 85-305
E-Mail: PinG@ESVmedien.de

Verlag: Erich Schmidt Verlag GmbH & Co. KG
Genthiner Straße 30 G, 10785 Berlin
Telefon (0 30) 25 00 85-0, Telefax (0 30) 25 00 85-305
E-Mail: ESV@ESVmedien.de, Internet: www.ESV.info

Vertrieb: Erich Schmidt Verlag GmbH & Co. KG
Genthiner Straße 30 G, 10785 Berlin
Postfach 30 42 40, 10724 Berlin
Telefon (0 30) 25 00 85-229, Telefax (0 30) 25 00 85-275
E-Mail: Abo-Vertrieb@ESVmedien.de
Konto: Deutsche Bank AG
IBAN: DE 31 1007 0848 0512 2031 01
BIC(SWIFT): DEUTDEDB110

Bezugsbedingungen: Jahresabonnementpreis € 138,–; Einzelheft im Abonnement (6 x jährlich) € 23,–; Einzelheft € 25,–; Sonderpreis für Studenten fachbezogener Studiengänge und Referendare (gegen Vorlage der Studienbescheinigung / Referendarurkunde): Jahresabonnementpreis € 96,–; Einzelheft im Abonnement € 16,–. Alle Preise jeweils einschl. Umsatzsteuer und zzgl. Versandkosten. Die Bezugsgebühr wird jährlich im Voraus erhoben. Abbestellungen sind mit einer Frist von 2 Monaten zum 1. 1. j. J. möglich.

Anzeigen: Erich Schmidt Verlag GmbH & Co. KG, Genthiner Straße 30 G, 10785 Berlin
Telefon (0 30) 25 00 85-629, Telefax (0 30) 25 00 85-630
E-Mail: Anzeigen@ESVmedien.de

Anzeigenleitung: Sibylle Böhler

Es gilt die Anzeigenpreisliste Nr. 5, vom 1. Januar 2017, die unter http://www.esv.info/z/PinG/zeitschriften.html bereitsteht oder auf Wunsch zugesandt wird.

Manuskripte: Hinweise für die Abfassung von Beiträgen stehen Ihnen auch als PDF zur Verfügung unter: www.ESV.info/zeitschriften.html.
Von Text und Tabellen erbitten wir neben einem sauberen Ausdruck auf Papier – möglichst ohne handschriftliche Zusätze – das Manuskript auf CD-ROM oder per E-Mail bevorzugt in Word, sonst zusätzlich im RTF-Format. Zur Veröffentlichung angebotene Beiträge müssen frei sein von Rechten Dritter. Sollten sie auch an anderer Stelle zur Veröffentlichung oder gewerblichen Nutzung angeboten worden sein, muss dies angegeben werden. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag das ausschließliche Verlagsrecht und das Recht zur Herstellung von Sonderdrucken für die Zeit bis zum Ablauf des Urheberrechts. Das Verlagsrecht umfasst auch die Rechte, den Beitrag in fremde Sprachen zu übersetzen, Übersetzungen zu vervielfältigen und zu verbreiten sowie die Befugnis, den Beitrag bzw. Übersetzungen davon in Datenbanken einzuspeichern und auf elektronischem Wege zu verbreiten (online und / oder offline), das Recht zur weiteren Vervielfältigung und Verbreitung zu gewerblichen Zwecken im Wege eines fotomechanischen oder eines anderen Verfahrens sowie das Recht zur Lizenzvergabe.
Dem Autor verbleibt das Recht, nach Ablauf eines Jahres eine einfache Abdruckgenehmigung zu erteilen; sich ggf. hieraus ergebende Honorare stehen dem Autor zu. Bei Leserbriefen sowie bei angeforderten oder auch bei unaufgefordert eingereichten Manuskripten behält sich die Redaktion das Recht der Kürzung und Modifikation der Manuskripte ohne Rücksprache mit dem Autor vor.

Zitierweise: PinG Jahr, Seite

ISSN: 2197-1862

Satz: multitext, Berlin
Druck: Ludwig Austermeier, Offsetdruck, Berlin

PRIVACY TOPICS

Chasing the Golden Goose: What is the path to effective anonymisation?

Omer Tene, Senior Fellow, Future of Privacy Forum

by Omer Tene and *Gabriela Zanfir-Fortuna*

Gabriela Zanfir-Fortuna, PhD; Fellow, Future of Privacy Forum

Searching for effective methods and frameworks of de-identification often looks like chasing the Golden Goose of privacy law. For each answer that claims to unlock the question of anonymisation, there seems to be a counter-answer that declares anonymisation dead. In an attempt to de-mystify this race and un-tangle de-identification in practical ways, the Future of Privacy Forum and the Brussels Privacy Hub joined forces to organize the Brussels Symposium on De-identification – "Identifiability: Policy and Practical Solutions for Anonymisation and Pseudonymisation". The event brought together researchers from the US and the EU, having academic, regulatory and industry background, discussing their latest solutions for such an important problem. This contribution looks at their work in detail, puts it in context and aggregates its results for the essential debate on anonymisation of personal data. The overview shows that there is a tendency to stop looking at anonymisation/identifiability in binary language, with the risk-based approach gaining the spotlight and the idea of a spectrum of identifiability already generating practical solutions, even under the General Data Protection Regulation.

I. Introduction

De-identifying personal data can very well represent a Golden Goose for protecting privacy and other rights of those whose data make up immense databases, while allowing the use of that data for unlimited purposes. The benefits of **anonymisation** are significant. For instance, framing this discussion under EU data protection law is clear: if a controller is processing data that has been de-identified so as to become anonymous, then the data protection regulatory framework does not apply to that processing operation because the data is not personal and, hence, does not fall in the material scope of data protection law. This principle, recognized under Directive 95/46,[1] is also spelled out in the General Data Protection Regulation[2] (GDPR), under Recital 26:

> *"The principles of data protection should therefore not apply to anonymous information, namely information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".*

The same stands true for most privacy laws worldwide, because their scope of application is defined based on whether information is identifiable or not.[3] However, in practice things are not at all as clear as they may seem in legal wording. Numerous studies have shown that re-identifying de-identified data, as well as identifying an individual using different categories of data points is usually

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 P. 0031–0050; see Recital 26.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27. April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, which will become applicable on 25 May 2018.

3 *I. Rubinstein* in his Framing the Discussion paper of the Brussels Privacy Symposium on Identifiability: Policy and Practical Solutions for Anonymisation and Pseudonymisation.

possible with the appropriate tools.[4] Should, then, anonymisation be considered unachievable?

Recent guidance from the Information Commissioner's Office (ICO) suggests that the answer to this question may not be relevant after all: "It may not be possible to establish with absolute certainty that an individual cannot be identified from a particular dataset, taken together with other data that may exist elsewhere. The issue is not about eliminating the risk of re-identification altogether, but whether it can be mitigated so it is no longer significant. Organisations should focus on mitigating the risks to the point where the chance of reidentification is extremely remote".[5] Furthermore, the regulator sees the value of anonymisation techniques beyond taking processing operations outside the scope of data protection laws: "it is also a means of mitigating the risk of inadvertent disclosure or loss of personal data".[6] In other words, even if data protection or privacy laws would apply to data that has been "reversibly anonymised", it would still pay off for organisations to anonymise the data they are processing. It then becomes essential to understand to what extent and how could compliance mechanisms be adjusted to accommodate processing of data that undergo "reversible anonymisation".

The French Supreme Administrative Court (*Conseil d'Etat*) recently dealt with the question of whether processing personal data that is subject to two specific de-identification techniques, "hashing" and "salting", would still allow individuals to be entitled to exercise their rights as data subjects.[7] The case concerned monitoring of MAC addresses of mobile phones by JCDecaux, through their panels showing ads in a Parisian public market. The French DPA (*CNIL*) did not authorize this processing operation because the controller did not provide mechanisms for the exercise of the data subjects, claiming that it anonymises the data to the extent that the French data protection law is not applicable.[8] The Court upheld the decision of the CNIL. The main argument of the French judges was that even if the "*hashing* and *salting* techniques have the purpose to obstruct access of third parties to that data, they allow the data controller the possibility to identify the data subjects and they do not prohibit correlation of records related to the same individual, or inferring information about him or her".[9] The Court considered that the purpose of the processing operation (monitoring the behavior of passersby, including measuring the repetitiveness of their walking-byes and the pattern of their movements between ad panels) is incompatible with processing anonymised data,[10] and therefore the claim of the controller that it processes anonymous data is not substantiated.

The area between what is personal and what is anonymous convincingly looks like quicksand, and the legal implications of understanding where in that area the processed data stands are momentous. Contributions presented and discussed within the Brussels Symposium on De-identification, organized[11] by the Future of Privacy Forum and the Brussels Privacy Hub substantially inform this debate.

Rubinstein provided a comprehensive framework to initiate the discussions, summarizing two decades of scholarship and policy-making on anonymisation/de-identification, exploring the visions of formalists, pragmatists and those who plead for convergence.[12] Rubinstein asks poignant questions – "Should we define these terms in binary fashion or are they better understood as the endpoints of a wide spectrum?"; "Given the inevitable tradeoffs between privacy and data utility, are there optimal ways to balance these competing interests?"; "Are the tools and techniques that support privacy-protective uses of datasets best understood in terms of appropriate safeguards that minimize risk under specific circumstance or should we insist on provable privacy guarantees that eliminate risk entirely?".

The contributions selected for the Summit tackled these questions, organized in four panels, which also delineate the structure of this paper, starting with analyzing practical (II) de-identification frameworks, followed by a closer look to (III) risk-based approaches, a discussion on (IV) new perspectives and (V) law and policy developments, with a focus on the GDPR. The conclusions (VI) will show that there is a tendency to stop looking at anonymisation/identifiability in binary language, with the risk-based approach gaining the spotlight and the idea of a spectrum of identifiability[13] already generating practical solutions.

II. De-identification frameworks

1. A ten-steps framework to anonymisation understood as a "risk management process"

Mackey, Elliot and O'Hara introduced their "Anonymisation Decision-making Framework" (ADF), which "attempts to unify the technical, legal, social and ethical aspects of anonymisation to provide a comprehensive guide to doing anonymisation in practice".

Their framework is built around five underpinning principles. The first one informs that one "cannot decide whether data are safe to share or not by examining the data alone". This means that practitioners will need to assess whether a set of data is anonymised in relation with the environment of that data. The second principle asserts that, notwithstanding the first one, the data still needs to be examined, together with the context. According to the third principle, "anonymisation is a process to produce safe data but it only makes sense if what you are producing is safe useful data". According to the fourth principle, "zero risk is not a realistic possibility if you are to produce useful data", therefore anonymisation "is best understood as a risk management process". The last principle shows that the measure one puts in place to manage re-identification risk "should be proportional to the risk and its likely impact".

4 See, for instance, *Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, V. D. Blondel*, Unique in the Crowd: the Privacy Bounds of Human Mobility, Nature Scientific Reports, Volume 3, 2013; *Paul Ohm*, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701, 1717–23, 2010; *Alessandro Acquisty, Ralph Gross*, Predicting Social Security Numbers from Public Data, Proceedings of the National Academy of Science, July 7, 2009; *Pierangela Samarati, Latanya Sweeney*, Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression, Technical Report SRI-CSL-98-04, 1998 and its second version *Latanya Sweeney*, K-Anonymity: A Model For Protecting Privacy, 10 (5) International Journal of Uncertainty, Fuzziness & Knowledge-based Systems 557, 2002.

5 ICO, "Big data, artificial intelligence, machine learning and data protection" Report, 1 March 2017, Paragraph 134.

6 Idem, Paragraph 139.

7 Conseil d'État, 10ème–9ème ch. réunies, Decision of 08.02.2017, "JCDecaux France".

8 Conseil d'État, "JCDecaux France", paragraph 3.

9 Conseil d'État, "JCDecaux France", paragraph 8 (unofficial translation).

10 Conseil d'État, "JCDecaux France", paragraph 8.

11 8. November 2016 in Brussels.

12 Available here https://fpf.org/wp-content/uploads/2016/11/Rubinstein_framing-paper.pdf (last time visited on 9 March 2017).

13 For an analysis of the spectrum of identifiability, see *J. Polonetsky, O. Tene and K. Finch*, Shades of Gray: Seeing the full spectrum of practical data de-identification, in Santa Clara Law Review, Vol. 56, 2016.

The ADF enshrines ten components, clustered in three core anonymisation activities: (1) a data situation audit – understanding the processing operation, its context, the legal obligations and the ethical dimension, (2) risk analysis and control – assessing disclosure risks and identifying the disclosure control processes that are relevant to your data situation and (3) impact management – identifying who the stakeholders are, planning further steps after anonymised data was shared and having a back-up plan if anything goes wrong after sharing data.

2. Choosing the appropriate de-identification technique based on the data-sharing scenario used

Levin and Salido propose in their paper "The Two Dimensions of Data Privacy Measures" a framework that would help data controllers choose the most effective de-identification technique for their datasets without factoring in the nature or content of data. The authors claim the grid they propose leads to identifying the appropriate de-identification technique across different industries.

Their model comprises eleven de-identification techniques applied to nine sharing scenarios. The authors classify the effectiveness of each technique for each scenario as "conservative", "optimal", "risky", "inappropriate", "for future study" or "not applicable". For instance, masking of identifiers is considered risky if access to data is provided under a Service Level Agreement or contract. But, if it were applied in the case where access to data is provided within a legal entity, masking of data would be an optimal de-identification technique.

The authors encourage regulators to use their model and "define a sufficiently protected area within the two axes such that the level of data protection inside this area would be considered sufficient in the eyes of data subjects and regulators and applicable to a wide range of industries and use cases". The terminology, classification and understanding of the characteristics of known techniques for de-identification of tabular data used for the paper were sourced from ISO/IEC JTC1 CD 20889 "Privacy enhancing data de-identification techniques" (which is currently under debate).

3. Borrowing best de-identification practices from researchers and their datasets

In their paper "Practical Approaches to Big Data Privacy Over Time", Altman, Wood, O'Brien and Gasser look at de-identification techniques and other privacy protections deployed by researchers to their datasets, aiming to inform commercial and government actors on best practices that have been tested by the research community. The authors argue that "many uses of big data, across academic, government, and industry settings, have characteristics similar to those of traditional long-term research studies". Starting from this hypothesis, they look in depth to how researchers have been deploying different combinations of privacy controls to their datasets.

Even if they found that the characteristics of using big data for research purposes and for commercial or governmental purposes are similar, the authors show that "the review processes and safeguards employed for long-term data collection and linkage activities in commercial and government settings differ from those used in the research context in a number of key respects". For instance, "commercial and government actors often rely heavily on certain approaches, such as notice and consent or de-identification, rather than drawing from the wider range of privacy interventions that are available and applying combinations of tailored privacy controls at each stage of the information lifecycle, from collection, to retention, analysis, release, and post-release".

The impact of time on privacy should play a more prominent role when deciding which are the most effective de-identification techniques. As highlighted in the paper, "key risk drivers for big data that are related to the time dimension include the age of the data, the period of collection, and the frequency of collection".

In their concluding remarks, the authors recommend "using a combination of controls to manage the overall risk resulting from identifiability, threats and vulnerabilities", pointing out that "several clusters of controls for addressing identifiability and sensitivity can be implemented, such as notice, consent, and terms of service mechanisms in combination with robust technical disclosure limitation techniques, formal application and review in combination with data use agreements and disclosure limitation techniques, and secure data enclaves with auditing procedures".

III. Risk-Based Approaches

1. Introducing "Flexible pseudonymous data" in the spectrum of identifiability

In their paper "The Seven States of Data: When is Pseudonymous Data not Personal Information?", El Emam, Gratton, Polonetsky and Arbuckle define the spectrum of identifiability and specific criteria for the placement of different types of data along this spectrum. They use a risk-based approach for evaluating identifiability which is consistent with practices in the disclosure control community. Using precise criteria for evaluating the different levels of identifiability, the authors proposed a new point on this spectrum that would allow broader uses of pseudonymous data under certain conditions.

The initial six states of data identified reflect the type of data sharing that is happening today, based on the authors' observations: public release of anonymized data, quasi-public release of anonymized data and non-public release of anonymized data qualify as "not-PII" (not-personally identifiable information), while protected pseudonymized data, "vanilla" pseudonymized data and raw personal data qualify as "PII". The first three states of data refer mainly to types of open data, as well as data that requires qualified access. *Protected pseudonymous data* refers to data where "only masking of direct identifiers has been applied and no de-identification methods are used", but which have "additional contractual, security, and privacy controls in place". "*Vanilla" pseudonymous data* is "pseudonymous data without any of the additional contractual, security or privacy controls in place", while *raw personal data* refers to "data that has not been modified in any way or that has been modified so little that the probability of re-identification is still very high".

The authors define in their paper three specific criteria that would further reduce the risk of re-identification for protected pseudonymous data: "(1) No processing by humans; (2) No PII leakage from analytics results; and (3) No sensitive data." Data that comply with these criteria would be "*flexible pseudonymized data*", an intermediary category between not-PII and PII, which would not require consent for processing.

In conclusion, by adding more conditions and safeguards to the existing state of protected pseudonymous data, the authors propose that "more flexibility can be granted for the use and disclosure of the data while still being consistent with contemporary risk management frameworks".

2. Testing the robustness of anonymization techniques with a machine learning process

In their paper "Testing the Robustness of Anonymisation Techniques: Acceptable versus Unacceptable Inferences", Acs, Castelluccia and Le Metayer dismantle the guidance issued by European Data Protection Authorities on anonymisation techniques,[14] by deeming the criteria laid out there as neither necessary, nor effective to decide upon the robustness of an anonymisation algorithm. The criteria put forward by the Article 29 Working Party in their 2014 Opinion referred to the following risks a data controller should consider: singling out, linkability and inference.

The authors consider that the criteria are not necessary "because they do not take into account the type of information that can be derived. In some cases, this information may actually be insignificant, noisy or even useless". As for their effectiveness, they consider that "it depends very much on the precise meaning of inference". According to their assessment, "the only way to make this criterion meaningful would be to qualify it and consider inferences of attributes about specific individuals with sufficient accuracy", which would lead to a threshold issue – "where should the red line be put to decide upon 'specific' and 'sufficient'".

The ability to perform inferences is "the key issue with respect to both privacy and utility". The authors believe that "there are acceptable and unacceptable disclosures: 'learning statistics about a large population of individuals is acceptable, but learning how an individual differs from the population is a privacy breach'". However, they acknowledge that certain group inferences "can still be harmful, which means that the release of the resulting anonymized dataset should still be reviewed and controlled by a privacy ethics committee".

The main challenge identified is "to provide criteria to distinguish between acceptable and unacceptable inferences". The solution found by the authors is to use a machine learning process, called "differential testing", to predict "the sensitive attribute of users (attributes that are usually not quasi-identifiers but rather represent some information not to be revealed about the user such as medical diagnosis, salary, locations, etc.)".

3. Anonymisation – key to publishing Clinical Study Reports by the European Medicines Agency

Spina, Dias and Petavy presented their ongoing work for the paper "Notes on the anonymisation of Clinical Study Reports for the purpose of ensuring regulatory transparency". The European Medicines Agency (EMA) adopted a Policy on the publication of clinical data for medicinal products for human use in 2014.[15] EMA started to publish clinical data submitted by pharmaceutical companies to support their regulatory applications for human medicines under the EU centralised procedure, on the basis of the Policy, in October 2016.[16]

The Policy generally refers to "ways and means to anonymise data and protect patients from retroactive identification". In order to implement this, EMA developed a guidance document addressed to pharmaceutical companies on the anonymisation of clinical reports. The paper aims to discuss the scientific methodology and the technical and legal challenges for the anonymisation of clinical study reports.

IV. New Perspectives

1. Pleading for a Systems-Science perspective to better inform the de-identification public policy

In his paper "Why a Systems-Science perspective is needed to better inform data protection de-identification public policy, regulation and law", Barth-Jones argues that "data privacy policy for de-identification must take a systems perspective in order to better understand how combined multi-dimensional (i.e., involving both technical de-identification and administrative/regulatory responses) interventions can effectively combine to create practical controls for countering widespread re-identification threats".

The author makes the case that "rumors of de-identification's death have been greatly exaggerated". He identifies the main reasons for this formalist approach – "the vast majority of re-identification demonstrations have been conducted against data without any proper statistical disclosure limitation methods applied, or have blatantly ignored the impact of disclosure controls where they have been applied"; and the fact that "it assumes as a default that the actors and forces of re-identification are omnipresent, omniscient, omnipotent and relentless". Barth-Jones seconds the conclusion of Rubinstein and Harzog, who argued that the first law of privacy policy is that "there are no silver-bullet solutions" and that the best way to move policy past the purported failures of anonymisation is to instead focus on the process of minimizing the risk of re-identification.[17]

Therefore, Barth-Jones pleads for de-identification to be given a fair chance, using "improved re-identification research steps, combined with the use of systems modeling and quantitative policy analyses including uncertainty analyses". These methods can provide "the necessary scientific tools to critically evaluate the potential impacts of pseudo/anonymisation in various regulatory schemas and should be pursued routinely when conducting data privacy policy evaluations".

2. Bringing the human dimension to anonymisation

Galdon Clavell and in't Veld build a framework to assess the societal impact of data intensive technologies, which they deem to be "sensitive both to the technological and economic concerns of engineers and decision-makers and to societal values and legislation". The purpose of their paper, "Tailoring Responsible Data Management Solutions to Specific Data-Intensive Technologies: A Societal Impact Assessment Framework", is to provide policymakers and engineers with the tools to think about ethics and technology and lead them "towards value-sensitive and privacy-enhancing solutions like anonymisation".

The authors recall that "data relates to human beings with rights and values". Therefore, "aspects of legality, ethics, desirability, acceptability and data management policy have to be critically considered in order to make sure that rights and values are respected". The proposed framework is called "Eticas" and it has four pillars: Law and Ethics, Desirability, Acceptability and Data Management.

The Law and Ethics dimension "relates to the legal and moral standards guiding a project and results in the preconditions for a project in a specific field". It focuses on the relevant legislation

14 Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, adopted 10. April 2014.

15 "European Medicines Agency policy on publication of clinical data for medicinal products for human use", EMA/240810/2013, 2 October 2014.

16 According to information available on the website of the institution. See http://www.ema.europa.eu/ema/?curl=pages/special_topics/general/general_content_000555.jsp (last time visited on 9 March 2017).

17 *Ira Rubinstein* and *Woodrow Hartzog*, Anonymization and Risk, Washington Law Review, June 2016 91 (2):703–760.

and the social values that are involved in a specific context. The Desirability dimension "refers to the justification of the need for a technology or its specific functionalities" and it involves a clear "problem definition". The purpose is to avoid "technological solutionism". The Acceptability dimension "involves the inclusion of public opinion and values in a technological innovation or research project". The outcome of stakeholder consultations could be implemented in the design process. Finally, the Data Management dimension refers to the legal framework of privacy and data protection, ethical principles, but also to broader considerations relating to individual control and consent, methods of anonymisation, and how privacy issues can be designed into technologies and projects.

The authors conclude that the Eticas framework is malleable, because "it can be adapted to different systems and contexts, as well as to the resources of the organizations performing the assessment". However, they acknowledge that its success "depends on a genuine commitment from all stakeholders", particularly from technology designers, "which should adopt a mind-shift from technology inventors to solution providers", while considering the values, needs and expectations of the communities beyond their user base.

3. De-identification as policy tool for Data Protection Authorities and Competition Authorities

Jentzsch explores the complicated environment at the interaction of competition law and data protection law in the era of Big Data, looking specifically at how "privacy guarantees" can enable "a more effective monitoring of industry players", both from the perspective of Data Protection Authorities (DPAs) and of Competition Authorities (CAs).

In his paper, "Competition and data protection policies in the era of Big Data: Privacy Guarantees as Policy Tools", Jentzsch starts from the assumption that "information asymmetries are a key ingredient for competition", because they protect trade secrets and they induce uncertainty about the competitors' innovations and future movements. The author observes that the increasing complexity of analytical methods used by companies creates transparency challenges, in the sense that firms are now able to monitor consumers and rivals in an unprecedented manner. This is why he argues that "we need to discuss how some of the recently developed privacy guarantees can be utilized as tools for upholding information asymmetries needed to ensure competition".

Jentzsch looks at how anonymisation of databases can play a part in evaluating mergers and preventing the abuse of a dominant position by CAs. "Authorities in charge for enforcing legislation relating to unfair commercial practices can use the 'degree of differentiation' spectrum to prosecute any misleading promises of firms regarding anonymisation of data. (...) For example, in merger cases, authorities need to define the relevant market (product-wise, geographic and temporal), before assessing dominance and its anticompetitive effects. If a merger creates or strengthens a dominant position stifling competition, it might be prohibited. Databases play a critical role in the merger of data-intensive firms or in evaluating the abuse of a dominant position". The author develops specific recommendations for both DPAs and CAs to use different privacy guarantees as policy tools. For instance, he proposes that CAs "should condition a merger of data-rich firms on provable privacy guarantees", such as "randomization and/or generalization or preventing linkability of the data".

One of the conclusions of the study is that using privacy guarantees for supervision provides an incentive for companies "to use de-personalized information to a greater extent in order to avoid scrutiny by supervisors". Moreover, "such deployment could spur investments in the development of more *efficient privacy guarantees and mechanisms*".

V. Law and policy

1. Looking at the incentives under the GDPR to anonymise and pseudonymise personal data

Kotschy analyses in his paper – "The new General Data Protection Regulation: Is there sufficient pay-off for taking the trouble to anonymize or pseudonymise data?", whether there are sufficient incentives for data controllers to anonymize and pseudonymise data in the framework of the new General Data Protection Regulation. He assesses all provisions and recitals of the GDPR relevant to the two processes and concludes that while using anonymised data results in clear, significant, consequences – "the GDPR is not applicable", the rewards for using pseudonymised data are not that clear. There are "no precise legal consequences", the author observes, pointing out that "the 'pay-off' for pseudonymisation in data protection has not (yet) been fully exploited".

The paper provides insight into how the Austrian data protection law differentiates between personal data and "indirectly personal data" – a concept introduced in 2000. These are still personal data, but they identify the data subject only indirectly, "in the sense that additional information would be needed to reveal the full identity of the data subject". According to the author, "all identifiers which together directly identify this person (such as the name, date of birth, residence etc.) are encrypted and the user of such data has no access to the encryption algorithm".

Kotschy explains that, under the Austrian law, using "indirectly personal data" triggers "several privileges for the controllers involved", such as having "no obligation to notify the processing of indirectly personal data to the DPA, no restriction for disclosing such data to third parties, no obligation to obtain permission from the DPA for transfers to third countries, no obligation to inform the data subjects about transfers to third parties". In addition, "access rights of data subjects are suspended". This is not the case under the GDPR, as Kotschy points out.

2. Proposing a fluid line between personal data and anonymised data, with a dynamic approach to anonymisation

Framing the debate under the GDPR, Stalla-Bourdillon and Knight argue in their paper "Anonymous data v. Personal data – A false debate: An EU perspective on anonymisation, pseudonymisation and personal data", that the state of anonymised data should be comprehended dynamically: "anonymised data can become personal data again, depending upon the purpose of the further processing and future data linkages, implying that recipients of anonymised data have to behave responsibly". They claim that the "attempts" of EU data protection regulators to clarify the terms of the dichotomy personal data/anonymised data "have partly failed".

The authors analyze the guidance issued by the ICO and the Article 29 Working Party on anonymisation techniques, as well as the legal requirements within Directive 95/46 and the GDPR with regard to anonymisation and the definition of personal data. They argue that, even if the Article 29 WP is "sympathetic to a risk-based approach", its position is problematic because it "suggests that an acceptable re-identification risk requires near-zero probability, an idealistic and impractical standard that cannot be guaranteed in a big data era". Looking at the provisions of the GDPR, the authors point out that, at least in its Preamble, the regulation adopts a risk-based approach to anonymisation, relying on the

test of "means reasonably likely to be used" by the data controller and third parties to identify a data subject. They consider it is necessary to "revisit the very concept of personal data as defined under EU law" in order to fully understand the implications of a dynamic approach to anonymisation.

Their argument is that identifiability is not the only key component of the concept of personal data, another component equally important being the context in which the personal data are processed, or the "relate to" component of the definition. To support their claim, the authors refer to the *Breyer*[18] case, where the Advocate General Campos Sanchez-Bordona considered that, indeed, "context is crucial for identifying personal data, and in particular characterizing IP addresses as personal data".[19] The Court followed the same approach, as it excludes identifiability "if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant".[20]

The authors conclude that "a dynamic approach to anonymisation therefore means assessing the data environment in context and over time and implies duties and obligations for both data controllers releasing datasets and dataset recipients". They also acknowledge that more research is necessary in the field to fully comprehend the variety of categories of processing and the interplay between the different components of data environments.

3. Making the case for de-identification as key for GDPR compliance

In his paper "Viewing the GDPR Through a De-Identification Lens: A Tool for Clarification and Compliance", Hintze makes a compelling analysis of the implications of de-identifying data for compliance with the GDPR, arguing that de-identification brings significant incentives for data controllers to comply with key requirements under the EU data protection law framework: lawful grounds for processing (in particular consent and legitimate interests), notice, data retention, data security, as well as data subject rights of access, deletion and other controls.

He identifies four levels of identifiability, looking at the provisions of the GDPR: identified data, identifiable data, Article 11 De-identified data and anonymous/aggregate data.

Identified data "identifies or is directly linked to data that identifies a specific natural person (such as a name, e-mail address, or government-issued ID number)". Identifiable data "relates to a specific person whose identity is not apparent from the data; the data is not directly linked with data that identifies the person; but there is a known, systematic way to reliably create or re-create a link with identifying data. Pseudonymous data as defined in the GDPR is a subset of Identifiable data". Article 11 De-identified data "may relate to a specific person whose identity is not apparent from the data; and the data is not directly linked with data that identifies the person", while anonymous/aggregate data "is (1) stored without any identifiers or other data that could identify the individual or device to whom the data relates; and (2) aggregated with data about enough individuals such that it does not contain individual-level entries or events linkable to a specific person".

The author argues that, for instance, "Article 6(4) of the GDPR supports the idea that de-identification can be used to help justify a basis for lawful processing other than consent". As for the notice obligation – he suggests that "the more strongly de-identified the data is, the more likely discoverable notice will be appropriate", which means that an individualized Notice for each kind of processing operation will not be required by the supervisory authorities.

Hintze also draws attention to the fact that "Article 12(2) of the GDPR specifies that if the controller can demonstrate that it is not in a position to identify the data subject (i. e., Article 11 De-Identified data), it need not comply with Articles 15 to 22. Those articles include the right of access (Article 15), rectification (Article 16), erasure (Article 17), data portability (Article 20), and the right to object to the processing of personal data or obtain a restriction of such processing under certain circumstances (Articles 18 and 21)".

A substantial conclusion of the article is that "the GDPR requirements in each area should be interpreted and enforced in a way that will encourage the highest practical level of de-identification and that doing so will advance the purposes of the regulation".

VI. Conclusion

The difficult questions surrounding anonymisation and identifiability are not going anywhere soon. As showed in the introductory part of this paper, the questions started to appear in Courts and regulators are paying more and more attention to them. With the entering into force of the GDPR and its vast (extra)territorial application, finding good and practical answers is more important than ever.

The "De-identification frameworks" proposed by the papers debated at the Brussels Privacy Symposium do just that. They describe possible practical solutions, organized in frameworks that understand anonymisation as a risk management process. One fundamental idea they have in common is that the assessment for identifying the most effective anonymisation technique should give more weight to the environment or context where that data is processed than to the content of the data itself (Subsections I.1 and I.2). On another hand, researchers suggest looking for inspiration at the tested de-identification methods used in research for decades to handle big data sets. A key ingredient for the effectiveness of these methods is factoring in the impact of time on privacy – the age of the data, the period of collection and the frequency of collection (Subsection I.3).

The "Risk-based approach" to anonymisation was further explored by authors who put efforts into classifying data throughout the de-identification spectrum. A new category of anonymized data that could allow broader uses of pseudonymous data was identified and defined – "flexible pseudonymous data" (Subsection II.1). A machine learning process called "differential testing" was proposed to be able to distinguish between acceptable and unacceptable inferences made from pseudonymised data, after the authors explained that the ability to perform inferences is the key issue with respect to both privacy and utility of data (Subsection II.2). Finally, a case study was presented as example of a risk based approach to anonymisation applied in practice – the disclosure of Clinical Study Reports made by pharmaceutical companies in Europe (Subsection II.3).

"New perspectives" were also proposed, ranging from a systemic approach referring to multi-dimensional interventions (technical and administrative/regulatory responses) that can effectively combine to create practical controls for countering wide-

18 CJEU, Case C-582/14, Breyer v Bundesrepublik Deutschland, 19. 10. 2016, ECLI:EU:C:2016:779.
19 Opinion of the Advocate General Campos Sánchez-Bordona, CJEU C-582/14, Breyer v Bundesrepublik Deutschland, 12. 05. 2016, ECLI:EU:C:2016:339, at [68].
20 CJEU, Case C-582/14, Breyer v Bundesrepublik Deutschland, 19. 10. 2016, ECLI:EU:C:2016:779, at [46].

spread re-identification threats (Subsection III.1), to an Impact Assessment Framework for data intensive technologies that takes into account moral standards, ethical values and the needs of communities (Subsection III.2), to analyzing the significant role anonymisation can play in the ever more complex interaction of data protection law and competition law (Subsection III.3).

Finally, the last contributions looked closely into the provisions of the GDPR and their significance for the anonymisation/identifiability debate. One of the questions looked into was whether there are sufficient incentives under the GDPR for controller to anonymise and pseudonymise the data they process (Subsection IV.1). The concept of a fluid line between personal data and anonymised data was introduced. It was claimed that identifiability is not the only key component of the concept of personal data, context in which the personal data are processed being another important component. The authors brought arguments from the recent case-law of the CJEU to support this idea (Subsection IV.2). Furthermore, a strong argument was made that de-identification techniques are fundamental to compliance with the GDPR. Looking closely to key GDPR provisions, including Articles 11, 12(2) and 6(4) it was argued that de-identification brings significant incentives for data controllers to comply with a series of key requirements, such as notice, data retention and data security (Subsection IV.3).

Concluding, the anonymisation/identifiability debate seems to significantly shift towards a risk-based approach understanding, which includes paying more attention to the spectrum of identifiability and to identifying concrete compliance mechanisms with privacy and data protection law for processing pseydonymised data.

Dr. Johannes Eichenhofer ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Staatslehre und Verfassungsgeschichte der Universität Bielefeld (Prof. Dr. Christoph Gusy) und Habilitand an der dortigen Fakultät für Rechtswissenschaft.

Vom Zweckbindungsgrundsatz zur Interessenabwägung?

*Dr. Johannes Eichenhofer**

Der Zweckbindungsgrundsatz stößt seit jeher, aber besonders angesichts der zunehmenden Digitalisierung unserer Lebenswelt, auf gespaltene Resonanz. Die Einen halten ihn im Zeitalter von Big Data für mindestens kontrafaktisch, wenn nicht gar für eine völlige Fehlkonstruktion. Andere betonen angesichts der mit dem Schlagwort „ubiquitous computing" bezeichneten fast schon allgegenwärtigen Datenverarbeitung die Notwendigkeit klarer Maximen der Datenverwendung. Vor diesem Hintergrund will der vorliegende Beitrag nach einer kurzen Einleitung (I.) zunächst Ursprung, Ziel, Inhalt und Kritik des Zweckbindungsgrundsatzes (II.) skizzieren. Sodann soll überprüft werden, ob und gegebenenfalls inwiefern die Datenschutz-Grundverordnung am Zweckbindungsgrundsatz festhält (III.).

I. Datenschutz im Internet-Zeitalter: „From collection to use"

Das digitale Zeitalter stellt das Datenschutzrecht vor enorme Herausforderungen.[1] Mit der zunehmenden Durchdringung der sozialen Lebenswelt durch internetbasierte Informations- und Kommunikationstechnologie ist auch die damit einhergehende Datenverarbeitung von einer rechtfertigungsbedürftigen Zwangsmaßnahme des Staates zu einem Alltagsphänomen geworden, an dem die Nutzer durch ihr Verhalten selbst mitwirken. Gleichzeitig wird es für sie angesichts der im World Wide Web fließenden globalen Datenströme immer schwerer zu durchschauen „wer was wann und bei welcher Gelegenheit über sie weiß."[2] Vor allem Big Data-Anwendungen[3] bergen die Gefahr, dass die bei einer Internetnutzung anfallenden personenbezogenen Daten von datenverarbeitenden Stellen zusammengeführt, zur Informationsgewinnung genutzt und gegen den Willen der User an Dritte übermittelt werden können, welche die Informationen wiederum zum Handeln gegen die Interessen der Nutzer einsetzen können. Das gel-

* Der Verfasser dankt Dr. *Enrico Peuker* und *Laura Schulte* für ihre kritischen Anmerkungen.

1 Vgl. etwa *Masing*, NJW 2012, 2305; am Beispiel neuer Web-Kollektive *Hoffmann-Riem*, JZ 2012, 1081; grundlegend: *Schaar*, Datenschutz im Internet (2002).

2 BVerfG, Urt. v. 15. 12. 1983 – 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83, BVerfGE 65, 1, 43.

3 Vgl. zu technischen Grundlagen etwa: *Markl*, in: Hoeren, Big Data und Recht, 2014, S. 3 ff.

tende Datenschutzrecht, so eine inzwischen sehr geläufige These,[4] könne dieser neuen Realität nicht mehr gerecht werden. Verwiesen wird nicht nur auf den auf das jeweilige Hoheitsgebiet beschränkten territorialen Anwendungsbereich des nationalen Datenschutzrechts, der mit der Datenschutz-Grundverordnung immerhin auf das Hoheitsgebiet der EU ausgeweitet wird. Vielmehr geraten auch immer mehr Grundsätze des Datenschutzrechts aufgrund ihrer mangelnden „Internettauglichkeit“[5] unter Beschuss. Daher gelten beispielsweise der Grundsatz der Direkterhebung (§ 4 Abs. 2 BDSG) oder das Prinzip der Datensparsamkeit (§ 3a BDSG) angesichts von „ubiquitous computing“ und „Big Data“ geradezu als Anachronismus. Da eine Internetnutzung ohne Datentransfer zwischen Server und Client nicht möglich ist, solle sich das Datenschutzrecht nicht mehr zum Ziel setzen, Vorgänge der Daten*erhebung* zu minimieren, sondern vielmehr, die Daten*verwendung* effektiven Regeln zu unterwerfen. Das Datenschutzrecht stehe daher vor einem Paradigmenwechsel, der sich trefflich auf die Formel „From collection to use“[6] bringen lässt. In ihrem 2010 erschienen Buch „Privacy in Context“ beschreibt die US-amerikanische Technikphilosophin *Helen Nissenbaum* diesen Paradigmenwechsel wie folgt: „What people care most about is not simply *restricting* the flow of information but ensuring that it *flows appropriately*...“.[7] Vor diesem Hintergrund versucht *Nissenbaum*, die „Angemessenheit“ der Datenflüsse danach zu bestimmen, ob die Integrität sozialer Kontexte gewahrt bleibt.

II. Der Zweckbindungsgrundsatz – Ursprung, Inhalt und Kritik

Im deutschen und europäischen, aber auch im internationalen Recht[8] wird die Zulässigkeit der Datenverarbeitung weniger durch Kontexte[9] als durch Zwecke bestimmt.[10] Dies geschieht durch den sog. Zweckbindungsgrundsatz. Dieser besagt sehr verkürzt: „Personenbezogene Daten dürfen *nur für den Zweck verwendet werden, für den sie rechtmäßig erhoben wurden.* (...) Das Motiv des Zweckbindungsgrundsatzes besteht“ also „in einer Eingrenzung der *Verwendung* personenbezogener Daten.“[11] Diese auf den ersten Blick simple Regel erweist sich bei näherer Betrachtung als in erheblichem Maße erklärungsbedürftig. Zwar soll die (wissenschafts-)theoretische Frage, was ein „Zweck“ überhaupt ist,[12] hier nicht weiter vertieft werden.[13] Allerdings fragt sich etwa, wer befugt ist, die Zwecke zu setzen, wie stark die Bindung der datenverarbeitenden Stelle an die Zwecke ausgestaltet ist und wer über die Einhaltung der Zweckbindung wacht. Um diese Fragen zu beantworten, sollen nun Ursprung (1.), Ziel und wesentlicher Inhalt (2.), sowie die wichtigste Kritik (3.) am Zweckbindungsgrundsatz näher dargestellt werden.

1. Ursprung des Zweckbindungsgrundsatzes

Auch wenn erste Begründungsansätze bereits in einer aus den frühen 1960er Jahren datierenden Erklärung der New Yorker Anwaltskammer enthalten waren,[14] wird der Ursprung des Zweckbindungsgrundsatzes hierzulande überwiegend im Volkszählungsurteil des BVerfG von 1983 verortet.[15] Hierin hatte das BVerfG u. a. entschieden, dass eine Rechts- und Gesellschaftsordnung, „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“,[16] mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar ist. Ein gesetzlich verordneter „Zwang zur Angabe personenbezogener Daten“ – wie er etwa in Gestalt der Volkszählung zum Ausdruck kam – setze daher aus verfassungsrechtlicher Sicht voraus, „dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind.“[17] Hierin kommt eine wichtige Wertung des BVerfG zum Ausdruck: Dass nämlich das Recht auf informationelle Selbstbestimmung vor allem dann gefährdet sei, wenn ein bestimmtes Datum vom ursprünglichen Erhebungs- in einen anderen Verarbeitungskontext eingeführt bzw. personenbezogene Daten zu anderen als den im Errechnungszeitpunkt festgelegten Zwecken verarbeitet werden.[18]

An dieser Stelle tritt jedoch die erste Unschärfe des Zweckbindungsgrundsatzes zu Tage, nämlich die Frage nach ihrem Adressaten. So bezieht sich diese Urteilspassage erkennbar auf den (Datenschutz-)Gesetzgeber und nicht auf die datenverarbeitenden Stellen – seien sie öffentlicher oder privater Natur. In dieser Lesart folgt die Notwendigkeit der Zweckbindung bereits aus dem Rechtsstaatsprinzip, konkret: dem Vorbehalt des Gesetzes. Hieraus ergibt sich nämlich, „dass eine Eingriffsnorm die Zwecke der Erhebung, Verarbeitung und Nutzung festlegen muss.“[19] Ferner lässt sich die Notwendigkeit der Zweckbindung für öffentlich-rechtliche Stellen aus dem – ebenfalls aus dem Rechtsstaatsprinzip folgenden – Grundsatz der informationellen Gewaltenteilung her-

4 So etwa bereits *Hassemer*, Grundrechte in der neuen Kommunikationswelt, in: Bartsch/Lutterbeck, Neues Recht für Neue Medien, 1998, S. 1 ff., 15 ff.; *Wolff*, Beschränkte Internettauglichkeit des BDSG, in: Hill/Schliesky, Die Vermessung des virtuellen Raums, 2012, S. 193 ff.

5 *Wolff*, Beschränkte Internettauglichkeit des BDSG, in: Hill/Schliesky, Die Vermessung des virtuellen Raums, 2012, S. 193 ff.

6 *van Hoboken*, From collection to use in privacy regulation? A forward looking comparison of European and US Frameworks for Personal Data Processing, in: Van Der Sloot, Broeders and Schrijvers, Exploring the Boundaries of Big Data, Netherlands Scientific Council for Government Policy, 2016, p. 231 ff.

7 *Nissenbaum*, Privacy in Context, 2010, S. 2.

8 Vgl. etwa *Lee Bygrave*, Data Privacy Law: An International Perspective (2014); vgl. auch den Kurzüberblick bei *Solove/Schwartz*, Information Privacy Law (2015), Chapter 13, p. 1095 ff.

9 Gleichwohl gibt es auch kontextspezifische Regelungen, beispielsweise Beschäftigten-, Gesundheits- oder Sozialdatenschutz. Auch die DSGVO nimmt an verschiedenen Stellen auf Kontexte Bezug.

10 Siehe aber *Hoffmann*, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes. Das Zweckproblem aus theoretischer und praktischer Sicht, 1991, S. 21, der betont, dass der Zweckbindungsgrundsatz letztlich der Sicherung der Einheit von Erhebungs- und Verwendungskontext diene.

11 *Wolff*, in: Wolff/Brink, BeckOK Datenschutzrecht, 17. Edition (01. 08. 2015), B Rn. 11.

12 Nach *Luhmann*, Zweckbegriff, 1973, S. 166, zeige sich einerseits „immer wieder die Unentbehrlichkeit des Zweckbegriffs“, andererseits aber auch „die Fragwürdigkeit seines theoretischen Status.“

13 Vgl. hierzu jedoch *Hoffmann*, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes. Das Zweckproblem aus theoretischer und praktischer Sicht, 1991, S. 28 ff.; *Wischmeyer*, Zwecke im Recht des Verfassungsstaates. Geschichte und Theorie einer juristischen Denkfigur, 2015.

14 Vgl. dazu *Pohle*, Datenschutz-Nachrichten (DANA) 2015, 141 ff.

15 Wichtige theoretische Vorarbeiten finden sich indes bei *Steinmüller* u. a., Grundfragen des Datenschutzes, S. 5 ff.

16 BVerfG, Urt. v. 15. 12. 1983 – 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83, BVerfGE 65, 1, 43.

17 BVerfG, Urt. v. 15. 12. 1983 – 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83, BVerfGE 65, 1, 46.

18 Vgl. *Hoffmann*, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes. Das Zweckproblem aus theoretischer und praktischer Sicht, 1991, S. 21. Hierin besteht auch die Hauptthese von *Nissenbaum*, Privacy in Context, 2010, S. 2.

19 Vgl. *Härting*, NJW 2015, 2584, 2584.

leiten.[20] Danach hat sich die funktionelle Aufgliederung der Verwaltung nach Aufgaben und Kompetenzen auch dahingehend niederzuschlagen, dass jeder Verwaltungseinheit zunächst einmal nur die für die Wahrnehmung ihrer Aufgaben bzw. Ausübung ihrer Kompetenzen erforderlichen Informationen zustehen sollen. Zweckbindung dient insofern einer durch den Gesetzgeber vorgegebenen Fremdbindung der Verwaltung in Gestalt konkreter Aufgabenzuweisung.[21] Auf die Datenverarbeitung durch private Stellen lässt sich diese Argumentation jedoch nicht übertragen. Daher bedarf es einer vertieften Auseinandersetzung mit dem Ziel und Inhalt des Zweckbindungsgrundsatzes.

2. Ziel und Inhalt des Zweckbindungsgrundsatzes

Zweck*bindung* als spezielle Form der Rechtsbindung[22] setzt zunächst einmal Zweck*festlegung* voraus. Zweckfestlegung bedeutet in den Worten *Hans-Heinrich Trutes*, „dass Daten als Informationsgrundlagen für bestimmte Aufgaben, die mit bestimmten Befugnissen erfüllt werden sollen, erhoben und verarbeitet werden können. Durch diese Regelungen entstehen bestimmte Verarbeitungszusammenhänge und damit – auf einer ersten und abstrakten Ebene – die erforderliche Transparenz und Begrenzung der Datenerhebung und Begrenzung der Datenerhebung und -verarbeitung."[23] Dagegen bedeutet Zweck*bindung* die Einhaltung der zuvor festgelegten Zwecke. Während der Betroffene ein Interesse daran hat, dass die Zwecke möglichst eng definiert bzw. festgelegt werden, ist für die datenverarbeitende Stelle eine möglichst weite bzw. Formulierung des Verarbeitungszwecks insofern vorteilhaft, als sie dann umso mehr Spielräume hat, die Daten der Betroffenen nach eigenem Belieben zu verarbeiten. Allerdings wohnt diesem Spielraum auch ein gewisses Maß an Rechtsunsicherheit inne, die sich auch für die datenverarbeitenden Stellen nachteilig auswirken kann, da diese unter Umständen Gefahr laufen, die Daten zweck- und rechtswidrig zu verarbeiten. Hierdurch erschließt sich zugleich der Sinn der Zweckfestlegung und -bindung: Ziel dieser Prinzipien ist es nämlich, das individuelle Recht auf informationelle Selbstbestimmung mit dem gesamtgesellschaftlichen Ziel des Datenschutzes zu verbinden, die Macht staatlicher oder privater Institutionen zu begrenzen.[24] Ist die datenverarbeitende eine öffentliche Stelle, gebietet der Verhältnismäßigkeitsgrundsatz, dass die Zweckfestlegung umso enger erfolgt, je grundrechtssensibler die Datenverarbeitung ist. Ist die datenverarbeitende Stelle hingegen eine nicht-öffentliche, bedeutet eine enge Zweckfestlegung zugleich eine Verkürzung ihrer Grundrechte. Hier ist der Gesetzgeber also nicht berufen, staatliches Handeln durch möglichst präzise Eingriffsgrundlagen zu beschränken, sondern die Freiheitssphären der Betroffenen und der datenverarbeitenden Stelle zu einem Ausgleich zu bringen.[25]

Allerdings kann der Gesetzgeber die Befugnis zur Zweckfestlegung auch an die datenverarbeitende Stelle delegieren, wie die Regelung des § 28 Abs. 1 S. 2 BDSG zeigt. Danach „sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen." In dieser Konstellation ist es folglich nicht der Gesetzgeber, sondern die datenverarbeitende Stelle, welche die Zwecke festlegt. Dies ist aus Sicht des Betroffenen jedenfalls dann problematisch, wenn ihm die datenverarbeitende Stelle die Zwecke der Datenverarbeitung nicht mitteilt. Das BDSG versucht dieses Ergebnis durch spezielle Benachrichtigungspflichten der datenverarbeitenden Stelle (§ 33 BDSG) und Auskunftsrechte (§ 34 BDSG) des Betroffenen zu kompensieren.

Doch der Gesetzgeber kann nicht nur die Zwecke eng oder weit definieren, sondern auch die Zweck*bindung* eng bzw. „starr" oder weit bzw. „flexibel" ausgestalten. Während eine starre Zweckbindung es der datenverarbeitenden Stelle unter keinen Umständen erlaubt, Daten zu anderen als dem vorab festgelegten Zweck zu verarbeiten, gewährt ein flexibler Zweckbindungsgrundsatz der datenverarbeitenden Stelle einen gewissen Entscheidungsspielraum. Hiernach wäre die Datenverarbeitung auch zu Zwecken zulässig, die mit dem ursprünglich festgelegten Verarbeitungszweck jedenfalls „vereinbar" sind (sog. „Zweckvereinbarkeitsgrundsatz").[26] Ob dies der Fall ist, hat zunächst die datenverarbeitende Stelle festzustellen. Der Betroffene hat lediglich die Möglichkeit, sich nach der Datenverarbeitung gerichtlich gegen diese Einschätzung zur Wehr zu setzen – was unter anderem voraussetzt, dass er von der datenverarbeiteten Stelle über den Datenverarbeitungsvorgang informiert wurde. Je nach dem, wie eng oder „starr" der Zweckbindungsgrundsatz interpretiert wird, wäre eine Zweckänderung – d. h. eine Verarbeitung der Daten zu einem anderen als dem Erhebungszweck – unzulässig, sodass die Ermächtigung zu einer neuen Datenerhebung erforderlich wäre.[27]

3. Kritik des Zweckbindungsgrundsatzes

Unter anderem an diesem – für die Praxis äußerst unbefriedigenden – Ergebnis entzündet sich die Kritik des Zweckbindungsgrundsatzes. So werde eine „rigide Zweckbindung ... vom Gesetzgeber regelmäßig nicht durchgehalten, sondern durch Ausnahmen immer weiter durchbrochen."[28] Mit der Zweckbindung werde also ein praxisuntauglicher und letztlich kontrafaktischer[29] Grundsatz postuliert. Dieser Einwand wird oftmals von denjenigen ins Feld geführt, die im Zweckbindungsgrundsatz eine unliebsame Begleiterscheinung datengetriebener Geschäftsmodelle – insbesondere in Gestalt von *Big Data*-Konzepten – sehen,[30] die ja gerade darauf

20 Vgl. BVerfG, Urt. v. 15. 12. 1983 – 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83, BVerfGE 65, 1, 68; zu diesem Grundsatz etwa *Bull*, Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 104; *Hoffmann*, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes. Das Zweckproblem aus theoretischer und praktischer Sicht, 1991, S. 21 f.

21 So zu Recht *Pohle*, Datenschutz-Nachrichten (DANA) 2015, 141, 143.

22 *Albers*, Zur Neukonzeption des grundrechtlichen „Daten"schutzes, in: Kugelmann/Haratsch/Repkewitz, Herausforderungen an das Recht der Informationsgesellschaft, 1996, S. 113, 133.

23 *Trute*, Verfassungsrechtliche Grundlagen, in: Rossnagel, Handbuch Datenschutzrecht, Kap. 2.5 Rn. 36 ff.; umfassend zur Zweckfestlegung *Dammann*, in: Simitis, BDSG, 8. Aufl. 2014, § 14 Rn. 41–44.

24 Vgl. *Hoffmann*, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes. Das Zweckproblem aus theoretischer und praktischer Sicht, 1991, S. 23; *Pohle*, Datenschutz-Nachrichten (DANA) 2015, 141, 143.

25 Vgl. *Masing*, NJW 2012, 2305, 2307 ff.

26 Dazu *Eifert*, in: W. Gropp/M. Lipp/H. Steiger, Rechtswissenschaft im Wandel. FS des Fachbereichs für Rechtswissenschaft zum 400-jährigen Gründungsjubiläum der JLU Gießen, 2007, S. 139 ff. Bereits die Europäische Datenschutzkonvention v. 28. 01. 1981 stellte auf die Vereinbarkeit (Kompatibilität) der Datenverwendung mit dem Zweck der ursprünglichen Erhebung oder Speicherung ab.

27 Zu den Rechtsfolgen eines Verstoßes gegen den Zweckbindungsgrundsatz etwa: *Dammann*, in: Simitis, BDSG, 8. Aufl. 2014, § 14 Rn. 338 ff.

28 *Trute*, Verfassungsrechtliche Grundlagen, in: Rossnagel, Handbuch Datenschutzrecht, Kap. 2.5 Rn. 40.

29 Siehe etwa *Bull*, Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 106: „Es ist ... sehr viel leichter, eine strenge Zweckbindung zu propagieren als sie durchzuhalten. Oft ist es schon unklar, ob für eine Datennutzung überhaupt ein Zweck festgelegt worden ist. Oft ist ungewiss, wie der Zweckbegriff auszulegen sei."

30 Vgl. etwa *Richter*, DuD 2015, 739, 740: „Big Data fordert aus datenschutzrechtlicher Sicht dazu heraus, die Zweckbindung effizienter und auf neue Weise durchzusetzen, nicht dazu sie abzuschwächen." Zum Spannungsverhältnis zwischen Zweckbindung und Big Data auch *Helbig*, K&R 2015, 145 ff.; *Werkmeister/Brandt*, CR 2016, 233 ff.; EDPS, Stellungnahme 7/2015, v. 19. 11. 2015; *Marnau*, DuD 2016, 428, 431 ff.; *Dammann*, ZD 2016, 307, 313 f.

beruhen, einmal erhobene Daten zu möglichst vielen Zwecken zu verwenden.[31] Während dieser Vorwurf letztlich auf eine Abwägungsfrage zwischen den Belangen der Betroffenen und der datenverarbeitenden Stellen abzielt und hier vorerst nicht weiter vertieft werden soll, wird dem Zweckbindungsgrundsatz noch ein weitaus tiefer liegender, da an seinen Grundannahmen rüttelnder Einwand entgegengehalten. So sei das Konstrukt der Zweckbindung „schon deshalb zweifelhaft, weil der Informationsgehalt oftmals erst nach der Erhebung deutlich werden und zudem natürlich in der Zeit einer Veränderung unterliegen kann."[32] Der Zweckbindungsansatz sieht sich also einerseits dem Vorwurf ausgesetzt, die datenverarbeitenden Stellen auf den Zeitpunkt der erstmaligen Datenerhebung festzulegen und sich damit technischen, wirtschaftlichen und sozialen Innovationen zu verschließen. Andererseits dient der Zweckbindungsgrundsatz den Betroffenen auch nur dann, wenn diese über die für die Erhebung und Verarbeitung festgelegten Zwecke informiert werden.

Der Zweckbindungsgrundsatz erweist sich also letztlich als ein „Artefakt",[33] das nur in Zusammenspiel mit anderen Prinzipien des Datenschutzes Bedeutung erlangen kann. Dies gilt zunächst für den – in den datenschutzrechtlichen Unterrichtungspflichten und Auskunftsrechten, sowie u. a. im Prinzip der Direkterhebung zum Ausdruck kommenden – *Transparenzgrundsatz*.[34] Einerseits schafft Zweckbindung dadurch Transparenz, dass sie dem Betroffenen vor Augen führt, wie die datenverarbeitende Stelle die sich auf den Betroffenen beziehenden Daten verarbeiten darf. Andererseits bedarf die Überprüfung der Einhaltung des Zweckbindungsgrundsatzes ihrerseits ein gewisses Maß an Transparenz, das etwa durch Unterrichtungspflichten der datenverarbeitenden Stelle hergestellt werden kann (siehe bereits oben, II. 2.). Weiterhin dient die Zweckbindung letztlich insofern der praktischen Umsetzung des *Einwilligungsgrundsatzes*, als der Betroffene regelmäßig in eine Datenverarbeitung nur einwilligen wird, wenn ihm die Zwecke der Datenverarbeitung bekannt sind. Zugleich kann die Einwilligung – neben einer gesetzlichen Regelung – eine Form der Zweckfestlegung sein.

III. Der Zweckbindungsgrundsatz in der DSGVO

Angesichts der soeben skizzierten Kritik fragt sich, ob und wie eng oder starr der Grundsatz der Zweckbindung in der Datenschutz-Grundverordnung ausgestaltet ist. In diesem Zusammenhang ist zunächst daran zu erinnern, dass die DSGVO im Kern zwei Ziele verfolgt, nämlich zum einen das europäische Datenschutzrecht an das digitale Zeitalter anzupassen und zum anderen – durch die Rechtsform der Verordnung[35] – ein europaweit hohes Datenschutzniveau sicherzustellen.[36] Im Folgenden soll die Grundregel der Zweckbindung in Art. 5 Abs. 1 lit. b) DSGVO vorgestellt werden (1.), bevor auf die Möglichkeiten der Zweckänderung gemäß Art. 6 Abs. 4 DSGVO (2.) und weitere Durchbrechungen des Zweckbindungsgrundsatzes (3.) eingegangen wird.

1. Die Grundregel des Art. 5 Abs. 1 lit. b) DSGVO

Der Zweckbindungsgrundsatz findet sich nicht nur in Art. 8 Abs. 2 S. 1 GRCh.[37] Vielmehr war er bereits in Art. 6 Abs. 1 lit. b) und c) der geltenden Datenschutz-RL 95/46/EG enthalten. Trotz zahlreicher Stimmen im Rat, die versuchten, den Zweckbindungsgrundsatz ganz aus der DSGVO herauszuverhandeln oder ihn jedenfalls erheblich einzuschränken,[38] findet er sich nun in fast identischem Wortlaut in Art. 5 Abs. 1 lit. b) DSGVO wieder. Während die Mitgliedstaaten gemäß Art. 6 Abs. 1 lit. b) RL 95/46/EG jedoch sicherzustellen hatten, dass personenbezogene Daten „für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden", heißt es in Art. 5 Abs. 1 lit. b) DSGVO, personenbezogene Daten müssten „für festgelegte, eindeutige und *legitime* Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden." Dass hier der Begriff der „Weiterverarbeitung" verwendet wird, erklärt sich daraus, dass auch das Erheben gemäß Art. 4 Abs. 1 Nr. 2 DSGVO eine Verarbeitung darstellt. Dabei ist allerdings zu beachten, dass die Weiterverarbeitung auch durch einen anderen als denjenigen „Verantwortlichen"[39] erfolgen kann, der die Daten ursprünglich erhoben hat.[40] Die DSGVO trifft allerdings keine abschließende Regelung darüber, zu welchen Zwecken eine solche Weiterverarbeitung zulässig ist. Während die Vorgabe des „eindeutigen" Zwecks für ein eher restriktives Zweckverständnis spricht,[41] ist andererseits zu berücksichtigen, dass die Zwecke gemäß Art. 5 Abs. 1 lit. b) DSGVO nicht mehr „rechtmäßig",[42] sondern nur noch „legitim" sein müssen. Letztlich überlässt die DSGVO die Konkretisierung dieser Frage weitergehenden unions- oder mitgliedstaatlicher Regelungen.[43] Erlassen diese jedoch keine konkretisierenden Regelungen, werden es oftmals die Verantwortlichen sein, welche die Zwecke der Weiterverarbeitung festlegen. Dann stellt sich jedoch die Frage, wann ein Zweck im Sinne von Art. 5 Abs. 1 lit. b) DSGVO „eindeutig", „festgelegt" und vor allem, wann er „legitim" ist. Da die DSGVO hier keinerlei Maßstäbe aufstellt, wird es vor allem eine Aufgabe der Mitgliedstaaten sein,

31 Vgl. im Einzelnen etwa *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 98 ff.
32 *Trute*, Verfassungsrechtliche Grundlagen, in: Rossnagel: Handbuch Datenschutzrecht, Kap. 2.5 Rn. 40.
33 *Pohle*, Datenschutz-Nachrichten (DANA) 2015, 141.
34 Zu ihm etwa *Wolff*, in: Wolff/Brink, BeckOK Datenschutzrecht, 17. Edition (01.08.2015), Syst. A, Rn. 43 f.
35 Allerdings handelt es sich lediglich um eine „Grund"-Verordnung, die zahlreiche – von den Mitgliedstaaten auszufüllende – Öffnungsklauseln enthält, sodass sich hier von einem „Handlungsformenhybrid" aus Richtlinie und Verordnungen sprechen ließe – vgl. etwa *Kühling/Martini*, EuZW 2016, 448, 449. Zu dem den Mitgliedstaaten aufgrund der zahlreichen „Öffnungsklauseln" verbleibenden Spielraum etwa: *Bennecke/Wagner*, DVBl. 2016, 600 ff.; *Kühling/Martini u. a.*, Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Gutachten, S. 14 ff.
36 Vgl. etwa http://www.europarl.europa.eu/news/de/news-room/20160407IPR21776/parlament-verabschiedet-eu-datenschutzreform-%E2%80%93-eu-fit-f%C3%BCrs-digitale-zeitalter (abgerufen am 06.03.2017).
37 Danach dürfen personenbezogene Daten „nur ... für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden."
38 Zum Gesetzgebungsprozess etwa *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 1 Rn. 40 ff.
39 In der DSGVO wird der Begriff der datenverarbeitenden Stelle durch den Begriff des Verantwortlichen ersetzt. Dieser Begriff ist in Art. 4 Nr. 7 DSGVO legal definiert.
40 Vgl. *Frenzel*, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 5 Rn. 29.
41 *Schantz*, NJW 2016, 1841, 1843 f.
42 So noch Art. 6 Abs. 1 lit. b) RL 95/46/EG.
43 Vgl. dazu den 45. Erwägungsgrund der DSGVO: Es „sollte im Unionsrecht oder im Recht der Mitgliedstaaten geregelt werden für welche Zwecke die Daten verarbeitet werden dürfen. Ferner könnte in diesem Recht die allgemeinen Bedingungen dieser Verordnung zur Regelung der Rechtmäßigkeit personenbezogener Daten präzisiert und es könnte darin festgelegt werden, wie der Verantwortliche zu bestimmen ist, welche Art von personenbezogenen Daten zu verarbeiten werden, welche Personen betroffen sind, welche Einrichtungen die personenbezogenen Daten offenlegt, für welche Zwecke und wie lange sie gespeichert werden dürfen und welche anderen Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung rechtmäßig und nach Treu und Glauben erfolgt."

hier für Rechtsklarheit zu sorgen.[44] Vor allem aber ordnet Art. 5 Abs. 1 lit. b) DSGVO keine starre Zweck*bindung*, sondern lediglich eine Zweck*vereinbarkeit* an. So genügt es nach dem Wortlaut des Art. 5 Abs. 1 lit. b) DSGVO, dass die Weiterverarbeitung mit der ursprünglichen Verarbeitung „vereinbar" ist. Für die Betroffenen hat dies nicht nur den Nachteil, dass sie die Frage der Vereinbarkeit selbst oftmals nicht abschätzen können.

2. Die Zulässigkeit von Zweckänderungen nach Art. 6 Abs. 4 DSGVO

Der Zweckbindungsgrundsatz erscheint in Art. 5 DSGVO als einer von mehreren „Grundsätzen für die Verarbeitung personenbezogener Daten". Diese sind von den in Art. 6 DSGVO niedergelegten Tatbeständen zu unterscheiden, die Aussagen über die „Rechtmäßigkeit" der Datenverarbeitung treffen. Allerdings sind beide Normen über Art. 6 Abs. 1 lit. a) DSGVO derart verklammert, dass die Datenverarbeitung „nur rechtmäßig" ist, wenn die betroffene Person „ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben" hat.

Daraus folgt jedoch zugleich, dass eine Datenverarbeitung zu einem bestimmten Zweck auch dann zulässig ist, wenn im Erhebungszeitpunkt noch ein anderer Zweck festgelegt wurde – solange der Betroffene vor der Datenverarbeitung zu den (neuen) Zwecken seine Einwilligung[45] erteilt hat. Konkretisiert wird diese Kompetenz der Verantwortlichen zur sog. Zweckänderung durch Art. 6 Abs. 4 DSGVO.[46] Danach ist eine Datenverarbeitung zu anderen als zu den im Erhebungszeitpunkt festgelegten Zwecken nur zulässig, wenn sie auf einer Einwilligung des Betroffenen oder auf einer Rechtsvorschrift der EU oder der Mitgliedstaaten[47] beruht, die einer der in Art. 23 Abs. 1 DSGVO genannten Ziele dient und außerdem verhältnismäßig ist. In diesen Fällen ist die Datenverarbeitung aber nicht per se zulässig. Vielmehr hat der Verantwortliche zu prüfen, ob die Datenverarbeitung zu den neuen Zwecken mit den ursprünglichen Erhebungszwecken „vereinbar" ist.[48] Damit postuliert die DSGVO – wie schon bei Art. 5 Abs. 1 lit. b) – keine strikte Zweckbindung, sondern eine bloße Zweckvereinbarkeitsregel.[49] Wie sich aus dem 50. Erwägungsgrund der DSGVO ergibt, ist im Falle der Zweckvereinbarkeit „keine andere Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten."[50]

Wann nun von einer solchen „Vereinbarkeit" von Erhebungs- und Verarbeitungszweck auszugehen ist, wird in Art. 6 Abs. 4 DSGVO durch eine Reihe von Gesichtspunkten konkretisiert.[51] Dazu zählen die „Verbindung" zwischen den Erhebungs- und den Verarbeitungszwecken (lit. a), der „Zusammenhang", in dem die Daten erhoben wurden (lit. b), die „Art" der betroffenen Daten (lit. c), die möglichen Folgen der Weiterverarbeitung für den Betroffenen (lit. d) und das Vorhandensein geeigneter Garantien, beispielsweise durch Pseudonymisierungen[52] (lit. e). Dabei soll für die Beurteilung, ob diese Kriterien vorliegen, die Perspektive der Betroffenen maßgeblich sein.[53]

Gleichwohl dürfte sich die in Art. 6 Abs. 4 DSGVO begründete Befugnis der Verantwortlichen zur Zweckänderung aus Sicht der Betroffenen als weitreichende Beeinträchtigung ihrer Rechtsposition darstellen. Hat ein Betroffener der Datenerhebung zugestimmt, muss er mit einer weitreichenden Datenverwendung durch den Verantwortlichen rechnen. Diese Beeinträchtigung soll nun durch ein verbessertes Zusammenspiel mit anderen Grundsätzen des Datenschutzes kompensiert werden. So ordnen die Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO noch vor der Zweckfestlegung weitreichende Informationspflichten des Verantwortlichen an. So hat dieser dem Betroffenen vor oder nach einer Zweckänderung die in Art. 13 Abs. 2 DSGVO bzw. Art. 14 Abs. 2 DSGVO genannten Informationen zur Verfügung zu stellen. Dazu zählen Informationen über die Dauer der Speicherung, das Bestehen eines Auskunfts-, Widerrufs- und eines Beschwerderechts, eine Information darüber, ob die Bereitstellung der Informationen gesetzlich oder vertraglich vorgeschrieben ist oder ob eine automatisierte Entscheidungsfindung einschließlich Profiling stattgefunden hat.

Wie im 42. Erwägungsgrund eindeutig zum Ausdruck kommt, sollen diese Informationspflichten sicherstellen, dass der Betroffene seine Einwilligung zur Datenverarbeitung „in Kenntnis der Sachlage" und letztlich freiwillig[54] abgegeben hat. Denn die Einwilligung „sollte sich" gemäß dem 32. Erwägungsgrund „auf alle zu demselben Zweck oder zu denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Zwecke eine Einwilligung gegeben werden."

Als irritierend und offenbar als Redaktionsversehen[55] muss dagegen die sich hieran anschließende Einschränkung in ErwG. 50 bezeichnet werden: „Hat die betroffene Person ihre Einwilligung erteilt (...), so sollte der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiter verarbeiten dürfen. In jedem Falle sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird." Würde diese Aussage nämlich tatsächlich zutreffen,

44 Vgl. jedoch die Kommentierung von *Härting*, Datenschutz-Grundverordnung, 2016, Art. 5 Rn. 95; *Frenzel*, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 5 Rn. 27 f., wonach sich das Merkmal der „Festlegung" eher formal und das Merkmal der „Eindeutigkeit" eher als materiell verstehen lasse. Das Merkmal der „Legitimität" sei mit dem in Art. 6 Abs. 1 lit. b) RL 95/46/EG enthaltenen Merkmal der „Rechtmäßigkeit" gleichbedeutend.

45 Die Anforderungen an die Freiwilligkeit der Einwilligung sind in Art. 7 DSGVO genannt.

46 Diese Bestimmung basiert auf einem Vorschlag der Article 29 working group – vgl. Article 29 Data Protection Working Party, WP 203, Opinion 03/2013 on purpose limitation, S. 28.

47 Zur Reichweite dieser Öffnungsklausel: *Peuker*, in: Sydow, DSGVO, i. E., Art. 23 Rn. 1 ff.

48 Vgl. aber *Schantz*, NJW 2016, 1841, 1844: „Ob überhaupt eine Zweckänderung vorliegt, hängt maßgeblich davon ab, wie weit oder eng der ursprüngliche Zweck auszulegen ist.".

49 So auch *Härting*, NJW 2015, 3284, 3288. Dagegen sprechen *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 3 Rn. 52 – allerdings ohne nähere Begründung – von einer „strengen Zweckbindung".

50 Dazu *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 3 Rn. 54: „Daraus folgt aber nicht, dass Verantwortliche Daten zweckkompatibel ohne weitere Rechtsgrundlage weiter verarbeiten dürfen ... Grundsätzlich muss schließlich jede Verarbeitung auf einen Erlaubnisgrund gestützt werden, Art. 5 Abs. 1 lit. a) i. V. m. Art. 6 DSGVO. Dementsprechend ist Art. 6 Abs. 4 DSGVO auch als Schranke (zulässiger) Weiterverarbeitungen formuliert und nicht als eigenständiger Erlaubnisgrund."

51 *Buchner*, DuD 2016, 155, 159 bezeichnet diese allerdings als „weitestgehend inhaltslos und dehnbar".

52 Vgl. dazu die Legaldefinition in Art. 4 Nr. 5 DSGVO.

53 Vgl. *Frenzel*, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 6 Rn. 47.

54 Weitere Konkretisierungen zur Freiwilligkeit der Einwilligung finden sich im 43. Erwägungsgrund.

55 Vgl. *Schantz*, NJW 2016, 1841, 1844: „Dies ergibt sich nicht nur – wie dargelegt – aus der Entstehungsgeschichte und Systematik der DSGVO. Andernfalls wäre etwa die Verarbeitung jedweder einmal zu einem anderen Zweck erhobener Daten für privilegierte Zwecke wie Statistik und Forschung ohne weitere Voraussetzung zulässig, weil die Vereinbarkeit dieser Zwecke mit dem Erhebungszweck gesetzlich vermutet wird (Art. 5 Abs. 1 Buchst. b) Hs. 2 DSGVO). Dies wäre wiederum kaum mit Art. 7 und 8 GRC vereinbar."

sodass das Erfordernis der Einwilligung durch eine nachträgliche Belehrung über das Widerspruchsrecht ersetzt werden könnte, wäre nicht nur der Zweckbindungs-, sondern auch der Einwilligungsgrundsatz weitestgehend ausgehebelt.

3. Weitere Durchbrechungen des Zweckbindungsgrundsatzes

Neben den soeben dargestellten Befugnissen der Verantwortlichen zur Zweckveränderung wird der Zweckbindungsgrundsatz in der DSGVO durch zahlreiche Regelungen durchbrochen. So sieht Art. 5 Abs. 1 lit. b) DSGVO selbst eine Bereichsausnahme für wissenschaftliche, historische und statistische Zwecke vor, deren genauer Inhalt in Art. 89 Abs. 1 DSGVO näher ausgeführt wird.[56] Hintergrund dieser Ausnahme ist ausweislich des 33. Erwägungsgrundes der DSGVO, dass der Zweck der Verarbeitung personenbezogener Daten bei der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung oftmals nicht vorhergesehen werden kann. Darüber hinaus ordnet Art. 23 Abs. 1 DSGVO zur Wahrung der dort genannten Interessen Ausnahmen von den in Art. 12 bis 22 DSGVO normierten Betroffenenrechten an. Diese Relativierungen dürften in hohem Maße zu einer Aushöhlung des Zweckbindungsgrundsatzes und letztlich dazu beizutragen, dass seine Kontrafaktizität weiter bestehen bleibt.

IV. Fazit und Ausblick auf die Ausführung in Deutschland

Der Zweckbindungsgrundsatz ist in der DSGVO zwar enthalten. Er erfährt jedoch zahlreiche Ausnahmen und Durchbrechungen. Die wichtigste Ausnahme dürfte wohl die in Art. 6 Abs. 4 DSGVO niedergelegte Regelung zur Zulässigkeit von Zweckänderungen darstellen, die den Zweckbindungsgrundsatz – wie die Grundregel des Art. 5 Abs. 1 lit. b) DSGVO – in einen Zweckvereinbarkeitsgrundsatz transformiert. Die Zulässigkeit von Zweckfestlegungen und -änderungen beruht entweder auf einer (noch von der EU oder den Mitgliedstaaten zu erlassenden) Rechtsvorschrift oder auf einer Einwilligung des Betroffenen. Die DSGVO geht dabei davon aus, dass eine solche bereits dann „freiwillig" ist, wenn der Betroffene über wesentliche Zusammenhänge der Datenverarbeitung Kenntnis hat. Um dem Betroffenen die notwendige Kenntnis zu verschaffen, sieht die DSGVO weitreichende Informationspflichten der Verantwortlichen vor. Statt einer eindeutigen Zweckfestlegung und einer starren Zweckbindung sieht die DSGVO vor, dass der Verantwortliche den Betroffenen fortlaufend über etwaige Zweckänderungen informiert. Beide Seiten treten so in ein gemeinsames Zweckmanagement. Ob dieses jedoch angesichts eines ohnehin schon hochgradig überlasteten Betroffenen praktikabel ist, erscheint fragwürdig. Insgesamt bleibt der Zweckbindungsgrundsatz in der DSGVO damit weitgehend konturenlos.

Umso mehr wird es für die Rechtspraxis in Deutschland daher darauf ankommen, welche Gestalt der Zweckbindungsgrundsatz durch das geplante „Datenschutz-Anpassungs- und Umsetzungsgesetz-EU" (DSAnpUG-EU)[57] erhält. Dieses enthält in seinem Teil 2, den Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Art. 2 der VO 679/2016, zunächst eine Reihe von Bestimmungen zur Konkretisierung des Zweckbindungsgrundsatzes. So regelt § 23 Abs. 1 DSAnpUG-EU, unter welchen Voraussetzungen eine Verarbeitung durch öffentliche Stellen zu anderen als zu den im Erhebungszeitpunkt bestimmten Zwecken zulässig ist. Dies soll nämlich u. a. der Fall sein, wenn „offensichtlich ist", dass die Verarbeitung „im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde" (Nr. 1), wenn Anhaltspunkte für die tatsächliche Unrichtigkeit von Angaben über eine Person bestehen (Nr. 2), wenn die Angaben ohnehin öffentlich zugänglich sind (Nr. 3) oder sie „zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit" (Nr. 4), der Verfolgung von Straftaten (Nr. 5), zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Dritter (Nr. 6) oder der Wahrung von Aufsichts- und Kontrollbefugnissen dienen.

Für nicht-öffentliche Stellen stellt § 24 Abs. 1 DSAnpUG-EU klar, dass eine Verarbeitung zu anderen als zu den ursprünglichen Erhebungszwecken nur zulässig ist, wenn sie „zur Abwehr einer von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verhütung von Straftaten erforderlich ist" (Nr. 1) oder wenn „sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist" (Nr. 2), „sofern nicht die Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen."

De lege ferenda befindet sich der Zweckbindungsgrundsatz also auch im deutschen Recht auf dem Rückzug. Zwar wird er als Grundsatz nach wie vor nicht aufgegeben, aber doch durch derart weitreichende Zweckänderungsbefugnisse ausgehöhlt, dass für den Grundsatz kaum noch Anwendungsfälle bestehen bleiben dürften. Wirksamkeit entfaltet der Zweckbindungsgrundsatz jedoch nur bei strikter Geltung. Die im europäischen und dem künftigen deutschen Recht angeordnete Bindung erweist sich aber als derart schwach, dass der Zweckbindungsgrundsatz künftig eher den Charakter einer Vorprüfung vor einer umfassenden Interessenabwägung aufweist.[58]

Diese Umstellung vom Zweckbindungsgrundsatz auf eine Interessenabwägung wird zwar nicht erst mit der DSGVO eingeleitet. Vielmehr sieht bereits § 28 Abs. 1 S. 1 Nr. 2, Abs. 2 Nr. 2, Abs. 6 Nr. 1 BDSG für die Datenverarbeitung durch nicht öffentliche Stellen eine solche Interessenabwägung vor.[59] Aufgrund des im Vorliegenden dargestellten Zusammenspiels von DSGVO und DSAnpUG-EU dürfte jedoch davon auszugehen sein, dass diese Interessenabwägung nun auch für die Datenverarbeitung durch öffentliche Stellen immer öfter zum Tragen kommt. Diese Entwicklung ist aus Sicht der Betroffenen insofern problematisch, als die Interessenabwägung viel weniger vorhersehbar ist als eine starre Zweckbindung. Andererseits ist die dem Zweckbindungsgrundsatz zugrundeliegende Vorstellung einer Welt mit eindeutig festlegbaren Zwecken und Aufgaben mit der Komplexität der digitalen Informationsgesellschaft kaum zu vereinbaren. Damit dürfte der Europäische Gesetzgeber jedenfalls eines seiner Hauptziele erreicht haben, nämlich eine Anpassung des Datenschutzrechts an das digitale Zeitalter. Ob es dem Europäischen Gesetzgeber allerdings auch gelungen ist, das Datenschutzniveau zu erhöhen, erscheint nach den obigen Ausführungen äußerst zweifelhaft.

56 Eingehend dazu etwa *Richter*, DuD 2015, 735, 737 ff.
57 BR-Drs. 110/17.
58 So auch *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 6 Rn. 38 f. angesichts der Kriterien des Art. 6 Abs. 4 DSGVO.
59 Vgl. dazu *Wolff*, in: Wolff/Brink, BeckOK Datenschutzrecht, § 28 Rn. 57 ff.

PRIVACY NEWS

PinG – Schlaglichter

Ausgewählte Rechtsprechung und Verfahren

Philipp Müller-Peltzer

VG Hamburg, Beschl. v. 24.04.2017 – 13 E 5912/16 – Datenweitergabe von WhatsApp an Facebook bleibt bis auf weiteres untersagt

Die 13. Kammer des Verwaltungsgerichts Hamburg hat der Facebook Ireland Ltd. Eilrechtsschutz gegen die datenschutzrechtliche Untersagungsverfügung des Hamburgischen Beauftragten für den Datenschutz und die Informationsfreiheit überwiegend versagt. Gegenstand des Verfahrens ist die beabsichtigte Übermittlung von Daten deutscher WhatsApp-Nutzer an den Facebook-Mutterkonzern bzw. seine irische Niederlassung, nachdem der Betreiber des WhatsApp-Messengers im Jahr 2014 von Facebook akquiriert wurde. WhatsApp hat die Nutzer zu diesem Zweck aufgefordert, einer Aktualisierung der Nutzungsbedingungen und der Datenschutzrichtlinie zuzustimmen.

Zwar wurde die sofortige Vollziehung zweier Teilverfügungen der Behörde aufgehoben, mit denen Facebook verpflichtet wird, Daten von WhatsApp-Nutzern zu löschen, die bereits erhoben und gespeichert wurden und die technischen Details der Datenweitergabe und die diesbezüglichen Weisungen an den Auftragsverarbeiter zu dokumentieren und vorzulegen. Mangels jeglicher Begründung durch die Behörde könne die Anordnung der sofortigen Vollziehung dieser Aspekte nicht aufrechterhalten werden. Die entscheidende Untersagungsverfügung bleibt jedoch bestehen. Damit darf die Weitergabe der Daten bis zur finalen Klärung der Rechtmäßigkeit der Verarbeitung im Hauptsacheverfahren nicht erfolgen.

Das Verfahren tangiert mehrere derzeit relevante und teilweise noch ungeklärte datenschutzrechtliche Rechtsfragen. Zum einen hatte sich das Verwaltungsgericht erneut mit der Frage auseinanderzusetzen, ob überhaupt deutsches Datenschutzrecht anwendbar ist, da mit der Facebook Ireland Ltd. eine europäische Niederlassung in einem Mitgliedstaat existiert.

Die Hamburgische Behörde stellt indes auf die in Hamburg belegene Facebook Germany GmbH ab, die neben der PR- und Öffentlichkeitsarbeit lokale Marktunterstützung für deutsche Werbekunden von Facebook erbringt, die eigentlichen Werbeplätze aber nicht veräußert. Für die Behörde sind die Aktivitäten der Hamburgischen Niederlassung ein ausreichender Anknüpfungspunkt für die streitgegenständliche Datenverarbeitung. Die Datenschutzaufsichtsbehörde zieht die Parallele zur Google Spain-Entscheidung und vertritt die Auffassung, dass das entscheidende Merkmal „im Rahmen der Tätigkeiten einer Niederlassung“ in § 1 Abs. 5 S. 1 BDSG i. V. m. Art. 4 der Datenschutzrichtlinie 95/46/EG nach dem EuGH denkbar weit auszulegen sei.

Das Verwaltungsgericht vermerkt, dass die vorliegende Binnenmarktkonstellation nicht mit dem Google Spain-Sachverhalt deckungsgleich sei und kommt diesbezüglich zu dem Schluss, dass eine abschließende Entscheidung über diese konkrete Rechtsfrage bislang nicht vorliegt. Die weite Auslegung des Begriffs könne in der vorliegenden Konstellation dazu führen, dass für denselben Verarbeitungsvorgang das Recht mehrerer Mitgliedstaaten anzuwenden ist. Im vorliegenden Fall sei dies das irische Recht am Ort der tatsächlichen Verarbeitung sowie das deutsche Recht am Ort der lediglich mittelbar unterstützenden Niederlassung des amerikanischen Mutterkonzerns. Der Richtlinientext enthalte keine Anhaltspunkte dahingehend, wie in dieser Konstellation zu differenzieren sei.

Philipp Müller-Peltzer ist Ständiger Autor bei „Privacy in Germany“. Er ist Rechtsanwalt bei Schürmann Wolschendorf Dreyer RAe in Berlin und auf IT- und Datenschutzrecht spezialisiert. Er ist außerdem als externer Datenschutzbeauftragter tätig.

In den bisherigen Entscheidungen hat sich der EuGH zu dieser Frage nicht ausdrücklich verhalten. Er verwies in seinem Urteil in der Rechtssache Amazon (EuGH, Urt. v. 28.07.2016, C-191/15) lediglich kommentarlos auf die Schlussfolgerungen des Generalanwaltes, der darauf abgestellt hatte, dass die Niederlassung zu bestimmen sei, im Rahmen derer Tätigkeiten die streitgegenständlichen Verarbeitungsvorgänge am unmittelbarsten erfolgen würden.

Mit seinen Ausführungen lässt das Verwaltungsgericht anklingen, dass die Verantwortlichkeit der irischen Gesellschaft

sowohl technisch, tatsächlich als auch in der Außendarstellung gegenüber den Nutzern maßgeblich und damit ausschließlich irisches Recht anwendbar sein könnte. Andererseits lässt das Gericht Raum für eine abweichende Beurteilung, indem es feststellt, dass vorliegend ausschließlich die Belange der deutschen WhatsApp-Nutzer betroffen seien.

Anknüpfend an diesen Aspekt wird im Hauptsacheverfahren des Weiteren geklärt werden müssen, ob die Hamburgische Aufsichtsbehörde bei Annahme der Anwendbarkeit deutschen Datenschutzrechtes zuständig ist oder ob allein die irische Behörde gegen die Facebook Ireland Ltd. vorgehen kann. Diesbezüglich schließt sich das Gericht der Bewertung des OVG Hamburg an und erachtet die Eingriffsbefugnis der Hamburgischen Behörde für zweifelhaft.

Materiell erachtete das Gericht die Untersagungsverfügung für jedenfalls nicht offensichtlich rechtswidrig, ein überwiegendes Aussetzungsinteresse der Facebook Ireland Ltd. sei nicht gegeben. Die geplante Datenweitergabe sei rechtswidrig, die eingeholte Einwilligung der Nutzer unwirksam. Aufgrund der gewählten Gestaltung und Formulierungen sei für den durchschnittlichen Nutzer nicht erkennbar, dass ein Klick auf den Button „Zustimmen“ unter der Erläuterung „WhatsApp aktualisiert die Nutzungsbedingungen und Datenschutzrichtlinie um neue Funktionen ( ) zu berücksichtigen.“ eine Einwilligung in die geplanten Datenverarbeitungsvorgänge bedeutet. Die Formulierungen suggerierten einen weitergehenden Schutz personenbezogener Daten und neue Funktionen, statt zusätzliche Verarbeitungsschritte. Die Nutzer würden daher durch diese Ausgestaltung auch in die Irre geführt, von einer bewussten Einwilligung dürfe nicht ausgegangen werden. Die Zwecke der Verarbeitung würden nicht erläutert. Auch der hinter dem Button „Lesen“ verlinkte Text stelle keine ausreichende Information der Nutzer her. Der dort platzierte Opt-out-Schalter lasse völlig offen, auf welche Datenkategorien er sich beziehe. Die datenschutzrechtliche Einwilligung sei zudem ohne gesonderte Hervorhebung in den Fließtext neben weiteren Hinweisen eingebunden.

Weitere datenschutzrechtlich brisante Fragen lässt das Gericht offen: Dies betrifft zum einen die Frage, ob wie von der Behörde zusätzlich beanstandet Minderjährige ab dem 13. Lebensjahr überhaupt ohne die Zustimmung der Erziehungsberechtigten einwilligen können. Zum anderen, ob neben WhatsApp auch die Facebook Ireland Ltd. eine Einwilligung einholen müsste, um die Weitergabe und Entgegennahme sowie die fortgesetzte Speicherung der Daten rechtfertigen zu können. Das Gericht bezieht zu diesen Aspekten nicht Stellung, da diese aufgrund der Unwirksamkeit des Einwilligungsverfahrens keine Änderung am Ergebnis der Bewertung bewirken würden.

Eine Berufung auf § 28 Abs. 1 S. 1 Nr. 2 BDSG komme nicht in Betracht, da Facebook nicht dargelegt habe, dass die von der Weitergabe betroffenen Daten für die beabsichtigten Zwecke tatsächlich erforderlich sind. In diesem Punkt setzt sich das Verwaltungsgericht mit den Ausführungen zu den einzelnen Verarbeitungszwecken auseinander. Die Richter lassen klar erkennen, dass die Erläuterungen, wonach die Weitergabe beispielsweise für den formulierten Zweck „Network/Security“ erforderlich sei, um Nutzer verifizieren, kompromittierte Accounts identifizieren und eine Zwei-Faktor-Authentifizierung anbieten zu können, zu pauschal sei, nicht ausreichend zwischen den jeweiligen Datenkategorien differenziere und nicht substantiiert vorgetragen worden sei, inwiefern die anlasslose Bereitstellung der Datensätze aller WhatsApp-Nutzer erforderlich ist. Nach Auffassung der Richter sollten die Verarbeitungsschritte einzelfallbezogen erfolgen und nicht eine Bevorratung aller WhatsApp-Daten angestrebt werden. Andere Optionen, wie die Account-Wiederherstellung oder die Zwei-Faktor-Authentifizierung sollten erst zu einer Weitergabe führen, wenn der Betroffene diese Option tatsächlich nutzt.

Im Ergebnis zeigen die Richter auf, dass beide Parteien sich darauf einstellen müssen, im Hauptsacheverfahren noch konkreter zu den aufgeworfenen Rechtsfragen Stellung beziehen zu müssen. Im Hinblick auf die Beurteilung des Einwilligungsprozederes hat das Gericht jedoch bereits eine klare Position bezogen. Die Anwendbarkeit des deutschen Rechtes und die Zuständigkeit der Behörde vorausgesetzt dürfte die von Facebook gewählte Ausgestaltung der Einwilligung kaum wirksame Rechtfertigungen für die Verarbeitungsschritte hervorbringen. Die klaren Worte der Richter sollten daher auch andere Anbieter dazu anhalten, klare Formulierungen und bestenfalls einen eindeutigen Wortlaut für Einwilligungserklärungen anzustreben.

Die Datenschutzaufsichtsbehörden sprechen sich diesbezüglich ausdrücklich dafür aus, die Einwilligungstexte unmissverständlich mit Formulierungen wie „ich willige ein“ einzuleiten oder entsprechend zu überschreiben. Für die Ausgestaltung der zusätzlichen Erläuterungen und generell die Formulierung von Datenschutzerklärungen sollte unbedingt echte Transparenz statt zu weichen Formulierungen angestrebt werden. Die wabernden Formulierungen, die sich bisweilen vor allem in den Rechtstexten von US-Anbietern finden, erfüllen diese Anforderung und damit den Zweck einer Kontrollmöglichkeit für den Nutzer oftmals nicht.

Quelle: justiz.hamburg.de

♦ VG Berlin, Beschl. v. 27.03.2017 – VG 6 L 250.17 – Internetportal, das Unterkünfte von „schwulen oder schwulenfreundlichen“ Gastgebern anbietet, muss einem Auskunftsverlangen des Bezirksamtes über Nutzer nachkommen

Der Anbieter eines Portals für die Vermittlung von Ferienwohnungen und Übernachtungsmöglichkeiten muss einer Anordnung des Berliner Bezirksamtes Tempelhof-Schöneberg nachkommen, mit der er aufgefordert wird, Namen von Nutzern und Adressen der vermittelten Wohnungen preiszugeben. Die Behörde verfolgt damit einen Verdacht auf Verstoß gegen das Berliner Zweckentfremdungsverbot-Gesetz, mit dem der angespannte Berliner Wohnungsmarkt geschützt werden soll, indem die Vermietung von Wohnraum als Ferienwohnung untersagt werden kann.

Während das Bezirksamt nach eigenen Angaben auf mehreren Portalen privat vermittelte Wohnungen ermittelt, weist der vorliegende Sachverhalt eine Besonderheit auf, da sich das Portal ausdrücklich an homosexuelle Reisende richtet und sich als „#1 Reise-Community für Schwule, Lesben & Freunde“ bezeichnet. Nach Auffassung des Anbieters und der in das Verfahren eingeschalteten Berliner Beauftragten für Datenschutz und Informationsfreiheit handelt es sich daher bei den Angaben über die Nutzer, die von der Behörde verlangt werden, um besondere Arten personenbezogener Daten, da zugleich die sexuelle Gesinnung der Wohnungsgeber kommuniziert werde. In der Folge sei die Erhebung und Speicherung dieser sensiblen Daten durch das Bezirksamt unzulässig, da andernfalls eine behördlich geführte Datensammlung entstünde, die Aufschluss über die sexuelle Orientierung des betroffenen Nutzerkreises gebe.

Soweit auf dem Portal auch „schwulenfreundliche Gastgeber“ akzeptiert würden, sei dies rein theoretischer Natur und diese „extrem liberale“ Einstellung müsse als „abseits der Norm“ aufgefasst werden, weshalb auch dieser Nutzerkreis der

„schwulenfreundlichen Gastgeber" eine „bestimmte liberale sexuelle Orientierung" habe und „dem Datenschutz unterfalle". Der Anbieter versicherte außerdem eidesstattlich, dass er überzeugt sei, dass 90% der Nutzer homosexuell und die Bestandsdaten der Nutzer demzufolge als besonders sensible Daten zu qualifizieren seien. Er wendete sich gegen die Anordnung der sofortigen Vollziehung des Auskunftsverlangens.

Die Berliner Verwaltungsrichter teilten die Bedenken hinsichtlich der befürchteten Verarbeitung der sensiblen Daten durch das Bezirksamt nicht. Nach § 5 Abs. 1, Abs. 2 S. 2 des Zweckentfremdungsverbot-Gesetzes sei das Bezirksamt befugt, die konkretisierten Personendaten sowie Wohnungsdaten und Nutzungsnachweise zu erheben. Die Behörde habe sich für die acht betroffenen Wohnungsangebote auf die erforderlichen Angaben beschränkt und einen Verdacht einer Zweckentfremdung von Wohnraum dargelegt. Eine Ermittlung auf anderem Wege, beispielsweise über eine Anmeldung auf dem Portal und eine anschließende Anmietung der Wohnungen sei mit unverhältnismäßigem Aufwand verbunden und der Behörde daher nicht zuzumuten.

Soweit die Berliner Datenschutzbeauftragte darauf verwiesen hat, das Bezirksamt müsse abwarten, bis Anzeigen der Nachbarschaft der betroffenen Wohnungen wegen störender Ferienwohnungsvermietung eingingen, sei dies ebenfalls kein geeignetes Mittel zur Erforschung des Sachverhaltes.

Die Richter waren zudem der Auffassung, dass der Erhebung keine schutzwürdigen Belange der Betroffenen entgegenstehen. Bei den von der Behörde erfragten Daten handele es sich schon nicht um besondere Arten personenbezogener Daten i. S. d. § 6a Abs. 1 BlnDSG bzw. Art. 8 Abs. 1 der Datenschutzrichtlinie 95/46/EG. Zwar speichere der Anbieter Daten, die Rückschluss auf die sexuelle Orientierung der Nutzer zulassen, da bei der Nutzerregistrierung zwingend eine Angabe über ein Drop-Down-Menü ausgewählt werden muss, das die Angaben „Ich bin Gay", „Ich bin gayfriendly" und „Ich mag keine Gays" enthält. Eine direkte Erhebung von Daten über das Sexualleben finde indes gerade nicht statt. Der Behörde sei es im Rahmen des Auskunftsverlangens allein um die Information der Wohnungsgeberschaft, nicht um Angaben zur sexuellen Orientierung gegangen.

Zwar wird in der Literatur auch vertreten, eine Angabe über einen sensiblen Sachverhalt könne sich auch mittelbar aus dem Gesamtzusammenhang ergeben, da andernfalls kein effektiver Schutz dieser besonderen Datenkategorien gewährleistet werden könne. In der Folge komme es auf die Zwecksetzung und Verarbeitungsintention nicht an, sondern allein darauf, inwieweit sie einem potentiellen Empfänger den Eindruck vermitteln, dass sich den jeweiligen Daten die Einstellung der Betroffenen z. B. zu bestimmten politischen Vereinigungen oder gesundheitlichen Risiken entnehmen lassen. Solange jedoch Zweifel bestünden, ob ein solcher Schluss angenommen werden kann, solle es sich nicht um besondere Arten personenbezogener Daten handeln.

Die Berliner Richter sahen eine derartige mittelbare Aussage über einen sensiblen Sachverhalt indes nicht als gegeben an. Die Daten werden gerade nicht im Hinblick auf die sexuelle Orientierung, sondern allein im Kontext der Wohnungsvermietung verarbeitet. Allein der Umstand, dass eine erhöhte statistische Wahrscheinlichkeit dafür spricht, dass unter den Nutzern des Portals Homosexuelle seien, führe noch nicht zur zwingenden Annahme von Daten, die unter die besonderen Arten personenbezogener Daten fallen. Dafür spreche auch der Umstand, dass eine bestimmte homosexuelle Orientierung weder durch den Anbieter noch durch die Vermieter vorausgesetzt werde.

Zuletzt äußerten sich die Richter zu den Ausführungen des Portalbetreibers über die liberale sexuelle Orientierung von „schwulenfreundlichen Gastgebern" eher dezent und tun diese als reine Spekulation ab. Im Ergebnis sprächen die datenschutzrechtlichen Erwägungen nicht gegen die Rechtmäßigkeit des Auskunftsverlangens, zumal das Bezirksamt ausreichende Garantien dargelegt habe, die auch für den Fall, dass sensible Daten angenommen werden müssten, eine Verarbeitung zuließen. Das Bezirksamt legte insbesondere dar, dass die Datenerhebung im Rahmen des Auskunftsverlangens vollkommen getrennt von den späteren Fallakten abgelegt und organisiert werde. So könne ein späterer Bearbeiter den Zusammenhang zu dem streitgegenständlichen Portal nicht mehr nachvollziehen.

Die Entscheidung setzt sich mit einem praktisch relevanten Aspekt des Datenschutzrechtes auseinander. Die besonderen Bestimmungen zum Schutz sensibler Sachverhalte führen bei extensiver Anwendung der Vorschriften potentiell zu nicht unerheblichen Verarbeitungshindernissen und unpraktischen Ergebnissen. Richtig ist, dass Datensätzen aus dem Gesamtzusammenhang ein erweiterter Aussagegehalt entnommen werden kann. Eine lediglich erhöhte statistische Wahrscheinlichkeit kann jedoch nicht dazu führen, dass die Verarbeitung besonders restriktiv bewertet werden muss. Auch muss der Verarbeitungskontext gebührend berücksichtigt werden, da andernfalls der Anwendungsbereich der besonderen Schutzvorschriften überdehnt wird. Nicht jedes Foto eines Brillenträgers oder die Erkennbarkeit einer Hautfarbe führen zur Annahme eines sensiblen Datums. Erst wenn diese Informationen spezifisch verarbeitet werden, kann eine besondere Gefährdungslage für die Betroffenen angenommen werden.

Quelle: berlin.de

♦ BGH, Urt. v. 14. 03. 2017 – VI ZR 721/15 – Umsetzung eines Widerspruchs eines Kunden gegen die Datenverarbeitung zu werblichen Zwecken

Der sechste Zivilsenat hat das Zusammenspiel aus einem sehr weit formulierten Widerspruch gegen die Verarbeitung zu werblichen Zwecken und der sich aus dem Unterlassungsanspruch ergebenden Verpflichtung zur Folgenbeseitigung auseinandergesetzt.

Der beklagte Verlag hatte dem Kläger Werbe-E-Mails zugesendet und sich dabei auf eine weit formulierte Generaleinwilligung gestützt, die der Kläger anlässlich eines Software-Downloads erklärt hatte. Die Einwilligung verwies auf eine nicht abschließende Sponsorenliste und genügte nach Ansicht des Berufungsgerichtes und der Richter am Bundesgerichtshof den Anforderungen an eine konkrete und informierte Einwilligung nicht. Nach dem zusätzlich erklärten Widerspruch folgten weitere Werbe-E-Mails.

Die Besonderheit der Konstellation ergab sich indes aus dem Umstand, dass der Kläger der Beklagten ausdrücklich die Weitergabe der betroffenen E-Mail-Adresse an die Werbepartner und Sponsoren untersagt und sich die Beklagte daher gehindert sah, dem Unterlassungsanspruch nachzukommen, da er die Partner nicht über das Werbeverbot informieren konnte. Nach Auffassung des Berufungsgerichtes vereitele der Kläger somit selbst die Durchsetzung des von ihm erwirkten Unterlassungsgebotes und er verlange von der Beklagten Unmögliches.

Die Richter am Bundesgerichtshof kamen indes zu dem Ergebnis, dass kein Fall des Rechtsmissbrauchs gem. § 242 BGB vorliegt. Die Rechtsordnung missbillige gerade nicht grundsätzlich widersprüchliches Verhalten, sondern eine Rechtsausübung sei erst dann unzulässig, wenn sich

objektiv das Gesamtbild eines widersprüchlichen Verhaltens ergibt, weil früheres und späteres Verhalten sachlich miteinander unvereinbar ist und die Interessen der Gegenpartei im Hinblick hierauf vorrangig schutzwürdig sind.

Die Voraussetzungen dieses engen Ausnahmetatbestandes des widersprüchlichen Verhaltens lägen in der streitgegenständlichen Konstellation indes nicht vor. Die Verpflichtung zur Unterlassung einer Handlung erfordere nicht nur das bloße Nichtstun, sondern auch die Vornahme aller möglichen und zumutbaren Handlungen zur Beseitigung der Störungsquelle, wenn nur dadurch dem Unterlassungsgebot sachgerecht Folge geleistet werden kann. In der vorliegenden Konstellation müsse die Beklagte daher erforderlichenfalls auch auf Dritte einwirken, um die Störungsquelle zu beseitigen. Um diese Einwirkung vornehmen zu können, könne sich die Beklagte gegebenenfalls auf die Wahrnehmung berechtigter Interessen berufen, sodass eine Weitergabe der betroffenen E-Mail-Adressen an die Werbepartner zur Umsetzung des Widerspruchs bzw. des Unterlassungsanspruchs auf § 28 Abs. 1 S. 1 Nr. 2 BDSG gestützt werden könne. Der ausdrücklich gegen die Weitergabe gerichtete Widerspruch sei insofern unbeachtlich. Das berechtigte Interesse an der Befolgung der aus dem bestehenden Unterlassungsanspruch resultierenden Verpflichtung zur Folgenbeseitigung überwiege die Interessen des Betroffenen, selbst wenn dieser einen ausdrücklichen Widerspruch gegen diese Verarbeitung ausgesprochen hat.

Die zur Folgenbeseitigung erforderlichen Verarbeitungsschritte, wie eine einmalige Weitergabe der Adresse zum Zweck der Löschung beim Empfänger kann daher datenschutzrechtlich zulässig sein. Die notwendigen Sachverhaltsfeststellungen müssen diesbezüglich vom Berufungsgericht getroffen werden.

Quelle: juris.bundesgerichtshof.de

D
Datenschutz-Anpassungs- und Umsetzungsgesetz-EU beschlossen

Nach Kritik und weiteren leichten Anpassungen hat nunmehr auch der Bundesrat dem Datenschutz-Anpassungs- und Umsetzungsgesetz-EU zugestimmt und somit das erste nationale Anpassungsgesetz zur Datenschutz-Grundverordnung geschaffen. Während des Gesetzgebungsverfahrens hatte die EU-Kommission bereits gemahnt, ein Vertragsverletzungsverfahren anzustreben, sollte Deutschland den neuen gemeinsamen Datenschutzstandard durch extensive Auslegung des Verordnungstextes und Nutzung der Öffnungsklauseln unterwandern.

Es darf davon ausgegangen werden, dass Rechtssicherheit erst nach zähen Gerichtsverfahren zu erwarten ist. Die teilweise uneinheitlichen Formulierungen des Verordnungsgebers könnten bis dahin zu graduellen Unterschieden bezüglich des gemeinsamen Standards in den Mitgliedstaaten führen, wenn in den nächsten Monaten mehr und mehr nationale Anpassungsgesetze vorgelegt werden. Entwürfe eines irischen und eines österreichischen Anpassungsgesetzes liegen bereits vor.

Quelle: cr-online.de; parlament.gv.at; justice.ie; heise.de

EU
Anhaltende Kritik am Entwurf der ePrivacy-Verordnung

Die EU-Kommission wird für den im Januar vorgelegten Entwurf der ePrivacy-Verordnung weiterhin erheblich kritisiert. Während unklare Schutzkonzepte, unpraktikable Einwilligungsvorbehalte und Widersprüche im Verordnungstext sowie im Gesamtgefüge mit der Datenschutz-Grundverordnung beklagt werden, beginnen Diensteanbieter zu realisieren, welche erheblichen Konsequenzen der Entwurf für digitale Geschäftskonzepte haben könnte.

Unterdessen versucht der Europäische Gesetzgeber den Trilog voranzutreiben, um eine rechtzeitige Verabschiedung der Verordnung nicht zu gefährden. Derzeit sind das Europäische Parlament und der Rat der Europäischen Union mit dem Entwurf befasst. Die Abstimmung im Parlamentsausschuss ist für Oktober diesen Jahres avisiert. Die Maltesische Ratspräsidentschaft hat den Zwischenstand der Diskussionen in einem Bericht zusammengefasst, in dem neben dem strengen Zeitplan auch der weite sachliche Anwendungsbereich, das Konzept der Erlaubnistatbestände und die Regelungen zur browser-gestützen Einwilligung für Cookies kritisiert werden.

Von privater Seite wenden sich europäische Verlage in einem offenen Brief an die Europäische Union. Sie beklagen die geplanten restriktiven Regelungen zum Tracking und zur Verarbeitung von Nutzungsdaten, die zukünftig unter einem weitreichenden Einwilligungsvorbehalt stehen soll. Diese Regelung benachteilige Verlage in Europa gegenüber den großen Plattformen, die es im Gegensatz zu den hiesigen Publishern relativ einfach hätten, von ihren ständig eingeloggten Nutzern entsprechende Einwilligungen einzuholen und auf dieser Grundlage individualisierte Inhalte und Werbung auszuspielen. Auf den Verlagsseiten würden stattdessen weiterhin ein Großteil der Nutzer ohne vorherigen Login und eigenen Account Inhalte konsumieren. Ein Wegfall der Möglichkeit Werbung auf Grundlage von Nutzungsdaten zu individualisieren könne die Finanzierung des digitalen Journalismus gefährden. Die Verlage sprechen sich daher gegen das browser-gestützte Einwilligungskonzept und die restriktive Handhabe von Third Party Cookies aus.

Quelle: delegedata.de; cr-online.de; consilium.europa.eu; theguardian.com.

D
Gemeinsamer Single Sign-On deutscher Konzerne geplant

Mehrere deutsche Konzerne planen den Aufbau einer gemeinsamen Single Sign-on-Plattform, die Nutzer sicher authentifizieren soll und dann bei allen angeschlossenen Diensten eine Nutzung ermöglicht. Allianz, Axel Springer, Daimler, die Deutsche Bank-Tochter Postbank und der Kartendienst Here versprechen sich von dem gemeinsamen Konzept, das unter anderem von dem IT Think-Tank Core entwickelt wird, Registrierungsvorgänge nutzerfreundlich und zugleich signifikant sicherer gestalten zu können.

Das Authentifizierungsmodell soll die eID-Funktion des neuen Personalausweises nutzen, die nach dem Willen des Gesetzgebers nunmehr zukünftig standardmäßig freigeschaltet sein soll, um für eine bessere Verbreitung der eID-Funktion zu sorgen. Die Interoperabilität mit anderen nationalen Identifizierungssystemen soll gemäß der eIDAS-Verordnung sichergestellt werden. Die Plattform soll zudem offen ausgestaltet sein und die Möglichkeit bieten, weitere Partner aufzunehmen und zusätzliche Funktionen anzubinden. Denkbar seien beispielsweise auch e-Government-Dienste, digitale Finanzdienstleistungen, Bezahldienste und Datenaustausch-Services, die somit unter höchsten Sicherheits- und Datenschutzstandards realisiert werden könnten.

Die Automobilwirtschaft könnte zukünftig sowohl Mobilitätsdienste als auch das Leasing- und Finanzierungsgeschäft der Autobanken über die Plattform anbieten. Das Konsortium möchte ausdrücklich eine sichere und zugleich progressive europäische Alternative zu den bestehenden Plattformen realisieren. Eine entsprechende gemeinsame Plattform hätte für die teilnehmenden Unternehmen auch den Vorteil, dass sich die aus der ePrivacy-Verordnung ergebenden Herausforderungen für die Einholung von Einwilligungen

besser meistern ließen. Ein bislang nicht medienwirksam platzierter Nutzen könnte daher auch ein plattformübergreifendes Konzept für die werbliche Verwendung von Nutzungsdaten sein.

In der zweiten Jahreshälfte 2018 könnte das Projekt Marktreife erreichen, vorausgesetzt die Kartellbehörden haben keine Einwände gegen den Zusammenschluss.

Quelle: coretechmonior.com; faz.net.

♦ US
Gesetzesinitiative zu Durchsuchung von Endgeräten und Cloud-Inhalten bei Grenzkontrollen

Während der vierte Verfassungszusatz der Verfassung der Vereinigten Staaten von Amerika grundsätzlich vor willkürlichen Durchsuchungen schützt, gilt eine entscheidende Ausnahme bei der Einreise in die USA. Die sog. *border search exception* ermöglicht es den Behörden, anlassunabhängig Endgeräte zu durchsuchen, die Entsperrung und Entschlüsselung von Datenträgern zu verlangen sowie ungehindert Nachforschungen in den persönlichen digitalen Accounts anhand der Zugangsdaten zu Onlinediensten anzustellen.

Vertreter der Republikaner und Demokraten haben nun einen Gesetzesentwurf vorgelegt, der die Durchsuchungen unter einen Richtervorbehalt stellt und weitreichende Beweisverwertungsverbote für rechtswidrig erhobene Informationen vorsieht. In einer Zeit, in der die Exekutive in den Vereinigten Staaten bemüht ist, die Grenzen rechtlich und tatsächlich zu schließen, ist die Initiative als Debattenbeitrag zu werten, echte Chancen werden ihr in der gegenwärtigen politischen Situation nicht beigemessen. Der Gesetzesentwurf soll sowohl US-Bürger als auch Reisende darauf aufmerksam machen, dass sich das Vorgehen der Behörden bei der Einreise derzeit erheblich ändert und die Zahl der Durchsuchungen von Endgeräten zunimmt.

Reisende sollten sich dieses Umstandes bewusst sein und sensible Informationen nicht auf Datenträgern in die USA einführen sowie erwägen, Cloud-Dienste während der Reisezeit von den mitgeführten Endgeräten zu entkoppeln. Auch Passwortsafes können von den Ermittlungsbefugnissen betroffen sein. Der Gesetzesentwurf würde an der Ermittlungspraxis gegenüber Reisenden überdies nichts ändern, da er lediglich US-Staatsbürger und Personen mit festem Wohnsitz in den USA schützen soll.

Hierzulande hat das Bundeskabinett unlängst den Gesetzesentwurf zur besseren Durchsetzung der Ausreisepflicht beschlossen und im Asylgesetz insbesondere die Möglichkeit geschaffen, mitgeführte Endgeräte zum Zweck der Identitätsfeststellung zu durchsuchen. Die Befugnisse dürfen indes nur angewandt werden, wenn keine gültigen Dokumente mitgeführt werden oder wenn der Einreisende an der Identitätsfeststellung nicht mitwirkt.

Quelle: arstechnica.com; senate.gov; netzpolitik.org.

Kritik, Anregungen oder Hinweise auf interessante Entscheidungen gern an mueller-peltzer@pingdigital.de

Österreich: Entwurf des Datenschutz-Anpassungsgesetzes 2018 – zwischen Evolution durch die Union und Tradition!

Dr. Max W. Mosing, LL.M, LL.M.

Mehr als ein Jahr nach dem Beschluss der Datenschutz-Grundverordnung und knapp ein Jahr vor deren Geltung wurde nunmehr ein Entwurf zum österreichischen Datenschutz-Anpassungsgesetz 2018[1] (in der Folge unscharf „(neues) Datenschutzgesetz – DSG") in die Begutachtung versendet. Der Entwurf sieht eine – mehr oder weniger – „Minimalumsetzung" vor, überlässt aber Weiteres der möglichen Materien-Gesetzgebung. Dazu ist auch festzuhalten, dass – so wie schon die DSGVO – der Entwurf keine Abgrenzung der Anwendbarkeit der nationalen Datenschutzgesetze der EU-Mitgliedstaaten regelt; Folge könnte sein, dass mehrere, unter Umständen nicht kompatible Datenschutzregelungen anwenbar werden.

I. DSG soll DSGVO und DSRL zu Straftaten umsetzen

Während die notwendige Durchführung der DSGVO überwiegend im neuen DSG erfolgen soll, sollen „Öffnungsklauseln" nur zu einem geringen Teil direkt im DSG geregelt bzw. sollen diese bewusst nicht geregelt werden. Der überwiegende Teil der Öffnungsklauseln fällt jedoch nicht in den Bereich der allgemeinen Angelegenheiten des Datenschutzes, sodass der Entwurf es den spezifischen Materiengesetzen überlässt, unter Umständen von der Möglichkeit der Öffnung Gebrauch zu machen.

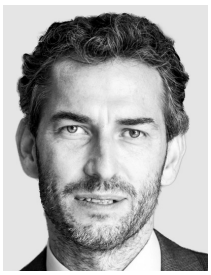
Der Entwurf des neuen DSG soll auch die – am gleichen Tag wie die DSGVO beschlossene – Datenschutz-Richtlinie zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung umsetzen.

Neben der Durchführung bzw. Umsetzung der beiden Unionsrechtsakte soll auch weiterhin ein Grundrecht auf Datenschutz in angepasster Form im DSG verankert werden.

II. Evolution durch die Union

1. Österreichweites neues DSG

Derzeit regelt das bundesweite DSG „nur" den Datenschutz im automationsunterstützten Datenverkehr; Datenschutz hinsichtlich manueller personenbezogener Dateien obliegt den neun Bundesländer-Gesetzgebern. Letzteres erwies sich zwar schon seit der Datenschutzrichtlinie 95/46/EG als unzweckmäßig, doch soll erst jetzt ein österreichweit einheitliches DSG für beide Bereiche entstehen. Unabhängig davon sollen spezifische datenschutzrechtliche Regelungen weiterhin auf die Kompetenztatbestände der jeweiligen Materie – also sowohl auf Bundes- als auch auf Landesebene – gestützt werden („materienspezifischer Datenschutz als Annexmaterie").



Dr. Max W. Mosing, LL.M. (IT-Law Wien), LL.M. (Strathclyde), Partner bei der auf IP/IT-Recht spezialisierten Kanzlei GEISTWERT Rechtsanwälte Lawyers Avvocati, Wien

2. Datenschutzbeauftragter

Da der verpflichtende Datenschutzbeauftragte schon in vergangenen Entwürfen zu Novellen des DSG vorgesehen war, aber politisch scheiterte, erwarteten viele Beobachter, dass der Entwurf zum neuen DSG eine Erweiterung der verpflichtenden Bestellung gegenüber der DSGVO bringen würde. Dies sieht der Entwurf aber nicht vor; sondern er regelt „nur" besondere gesetzliche Geheimhaltungsverpflichtungen und Aussageverweigerungsrechte. Weiters

1 Der Entwurf und weitere Dokumente sind abrufbar unter: https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00322/index.shtml.

sollen Datenschutzbeauftragte im Bereich der Bundesministerien verpflichtet werden, einen regelmäßigen Erfahrungsaustausch zu pflegen, insbesondere im Hinblick auf die Gewährleistung eines einheitlichen Datenschutzstandards.

3. Datenschutzbehörde als inquisitorische Strafbehörde

Die zahlreichen Melde- und Vorabgenehmigungspflichten bei der Datenschutzbehörde fallen – mit in der Regel nicht relevanten Ausnahmen – mit 25. Mai 2018 weg. Die Datenschutzbehörde soll als nationale unabhängige Aufsichtsbehörde und auch einzige nationale Akkreditierungsstelle (i. S. d. Art. 43 Abs. 1 lit. a) DSGVO) eingerichtet werden. Nach dem Entwurf soll die Datenschutzbehörde (weiterhin) nur im Fall „*eines begründeten Verdachtes auf Verletzung*" entsprechende Datenverarbeitungen überprüfen können. Es würde also (weiterhin) eines entsprechend begründeten Anfangsverdachts bedürfen, damit die Datenschutzbehörde überhaupt auditieren darf. Andererseits soll ihr die Zuständigkeit der Verhängung von Geldbußen sowohl gegenüber juristischen Personen – und deren Organen und verantwortlichen Beauftragten – als auch gegenüber natürlichen Personen zukommen. Gegen Behörden und öffentliche Stellen sollen aber keine Geldbußen verhängt werden können.

Jede betroffene Person wird das Recht auf Beschwerde bei der Datenschutzbehörde haben, wobei der Beschwerdegegner bis zum Abschluss des Verfahrens „tätige Reue" zeigen können soll, indem er den Anträgen des Beschwerdeführers entspricht. Erscheint der Datenschutzbehörde die Beschwerde dann als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören und aufmerksam zu machen, dass sie das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Die Datenschutzbehörde kann stets – soweit erforderlich – Amtssachverständige im Verfahren beiziehen. Erwähnenswert ist auch, dass der Beschwerdeanspruch erlöschen soll, wenn er nicht binnen eines Jahres nach Kenntnis, längstens aber binnen dreier Jahre geltend gemacht wird.

4. Schadenersatz, Gerichtszuständigkeit und Verbandsklagen

Jede Person, der wegen eines Verstoßes ein materieller oder immaterieller Schaden entstanden ist, soll Anspruch auf Schadenersatz nach Art. 82 DSGVO gegen den Verantwortlichen oder gegen den Auftragsverarbeiter haben. Für diesen Schadenersatzanspruch sollen die allgemeinen Bestimmungen des bürgerlichen Rechts gelten. Letzteres erscheint insoweit inkonsistent, als das österreichische Schadenersatzrecht im Allgemeinen keinen immateriellen Schadenersatz kennt.

Für Klagen auf Schadenersatz soll in erster Instanz sowohl das Landesgericht zuständig sein, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat, als auch jenes des Sprengels des Beklagten. Neu ist auch, dass – im Zweifel von der Datenschutzbehörde „festgestellte" – Datenschutz-Interessensverbände in diesen Verfahren vertretungsbefugt sein sollen.

III. Tradition

Gestützt auf Art. 6 Abs. 2 DSGVO, wonach spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO möglich sind, sieht der Entwurf zum neuen DSG vor, bereits im heutigen DSG Geregeltes insbesondere (i) zu besonderen Verwendungszwecken bzw. (ii) zur Videoüberwachung „aufrechtzuerhalten".

1. Grundrecht auf Datenschutz

Das Grundrecht auf Datenschutz mit Drittwirkung – also nicht nur gegenüber dem Staat, sondern auch zwischen Privaten – soll im Verfassungsrang verankert bleiben. Der Text soll leicht angepasst lauten wie folgt: „*Jede natürliche Person hat Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten, auf Auskunft über die Verarbeitung solcher Daten sowie auf Richtigstellung unrichtiger Daten und auf Löschung unzulässigerweise verarbeiteter Daten.*" Im Lichte des grundrechtlich abgesicherten „Datenverarbeitungsverbots mit Erlaubnisvorbehalt" soll Letzterer auch im Verfassungsrang abgebildet werden, nämlich: „*Beschränkungen sind nur mit Einwilligung der betroffenen Person, in dessen lebenswichtigem Interesse, im öffentlichen Interesse, und zwar nur aufgrund einer gesetzlichen Grundlage, oder im überwiegenden berechtigten Interesse eines anderen zulässig. Diese Beschränkungen müssen notwendig und verhältnismäßig und* (...) *für die betroffene Person vorhersehbar sein.* (...)".

2. Datengeheimnis und Freiheitsstrafe

„Aufrechterhalten" soll auch die Verpflichtung zum Datengeheimnis und die angedrohte Freiheitsstrafe von bis zu einem Jahr (oder Geldstrafe bis zu 720 Tagessätzen) bei dessen vorsätzlichem Bruch in Gewinn- bzw. Schädigungsabsicht werden. Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, geheim zu halten, soweit kein rechtlich zulässiger Grund „(...) *für eine Übermittlung* (...)" besteht (Datengeheimnis). Im Entwurf wurde offensichtlich übersehen, dass es den im derzeitigen DSG definierten Begriff der „Übermittlung" in Zukunft nicht mehr geben wird. Derzeit ist die Übermittlung nämlich die Weitergabe von Daten, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet.

Erwähnenswert ist auch, dass derzeit im DSG bestehende „Begleitverwaltungsstraftatbestände" weiter bestehen bleiben sollen. Eine (neu: durch die Datenschutzbehörde) mit Geldstrafe bis zu 50.000 Euro zu ahndende Verwaltungsübertretung würde begehen, wer (i) sich vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält, (ii) Daten vorsätzlich in Verletzung des Datengeheimnisses übermittelt, (iii) sich unter Vortäuschung falscher Tatsachen vorsätzlich personenbezogene Daten im Katastrophenfall verschafft, (iv) widerrechtlich eine Bildverarbeitung (siehe unten) betreibt oder (v) der Datenschutzbehörde die Einschau verweigert. Auch soll weiterhin die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten ausgesprochen werden können.

3. „Zeitliche Erleichterung" bei Löschung

Da eine Entscheidung des Obersten Gerichtshofs beim berechtigten Löschungsantrag die „sofortige physische" Löschung in allen Systemen gefordert hatte, wurde vom Gesetzgeber das derzeitige DSG angepasst und soll auch in Zukunft eine „zeitliche Erleichterung" bei Berichtigung und Löschung als Durchführungsbestimmung „aufrecht" bleiben: Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt einzuschränken.

4. Abgrenzung des öffentlichen Bereichs

Dem derzeitigen DSG treu bleibt der Entwurf auch hinsichtlich der Abgrenzung des öffentlichen vom privaten Bereich. Verantwortliche des öffentlichen Bereichs sollen (auch in Zukunft) Verantwortliche sein, die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

5. Nichts Neues im Beschäftigungskontext

Der Entwurf sieht keine Änderungen im „Arbeitnehmerdatenschutzrecht" gegenüber der derzeitigen Rechtslage vor. Es soll bei den derzeitigen Regelungen zu Betriebsvereinbarungen zwischen Geschäftsführung und Betriebsrat, insbesondere bei der über das gesetzlich Notwendige hinausgehenden Datenverarbeitung im Beschäftigungskontext (mit Ausnahme der leitenden Angestellten), bleiben.

6. Bildverarbeitung

Der Entwurf will auch die derzeitigen Sonderbestimmungen zur Videoüberwachung im Abschnitt „*Bildverarbeitung*" weiter – wenn auch in angepasster Form – bestehen lassen, nämlich hinsichtlich der eingeschränkten Zulässigkeit, *per se*-Verboten, besonderer Datensicherheitsmaßnahmen und der Kennzeichnung.

NIS-Richtlinie und IT-Sicherheitsgesetz in 2017

Simone Rosenthal und *Frank Trautwein*

Globale Cyberangriffe wie die WannaCry-Ransomware sollten als letztes Warnsignal verstanden werden. Ohne supranationale Zusammenarbeit und zwingende Meldepflichten sind Angriffen auf globale IT-Infrastrukturen und der Verbreitung von Viren keine Grenzen gesetzt. Einen durchaus sinnvollen Anfang machte der deutsche Gesetzgeber bereits mit dem IT-Sicherheitsgesetz im Bereich kritischer Infrastrukturen (KRITIS). Auf europäischer Ebene folgte die NIS-Richtlinie, die einen einheitlichen Rechtsrahmen zur Stärkung der Cybersicherheit in der EU vorsieht. Trotz bestehender Gesetze im Bereich IT-Sicherheitsrecht, ist auch Deutschland von erweiterten Anpassungserfordernissen betroffen, die ähnlich der DSGVO bis Mai 2018 in nationales Recht umzusetzen sind. Die Bundesregierung brachte im Zuge dessen Anfang des Jahres einen ersten Gesetzesentwurf auf den Weg. Im Nachfolgenden soll ein aktueller Überblick der bestehenden Regelungen im Bereich IT- und Cybersicherheit gewährt werden.

I. Bisheriger Stand

Als früher Startpunkt dient zunächst die gesetzlich normierte Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, gültig vom 01. 01. 1991 bis 19. 08. 2009). Darauffolgend wurden dem BSI mit dem am 20. August 2009 in Kraft getretenen Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz) erweiterte Befugnisse eingeräumt, um Bedrohungen für die IT-Sicherheit in Deutschland frühzeitig zu erkennen und eine zentrale Meldestelle auszubauen. Die Befugnisse des BSI als Meldestelle waren dennoch nur präventiver Natur. Größere Änderungen erfuhren das BSI-Gesetz und die nationale Cybersicherheit sodann mit dem am 25. Juli 2015 in Kraft getretenen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Das IT-Sicherheitsgesetz nimmt als sogenanntes Artikelgesetz Änderungen und Ergänzungen in anderen Gesetzen vor, neben dem BSI-Gesetz etwa auch im Energiewirtschaftsgesetz, TKG, TMG und SGB.

Der europäische Vorstoß zur sogenannten NIS-Richtlinie lief demgegenüber in der Vergangenheit eher langsam voran: Das EU-Parlament und der Europäische Rat hatten zum Zeitpunkt des in Kraft getretenen IT-Sicherheitsgesetzes gerade einmal die letzte Trilog-Verhandlung abgeschlossen. Ein gutes Jahr später als das IT-Sicherheitsgesetz wurde am 19. Juli 2016 schließlich die lang erwartete Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen

Simone Rosenthal ist Rechtsanwältin und Partnerin bei Schürmann Wolschendorf Dreyer RAe sowie Geschäftsführerin der ISiCO Datenschutz GmbH.

Frank Trautwein ist auf Rechtsinformatik spezialisiert und als Jurist sowie zertifizierter Lead Auditor (ISO 27001) für die ISiCO Datenschutz GmbH tätig. In dieser Funktion unterstützt er Unternehmen als externer Datenschutz- und IT-Sicherheitsbeauftragter.

gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen – die NIS-Richtlinie – im Amtsblatt der EU veröffentlicht. Im August 2016 trat das Gesetz in Kraft, wobei die Umsetzung in nationales Recht gemäß Art. 25 Abs. 1 NIS-Richtlinie bis zum 9. Mai 2018 erfolgen muss.

1. Europäische Ebene

Die NIS-Richtlinie ist Teil der europäischen Cyber-Sicherheitsstrategie der EU, mit der man das Ausmaß von Hackerangriffen sowie technischen Ausfällen begrenzen möchte. Nach Einschätzungen der ENISA *(European Union Agency for Network and Information Security)* führten diese zuletzt zu Verlusten von 260 bis 340 Milliarden Euro pro Jahr.[1] Zudem soll die diesbezügliche Zusammenarbeit der EU-Mitgliedstaaten verstärkt und gefördert werden. Die konkrete Zielsetzung der europäischen Richtlinie ähnelt teilweise der des IT-Sicherheitsgesetzes: Vorgesehen ist ein hohes Sicherheitsniveau informationstechnischer Systeme, das den Stand der Technik abbildet.

Bei Richtlinien der EU – wie der NIS-Richtlinie – handelt es sich um Rechtsakte, die eine Zielsetzung vorgeben, den Mitgliedstaaten jedoch die Wahl der Mittel überlassen. Ein wichtiger Ausgangspunkt ist die sogenannte Mindestharmonisierung (im Gegensatz zur Vollharmonisierung), die sich in Art. 3 der NIS-Richtlinie manifestiert. Demnach besteht nur dort erneuter Anpassungsbedarf, wo das Mindestschutzniveau der Richtlinie unterschritten wird. Die Cybersicherheit in der EU als Ganzes soll demnach auf einen annehmbaren Stand gebracht werden, denn einzelne, schwache Teilstücke gefährden in vernetzten Infrastrukturen bekanntlich alle.

2. Nationale Ebene

Der deutsche Gesetzgeber ist im Rahmen der europäischen Cyber-Sicherheitsstrategie – also derselben rechtsdogmatischen Grundlage, der auch die NIS-Richtlinie folgt – mit dem IT-Sicherheitsgesetz gegenüber anderen europäischen Staaten bereits in Vorleistung getreten. Durch die enge Ausrichtung an der europäischen Strategie und des laufenden Trilogs zur NIS-Richtlinie sind viele der europäischen Vorgaben bereits im IT-Sicherheitsgesetz enthalten. Weitergehende, noch erforderliche Anpassungen erfolgen anhand nationaler Umsetzungsgesetze. Auf den Entwurf des deutschen Umsetzungsgesetzes soll im zweiten Abschnitt genauer eingegangen werden.

> „Vorgesehen ist ein hohes Sicherheitsniveau informationstechnischer Systeme, das den Stand der Technik abbildet."

3. Unterschiede und Gemeinsamkeiten

In vielen Punkten gleichen sich die Regelungen, etwa bei der obligatorischen Meldung von Sicherheitsvorfällen und der Einhaltung von Sicherheitsanforderungen (Stichwort: Verhältnismäßigkeit). Der Anwendungsbereich des IT-Sicherheitsgesetzes erstreckte sich zuvorderst auf „kritische Infrastrukturen" (KRITIS), während die NIS-Richtlinie nur von „wesentlichen Diensten" spricht. Gemeint sind aber in erster Linie besonders gefährdete Bereiche, die einerseits wichtige Dienstleistungen für das Gemeinwohl bereitstellen und zugleich aufgrund einer weitreichenden Vernetzung einer besonderen Bedrohungslage ausgesetzt sind, im Einzelnen:

„Betreiber wesentlicher Dienste"
(gemäß Anhang II der NIS-Richtlinie[2])
- Energie (Elektrizität, Erdöl, Erdgas)
- Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr)
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen (einschließlich Krankenhäuser und Privatkliniken)
- Trinkwasserlieferung und -Versorgung
- Digitale Infrastruktur

„Betreiber kritischer Infrastrukturen"
(gemäß § 2 Abs. 10 BSI-Gesetz; konkretisiert durch den 1. Teil der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz[3])
- Energie (Elektrizität, Gas, Kraftstoff und Heizöl, Fernwärme)
- Informationstechnik und Telekommunikation (Sprach- und Datenübertragung, Datenspeicherung und -verarbeitung)
- Transport und Verkehr
- Gesundheit
- Wasser (Trinkwasserversorgung und Abwasserbeseitigung)
- Ernährung (u. a. Lebensmittelversorgung)
- Finanz- und Versicherungswesen

An anderer Stelle fordert die NIS-Richtlinie die Einrichtung nationaler Behörden, um den neuen europarechtlichen Anforderungen an die IT-Sicherheit Herr zu werden. Deutschland ist mit dem Bundesamt für Sicherheit in der Informationstechnik bereits gut aufgestellt. Anders als im IT-Sicherheitsgesetz finden sich aber verbindliche Regelungen zu sogenannten Computer Security Incident Response Teams (CSIRTs) und deren Vernetzung untereinander. Auf nationaler Ebene hat sich der CERT-Bund als zentrale Anlaufstelle für IT-Notfallteams in Unternehmen bewährt. Auf internationaler Ebene wird weitergehender Austausch gefordert, der bisher – etwa mit Blick auf die WannaCry-Ransomware – noch mehrheitlich auf inoffiziellen Kommunikationskanälen funktioniert. Neuerungen können sich im Zuge der NIS-Richtlinie für Unternehmen ergeben, die als „digitale Dienste" gelten. Ob Online-Händler, Suchmaschinen oder Cloud-Dienste, bei Überschreitung bestimmter Schwellenwerte (Kleinst- und Kleinunternehmen sind ausgeschlossen), sind verpflichtend Sicherheitsvorfälle zu melden und z. B. das Notfallmanagement um Business Continuity Maßnahmen zu erweitern. Das IT-Sicherheitsgesetz kennt die obligatorische Meldung bisher nur bei den Betreibern kritischer Infrastrukturen und wird auch bei den Maßnahmen nicht konkreter. Ziel soll die Schaffung einer Kultur des Risikomanagements sein. Betroffene Unternehmen, die bereits risikobasierte Managementsysteme einsetzen, etwa ein ISMS nach ISO 27001, werden aber auch hier keine größeren Überraschungen erleben.

II. Nationales Umsetzungsgesetz

Auf nationaler Ebene wurde am 27. Januar 2017 der erste Gesetzentwurf[4] zur Umsetzung der NIS-Richtlinie veröffentlicht, der sodann am 27. April 2017 vom Bundestag

1 Der aktuelle „Threat Landscape Report" der ENISA ist abrufbar unter: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport.

2 Abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L1148&from=DE.

3 Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/BSI_Kritis_VO.pdf?__blob=publicationFile&v=3.

4 Abrufbar unter: https://www.bundesrat.de/SharedDocs/drucksachen/2017/0001-0100/64-17.pdf?__blob=publicationFile&v=5.

mit lediglich einer kleineren Änderung[5] beschlossen wurde. Im vorliegenden Entwurf wird explizit vermerkt, dass gerade im Bereich KRITIS wenige Anpassungen erforderlich sind, da das IT-Sicherheitsgesetz – wie auch bereits angedeutet – ausreichende sicherheitstechnische Regelungen vorgibt, die sich mit den Anforderungen der NIS-Richtlinie decken oder diese sogar übertreffen (etwa im Bereich Versicherungswesen und Abwasserbeseitigung).

1. Digitale Dienste

Mit großem Interesse blickte die Security-Community auf den Umgang „digitaler Dienste", die bisher aufgrund nicht eindeutiger Begriffsbestimmungen noch einige Unklarheiten aufwiesen. Die Bundesregierung folgt hier gemäß Art. 1 jedoch den Vorgaben und zudem auch der Definition der NIS-Richtlinie, womit nach wie vor die nachfolgenden Kategorien als „digitale Dienste" verstanden werden:

- Online-Marktplätze
- Online-Suchmaschinen
- Cloud-Computing-Dienste

Die Anbieter „digitaler Dienste" stellen erhöhte Anforderungen hinsichtlich der technischen und organisatorischen Ausgestaltung der unternehmensinternen IT-Sicherheit. Folgende Aspekte sollen beim Schutz der IT-Infrastrukturen und -Systeme dabei besonders berücksichtigt werden:

- die Sicherheit der Systeme und Anlagen,
- die Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen (SIM),
- das Betriebskontinuitätsmanagement (BCM),
- die Überwachung, Überprüfung und Erprobung,
- die Einhaltung internationaler Normen.

Die vielfach geforderten dahingehenden Klarstellungen und Konkretisierungen sind jedoch im Umsetzungsgesetz – abseits allgemeiner Regelungen – nicht enthalten. Der Gesetzgeber verweist hier auf zukünftige, noch ausstehende Rechtsakte der EU-Kommission: *„Die notwendigen Maßnahmen werden durch Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 näher bestimmt".*

2. Neuerungen

Maßgebliche Neuerungen finden sich im Rahmen erweiterter Befugnisse des BSI. Allen voran wird die operative Gefahrenabwehr nun zentraler Bestandteil des BSI, indem sogenannte **Mobile Incident Response Teams** geschaffen, wie auch von der Cyberstrategie der EU gefordert *(siehe CSIRTs)*. Hiernach kann das BSI in besonders schweren Fällen („herausgehobene Fälle") erstmals selbst aktiv tätig werden und z. B. ein Telekommunikationsunternehmen bei der Wiederherstellung der IT-Infrastruktur unterstützen oder technische Vor-Ort-Beratung eines Krankenhauses leisten, das von einer schädlichen Ransomware wie WannaCry betroffen ist.

Betreiber von KRITIS müssen sich mit zusätzlichen Anforderungen im Bereich der **Meldepflichten** auseinandersetzen, wonach bei tatsächlichen Ausfällen oder erheblichen Beeinträchtigungen der Infrastruktur zukünftig alle verantwortlichen IT-Störungen gemeldet werden müssen. Erhebliche Störungen der IT-Infrastruktur sind dann zu melden, wenn ein Ausfall oder eine erhebliche Beeinträchtigung droht. Wie von der europäischen Richtlinie zur Verbesserung der Zusammenarbeit gefordert, kann zukünftig ein internationaler Austausch von Sicherheitsmeldungen stattfinden, da die deutschen Behörden entsprechende Vorfälle laut Gesetz unter bestimmten Bedingungen an europäische Behörden weiterleiten (dürfen).

KRITIS-Betreiber treffen zudem nochmals **erweiterte Nachweispflichten.** Das BSI kann derzeit die KRITIS-Betreiber nur dann überprüfen, sofern Mängel nachgewiesen werden. Nach Art. 15 der NIS-Richtlinie sollte dies unabhängig hiervon möglich sein. Im Zuge der NIS-Richtlinie und des nationalen Umsetzungsgesetzes ist es deshalb erforderlich, entsprechende Audits, Prüfungen oder Zertifizierungen (einschließlich der dabei aufgedeckten Sicherheitsmängel) jederzeit vorlegen zu können. Informationssicherheitsmanagement-Systeme (ISMS) werden hier nach wie vor eine gute Grundlage für eine revisionssichere Dokumentation und Auditierung bieten. Maßgeblich ist damit einhergehend jedoch die neue Befugnis des BSI, die KRITIS-Einrichtungen zur Begutachtung der vorgenannten Dokumentationen und Nachweise aufzusuchen und somit einen **Kontrollbesuch** (ähnlich der datenschutzrechtlichen Aufsichtsbehörde durchzuführen. Der Gesetzgeber sieht in dieser Maßnahme – die auch von BSI-zertifizierten IT-Sicherheitsdienstleistern, Penetrationstestern oder Grundschutz-Auditoren durchgeführt werden kann – eine gleichwohl geringere Belastung als die entfernte Vorlage vollumfänglicher (interner) Dokumentationen.

5 Abrufbar unter: http://www.bundesrat.de/SharedDocs/drucksachen/2017/0301-0400/335-17.pdf?__blob=publicationFile&v=1.

STIFTUNG DATENSCHUTZ

Aus Sicht der Stiftung Datenschutz – Datenschutz – kein Wahlkampfschlager (?)

Frederick Richter, LL. M.

Das Thema Datenschutz gehört zu den Themen, die in jedem Wahlprogramm irgendwie und irgendwo vorkommen, jedoch fast nie fettgedruckt und weit vorne platziert. In diesem Jahr, mit drei Landtagswahlen und der kommenden Wahl im Bund, fällt dies einmal mehr auf. Ansatzpunkte zur Positionierung und Differenzierung gäbe es gleichwohl genug.

Angesichts der notorischen personellen Unterausstattung nahezu sämtlicher Landesdatenschutzbehörden wäre es zum Beispiel zu erwarten, dass interessierte politische Kräfte eine massive Aufstockung derer Kapazitäten fordern – erst recht angesichts neuer Aufgaben aus der EU-Datenschutzreform. Fundierte Empfehlungen seitens der Wissenschaft liegen vor. So hat *Prof. Roßnagel* von der Universität Kassel Anfang des Jahres in einer Studie den allein durch die DSGVO entstehenden zusätzlichen Personalbedarf bei den Landesaufsichten auf jeweils zwischen 24 und 33 Stellen geschätzt.[1] Am Beispiel von Nordrhein-Westfalen zeigt sich, dass die tatsächliche Personalausstattung hinterherhinkt. So wurden zur Anpassung an die neuen europäischen Regelungen gerade einmal neun neue Stellen geschaffen.[2]

Wenn sich die Datenschutzaufsicht nicht nur als sanktionierende Exekutivgewalt, sondern gleichfalls als Beraterin der von der Datenschutz-Grundverordnung betroffenen Unternehmen versteht, dann ist das zu wenig.

Es gäbe viel zu fordern

Aufgegriffen wurde dieser offensichtliche Missstand zu den Landtagswahlen dieses Jahres derweil kaum, wie eine exemplarische Betrachtung der zurückliegenden Wahlen im bevölkerungsreichsten Bundesland zeigt. So taucht der Datenschutz bei der CDU als Wahlgewinnerin von Nordrhein-Westfalen im Wahlprogramm als eigener Punkt gar nicht erst auf. Er wird lediglich am Rande erwähnt – wenn es darum geht, inwieweit den Kommunen eine Videoüberwachung im öffentlichen Raum ermöglicht werden könne.[3] Bei der SPD als zweitplatzierter Partei wird der Datenschutz im Wahlprogramm zumindest angeführt, wenn es um die Rahmenbedingungen der digitalen Wirtschaft geht: „Wenn große Datenmengen immer mehr über wirtschaftlichen Erfolg und Misserfolg entscheiden, gewinnen auch Datensicherheit und Datenschutz eine immer größere Bedeutung“.[4] Außerdem wollten die Sozialdemokraten „eine datenschutzrechtliche Strategie auf den Weg bringen, um Cyber-Spionage besser zu verhindern“.[5]

Frederick Richter ist Ständiger Autor bei „Privacy in Germany“. Seit Anfang 2013 leitet er die in Leipzig ansässige Bundesstiftung für Privatheit und Datenschutz. *(Foto: Lorenz Becker)*

Ein Thema der Kleinen?

Bei den kleineren Parteien ergibt sich am Beispiel von Nordrhein-Westfalen ein gemischtes Bild: Die AfD erwähnt den Datenschutz nicht gesondert; lediglich beim geforderten Erhalt des Bargeldes wird er im Wahlprogramm 2017 als Stichwort gebracht.[6]

1 Abrufbar unter: www.uni-kassel.de/uni/universitaet/pressekommunikation/neues-vom-campus/meldung/article/studie-zu-eu-datenschutzgrundverordnung-rund-30-neue-stellen-in-jeder-aufsichtsbehoerde-noetig.html.

2 Abrufbar unter: www.datenschutzbeauftragter-online.de/datenschutzbeauftragte-nordrhein-westfalen-glatter-rollenwechsel/10567/.

3 Abrufbar unter: www.cdu-nrw.de/sites/default/files/media/docs/2017-04-01_regierungsprogramm_cdu_fuer_nrw_2017-2022.pdf.

4 Abrufbar unter: www.nrwspd.de/wp-content/uploads/sites/2/2017/03/regierungsprogramm_der_nrwspd.pdf, S. 25.

5 Abrufbar unter: www.nrwspd.de/wp-content/uploads/sites/2/2017/03/regierungsprogramm_der_nrwspd.pdf, S. 27.

6 Abrufbar unter: https://cdn.afd.tools/sites/2/2017/03/24145045/LWP_Komplettprogramm_AK9_RZ_Low.pdf.

Die FDP wird schon konkreter. Sie warb u. a. schon in den vorangestellten Kernpunkten ihres Landtagswahlprogrammes mit einem „NRW-Datenschutzsiegel“ zur Verbesserung von Datenschutzstandards in Unternehmen.[7] In einem ganzen Kapitel geht es dann um „Bürgerrechte und Datenschutz“, wo man sich gegen die Vorratsdatenspeicherung und für mehr Aufklärungsmaßnahmen ausspricht.[8]

Die GRÜNEN schließlich widmeten zur NRW-Wahl dem Datenschutz den meisten Raum im Programm, an diversen Stellen wird er erwähnt und in andere Forderungen einbezogen. In einem eigenen Kapitel wird zudem auf den Erfolg einer gestärkten Aufsichtsbehörde hingewiesen.[9]

Eine geringe Priorität des Themas im Wahlkampfangebot wäre dann folgerichtig, wenn es auf der Nachfrageseite – sprich: bei den Bürgerinnen und Bürgern – ebenfalls keine große Rolle spielte. Auch, wenn es viele der die Bürgerrechte engagiert Verfechtenden kaum wahrhaben wollen: Es stimmt anscheinend.

Angebot und Nachfrage

Der Wahlausgang erlaubte zwar keine klare Bewertung aus einer auf Datenschutzthemen zentrierten Sicht. Doch lässt sich – einmal eingegrenzt auf dieses Thema – festhalten, dass die GRÜNEN *trotz* starker Datenschutzbetonung verloren haben und die CDU *trotz* fehlender Datenschutzbetonung gewonnen hat. Auch wenn das tatsächliche Abschneiden der politischen Parteien bei Wahlen hauptsächlich andere Gründe haben mag: Fast scheint es, als nützt das Thema beim Werben um Wähler ebenso wenig wie eine Auslassung dort schadet. Seien wir also gespannt auf die Bundestagswahl. Noch ist nicht bekannt, welche Themen die Agenda in der heißen Wahlkampfphase bestimmen werden. Doch Hellseher brauche ich nicht zu sein, um zu wissen, dass es der Datenschutz ganz sicher nicht sein wird – selbst wenn in wenigen Wochen ein neuer *Edward Snowden* die Weltbühne beträte. Es ginge dann nämlich das Angebot an der Nachfrage vorbei. Umfragen zufolge sind das Flüchtlingsthema und die innere Sicherheit beherrschend; Datenschutz läuft gewohntermaßen unter „Sonstiges“.[10]

Compliance im Wahlkampf

Wenn es aber darum geht, die wahlentscheidenden Themen rechtskonform zu bewerben, dann hat der Datenschutz alle zu interessieren – allein schon, um sich nicht angreifbar zu machen. Ob datenpolitische Themen eine Rolle spielen oder nicht: Geltendes Datenschutzrecht muss immer eingehalten werden. Ein „Vorsprung durch Rechtsbruch“ auf Kosten der Privatsphäre wäre sicher kein guter Ausweis wohlverstandener Nähe zu den Bürgerinnen und Bürgern, um deren Stimmen man wirbt.

Als Dialogplattform zwischen Politik, Gesellschaft und Wirtschaft wollen wir daher unseren Teil dazu beitragen, eine Brücke vom oft abstrakt daherkommenden Datenschutzrecht zur Praxis vor Ort zu schlagen. Deswegen haben wir eine übersichtliche Handreichung erstellt, die wir den Abgeordneten des Deutschen Bundestags und den politischen Parteien für den beginnenden Wahlkampf im Bund zur Verfügung stellen. Auch allen anderen Interessierten steht das Informationsmaterial natürlich zum kostenlosen Herunterladen auf unserer Webpräsenz bereit.[11]

7 S. 4; Abrufbar unter: www.fdp.nrw/sites/default/files/2017-05/Landtagswahlprogramm2017.pdf, S. 50.

8 Abrufbar unter: www.fdp.nrw/sites/default/files/2017-05/Landtagswahlprogramm2017.pdf, S. 34f.

9 Abrufbar unter: https://gruene-nrw.de/dateien/wahlprogramm2017.pdf, S. 183.

10 Abrufbar unter: https://de.statista.com/statistik/daten/studie/500465/umfrage/umfrage-zu-den-wichtigsten-politischen-themen-in-deutschland.

11 Abrufbar unter: www.stiftungdatenschutz.org/wahlkampf.

PRIVACY COMPLIANCE

Christian Volkmer ist Geschäftsführender Inhaber der Projekt 29 Unternehmensgruppe und Sachverständiger für Datenschutz und Informationssicherheit.

Ingo Kaiser ist Büroleiter der Projekt 29 GmbH in Regensburg, geschulter Informationssicherheitsbeauftragter und zertifizierter Datenschutzbeauftragter DSB-TÜV.

Das Verzeichnis von Verarbeitungstätigkeiten und die Datenschutz-Folgenabschätzung in der Praxis

Christian Volkmer und *Ingo Kaiser*

I. Verfahrensverzeichnis

1. Rechtslage bis zum 25. Mai 2018

Nach geltendem Recht wird die Transparenz der Datenverarbeitungsprozesse durch Verfahrensverzeichnisse gesichert. Die Führung eines Verfahrensverzeichnisses, wie es in § 4g Abs. 2 S. 1 i. V. m. § 4e S. 1 BDSG beschrieben wird, gehört zu den Kernaufgaben des betrieblichen Datenschutzbeauftragten. Allerdings ist es nicht etwa vom Datenschutzbeauftragten selbst zu erstellen ist, sondern es ist ihm von der verantwortlichen Stelle zur Verfügung zu stellen. In der Praxis sieht das nahezu immer anders aus. Das interne Verfahrensverzeichnis wird quasi immer nur dann erstellt, wenn der Datenschutzbeauftragte diese Informationen bei sämtlichen Ansprechpartnern diverser Abteilungen im Unternehmen zusammengetragen und dokumentiert hat.

Bei den Verfahrensverzeichnissen geht es einerseits um Software, andererseits aber vor allem um Prozesse, beispielsweise um die Verwaltung der Mitarbeiterdaten in der Personalabteilung, Lieferantendatenbanken, die Internetpräsenz des Unternehmens, den Terminkalender z. B. in Outlook oder aber die Lohn- und Finanzbuchhaltung. All diese Verfahren, sprich Tätigkeiten, die personenbezogene Daten erheben, verarbeiten oder nutzen, müssen in einem Verfahrensverzeichnis zumindest grundlegend beschrieben werden. § 4e BDSG schreibt folgende Angaben als „Inhalt der Meldepflicht" vor:

1. *Name oder Firma der verantwortlichen Stelle,*
2. *Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,*
3. *Anschrift der verantwortlichen Stelle,*
4. *Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,*
5. *eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,*
6. *Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,*
7. *Regelfristen für die Löschung der Daten,*
8. *eine geplante Datenübermittlung in Drittstaaten,*
9. *eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.*

Der Unterschied zwischen einem internen und einem öffentlichen Verfahrensverzeichnis – daher auch „Jedermannsverzeichnis" genannt – liegt hauptsächlich im Umfang der Aufstellung und der entsprechenden Verpflichtung, die Inhalte jedermann – also auch Dritten – zugänglich zu machen. Daher ist das öffentliche Verfahrensverzeichnis mindestens um die technischen und organisatorischen Maßnahmen, die nicht für die Augen Jedermanns gedacht sind, bereinigt. Das interne Verfahrensverzeichnis enthält entsprechend umfangreichere Angaben als das öffentliche Verfahrensverzeichnis. Es dient dazu, eine betriebsinterne Selbstkontrolle zu ermöglichen. Das öffentliche Verfahrensverzeichnis andererseits, soll nach außen hin Transparenz über die Datenverarbeitungsvorgänge gewähren. Auf Anfrage ist es im Gegensatz zum internen Verfahrensverzeichnis jedermann zugänglich zu machen. Eine generelle Pflicht zur Veröffentlichung, z. B. auf der Unternehmens-Homepage besteht allerdings nicht.

2. Rechtslage nach der DSGVO

Mit Inkrafttreten der Datenschutz-Grundverordnung ab Mai 2018, ändert sich nicht nur die Bezeichnung. Zum einen bekommt das „Kind" den neuen Namen „Verzeichnis von Verarbeitungstätigkeiten", zum anderen auch einige inhaltlich neue Anforderungen.

Art. 30 Abs. 1 DSGVO listet die Angaben auf, die das Verzeichnis zukünftig enthalten muss:

Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
b) die Zwecke der Verarbeitung;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1".

Die gravierenden Neuerungen im Rahmen der DSGVO sind hier:

- Das Verzeichnis von Verarbeitungstätigkeiten muss nur noch der Aufsichtsbehörde zur Verfügung gestellt werden. Somit fällt bei Inkrafttreten der DSGVO die Pflicht zur Führung eines öffentlichen Verfahrensverzeichnisses weg.
- Die Verpflichtung, ein Verzeichnis von Verarbeitungstätigkeiten führen zu müssen, entfällt gänzlich für Unternehmen, die weniger als 250 Mitarbeiter haben und sofern bestimmte Kriterien erfüllt werden. Hierzu führt Art. 30 Abs. 5 konkret aus:

  Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt".

  Die Beurteilung, wann eine Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, dürfte wohl noch zu einigen Diskussionen mit den Aufsichtsbehörden führen – gerade in der Anfangsphase. Praktisch bedeutsamer ist jedoch die zweite Rückausnahme, wonach nur dann keine Pflicht zum Führen eines Verarbeitungsverzeichnisses besteht, sofern die Verarbeitung nur gelegentlich erfolgt. In der Praxis ist das wohl bei keiner Verarbeitung der Fall, was den Ausschluss in der Praxis hinfällig werden lässt. Für alle Standardverfahren des Unternehmens (z. B. Finanzbuchhaltung, Personalakten, Lieferantendatenbank, ...) bedeutet das keine Änderung. Es bleibt bei der Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.
- Zukünftig müssen auch Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten führen. Der Umfang weicht etwas von dem für Verantwortliche ab. Es enthält zusätzlich auch die Information, für welche Verantwortliche (also für welche Auftraggeber) die Verarbeitungen durchgeführt werden. Dafür kann die Beschreibung des Zwecks und die Löschungsfristen entfallen. Die Pflicht des Auftragsverarbeiters entbindet die für die Verarbeitung Verantwortlichen aber nicht von der Verpflichtung zur Führung eines separaten Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO für die eigenen Geschäftsprozesse.
- Ab Inkrafttreten der DSGVO ist die Unternehmensleitung und nicht mehr der betriebliche Datenschutzbeauftragte für die Verfahrensverzeichnisse verantwortlich (Art. 30 Abs. 1 DSGVO).
- Bei einem Datentransfer in einen Drittstaat auf der Grundlage des Art. 49 Abs. 1 S. 2 DSGVO sind die Risikoabschätzung und die ergriffenen Schutzmaßnahmen nach Art. 28 DSGVO zu dokumentieren (vgl. Art. 49 Abs. 6 DSGVO). Bei einem neuen Verarbeitungsverfahren ist somit ein neues Verzeichnis zu erstellen, anderenfalls ist das bereits bestehende Verzeichnis um die durch Art. 49 Abs. 6 DSGVO vorgeschriebenen Angaben zu ergänzen.

II. Datenschutz-Folgenabschätzung

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) sieht in ihrer Praxishilfe das Verzeichnis von Verarbeitungstätigkeiten als zentralen Bestandteil der gesamten Dokumentation: *„Das VVT kann beispielsweise zur Grundlage für Risikobewertungen durch den DSB für dessen risikoorientierten Überwachungsauftrag werden (Art. 39 Abs. 2 DSGVO). Ohne eine solche strukturierte Dokumentation sind die Beratungs- und Kontrollpflichten des DSB kaum umsetzbar. Denkbar sind interne Erweiterungen des VVT durch Risikoabschätzungen bzw. eine zusätzliche Strukturierung, die festhält, welche Verarbeitungen ggf. eine Datenschutz-Folgenabschätzung erfordern und welche nicht. Daneben können die durchgeführten Prüfungen aufgenommen werden".*

Das Verzeichnis der Verarbeitungstätigkeiten ist somit also durchaus auch von Bedeutung für eine weitere wesentliche Neuerung der Datenschutz-Grundverordnung: Die sogenannte Datenschutz-Folgenabschätzung oder kurz DSFA. Zwar kennt man hierzulande bedingt durch § 4d BDSG bereits die Vorabkontrolle, jedoch weitet das europäische Gesetz diese erheblich aus, sodass man wohl kaum noch von einer Vorabkontrolle 2.0 sprechen kann.

1. Vorabkontrolle nach derzeit geltendem Recht

Dabei ist die Folgenabschätzung keine wirkliche Innovation. In Großbritannien beispielsweise, gibt es einen *„Privacy Impact Assessment Code of Practice"* der Datenschutzaufsichtsbehörde ICO, welcher als Prozess zur Identifizierung und Reduzierung von Risiken für private Daten innerhalb eines Projektes beschrieben wird. In Frankreich hat die dortige Datenschutzaufsichtsbehörde *Commission Nationale de l'Informatique et des Libertés* (CNIL) ebenfalls ein Privacy Impact Assessment (PIA) als unverzichtbares Instrument zur Einschätzung und Reduzierung von Risiken für private Daten etabliert. Während es in Deutschland in verschiedensten Bundes- bzw. Landesgesetzen immer wieder Versuche gab, eine Folgenabschätzung unterzubringen, schaffte es letztendlich nur die abgeschwächte Vorabkontrolle in die Gesetzesbücher.

Nach noch geltendem Recht zuständig für die Vorabkontrolle ist, sofern vorhanden, der betriebliche Datenschutzbeauftragte (§ 4d Abs. 6 S. 1 BDSG). Damit der Datenschutzbeauftragte eine Vorabkontrolle durchführen kann, muss er zuerst einmal wissen, ob überhaupt ein automatisiertes Verfahren zum Einsatz kommen soll, das einer solchen Vorabkontrolle unterliegt. Wenn ihm das gesetzlich vorgesehene Verfahrensverzeichnis vorgelegt wird (§ 4d Abs. 6 S. 2 unter Verweis auf § 4g Abs. 2 S. 1 BDSG) muss er aktiv werden.

In der Praxis sieht es aber normalerweise so aus, dass der Datenschutzbeauftragte das Unternehmen überhaupt erst einmal darauf hinweist, dass es eine Pflicht zur Vorabkontrolle gibt. Die Pflicht des Unternehmens ist dabei eigentlich nur die, den Datenschutzbeauftragten zu

informieren, wenn ein neues Verfahren zum Einsatz kommt, damit dieser dann entscheiden kann, ob eine Vorabkontrolle notwendig ist. Tatsächlich notwendig ist nach aktueller Gesetzeslage eine Vorabkontrolle dann aber nur bei automatisierten Verfahren, die „besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen", wie sich § 4d Abs. 5 S. 1 BDSG entnehmen lässt. Wann ein „besonderes Risiko" vorliegt wird, im gleichen Paragraphen in Satz 2 erklärt, nämlich wenn besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) verarbeitet werden (Nr. 1) oder die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten, einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens (Nr. 2). Um zwei Beispiele zu nennen: Die Religionszugehörigkeit zählt zwar eindeutig zu den besonderen Daten nach § 3 Abs. 9 BDSG und unterliegen damit eigentlich der Vorabkontrolle. Im Rahmen der Kirchensteuer ist ihre Erhebung und Speicherung jedoch gesetzlich vorgeschrieben, weshalb eine Vorabkontrolle entfällt. Videoüberwachung am Arbeitsplatz hingegen muss so implementiert werden, dass keinerlei Leistungskontrolle durchgeführt werden kann. Ein klarer Fall für eine Vorabkontrolle. Im Zweifel gilt stets die Faustregel: Lieber eine Vorabkontrolle durchführen, denn das Verfahren ist schneller geprüft als nachträglich geändert!

2. Die Datenschutz-Folgenabschätzung nach der DSGVO

Art. 35 DSGVO legt fest, dass eine DSFA nur für eine Datenverarbeitung vorgenommen werden muss, die am oder nach dem 28.05.2018 begonnen wird. Alles, was vorher also noch regulär über die Vorabkontrolle legitimiert wurde, bleibt rechtlich bestehen. Allerdings empfiehlt die Artikel-29-Datenschutzgruppe in Ihrem Arbeitspapier (WP 248 vom 4. April 2017), dies auch für alle bestehenden Datenverarbeitungen nachzuholen.[1]

a) Voraussichtlich hohes Risiko

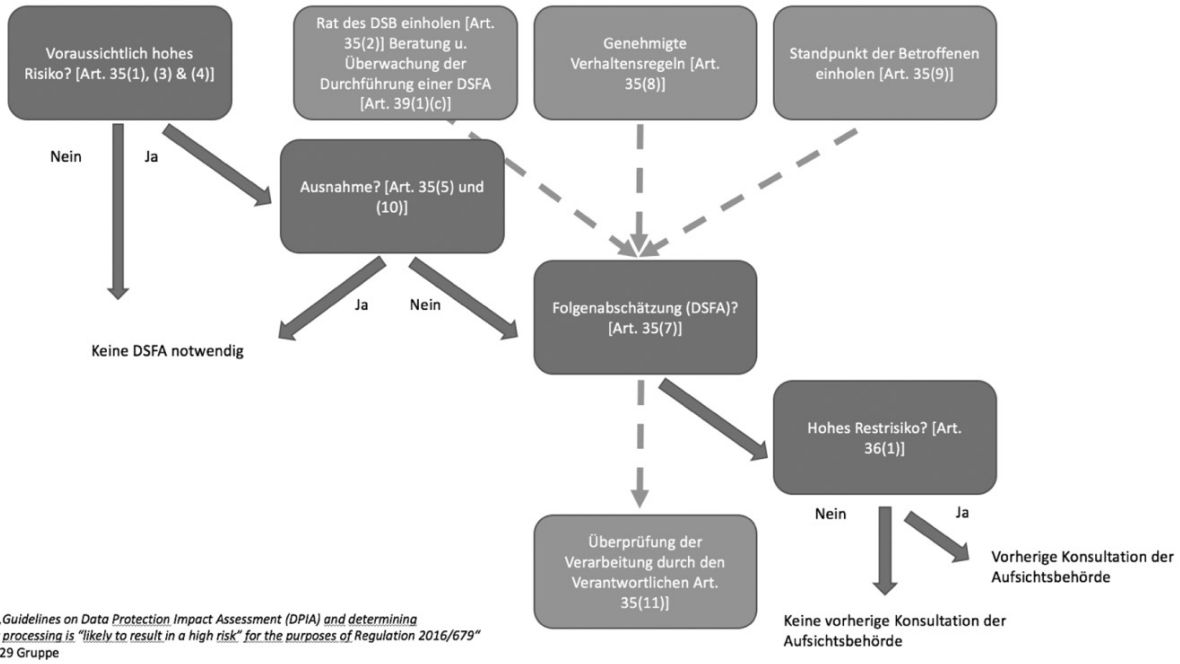
Die DSGVO verpflichtet den Verantwortlichen zukünftig – für alle Datenverarbeitungen nach diesem Stichtag – laut Art. 35 eine DSFA vorzunehmen, wenn ein „voraussichtlich hohes Risiko" mit der Verarbeitung der Daten verbunden ist. Diese Pflicht besteht unabhängig davon, ob ein Datenschutzbeauftragter bestellt ist oder nicht.
Die Artikel-29-Datenschutzgruppe hat in ihrem Arbeitspapier den Workflow einer DSFA einleuchtend visualisiert:

Eine DSFA erfordert folgende 3-stufige Vorgehensweise:
- Einschätzung der Eigenart der betreffenden Verarbeitung, des Umfangs, Kontextes und Zwecks
- Einschätzung der Risiken, insbesondere der Eintrittswahrscheinlichkeit und Schwere der möglichen Verletzung von Rechten
- Risikominimierung, Sicherstellung der Einhaltung der DSGVO, Dokumentation

Entscheidend ist also zunächst: Liegt ein voraussichtlich hohes Risiko vor oder nicht?
ErwG. 75 DSGVO zählt dabei physische, materielle und immaterielle Schäden auf, die eine Verarbeitung mit sich bringen kann:
- Diskriminierung
- Identitätsdiebstahl oder -betrug
- finanzieller Verlust
- Rufschädigung
- Verlust der Vertraulichkeit von personenbezogenen Daten
- unbefugte Aufhebung der Pseudonymisierung
- Hinderung der Kontrolle über eigene Daten
- Profilbildung mit Standortdaten

b) Empfehlungen der Artikel-29-Datenschutzgruppe zur Risikobestimmung

Die Artikel-29-Datenschutzgruppe hat in ihrem WP 248 zur Risikobestimmung diese Liste auf insgesamt zehn Kriterien ausgeweitet und präzisiert. Sollten mindestens zwei davon erfüllt werden, muss eine Folgenabschätzung erfolgen. Die zehn Punkte sind:
- Scoring, Profiling, Evaluation, z. B. Einschätzung der Kreditwürdigkeit, Behavioral Marketing etc.,
- automatisierte Einzelfallentscheidungen,
- systematische Überwachung,
- Verarbeitung sensibler Daten,
- umfangreiche Datenverarbeitungen (bezogen auf die Anzahl betroffener Personen und Datenkategorien, die Dauer der Verarbeitung, die geographische Ausdehnung),
- das Zusammenführen oder Abgleichen von Datenbeständen, wenn Betroffene nicht damit rechnen können,
- die Verarbeitung von Daten besonders schutzbedürftiger Personen,



Quelle: *„Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679"* der Art. 29 Gruppe

1 Abrufbar unter: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

- Neuartigkeit von Verarbeitungsvorgängen, Verwendung neuer Technologien (bspw. Fingerabdrucksensoren oder Gesichtserkennung),
- Übermittlung von personenbezogenen Daten an Empfänger außerhalb der EU,
- Verarbeitungen, die es betroffenen Personen erschweren, ihre Rechte auszuüben oder eine Leistung in Anspruch zu nehmen, z. B. die Beurteilung der Kreditwürdigkeit durch eine Bank vor der Vergabe eines Darlehens.

c) Matrix zur Risikobewertung

Nicht jede Verarbeitung wird sich zwangsläufig immer über diese Punkte bestimmen lassen. Wie sonst kann man dann ein möglicherweise hohes Risiko erkennen?

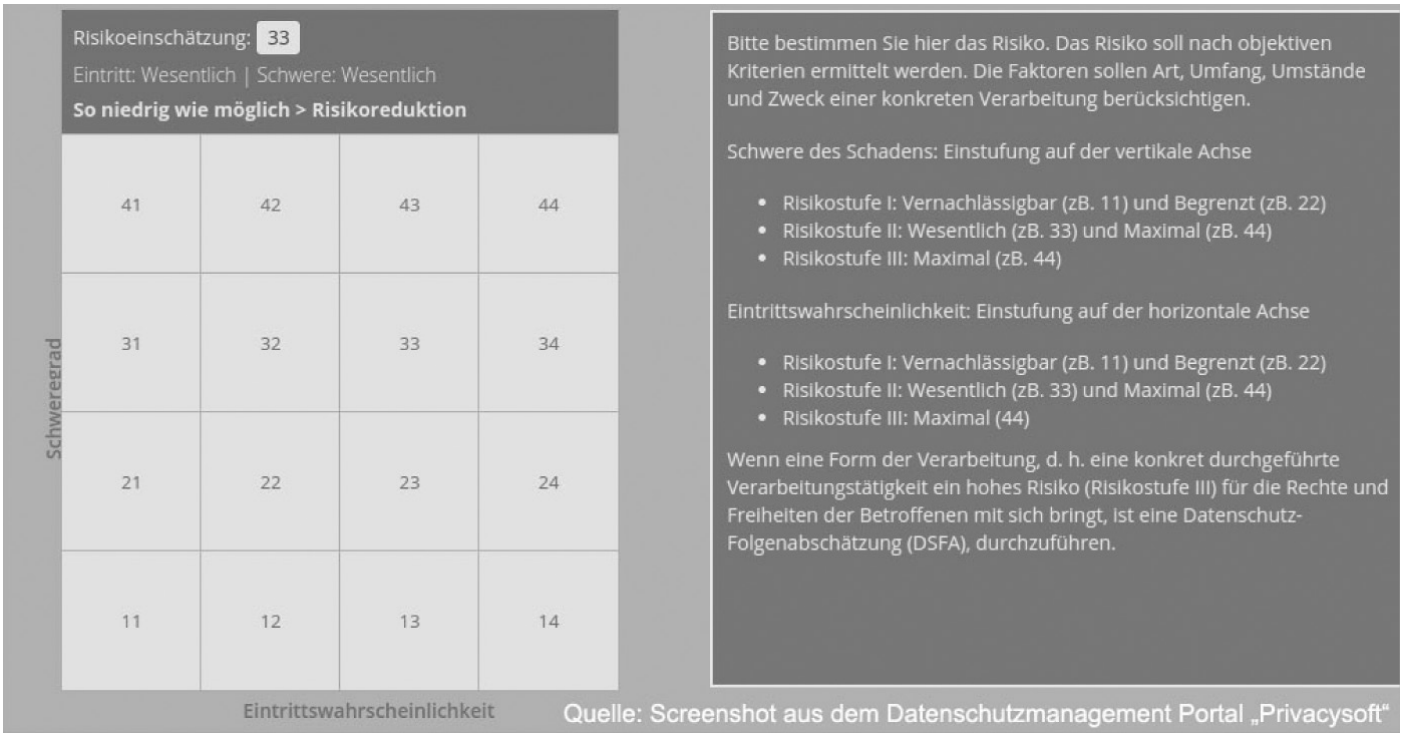
Die Aufsichtsbehörde in Ansbach, das Bayerische Landesamt für Datenschutz, hat in ihrem Whitepaper zur Folgenabschätzung betont, dass ein hoher Schutzbedarf nicht zwangsläufig auch in einem hohen Risiko resultieren muss, da diesem durchaus eine geringe Eintrittswahrscheinlichkeit entgegenstehen könnte. Um das Risiko einer in ErwG. 76 DSGVO geforderten „objektiven Bewertung" zu unterziehen, hat sich daher eine Matrix etabliert, die die Schwere eines Schadens gegen die Eintrittswahrscheinlichkeit abwägt. Dadurch lassen sich primär drei Risikobereiche eingrenzen: Geringes Risiko (akzeptabel), Risiko (so niedrig wie möglich) und Hohes Risiko (inakzeptabel).

d) Pflicht des Verantwortlichen

Der Verantwortliche hat grundsätzlich die Pflicht, Risiken bei der Verarbeitung zu berücksichtigen und zu dokumentieren – auch, wenn diese als nicht hoch einzustufen sind.

> „Da sich beispielsweise die ISO 27000er Reihe stark mit dem Thema Risikobewertung befasst und die ISO 29134 direkt das „Privacy Impact Assessment" thematisiert, werden diese im Zusammenhang mit der Datenschutz-Folgenabschätzung sicherlich noch mehr an Popularität gewinnen."

Der Verantwortliche hat dazu eine Stellungnahme des Datenschutzbeauftragten einzuholen. Gegebenenfalls ist auch der Standpunkt der betroffenen Personen zu erfragen und zu dokumentieren. Falls deren Standpunkt dann nicht berücksichtigt wird, sind Beweggründe dafür darzulegen. Art. 35 Abs. 8 DSGVO bzw. ErwG. 77 DSGVO nennen auch die Einhaltung von anerkannten Verhaltensregeln oder genehmigten Zertifizierungsverfahren als relevantes Merkmal für die Beurteilung der Auswirkungen von Datenverarbeitungen. Da sich beispielsweise die ISO 27000er Reihe stark mit dem Thema Risikobewertung befasst und die



Quelle: Screenshot aus dem Datenschutzmanagement Portal „Privacysoft"

In jedem Falle aber ist eine DSFA vorzunehmen, wenn die Daten von Kindern oder etwa biometrische Daten betroffen sind. Ausnahmen von der Pflicht zur Folgenabschätzung bestehen gemäß Art. 35 Abs. 10 DSGVO, weiterhin dann, wenn die Verarbeitung auf der Grundlage einer europäischen oder nationalen Rechtsvorschrift beruht. Hier liegt es im Ermessen der einzelnen Mitgliedstaaten, ob sie eine Folgenabschätzung im Einzelfall als erforderlich ansehen.

Über Art. 35 Abs. 4 und Abs. 5 DSGVO werden die Aufsichtsbehörden vom Gesetzgeber in die Pflicht genommen, eine sogenannte Blacklists zur Orientierung zu veröffentlichen, also eine Liste, die Datenverarbeitungen aufzählt, für die typischerweise eine Folgenabschätzung vorzunehmen ist. Darüber hinaus können die Aufsichtsbehörden auch Whitelists zur Verfügung stellen, die wiederum Datenverarbeitungen aufzählen, die regelmäßig keine Folgenabschätzung mit sich bringen.

ISO 29134 direkt das „Privacy Impact Assessment" thematisiert, werden diese im Zusammenhang mit der Datenschutz-Folgenabschätzung sicherlich noch mehr an Popularität gewinnen. *Kranig*, *Sachs* und *Gierschmann* empfehlen sogar eine Orientierung an der ISO 29134 in Ihrem Buch „Datenschutz-Compliance nach der DSGVO".

e) Technische und organisatorische Maßnahmen zur Risikominimierung

Um das Risiko zu minimieren, sind vom Unternehmen sogenannte „technische und organisatorische Maßnahmen" (TOM) zu treffen und auf das jeweilige Risiko anzuwenden. Die Auswahl der Maßnahmen ist grundsätzlich offen formuliert. Allerdings werden einige Maßnahmen genannt, die umgesetzt werden müssen, sofern diese für die konkrete Anwendung geeignet sind (Art. 32 Abs. 1 DSGVO):

- Pseudonymisierung
- Verschlüsselung (Kryptographie)
- Sicherstellung der „klassischen" Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit)
- Verfahren zur Wirksamkeitsprüfung

f) Inhalt der Datenschutz-Folgenabschätzung

Inhaltlich hat eine Datenschutz-Folgenabschätzung grundsätzlich folgendermaßen auszusehen:

1. Systematische Beschreibung der geplanten Verarbeitungsvorgänge
2. Systematische Beschreibung des Zwecks der Verarbeitung
3. Systematische Beschreibung der berechtigten Interessen des Verantwortlichen
4. Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
5. Bewertung der Risiken
6. Zur Minimierung der Risiken geplante
   a) Abhilfemaßnahmen,
   b) Garantien,
   c) Sicherheitsvorkehrungen und
   d) Verfahren,

   durch die der Schutz sichergestellt und der Nachweis zur Einhaltung der Verordnung erbracht wird.

g) Konsultation der Datenschutzbehörde

Sollte im Ergebnis der Datenschutz-Folgenabschätzung trotz Maßnahmen zur Risikominimierung das Restrisiko weiterhin hoch sein, so ist die Datenschutzaufsichtsbehörde hinzuzuziehen. Kommt diese zu dem Ergebnis, dass die Maßnahmen ausreichen, kommt die Folgenabschätzung an dieser Stelle zu einem Ende. Sollte die Aufsichtsbehörde die Maßnahmen jedoch nicht als ausreichend bewerten, kann diese dem Unternehmen innerhalb einer Frist von acht Wochen konkrete Empfehlungen geben, in welchen Bereichen Nachbesserungen vorzunehmen sind.

Um die DSFA entsprechend prüfen zu können, müssen der Datenschutzbehörde entsprechende Informationen zur Verfügung gestellt werden. Diese sind:

- Zweck und Mittel der Verarbeitung
- Maßnahmen und Garantien
- Ggf. Kontaktdaten des Datenschutzbeauftragten
- Datenschutz-Folgenabschätzung
- Alle weiteren geforderten Informationen

Eine Pflicht zur Veröffentlichung einer Datenschutz-Folgenabschätzung sieht die Datenschutz-Grundverordnung nicht vor. Die Artikel-29-Datenschutzgruppe empfiehlt jedoch, aus Transparenzgründen eine solche in Betracht zu ziehen, vor allem, wenn Risiken für die Öffentlichkeit bestehen. Auch empfiehlt sie, eine DSFA jeweils im Turnus von drei Jahren zu wiederholen. Eine Pflicht hierzu besteht gleichwohl nicht, sofern die Risikoeinschätzung noch dieselbe ist. Wenn sich die Umstände zur Verarbeitung ändern, sieht das selbstverständlich anders aus.

h) Bußgeldgefahr

Die Pflicht zur Datenschutz-Folgenabschätzung ist, genau wie die zur Führung des Verzeichnisses von Verarbeitungstätigkeiten, in jedem Falle ernst zu nehmen. Art. 83 Abs. 4 DSGVO setzt hier bei Verstößen ein Bußgeld in Höhe von bis zu 10.000.000 Euro bzw. bis zu 2 Prozent des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens an.

Daniela Gaub ist Referentin für Rechtspolitik beim Bundesverband Deutscher Inkasso-Unternehmen e.V. (BDIU).

Leitfäden zur Anwendung und Umsetzung der DSGVO – Hinweise zur Erstellung am Beispiel des Best Practice Guides 1.0 für den Bereich des Forderungsmanagements

Rechtsanwalt Kay Uwe Berg ist Hauptgeschäftsführer des Bundesverbandes Deutscher Inkasso-Unternehmen e.V. (BDIU).

Daniela Gaub und *Kay Uwe Berg*

Der Bundesverband Deutscher Inkasso-Unternehmen e.V. (BDIU) hat als einer der Ersten einen Best Practice Guide[1] erstellt, mit dem nicht nur ein Überblick zu den einzelnen Regelungen der Europäischen Datenschutz-Grundverordnung gegeben wird, sondern mit dem auch erste Beispiele, Tipps und Hinweise aufgezeigt werden, wie die rechtlichen Anforderungen in der Praxis umgesetzt werden können. Mit dem folgenden Beitrag werden der Hintergrund, der Unterschied zu Verhaltensregeln nach Art. 40 DSGVO, ein Kurzüberblick zum Inhalt sowie die Entwicklung des Leitfadens dargestellt.

I. Hintergrund

Spätestens seitdem die Europäische Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2016 in Kraft getreten und damit klar ist, dass sie genau zwei Jahre später Anwendung finden wird, heißt es Ärmel hochkrempeln, um die nach der DSGVO für die Datenverarbeitungen Verantwortlichen auf das neue Datenschutzrecht ab dem 25. Mai 2018 vorzubereiten.

Für den Bundesverband Deutscher Inkasso-Unternehmen e.V. (BDIU) stand schnell fest, dass die Mitgliedsunternehmen, aber auch darüber hinaus Interessierte und im Forderungsmanagement Tätige bei der Umstellung auf die neuen Anforderungen unterstützt werden müssen. Viele der insgesamt 560 BDIU-Mitgliedsunternehmen sind Einzel- und kleine Unternehmen, die oftmals keinen Datenschutzbeauftragten haben und bei datenschutzrechtlichen Fragen auf externen Input angewiesen sind. Damit sich nicht jedes Unternehmen für sich überlegen muss, wie die DSGVO-Vorgaben in der Praxis berücksichtigt werden müssen, wollte der Verband für alle erste Hinweise geben, wie Datenflüsse und Datenverarbeitungen künftig vonstatten gehen werden.

II. Verhaltensregeln gemäß Art. 40 DSGVO versus Best Practice Guide

1. Überblick

Eine Möglichkeit dazu wäre gewesen, dass sich der BDIU an die Ausarbeitung von Verhaltensregeln im Sinne von Art. 40 DSGVO macht. Art. 40 Abs. 2 DSGVO regelt nämlich, dass Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen und Auftragsverarbeitern vertreten, solch grundlegende Handlungsorientierungen entwickeln können, um die wirksame Anwendung der Verordnung zu erleichtern und die Verordnungsvorgaben zu präzisieren. Solche Regeln können sowohl von nationalen als auch europäischen Verbänden entwickelt werden; die DSGVO stellt dazu keine Vorgaben auf.

Beispielsweise können durch Verhaltensregeln die faire und transparente Verarbeitung (Art. 40 Abs. 2 lit. a), die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen (lit. b), die Erhebung personenbezogener Daten (lit. c), die Ausübung der Rechte der betroffenen Personen (lit. f) und die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung nach Art. 32 (lit. h) näher geregelt werden. Nach ErwG. 98 DSGVO soll dabei stets den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung getragen werden.[2]

1 Download möglich unter: www.inkasso.de/positionen/standpunkte/best-practice-guide-dsgvo.

2 Einen dezidierten Überblick zu Verhaltensregeln nach Art. 40 DSGVO sowie deren Reichweite und Rechtsfolgen gibt *Spindler* in ZD 2016, Selbstregulierung und Zertifizierungsverfahren nach der DSGVO, 407.

Nähere und vor allem für alle einheitliche Hinweise und Beispiele sind nach weitverbreiteter Einschätzung tatsächlich besonders hilfreich für die Kleinst-, kleinen und mittleren Unternehmen.

Aufgrund der Struktur der Mitgliedsunternehmen des BDIU gab es daher zunächst bei diesem Überlegungen, Verhaltensregeln im Sinne der DSGVO auszuarbeiten. Grundsätzlich wurden und werden diese immer noch als sinnvoll erachtet, denn Regeln und Verfahren im Rahmen einer freiwilligen Selbstbindung aus einer Branche heraus sind sicherlich mehr wert als abstrakt-generelle Regelungen. Sie können sowohl dem Anwender als auch der Aufsicht einen detaillierteren Einblick in einzelne Abläufe und die Besonderheiten einer Branche gewähren.

2. Gründe gegen Verhaltensregeln auf nationaler Ebene für den Bereich Forderungsmanagement

Ein maßgeblicher Grund, warum der BDIU nun aber doch von der Erstellung von Verhaltensregeln abgesehen hat, liegt an Art. 40 Abs. 5 DSGVO, der explizit eine Einbeziehung der nach Art. 55 DSGVO zuständigen Aufsichtsbehörde erfordert.

Dass die bzw. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die Aufsichtsbehörde in Deutschland ist, die die Aufgaben nach Art. 57 DSGVO wahrnimmt, steht jedoch erst seit Kurzem fest.[3] Verhaltensregeln für (ausschließlich) in Deutschland ansässige datenverarbeitende Unternehmen können also – möchte man das in der DSGVO vorgegebene Verfahren einhalten – faktisch erst jetzt in Kollaboration mit der bzw. dem BfDI ausgearbeitet werden.

In Anbetracht der vielfältigen Aufgaben der bzw. des BfDI allein bis zum Anwendungsbeginn der DSGVO rechnete der BDIU nicht mit einem schnellen Abstimmungsprozess, selbst wenn die Aufsichtsbehörde gemäß DSGVO dazu angehalten ist, die Ausarbeitung von Verhaltensregeln zu fördern.

Ein weiterer Grund, warum sich der BDIU zum jetzigen Zeitpunkt gegen nationale Verhaltensregeln für den Bereich Forderungsmanagement ausgesprochen hat, liegt darin, dass der europäische Dachverband, die Federation of European National Collection Associations (FENCA),[4] die Ausarbeitung von Verhaltensregeln beschlossen hat. Der Code of Conduct[5] wird dabei nach den Vorgaben des Art. 40 DSGVO erstellt werden und soll europaweit für den Bereich des Forderungsmanagements gelten.[6] Blickt man auf das Ziel der DSGVO, das Datenschutzrecht europaweit vereinheitlichen zu wollen, ist die Erstellung von ebenso europaweit einheitlichen Präzisierungen zur Anwendung der Verordnung folgerichtig.

Da also zum einen auf nationaler Ebene bislang nicht klar war, mit welcher Aufsichtsbehörde die Abstimmung nach Art. 40 Abs. 5 DSGVO erfolgen soll, zum anderen die paneuropäischen Verhaltensregeln der FENCA erwartet werden, entschied sich der BDIU im Frühsommer 2016 für einen anderen Weg – die Ausarbeitung eines Best Practice Guides.

III. Best Practice Guide – Inhalt und Entwicklung

Die Idee dahinter war es, den Unternehmen der Branche und weiteren Tätigen im Bereich des Forderungsmanagements einen Leitfaden an die Hand geben zu wollen, aus dem in ersten Grundzügen hervorgeht, wie bis Mai 2018 die Datenverarbeitungen konform mit den neuen DSGVO-Anforderungen ausgestaltet werden sollten.

Die Anpassung der Prozessabläufe und die weitere Implementierung der DSGVO-Vorgaben, v. a. was die Dokumentationsanforderungen anbelangt, kann nämlich nicht von heute auf morgen geschehen, sodass eine zügige erste Hilfestellung unabdingbar war. Der Best Practice Guide wurde daher schnellstmöglich erstellt und war Anfang 2017 fertiggestellt.

1. Inhalt

Die 41 Seiten umfassende Handlungsempfehlung des BDIU beginnt mit einem Vorwort der BDIU-Präsidentin *Kirsten Pedd*, mit dem bereits klar wird, dass der Best Practice Guide ein wirkliches Hilfsmittel für die Unternehmen der Branche sein soll.

Da sich aber sicherlich nicht alle Adressaten des Best Practice Guides mit europäischen Gesetzgebungsverfahren auskennen, wird als eigentlicher Beginn des BDIU-Leitfadens zunächst ein Kurzüberblick dazu gegeben, was die Regelung in Form einer europäischen Verordnung bedeutet und im Weiteren – auch zum besseren Verständnis für die weitere Lektüre – die wichtigsten Begriffe der DSGVO vorgestellt, dies bereits mit branchenrelevanten Erläuterungen.

Danach folgt der eigentliche Inhalt: Die DSGVO-Regelungen zu den Grundlagen der Datenverarbeitung, die Informationspflichten und die Betroffenenrechte werden beleuchtet. Dabei werden stets für den Bereich des Forderungsmanagements einschlägige Beispiele aufgeführt und aufgezeigt, Besonderheiten herausgehoben und hilfreiche Tipps für die Praxis gegeben. In gleicher Weise werden v. a. die Anforderungen an die Dokumentation, der sichere Umgang mit Daten durch technisch-organisatorische Maßnahmen, die Stellung des betrieblichen Datenschutzbeauftragten, die Auftragsverarbeitung, mögliche Sanktionen und die Tätigkeit der Aufsicht in den Blick genommen.

Der Leitfaden endet schließlich mit einem Katalog der für Inkassodienstleister maßgeblichen Begriffsbestimmungen sowie einer Synopse, die die einzelnen Artikel der DSGVO den jeweils passenden Erwägungsgründen gegenüberstellt.

2. Entwicklung

Der Weg bis zur Druckfassung des Leitfadens war zwar – im Vergleich zu manch anderen Druckerzeugnissen – nicht lang: Den Startschuss gab es im Frühsommer 2016. Anfang Februar 2017 wurde der Best Practice Guide veröffentlicht.

Dennoch: die Entwicklungsphase von guten acht Monaten war mehr als intensiv und bedeutete für alle Beteiligten eine nicht zu unterschätzende Zusatzbelastung. Wenn man sich genau anschaut, wer an der Erstellung mitgewirkt hat, wird schnell klar, dass es nicht als selbstverständlich angesehen werden kann, dass in dieser Zeit ein Werk dieses Umfangs und dieser Qualität entstehen kann.

Auch wenn der BDIU mit seinen hauptamtlichen Mitarbeitern mit am Werk war, wurde der Inhalt zum Großteil von Praktikern beigesteuert. So haben alle Mitglieder des BDIU-Datenschutzausschusses, die in dieser Position ehrenamtlich und damit neben ihrer eigentlich Tätigkeit (zumeist als Datenschutzbeauftragte in den oder für Inkassounternehmen) tätig sind, an der Erstellung mitgewirkt. Auch der Verbandsbeauftragte für den Datenschutz des BDIU hat bei der Entwicklung des Leitfadens seine Expertise eingebracht.

Nach Verteilung einzelner Themenbereiche durch die BDIU-Geschäftsstelle hat sich jeder der Beteiligten an die Ausarbeitung seines Parts gemacht und nahm die jeweiligen DSGVO-Regelungen aus Praxissicht in den Blick. Die innerhalb einer gesetzten Frist übersandten Manuskripte der Einzelnen hat die BDIU-Geschäftsstelle anschließend zusammengefügt und bereits eine erste sprachliche Anpassung vorgenommen. Bei einem ersten Treffen gut zweieinhalb Monate nach der Themenvergabe wurde in einem Arbeitstreffen des

3 Der Bundestag hat das BDSG-neu als Bestandteil des DSAnpUG-EU (BT-Drs. 18/11325) am 27. April 2017 in der Fassung der Beschlussempfehlung des Innenausschusses (BT-Drs. 18/12084) verabschiedet. Der Bundesrat hat am 12. Mai 2017 dem Gesetz zugestimmt.

4 Der BDIU ist Gründungsmitglied der FENCA.

5 In der englischen Sprachfassung der DSGVO werden die Verhaltensregeln in Art. 40 mit Codes of Conduct bezeichnet.

6 FENCA-News zum Code of Conduct: http://fenca.eu/detail/article/fenca-is-working-on-a-pan-european-code-of-conduct/.

BDIU-Datenschutzausschusses der erste Teil des Manuskripts besprochen und dezidiert über jedes einzelne Kapitel diskutiert, bis zu allen Punkten Einigkeit herrschte. Die BDIU-Geschäftsstelle passte das Manuskript im Nachgang entsprechend der Ergebnisse des Arbeitstreffens an. Das gleiche Vorgehen erfolgte bezüglich der noch verbleibenden Teile bei weiteren Arbeitstreffen bzw. regulären Ausschusssitzungen, bis Anfang Dezember 2016 die finale Ausarbeitung der Verfasser auf dem Tisch lag.

Um die Lesbarkeit und damit das Verständnis auch für die Leser zu gewährleisten, die sich bislang noch nicht intensiv mit dem Datenschutzrecht auseinandergesetzt haben, erfolgte noch von externer Seite eine sprachliche Überarbeitung des Best Practice Guides. Im Folgenden musste noch ein letzter Abgleich zwischen der ursprünglichen Finalfassung und der Fassung nach der sprachlichen Überarbeitung stattfinden, um sicherzugehen, dass trotz der Überarbeitung die inhaltlichen Aussagen gleichgeblieben waren.

Schließlich stimmte die BDIU-Geschäftsstelle mit einer beauftragten Agentur das Layout des Best Practice Guides ab, bevor dieser dann in der Printfassung an die Mitglieder des BDIU versandt, als (kostenfrei) downloadbares PDF auf die Verbandshomepage gestellt und beim BDIU-Kongress am 7. April 2017 im Rahmen eines Workshops vorgestellt wurde.[7] Bei dieser Gelegenheit war es bereits möglich, erste Fragen zum Best Practice Guide bzw. zur Anwendbarkeit der DSGVO zu stellen.

IV. Ausblick

In den kommenden Monaten wird der BDIU auch noch näher den Inhalt des Best Practice Guides bei den Sitzungen der regionalen Arbeitskreise des Verbandes vorstellen und den dortigen Teilnehmern Rede und Antwort zu datenschutzrechtlichen Fragen stehen.

Bis zum Anwendungsbeginn der DSGVO wird der BDIU seinen Mitgliedern zudem regelmäßig Factsheets zur Verfügung stellen, aus denen für die Unternehmen vertiefende, dabei prägnante Erläuterungen und Tipps zu einzelnen Themen der DSGVO hervorgehen, bestenfalls auch bereits erste Anwendungshinweise der Datenschutzaufsichtsbehörden.

Der Titel „Best Practice Guide 1.0 – Leitfaden für den Bereich Forderungsmanagement“ lässt es ansonsten bereits erkennen, dass er und der Umgang mit der DSGVO „work in progress“ sind. So berücksichtigt der Leitfaden noch nicht die Regelungen des deutschen BDSG-neu, das als Bestandteil des DSAnpUG-EU bereits beschlossen wurde,[8] sondern nur die DSGVO-Regelungen. Es sind schon allein deshalb noch genügend Fragen offen, zu denen es sicherlich zu gegebener Zeit noch Antworten geben wird – vielleicht in einem „Best Practice Guide 2.0“ ...

7 Siehe Fußnote 1.

8 Siehe Fußnote 3.

Dr. Kai-Uwe Plath, LL.M. (New York) ist Partner der Kanzlei KNPZ Rechtsanwälte in Hamburg und Herausgeber des nach ihm benannten Kommentars zum BDSG sowie zur DSGVO.

„The MLAT-Route“

Übermittlung personenbezogener Daten an US-Behörden im Rahmen von Compliance-Untersuchungen – Zum Verhältnis zwischen Rechtshilfeabkommen und BDSG/DSGVO

Dr. Kai-Uwe Plath, LL. M.

Im Rahmen von internationalen Compliance-Untersuchungen stehen deutsche Unternehmen regelmäßig vor der Grundsatzfrage, ob sie den Auskunftsverlangen US-amerikanischer Behörden nachkommen dürfen bzw. müssen, oder ob sie aufgrund datenschutzrechtlicher Beschränkungen daran gehindert sind, personenbezogene Daten in die USA zu übermitteln. Im Kern dreht sich diese Diskussion um die Auslegung der bekannten Erlaubnistatbestände unter dem BDSG. Ganz ungeachtet dessen stellt sich aber die Frage, ob die betroffenen Unternehmen nicht per se daran gehindert sind, auf ein Auskunftsverlangen der US-Behörden zu reagieren, nämlich weil die US-Behörden mit ihrem Verlangen möglicherweise gegen das Völkerrecht verstoßen. Konkret geht es darum, ob die US-Behörden verpflichtet sind, ihre Forderungen im Wege der Rechtshilfe über die deutschen Behörden geltend zu machen, und nicht etwa direkt gegenüber den betroffenen Unternehmen.

1. Einleitung

Immer wieder sehen sich deutsche Unternehmen Untersuchungen seitens der US-amerikanischen Aufsichtsbehörden ausgesetzt. Die im Raum stehenden Bußgelder sind beträchtlich und bemessen sich u. a. danach, in welchem Maße die betroffenen Unternehmen mit den US-Behörden kooperieren.

Vor allem fordern die US-Behörden eine umfassende Mitwirkung bei der Aufklärung der möglichen Rechtsverstöße und die Offenlegung aller einschlägigen Dokumente und Informationen.[1] Für die betroffenen Unternehmen führt dies zu einem scheinbar unauflöslichen Zielkonflikt. Einerseits besteht der Wille und möglicherweise auch die Pflicht nach US-Recht, die angeforderten Informationen zu liefern. Andererseits sehen sich die Unternehmen der latenten Gefahr ausgesetzt, mit der Bereitstellung der angeforderten Informationen gegen deutsches Datenschutzrecht zu verstoßen.

Besonders heikel ist die Situation, wenn sich die US-Behörden zur Durchsetzung ihrer Forderungen des Instruments einer Subpoena bedienen. Dabei handelt es sich um eine behördliche Anordnung, mit der die betroffenen Unternehmen unter Androhung von Zwangsmitteln dazu aufgefordert werden, bestimmte Dokumente herauszugeben bzw. Auskünfte zu erteilen. Vordergründig betrachtet macht die Subpoena die Sache für die betroffenen Unternehmen einfacher. Denn wenn eine rechtliche Verpflichtung zur Herausgabe bestimmter Daten besteht, kann es nicht Unrecht sein, dieser Verpflichtung nachzukommen. Indes wird insoweit diskutiert, ob die Unternehmen nicht gleichwohl gezwungen sind, die Subpoena zu ignorieren. Argumentiert wird damit, dass eine Subpoena gegenüber einem deutschen Unternehmen unbeachtlich sei, da sie gegen das Völkerrecht verstoße. Konkret geht es dabei um den „Vertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen“ vom 14. Oktober 2003. Es stellt sich also die Frage, welche Auswirkungen dieses Rechtshilfeabkommen, englisch „Mutual Legal Assistance Treaty“ (MLAT), auf das Recht und die Pflicht deutscher Unternehmen hat, Daten an US-Behörden zu übermitteln. Untersucht wird zunächst die Rechtslage unter dem BDSG. Im Anschluss wird ein kurzer Ausblick unter der DSGVO gegeben.

2. Rechtliche Rahmenbedingungen für Compliance-Untersuchungen unter dem BDSG

Die Frage, ob und unter welchen Voraussetzungen ein in Deutschland ansässiges Unternehmen personenbezogene Daten an US-Behörden übermitteln darf, richtet sich in erster Linie nach dem BDSG.

2.1 Anwendbarkeit des BDSG auf Compliance-Untersuchungen

Das BDSG ist anwendbar, soweit eine Erhebung, Verarbeitung oder Nutzung „personenbezogener Daten“ erfolgt, und zwar unter „Einsatz von Datenverarbeitungsanlagen“ oder in bzw. aus „nicht automatisierten Dateien“ (§ 1 Abs. 2 Nr. 3 BDSG). „Personenbezogene Daten“ sind nach § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“. Diese Definition ist denkbar weit gefasst. Dies führt dazu, dass nahezu sämtliche Informationen, die üblicherweise im Rahmen einer Compliance-Untersuchung anfallen, dem Begriff der „personenbezogenen Daten“ unterfallen können.

Weitere Voraussetzung für die Anwendbarkeit des BDSG ist der „Einsatz von Datenverarbeitungsanlagen“, also typischerweise Computern. Dies wird bei einer Compliance-Untersuchung der Regelfall sein, insbesondere bei der Auswertung von E-Mails. Soweit es um Daten von Beschäftigten eines Unternehmens geht, kommt das BDSG selbst dann zur Anwendung, wenn kein Einsatz von Datenverarbeitungsanlagen erfolgt (vgl. § 32 Abs. 2 BDSG).

2.2 Erlaubnisnorm zur Durchführung von Compliance-Untersuchungen nach dem BDSG

Das BDSG beruht auf dem Konzept des Verbots mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG). Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift diese erlaubt bzw. anordnet oder der Betroffene eingewilligt hat (vgl. § 4 Abs. 1 BDSG sowie § 4c Abs. 1 S. 1 Nr. 1 BDSG in Anbetracht des US-Bezugs).

Soweit also keine Einwilligung der Betroffenen vorliegt,[2] muss sich das Unternehmen auf die gesetzlichen Erlaubnistatbestände stützen. Diskutiert wird insoweit, ob die Untersuchung auf Grundlage der generellen Erlaubnisnorm des § 28 BDSG durchgeführt werden kann, oder ob der im Bereich der Beschäftigungsverhältnisse vorrangige § 32 BDSG zur Anwendung kommt. Die Frage ist bislang nicht abschließend geklärt. Nach der hier vertretenen Ansicht ist auf den Schwerpunkt der Untersuchung abzustellen. Geht es konkret darum, das Fehlverhalten eines bestimmten Mitarbeiters zu untersuchen, so liegt die Anwendbarkeit des § 32 BDSG nahe. Dient die Untersuchung hingegen eher übergreifenden Compliance-Zwecken, so erscheint ein Rückgriff auf § 28 BDSG naheliegender. Dies gilt nach der hier vertretenen Ansicht auch dann, wenn im Rahmen der grundsätzlicheren Untersuchung auch nachgelagert das mögliche Fehlverhalten einzelner Personen untersucht wird. In solchen Fällen sind allerdings die Wertung des § 32 BDSG im Rahmen der Abwägung nach § 28 BDSG zu berücksichtigen. Wenn also z. B. mögliche Straftaten eines Arbeitnehmers in Rede stehen, so werden hohe Anforderungen an die Darlegung der Verdachtsmomente zu stellen sein (vgl. § 32 Abs. 1 S. 3 BDSG).[3]

2.3 Erlaubnisnorm zur Übermittlung von Daten an US-Behörden unter dem BDSG

Soweit es an einer Einwilligung des Betroffenen fehlt, ist wiederum der Rückgriff auf die gesetzlichen Erlaubnisnormen erforderlich und zwar auf Basis eines „Zwei-Stufen-Tests“.

Zunächst fragt sich, ob die Daten überhaupt für die Zwecke der Untersuchung verwendet und an einen Dritten, wie eben eine US-Behörde, übermittelt werden dürfen. Dies richtet sich, wie soeben dargestellt, regelmäßig nach § 28 BDSG. Auf der zweiten Stufe fragt sich dann, ob die Daten in die USA oder einen sonstigen Drittstaat außerhalb der EU bzw. des EWR übermittelt werden dürfen.

Nach § 4b Abs. 2 BDSG hat eine Übermittlung zu unterbleiben, „soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen (hier: den US-Behörden) ein angemessenes Datenschutzniveau nicht gewährleistet ist“. Nach Einschätzung der EU-Kommission fehlt es in den USA an einem „angemessenen Datenschutzniveau“, sodass das Verbot des § 4b Abs. 2 BDSG grundsätzlich zur Anwendung kommt.

Allerdings gelten nach § 4c BDSG gewisse Ausnahmen von diesem Verbot, die im Rahmen von Compliance-Untersuchungen relevant sein

1 Vgl. z. B. den sog. Seaboard Report der SEC, wonach u. a. Folgendes gefordert wird: "Cooperation with law enforcement authorities, including providing the Commission staff with all information relevant to the underlying violations and the company's remedial efforts" (abrufbar unter: https://www.sec.gov/spotlight/enforcement-cooperation-initiative.shtml).

2 Zur Möglichkeit, Compliance-Untersuchungen auf das Instrument der Einwilligung zu stützen, siehe *Plath*, Compliance Untersuchungen und Datenschutz, DGRI Jahrbuch 2015, 183, 189.

3 Siehe dazu auch *Plath*, Compliance Untersuchungen und Datenschutz, DGRI Jahrbuch 2015, 183, 194.

können. Die für den Fall der Compliance-Untersuchungen maßgebliche Ausnahme findet sich in § 4c Abs. 1 S. 1 Nr. 4 BDSG. Danach ist die Übermittlung zulässig, wenn „die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist“.

Die Auslegung des Begriffs des wichtigen öffentlichen Interesses ist umstritten. Teilweise wird vertreten, dass sich ohnehin nur öffentliche Stellen auf diesen Tatbestand stützen könnten. Soweit die Untersuchung vornehmlich Verfehlungen einzelner Mitarbeiter eines Unternehmens mit interner Wirkung betrifft, so ist es in der Tat kaum denkbar, dass sich ein Unternehmen auf diesen Tatbestand stützen kann. Steht hingegen eine umfassende Untersuchung, etwa des Finanzsektors, im Raum, erscheint eine Berufung auf öffentliche Interessen nach der hier vertretenen Ansicht denkbar.[4]

Vor allem aber ist eine Übermittlung möglich, wenn diese zur Rechtsverteidigung erforderlich ist. Auch insoweit kommt es auf die konkrete Konstellation des Einzelfalles an, z. B. auf die Frage, in welchem Stadium sich die Untersuchung der US-Behörden befindet. Relevant ist dies u. a. deshalb, weil die Norm auf eine Verteidigung „vor Gericht“ abstellt, was die Frage aufwirft, ob auch außer- bzw. vorgerichtliche Maßnahmen eine Übermittlung ermöglichen, wenn diese eine Rechtsverteidigung erfordern. Hierzu werden teilweise eher restriktive Auffassungen vertreten.[5] Richtigerweise darf die Norm allerdings nicht zu eng ausgelegt werden, sodass die Rechtsverteidigung im weitesten Sinne zu verstehen ist und auch außer- bzw. vorgerichtliche Maßnahmen mit umfasst.[6]

Weiterhin muss stets der Erforderlichkeitsgrundsatz gewahrt bleiben. Insoweit stellt sich insbesondere die Frage, in welchem Umfang die übermittelten Daten zu pseudonymisieren sind, um diesen Anforderungen zu genügen.[7] In einer Stellungnahme der Artikel-29-Datenschutzgruppe zum thematisch ähnlich gelagerten Pre-Trial–Discovery-Verfahren heißt es dazu wörtlich:[8] „Als ersten Schritt sollten die für die Verarbeitung Verantwortlichen die Offenlegung nach Möglichkeit auf anonymisierte oder zumindest pseudonymisierte Daten beschränken. Nach dem Herausfiltern irrelevanter Daten – möglicherweise durch eine vertrauenswürdige dritte Partei in der Europäischen Union – würden in einem zweiten Schritt personenbezogene Daten in einem sehr viel begrenzteren Umfang offen gelegt werden“.[9]

3. Vorrang des MLAT?

Unterstellt man also, dass die Übermittlung personenbezogener Daten an die US-Behörden in den dargestellten – engen – Grenzen grundsätzlich möglich ist, so stellt sich die Frage, ob das MLAT dieser Wertung entgegensteht. Die Befürworter dieser Ansicht argumentieren, dass das MLAT die US-Behörden in seinem Anwendungsbereich dazu verpflichtet, sich im Rahmen von Auskunftsverlangen gegenüber deutschen Unternehmen an die deutschen Behörden zu wenden, die dann ihrerseits das Auskunftsverlangen durchsetzen müssen.

3.1 Anwendungsbereich des MLAT

Der Anwendungsbereich des MLAT ist dort in Art. 1 Abs. 1 S. 1 wie folgt definiert: „Die Vertragsparteien verpflichten sich, gemäß den Bestimmungen dieses Vertrags einander durch ihre zuständigen Behörden soweit wie möglich Rechtshilfe in strafrechtlichen Ermittlungsverfahren und in Strafverfahren […] zu leisten“. Erforderlich ist also zunächst, dass die Ermittlung der US-Behörde entweder als „strafrechtliches Ermittlungsverfahren“ oder gar als „Strafverfahren“ zu qualifizieren ist. Zu beachten ist dabei Art. 1 Abs. 1 S. 3 MLAT, wonach die entsprechenden Begriffe weit auszulegen sind, wenn es dort nämlich heißt: „Strafrechtliche Ermittlungsverfahren oder Strafverfahren nach diesem Vertrag sind auch Ermittlungen und Verfahren wegen Ordnungswidrigkeiten, soweit sie im ersuchenden Staat zu Gerichts- oder Strafverfahren führen können und soweit sie im ersuchten Staat Straftaten darstellen würden“.

Zu prüfen ist also zunächst, ob die in Rede stehende Subpoena im Rahmen eines entsprechenden Verfahrens erlassen worden ist, also zumindest im Rahmen eines Ordnungswidrigkeitenverfahrens. Dies wird in der Regel der Fall sein.

3.2 Pflicht zur Inanspruchnahme von Rechtshilfe unter dem MLAT

Soweit der Anwendungsbereich des MLAT eröffnet ist, fragt sich dann weiter, ob die US-Behörde aufgrund dieses Umstandes daran gehindert ist, selbst Zwangsmaßnahmen in Form einer Subpoena zu ergreifen. Wie die soeben zitierte Regelung des Art. 1 Abs. 1 S. 1 MLAT zeigt, regelt das MLAT zunächst die Pflicht der jeweils angefragten Behörden, auf Ersuchen der anfragenden Behörde hin Rechtshilfe zu leisten. Die Frage bleibt daher, ob das MLAT die jeweiligen lokalen Behörden der Bundesrepublik Deutschland bzw. der USA auch dazu verpflichtet, eine entsprechende Anfrage zu stellen.

Für eine solche Verpflichtung könnte die Regelung des Art. 1 Abs. 5 MLAT sprechen, der wie folgt lautet: „Eine Vertragspartei ersucht um Rechtshilfe gemäß den Bestimmungen dieses Vertrags, wenn Urkunden, Akten und andere Gegenstände, die sich im Hoheitsgebiet der anderen Vertragspartei befinden und im Zusammenhang mit einem unter den Geltungsbereich dieses Vertrags fallenden strafrechtlichen Ermittlungsverfahren oder Strafverfahren benötigt werden, durch Anwendung von Zwangsmaßnahmen oder Durchsuchung und Beschlagnahme beschafft werden sollen“. Der Wortlaut der Norm spricht in der Tat für eine entsprechende Pflicht. Und auch die Systematik der Norm spricht für eine solche Verpflichtung. Denn in den nachfolgenden Regelungen des Art. 1 Abs. 5 MLAT ist festgelegt, unter welchen Voraussetzungen die anfragende Partei ihren „vertraglichen Verpflichtungen“ unter dieser Norm erfüllt hat.

Andererseits ist der Anwendungsbereich der Norm auf „Urkunden, Akten und andere Gegenstände“ beschränkt. Der Wortlaut der Formulierung legt nahe, dass sich der Anwendungsbereich dieser Bestimmung lediglich auf physische „Gegenstände“ beschränkt, und damit z. B. elektronische Daten und insbesondere E-Mails nicht umfasst.

Hinzu kommt, dass die erfassten Rechtshilfetätigkeiten gemäß Art. 1 Abs. 2 MLAT insgesamt neun verschiedene Kategorien erfassen, von denen die „Überlassung von Urkunden, Akten und anderen Gegenständen“ lediglich eine der möglichen Maßnahmen darstellt. Dass in Art. 1 Abs. 5 MLAT eben nur diese eine Kategorie von Maßnahmen erwähnt ist, spricht dann im Umkehrschluss dafür, dass für alle weiteren Kategorien von Rechtshilfemaßnahmen gerade keine Pflicht besteht, sich an die Behörden des jeweils anderen Landes zu wenden.

Dieses Ergebnis überzeugt jedoch nicht. Denn es ist kaum nachvollziehbar, warum gerade für nur eine Kategorie von Maßnahmen die Pflicht bestehen soll, sich an die Behörden des jeweils anderen Landes zu wenden. Und noch weniger leuchtet es ein, warum elektronische Informationen anders behandelt werden sollten als etwa in Aktenordnern verkörperte Informationen. Insofern liegt es nahe, dass es sich bei

4 So auch *v. d. Bussche*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 4c BDSG, Rn. 12.
5 So etwa *Kopp/Pfisterer*, CCZ 2015, 151, 155.
6 Zur Abgrenzung anhand des Beispiels der Pre-Trial Discovery Verfahren siehe *v. d. Bussche*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 4c BDSG, Rn. 14; zum Meinungsstand und den Sichtweisen des Düsseldorfer Kreises sowie der Art. 29 Arbeitsgruppe siehe *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 4c, Rn. 7a.
7 Restriktiver *Spoerr*, in: Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 16. Edition, Stand: 01. 11. 2015, Grundlagen und bereichsspezifischer Datenschutz, Finanzwesen, Kapitel F, Rz. 145: „im Regelfall anonymisiert werden müssen sämtliche Angaben zu inländischen natürlichen Personen“.
8 Artikel-29-Datenschutzgruppe, Arbeitsunterlage 1/2009 über Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung bei grenzübergreifenden zivilrechtlichen Verfahren (pre-trial discovery) vom 11. Februar 2009.
9 Zum Merkmal der Erforderlichkeit im Rahmen von Compliance-Untersuchungen vgl. *Plath*, Compliance Untersuchungen und Datenschutz, DGRI Jahrbuch 2015, 183, 196.

der Vorschrift des Art. 1 Abs. 5 MLAT um eine redaktionell missglückte Regelung handelt. Schaut man nämlich auf den Regelungskontext, so wird deutlich, dass der gesamte Art. 1, wie auch das MLAT insgesamt, in erster Linie auf die Pflichten der angefragten bzw. ersuchten Behörden abstellt, und weniger auf die Pflicht, ein solches Ersuchen zu stellen. Und in diesem Lichte ist auch die Regelung des Art. 1 Abs. 5 S. 3 MLAT zu lesen, der in Verbindung mit S. 2 regelt, was gilt, wenn die angefragte Behörde das Ersuchen ablehnt bzw. zu spät reagiert.

Das deutsche Bundesministerium der Justiz sieht dies offenbar anders. Dies geht aus einem Schreiben vom 31. Januar 2007 hervor, welches das Ministerium auf Anfrage an den Berliner Beauftragten für Datenschutz und Informationsfreiheit gesendet hat.[10] Dort heißt es mit Blick auf die Rechtswirkungen des MLAT: „Artikel 1 Abs. 5 des Vertrags sieht vor, dass eine Vertragspartei den anderen Staat vorrangig um Rechtshilfe nach Maßgabe der Bestimmungen des Vertrags ersuchen muss, wenn sie Beweismittel aus dem Ausland benötigt. Die Vorschrift bezieht sich nach Auffassung der Vertragsparteien auf die oben erwähnten exterritorial wirkenden Maßnahmen. Nach Artikel 1 Abs. 5 sind derartige Maßnahmen grundsätzlich nicht mehr zulässig. Vielmehr ist zunächst der Rechtshilfeweg zu beschreiten. Demnach steht künftig der Rechtshilfevertrag nach seinem Inkrafttreten einer in Ihrer ersten Frage angesprochenen unmittelbaren Verpflichtung deutscher Unternehmen gegenüber dem US-Justizministerium zur Herausgabe von Daten ausdrücklich entgegen“.

Der Verweis auf die vermeintlich übereinstimmende Sichtweise der „Vertragsparteien“ wird jedenfalls seitens der US-Behörden so allerdings nicht geteilt. Denn der Umstand, dass immer wieder Subpoenas erlassen werden, zeigt, dass die US-Behörden sich weiterhin berechtigt sehen, zu diesem Mittel zu greifen.

Zusammenfassend ist das MLAT nach der hier vertretenen Ansicht damit dahingehend auszulegen, dass es zwar eine Pflicht zur Kooperation statuiert, falls die Behörde des anderen Landes ein Rechtshilfeersuchen stellt. Das MLAT enthält jedoch keine Pflicht, überhaupt so ein Ersuchen zu stellen.

3.3 Verhältnis des MLAT zu BDSG

Wenn man dem obigen Ergebnis folgt, wonach das MLAT die US-Behörden nicht davon abhält, die Herausgabe von Dokumenten und Informationen im Rahmen einer Subpoena zu verlangen, so liegt es auf der Hand, dass die Befolgung einer solchen Anordnung im Sinne des § 4c Abs. 1 S. 1 Nr. 4 BDSG „erforderlich“ ist.

Geht man aber mit den Befürwortern der Gegenansicht davon aus, dass die US-Behörden an sich verpflichtet wären, die Ansprüche im Wege eines Rechtshilfeersuchens durchzusetzen, so stellt sich die Frage, wie sich ein möglicher Verstoß gegen das MLAT – wohlgemerkt durch die US-Behörde, da sich die Pflichten des MLAT an die Organe der USA richten – auf die Rechtslage unter dem BDSG und auf die Position der für eine Datenweitergabe verantwortlichen Stelle in Deutschland auswirkt. In § 4b Abs. 1 BDSG ist insoweit zunächst ein Vorrang der einschlägigen Spezialgesetze vorgesehen. Ein solches stellt z. B. das Bundeskriminalamtgesetz dar, welches in § 37 BKAG ausdrücklich den Vorrang vor dem BDSG regelt. Indes sind die als „verantwortliche Stelle“ i. S. d. BDSG agierenden deutschen Unternehmen nicht Vertragspartei des MLAT, so dass ein Vorrang des MLAT vor dem BDSG insoweit gegenüber dem mit der Subpoena konfrontierten Unternehmen ausscheidet.[11]

Die Frage bleibt indes, ob die Anforderungen an die Erlaubnistatbestände unter dem BDSG überhaupt erfüllt sein können, wenn die in Rede stehende Maßnahme der US-Behörde einen Verstoß gegen das Völkerrecht begründet haben könnte. Wie dargestellt, ist die Übermittlung von personenbezogenen Daten an US-Behörden nach § 4c Abs. 1 S. 1 Nr. 4 BDSG zulässig, wenn die Übermittlung „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist“. Bei der hier behandelten Konstellation handelt das betroffene deutsche Unternehmen, um sich gegen die von den US-Behörden geltend gemachten Ansprüche zu verteidigen. Die Norm stellt dabei aber gerade nicht darauf ab, ob die Ansprüche seitens des Angreifers zu Recht erhoben worden sind. Denn zunächst einmal geht es darum, dass das Unternehmen im Rahmen des Erforderlichen das Recht haben muss, sich bestmöglich zu verteidigen.

Einschränkend könnte eingewandt werden, dass die Übermittlung von Daten in Reaktion auf eine (völker-)rechtswidrige Subpoena niemals „erforderlich“ sein kann, wie es die Regelung des § 4c Abs. 1 S. 1 Nr. 4 BDSG verlangt.[12] Allerdings ist insoweit erneut zu berücksichtigen, dass ein Verstoß gegen das MLAT zunächst lediglich einen Vertragsbruch seitens der US-Behörde darstellen würde, womit noch nicht gesagt wäre, dass ein US-Gericht der Subpoena tatsächlich deren Durchsetzbarkeit absprechen würde. Ganz im Gegenteil ist – wie nicht anders zu erwarten war – bereits entschieden worden, dass Beweise, die seitens der US-Behörden unter Verstoß gegen ein Rechtshilfeabkommen, hier mit den Niederlanden, gewonnen worden sind, weiter verwertet werden dürfen.[13]

Sachgerecht erscheint vor diesem Hintergrund eine Abgrenzung dahingehend, dass die Übermittlung allenfalls dann zu unterbleiben hat, wenn die Zwangsmaßnahme – hier die Subpoena – einen offensichtlichen Rechtsverstoß darstellt.[14] Denn die Grundsätze des Europäischen Datenschutzrechts dürfen nicht durch Maßnahmen der Behörden aus Drittstaaten untergraben werden, die offensichtlich nicht mit dem geltenden Recht im Einklang stehen. Fehlt es aber – wie vorliegend – an dieser Offensichtlichkeit, so müssen die deutschen Unternehmen als verantwortliche Stelle das Recht haben, sich innerhalb der Grenzen der Erlaubnistatbestände des BDSG und insbesondere des Erforderlichkeitsgrundsatzes bestmöglich zu verteidigen.

Für dieses Ergebnis spricht auch eine wertungsmäßige Betrachtung. Wenn man nämlich davon ausgeht, dass sich die deutschen Unternehmen im Rahmen einer freiwilligen Kooperation mit den US-Behörden auf die Erlaubnisnorm des § 4c Abs. 1 S. 1 Nr. 4 BDSG stützen können, dann ist nicht einzusehen, warum den Unternehmen dieses Recht genommen sein soll, sobald die US-Behörden zum Mittel der Subpoena greifen.[15]

4. Ergebnis zum BDSG

Das BDSG erlaubt die Verwendung personenbezogener Daten im Rahmen von Compliance-Untersuchungen, soweit der Erforderlichkeitsgrundsatz gewahrt bleibt. Zulässig ist in diesem Zusammenhang auch die Übermittlung personenbezogener Daten in die USA und zwar auf Grundlage des § 4c Abs. 1 S. 1 Nr. 4 BDSG, soweit die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Das MLAT zwischen der Bundesrepublik Deutschland und den USA steht diesem Ergebnis nicht entgegen. Denn das MLAT ist dahingehend

10 Veröffentlicht im Jahresbericht des Berliner Datenschutzbeauftragten aus dem Jahre 2007, abrufbar unter https://datenschutz-berlin.de/content/veroeffentlichungen/jahresberichte/bericht-07, dort S. 191.

11 So auch *v. d. Bussche*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 4c BDSG, Rn. 14a; a. A. *Kopp/Pfisterer*, CCZ 2015, 151, 152.

12 Siehe dazu auch *Kopp/Pfisterer*, CCZ 2015, 151, 155.

13 Vgl. U. S. v. Rommy, 506 F. 3d 108, 129 (2d Cir. 2007): "The admissibility of evidence in a United States court depends solely on compliance with United States law."

14 In diese Richtung auch bereits *Kopp/Pfisterer*, CCZ 2015, 151, 153.

15 Zur Frage der „freiwilligen“ Kooperation siehe bereits *Kopp/Pfisterer*, CCZ 2015, 151, 154.

auszulegen, dass es zwar eine Pflicht der deutschen Behörden zur Kooperation statuiert, falls die US-Behörden ein Rechtshilfeersuchen stellen. Das MLAT enthält jedoch keine ausdrückliche Pflicht, überhaupt so ein Ersuchen zu stellen. Vielmehr bleibt es den US-Behörden weiterhin möglich, ihre Ansprüche im Rahmen einer Subpoena zu verfolgen. Die andauernde Diskussion um die Zulässigkeit solcher Maßnahmen vor dem Hintergrund des bestehenden MLAT darf nicht auf dem Rücken der deutschen Unternehmen ausgetragen werden. Aus Sicht der deutschen Unternehmen besteht damit durchaus die „Erforderlichkeit“, den Anordnungen der Subpoena nachzukommen. Ihre Grenze findet diese Pflicht freilich in den Regelungen des BDSG, so z. B. bei der Frage, ob der Grundsatz der Erforderlichkeit die Übermittlung der Daten lediglich in pseudonymisierter Form verlangt.

5. Ausblick auf die Rechtslage unter der DSGVO

Unter der DSGVO ist die Übermittlung personenbezogener Daten in die USA und sonstige Drittländer in Art. 44 ff. DSGVO geregelt. Nach Art. 45 Abs. 1 DSGVO ist die Übermittlung zulässig auf Grundlage eines sog. „Angemessenheitsbeschlusses“ der Europäischen Kommission, mit dem festgestellt wird, dass in dem Drittland ein „angemessenes Datenschutzniveau“ herrscht. Davon ausgehend, dass die Kommission für die USA keinen entsprechenden Beschluss fassen wird, kommt eine Übermittlung auf Basis des Art. 46 DSGVO in Betracht. Danach ist eine Übermittlung möglich, wenn geeignete „Garantien“ für die Einhaltung des europäischen Datenschutzniveaus vorliegen. Zu diesen Garantien gehören z. B. von der Kommission erlassene „Standarddatenschutzklauseln“ oder „Verwaltungsvereinbarungen“. Die Entwicklung bleibt hier abzuwarten, wobei wohl davon ausgegangen werden kann, dass sich die US-Behörden kaum bereit erklären werden, Verpflichtungen zur Einhaltung des europäischen Datenschutzniveaus zu akzeptieren.

Art. 48 DSGVO regelt zudem ausdrücklich den Fall, dass die Behörde eines Drittlands die Übermittlung personenbezogener Daten verlangt. Nach Art. 48 DSGVO darf die entsprechende Entscheidung der Behörde nur dann anerkannt werden, wenn sie auf einer internationalen Übereinkunft wie etwa einem Rechtshilfeabkommen beruht. Bei der hier in Rede stehenden Konstellation einer Subpoena wäre dies gerade nicht der Fall, denn insoweit legitimiert das MLAT den Erlass der Subpoena gerade nicht; vielmehr wird diskutiert, ob das MLAT den Erlass der Subpoena sperrt. Gleichwohl führt dies nicht etwa dazu, dass die Übermittlung der Daten in Reaktion auf die Subpoena damit per se unzulässig wäre. Vielmehr sieht Art. 48 DSGVO ausdrücklich vor, dass die dargestellte Einschränkung lediglich „unbeschadet anderer Gründe für die Übermittlung“ gilt. Damit bleibt insbesondere ein Rückgriff auf Art. 49 DSGVO möglich, der bestimmte Ausnahmen von dem Übermittlungsverbot regelt.[16] Einschlägig ist insoweit die Regelung des Art. 49 Abs. 1 lit. e) DSGVO. Danach ist die Übermittlung zulässig, wenn sie „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich“ ist. Die Regelung ist damit weitgehend gleichlautend mit der derzeitigen Regelung unter dem BDSG, wobei der einschränkende Zusatz fehlt, dass diese Ansprüche „vor Gericht“ geltend gemacht werden müssen. Damit werden sich die Unternehmen auch nach Inkrafttreten der DSGVO auf diese Erlaubnisnorm stützen können.

16 *v. d. Bussche*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 48 DSGVO, Rn. 1.

Der Erich Schmidt Verlag zählt zu den führenden Fachverlagen im deutschen Sprachraum. 1924 gegründet, publiziert das Berliner Unternehmen heute crossmedial Fachinformationen in den Bereichen Recht, Wirtschaft, Steuern, Arbeitsschutz und Philologie. Mehr als 2.300 Titel umfasst das aktuelle Gesamtprogramm, davon etwa 400 in Form von Datenbanken, Zeitschriften, eJournals, Loseblattwerken und CD-ROMs. Der ESV empfiehlt sich über die ESV-Akademie als Veranstalter von Kongressen, Fachtagungen, Seminaren und Lehrgängen. Am Berliner Standort beschäftigt das Haus rund 120 Mitarbeiter.

Wir bieten:

Wahlstation für Rechtsreferendarinnen / Rechtsreferendare

Ihre Aufgaben

Mitarbeit in den juristischen Lektoraten, den Zeitschriftenredaktionen und der Online-Redaktion, u. a.:

- Inhaltliche und sprachliche Überprüfung von Manuskripten
- Konzeptionelle Überlegungen für neue Projekte
- Fahnenkorrektur und Endredaktion von Zeitschriftenausgaben
- Marktanalysen und Konkurrenzrecherchen
- Unterstützung bei der Autorenakquise
- Textentwürfe für redaktionelle Meldungen
- Teilnahme an Autorengesprächen

Ihr Profil

- Großes Interesse am Verlagsgeschäft
- Gute juristische und hervorragende Deutschkenntnisse sowie sicheres Sprachgefühl
- Selbstständige, strukturierte und verantwortungsvolle Arbeitsweise
- Hohe Zuverlässigkeit und Einsatzbereitschaft
- Gute MS-Office-Kenntnisse

Wenn wir Ihr Interesse wecken konnten und Sie Ihre Wahlstation etwas abseits des Mainstreams ableisten wollen, senden Sie bitte Ihre Bewerbungsunterlagen, gern auch per Mail, mit Angabe des bevorzugten Zeitraumes an:

Erich Schmidt Verlag GmbH & Co. KG
Personalabteilung
Genthiner Str. 30 G
10785 Berlin

E-Mail: Personalabteilung@ESVmedien.de
www.ESV.info

ESV ERICH SCHMIDT VERLAG

Unternehmen professionell führen und überwachen

Zeitschrift für Corporate Governance

Leitung und Überwachung in der Unternehmens- und Prüfungspraxis

Chefredaktion: **Dr. Joachim Schmidt**
Redaktion: **Dr. Hans-Jürgen Hillmer**

Zeitschrift und eJournal
12. Jahrgang 2017, 6 Ausgaben jährlich,
48 Seiten pro Heft, ISSN 1862-8702

Die ZCG informiert Sie alle zwei Monate über **neueste fachliche und regulatorische Entwicklungen** zur Corporate Governance. So bleiben Sie auf dem Laufenden, um die Standards guter Unternehmensführung zu erfüllen, eine professionelle Aufsicht auszuüben und souverän zu diesem Thema zu entscheiden.

Praxisnah. International ausgerichtet.

Namhafte Corporate-Governance-Experten berichten in den Rubriken **Management**, **Recht**, **Prüfung** und **Rechnungslegung** aus Unternehmenspraxis und Forschung – mit klarem Blick auf bestehende unternehmerische und persönliche Risiken und die immer anspruchsvolleren Qualifikationsanforderungen.

- **Analysen, Fallstudien und Best Practices** über das gesamte Themenspektrum professioneller Unternehmensführung und -überwachung
- **Nationale und internationale Richtlinien** sowie Initiativen und Diskussionspapiere der Corporate-Governance-Organisationen und Berufsverbände
- **Aktuelle Rechtsprechung** – die wichtigsten Urteile zur Corporate Governance, inklusive einer ausführlichen Kommentierung
- **Nachrichten und Services** wie Literatur-/Veranstaltungstipps u. v. m.

Jetzt gratis kennen lernen:

www.ZCGdigital.de/info

ESV ERICH SCHMIDT VERLAG
Auf Wissen vertrauen

Bestellungen bitte an den Buchhandel oder: Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-225 · Fax (030) 25 00 85-275 · ESV@ESVmedien.de · www.ESV.info

Warnsignale erkennen

„Korruption ist schuld am Pfusch" – solch eine Schlagzeile mag auf den ersten Blick zutreffen, doch folgt bei tieferer Betrachtung oft die Erkenntnis, dass eine **qualifizierte Aufsicht** in vielen Fällen die damit umschriebenen Wirtschaftsstraftaten verhindert hätte. Denn manipulierte Ausschreibungen und Korruption haben meist gemeinsam, dass auf Täter- wie auf Opferseite die unter anderem zur **Prävention unlauterer Geschäftspraktiken** installierte Aufsichtsfunktion versagt hat.

Fraud-Risiken wirksam überwachen

Hans J. Marschdorf stellt einen praktischen Leitfaden für die **Aufsicht über Beschaffungsprozesse und Verkaufspraktiken** bereit. Basierend auf 25 Jahren Ermittlungsarbeit als Forensic Accountant erläutert er

- **Ausprägungsformen** von Transaktionsmustern unlauterer Geschäftspraktiken,
- **Warnsignale**, welche auf entsprechende Ausprägungen von Korruption und Manipulation hinweisen,
- **Handlungskonzepte** für Analysen durch qualifizierte Nachfragen.

Anonymisierte **Beispiele tatsächlicher Fälle** geben anschauliche Einblicke. Ein **systematischer Fragenkatalog** unterstützt Mandatsträger bei der zielgerichteten Wahrnehmung ihrer Pflichten und Aufgaben.

Früherkennung unlauterer Geschäftspraktiken
Leitfaden für Aufsichtsgremien

Von **Dr. Hans J. Marschdorf**

2016, 157 Seiten, fester Einband, € (D) 29,95
ISBN 978-3-503-17098-2
Edition Governance

Auch als eBook erhältlich mit komplett verlinkten Inhalts- und Stichwortverzeichnissen.
www.ESV.info/17099

Weitere Informationen:
www.ESV.info/17098

ESV ERICH SCHMIDT VERLAG
Auf Wissen vertrauen

Bestellungen bitte an den Buchhandel oder: Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-265 · Fax (030) 25 00 85-275 · ESV@ESVmedien.de · www.ESV.info

Updates für Neustarter

Einführung in das IT-Management

Grundlagen, Umsetzung, Best Practice

Von **Prof. Dr. Olaf Resch**

4., neu bearbeitete Auflage 2016,
335 Seiten, mit zahlreichen Abbildungen,
€ (D) 29,95, ISBN 978-3-503-16747-0

Wie angehende IT-Manager mit analytischem und zielorientiertem Vorgehen ihr anspruchsvolles Fach meistern, zeigt Ihnen Olaf Resch:

- Grundlagen und Zusammenhänge des IT-Managements
- Vorstellung eines generischen IT-Management-Modells
- ausgewählte Best Practices und Pragmatiken
- IT-Governance – als umfangreiches Praxisbeispiel
- mit vielen Übungen, interaktiv vernetzt über ein begleitendes Wiki

Aktuelle Erweiterungen

Neu berücksichtigt in der **4. Auflage des beliebten Einführungswerks** wurde der immer wichtigere Bereich Cyber-Sicherheit und das Management komplexer Unternehmensarchitekturen. Neben COBIT 5 und ITIL werden auch TOGAF und IT-Grundschutz behandelt.

Stimmen zur Vorauflage

»Wohl eines der besten Standardwerke für diese Thematik!«
amazon.de, 31. Mai 2013

»... ideale Ergänzung zu einer Weiterbildung bzw. zum Studium.«
amazon.de, 2. Februar 2013

Weitere Informationen:
www.ESV.info/16747

ESV ERICH SCHMIDT VERLAG
Auf Wissen vertrauen

Bestellungen bitte an den Buchhandel oder: Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-265 · Fax (030) 25 00 85-275 · ESV@ESVmedien.de · www.ESV.info

Von Compliance überzeugen

Compliance-Kommunikation

Professionell – international – zielgruppengerecht

Herausgegeben von
Dr. Katharina Hastenrath

2017, 446 Seiten, mit zahlreichen Abbildungen,
fester Einband, € (D) 79,95, ISBN 978-3-503-16756-2

Auch als eBook erhältlich: mit komplett verlinkten Inhalts- und Stichwortverzeichnissen.
www.ESV.info/16757

Kommunikation ist ein wesentlicher Erfolgsfaktor jeder Compliance-Organisation und spätestens seit dem BGH-Urteil zur Unterlassensstrafbarkeit von Compliance-Officern auch haftungsrelevant. Nur wer Klarheit über Erwartungen und Pflichten, Sinn und Funktionen der eingesetzten Steuerungsinstrumente schafft, kann mit der Akzeptanz, dem Engagement und dem notwendigen Risikobewusstsein aller Beteiligten rechnen.

Beteiligte Stakeholder richtig adressieren

Wie Sie Führungskräfte, Mitarbeiter und Geschäftspartner erreichen und zielgerichtet einbinden, betrachtet dieser Band konsequent mit Fokus auf Compliance.

- **Risikoprävention und Enthaftung** von Organen und Mitarbeitern z. B. durch adressatengerechte Mitarbeiterinformation
- **HR-Compliance und Kommunikation** unter Berücksichtigung arbeitsrechtlicher Fragen
- **Spezielle Kommunikationselemente**, z. B. zur Gestaltung der Ombudsmann-/Whistleblowing-Funktion
- **Best Practice, Tools und Technologien** für die Darstellung von Compliance-Aufgaben, Gesprächsführung und Konfliktlösung
- **Interkulturelle Kompetenz** als Herausforderung internationaler Compliance-Kommunikation

Mit den Beiträgen eines **BGH-Richters** sowie von **Compliance- und Risikospezialisten** aus Unternehmen und Anwaltschaft, von **Kommunikationsexperten** und **Psychologen**.

Weitere Informationen:
www.ESV.info/16756

ESV ERICH SCHMIDT VERLAG
Auf Wissen vertrauen

Bestellungen bitte an den Buchhandel oder: Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-265 · Fax (030) 25 00 85-275 · ESV@ESVmedien.de · www.ESV.info

Das Komplettpaket.

COMPLIANCEdigital

Alles für € (D) 22,95* im Monat

COMPLIANCEdigital – die Datenbank bündelt erstklassige Fachinformationen und Entscheidungshilfen für das Compliance-Management: Artikel aus führenden Fachzeitschriften wie der *Risk, Fraud & Compliance (ZRFC)* und der *PinG Privacy in Germany* sowie eBooks zu zentralen Compliance-Themen. Checklisten, Leitfäden, Mustervorlagen und andere Arbeitsdokumente unterstützen Sie ebenso wie die treffsichere Suchfunktion.

Das Plus: Arbeitshilfen · News · aktuelle Rechtsprechung · Literaturempfehlungen · Stellenanzeigen · Veranstaltungskalender!

Mehr als 6.200 Dokumente, 6 eJournals und über 230 eBooks stehen für Sie bereit – jetzt reinschauen:

www.COMPLIANCEdigital.de

COMPLIANCEdigital

Datenbank, Jahresabonnement monatlich € (D) 22,95*

ISBN 978-3-503-11626-3

* Preis zzgl. 19 % USt.

ERICH SCHMIDT VERLAG

Auf Wissen vertrauen

Bestellungen bitte an den Buchhandel oder: Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-227 · **Fax** (030) 25 00 85-275 · **ESV@ESVmedien.de** · **www.ESV.info**