ISSN 0178-8930

G 20 141

RDV

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

5/2016

Recht der Datenverarbeitung

Herausgegeben von

Peter Gola · Andreas Jaspers · Rolf Schwartmann · Gregor Thüsing
in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Aufsätze

TAVANTI, Datenverarbeitung zu Werbezwecken nach der Datenschutz-Grundverordnung (Teil 1)

SCHWARTMANN/WEIß, Ko-Regulierung vor einer neuen Blüte: Impulse für datenschutzspezifische Zertifizierungsverfahren und Verhaltensregelungen (2. Teil Verhaltensregeln)

HEIDRICH/WEGENER/SCHEUCH, Prüfungspflichten beim Verbot der Nutzung von Internet und E-Mail im Unternehmen

Kurzbeiträge

BORNEMANN/WETZEL, Die EU-Datenschutz-Grundverordnung in der Umsetzung: Eine Diskussion über Chancen und Herausforderungen

GOLA, Aus den Aktuellen Berichten der Aufsichtsbehörden (27): Kommunales

Rechtsprechung

Aus dem Inhalt

BVERFG, Zur Gewährung von Schmerzensgeld nach rechtswidrigem Freiheitsentzug (Ls)

BVERFG, Wahre Tatsachenbehauptungen über Vorgänge aus der Sozialsphäre sind grundsätzlich hinzunehmen (Ls)

BVERFG, Die falsche Einordnung einer Äußerung als Schmähkritik verkürzt den grundrechtlichen Schutz der Meinungsfreiheit (Ls)

BVERFG, Eilanträge gegen das Vorratsdatenspeicherungsgesetz erfolglos

BGH, Zur Wirksamkeit eines im Rahmen eines „Cold Calls“ abgeschlossenen Vertrages

BAG, Entschädigung nach § 15 Abs. 2 AGG aufgrund einer Diskriminierung wegen Schwerbehinderung (Ls)

32. Jahrgang
Oktober 2016
Seiten 229–282

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Wir suchen Verstärkung!

Datenschutzberater (m/w)

Wir suchen einen kompetenten Mitarbeiter (m/w) für die Gebiete der Datenschutzberatung und der externen Datenschutzbeauftragung.

Ihre Aufgaben

Im Rahmen der Tätigkeiten für unsere Kunden werden Sie u. a. mit folgenden Aufgaben betraut:

- Beratung zu Grundsatzfragen und komplexen Einzelfallentscheidungen im Datenschutz
- Durchführung von Audits, Revisionen und Analysen
- Prüfung der Angemessenheit von sicherheitstechnischen Maßnahmen zum Schutz personenbezogener Daten
- Ausarbeitung, Erstellung und Fortschreibung einer übergreifenden Datenschutzkonzeption
- Information und Schulung der Mitarbeiter

Voraussetzungen

Für diese anspruchsvolle Aufgabe sollten Sie folgende Voraussetzungen mitbringen:

- solide Grundkenntnisse auf dem Gebiet des Datenschutzes (Datenschutzrecht & -technik)
- Erfahrungen in den Branchen Gesundheit, Energie, Hochschule oder Industrie
- Fähigkeit zu fachlich hochwertiger Beratung
- Kontaktfähigkeit und Freude am Umgang mit Kunden
- Fähigkeit zum klaren Ausdruck in Wort und Schrift (in Deutsch und weiterer Sprache)
- gute Kenntnisse im Umgang mit modernen Kommunikationsmitteln & Computersystemen
- Bereitschaft zum Reisen - auch europaweit - und PKW-Führerschein

Wir bieten einen sicheren Arbeitsplatz und die Möglichkeit, das Einkommen erfolgsorientiert zu steuern. Eine profunde Einarbeitung in das Unternehmen, die zu betreuenden Kunden und eine tiefgehende Fortbildung in die spezifischen Datenschutzproblematiken sind selbstverständlich. Ein Teil Ihrer Bürotätigkeit kann ggf. im Home-Office erbracht werden.

Bewerbungsanschrift

UIMC Dr. Vossbein GmbH & Co KG
Frau Monika von Waldowski
Nützenberger Straße 119
42115 Wuppertal

Wenn Sie sich angesprochen fühlen, freuen wir uns auf Ihre Bewerbungsunterlagen! Hierbei bitten wir Sie auch um die Angabe Ihrer Gehaltsvorstellungen und des nächstmöglichen Einstiegsdatums.

Wir sind eine gesellschaftergeführte, mittelständische Unternehmensberatung mit Standorten in Wuppertal, Saarbrücken und Wien. Im Datenschutz gehören wir zu den marktführenden Dienstleistern und bieten als Vollsortimenter von einzelnen Tools und Stellungnahmen bis hin zum Komplett-Outsourcing in Form einer externen Datenschutzbeauftragung sämtliche Unterstützungsmöglichkeiten der Analyse, Beratung, Umsetzung und Schulung/Sensibilisierung an. Dies gilt im Übrigen für alle relevanten Rechtsnormen aus Bund, Land und Kirche.

Wir beraten eine Vielzahl von mittelständischen sowie großen Institutionen und sind im Bereich des Datenschutzes bei einer beachtlichen Anzahl von Unternehmen als externer Datenschutzbeauftragter bestellt. Die auch aufgrund der hohen Qualität und Zufriedenheit langfristigen Kundenbeziehungen haben zu einer stetigen Ausdehnung unseres Tätigkeitsgebiets geführt. Unsere Erfolge haben dazu geführt, dass wir unser Mitarbeiterteam vergrößern möchten.

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

32. Jahrgang 2016
Heft 5
Seiten 229–282

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial

229

Veranstaltungen

230

Aufsätze

Pascal TAVANTI
Datenverarbeitung zu Werbezwecken nach der Datenschutz-Grundverordnung (Teil 1) **231**

Prof. Dr. Rolf SCHWARTMANN/Steffen WEIß
Ko-Regulierung vor einer neuen Blüte: Impulse für datenschutzspezifische Zertifizierungsverfahren und Verhaltensregelungen (2. Teil Verhaltensregeln) **240**

Joerg HEIDRICH/Dr. Christoph WEGENER/
Brian SCHEUCH
Prüfungspflichten beim Verbot der Nutzung von Internet und E-Mail im Unternehmen **246**

Kurzbeiträge

Dr. Dirk BORNEMANN/Lennart WETZEL
Die EU-Datenschutz-Grundverordnung in der Umsetzung: Eine Diskussion über Chancen und Herausforderungen **253**

Prof. Peter GOLA
Aus den Aktuellen Berichten der Aufsichtsbehörden (27): Kommunales **259**

Rechtsprechung

Zur Gewährung von Schmerzensgeld nach rechtswidrigem Freiheitsentzug (Ls)
(BVerfG, Beschluss vom 29.06.2016) **262**

Wahre Tatsachenbehauptungen über Vorgänge aus der Sozialsphäre sind grundsätzlich hinzunehmen (Ls)
(BVerfG, Beschluss vom 29.06.2016) **262**

Die falsche Einordnung einer Äußerung als Schmähkritik verkürzt den grundrechtlichen Schutz der Meinungsfreiheit (Ls)
(BVerfG, Beschluss vom 29.06.2016) **263**

Eilanträge gegen das Vorratsdatenspeicherungsgesetz erfolglos
(BVerfG, Beschlüsse vom 08.06.2016) **263**

Zur Wirksamkeit eines im Rahmen eines „Cold Calls" abgeschlossenen Vertrages
(BGH, Urteil vom 21.04.2016) **267**

Entschädigung nach § 15 Abs. 2 AGG aufgrund einer Diskriminierung wegen Schwerbehinderung (Ls)
(BAG, Urteil vom 11.08.2016) **270**

Einsicht in Personalakten unter Hinzuziehung eines Rechtsanwalts (Ls)
(BAG, Urteil vom 12.07.2016) **270**

An- und Abmeldepflicht freigestellter Betriebsratsmitglieder (Ls)
(BAG, Beschluss vom 24.01.2016) **270**

Auskunft eines freigestellten Betriebsratsmitglieds über Gehälter vergleichbarer Arbeitnehmer
(BAG, Urteil vom 04.11.2015) **270**

Pflicht zur Vorlage der elektronischen Gesundheitskarte
(LSG Baden-Württemberg, Urteil vom 21.06.2016) **274**

Anforderungen an Einwilligungen bei Smart TV (Ls)
(LG Frankfurt a.M., Urteil vom 10.06.2016) **276**

Berichte, Informationen, Sonstiges

Tagungsbericht „Vertrauen und Vergessen(werden) in der digitalen Gesellschaft" am 31.05. und 01.06. im Fraunhofer-Forum Berlin (KEBER) **277**

Zwei von drei Internetnutzern sind in sozialen Netzwerken aktiv **278**

Bundesinnenminister will Vorratsdatenspeicherung auf Messenger-Dienste erweitern **278**

Große Mehrheit der Fluggäste will Ganzkörperscanner am Airport **279**

Literaturhinweise

Buchbesprechungen

Tamina Preuß (Hrsg), Die Kontrolle von E-Mails und sonstigen elektronischen Dokumenten im Rahmen unternehmensinterner Ermittlungen (REDAKTION) **280**

Neuerscheinungen

Aufsätze **281**

Nachgefasst

282

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

Prof. Dr. Rolf SCHWARTMANN, Fachhochschule Köln

Prof. Dr. Gregor THÜSING, LL.M. (Harvard), Universität Bonn

in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

Dietrich BOEWER, Vorsitzender Richter am Landesarbeitsgericht Düsseldorf i.R.

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

Dr. Joachim W. JACOB, Bundesbeauftragter für den Datenschutz a.D.

Prof. Dr. Friedhelm JOBS, Richter am Bundesarbeitsgericht a.D.

Prof. Dr. Tobias O. KEBER, Hochschule der Medien, Stuttgart

Prof. Dr. Karl LINNENKOHL, Universität Kassel

Dr. h.c. Hans-Christoph MATTHES, Vorsitzender Richter am Bundesarbeitsgericht a.D.

Dr. Alexander OSTROWICZ, Präsident des Landesarbeitsgerichts Schleswig-Holstein a.D.

Prof. Dr. Michael RONELLENFITSCH, Hessischer Datenschutzbeauftragter

Prof. Dr. Friedhelm ROST, Vorsitzender Richter am Bundesarbeitsgericht a.D.

Peter SCHAAR, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D.

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

Prof. Dr. Dres. h.c. Spiros SIMITIS, Universität Frankfurt

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis GDD-Mitteilungen 5/2016;

Manuskripte:
Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an die Schriftleitung erbeten. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Beiträge werden grundsätzlich nur angenommen, wenn sie nicht einer anderen Zeitschrift zur Veröffentlichung angeboten wurden. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Autor alle Rechte, insbesondere das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken mit Hilfe fotomechanischer oder anderer Verfahren.

Urheber- und Verlagsrechte:
Sie sind einschließlich der Veröffentlichung als PDF im Online-Archiv vorbehalten. Sie erstrecken sich auch auf die veröffentlichten Gerichtsentscheidungen und deren Leitsätze; diese sind geschützt, soweit sie vom Einsender oder von der Schriftleitung erstellt oder bearbeitet sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen: Diese bedürfen zur Auswertung einer Genehmigung des Verlages.
Der Verlag gestattet in der Regel die Herstellung von Fotokopien zu innerbetrieblichen Zwecken, wenn dafür eine Gebühr an die VG Wort, Abteilung Wissenschaft, Goethestraße 49, 80336 München, entrichtet wird, von der die Zahlungsweise zu erfragen ist.

Schriftleitung
Prof. Peter Gola (federführend)
RA Dr. Georg Wronka
RA Andreas Jaspers
RDV-Schriftleitung@gdd.de

Redaktionsanschrift
Birgit Koppitsch
Heinrich-Böll-Ring 10, 53119 Bonn
Telefon: (02 28) 96 96 75-00
Telefax: (02 28) 96 96 75-25
RDV-Redaktion@gdd.de

Erscheinungsweise
6 x jährlich

Bezugspreis

Jahresabonnement	€ 139,–
Einzelheft	€ 25,–

MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Bestellungen
DATAKONTEXT GmbH, Frechen
Jürgen Weiß
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-71
Telefax: (0 22 34) 9 89 49-32
E-Mail: weiss@datakontext.com
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Abbestellungen
Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Verlag
DATAKONTEXT GmbH, Frechen
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-30
Telefax: (0 22 34) 9 89 49-32
www.datakontext.com
Geschäftsführung: Dr. Karl Ulrich;
Hans-Günter Böse
HRB 337678

Satz
alka mediengestaltung gmbh
Ottostraße 6, 53332 Bornheim-Sechtem

Druck
AZ Druck und Datentechnik GmbH
Heisinger Straße 16, 87437 Kempten

Anzeigenverwaltung
DATAKONTEXT GmbH, Frechen
Thomas Reinhard-Rief
Hultschiner Straße 8
D-81677 München
Telefon: (089) 21 83-89 35
Fax: (089) 21 83-96 02 33
E-Mail: reinhard@datakontext.com
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Zeitschrift für
Datenschutz-, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
32. Jahrgang 2016 Heft 5
Seiten 229–282

RDV
Recht der Datenverarbeitung

32. Jahrgang · Oktober 2016 · Seiten 229–282

Editorial

Was werden Datenschutzverstöße kosten?

Onlinedienste nutzen die meisten am liebsten unkompliziert. Mit Grummeln im Bauch haben wir uns daran gewöhnt, bei Einwilligungserklärungen nach Software-Updates für Smartphones, Messangerdienste & Co. einfach zu lügen. Die Aussage „Ich habe die Datenschutzerklärung gelesen und stimme der Nutzung zu" ist in der Lebenswirklichkeit nicht ernst zu nehmen. Onlinedienste nutzen das aus. Twitter hat seine Nutzer kürzlich per Mail über die Verbesserung seiner Allgemeinen Geschäftsbedingungen und Datenschutzrichtlinien informiert. Es wurde etwa ein Abschnitt zum EU-US Privacy Shield aufgenommen. Genaueres erfährt man online im „Hilfecenter". Zudem wird man aufgefordert, sich „einen Moment" Zeit zu nehmen, die neuen Informationen zu lesen. Soweit so gut. Danach wird es rechtlich interessant. „Wenn du unsere Services am oder nach dem 30. September 2016 nutzt, erklärst du dich mit den Änderungen einverstanden.

Danke, dass Du Twitter nutzt."

Ohne lange über die Anforderungen an Freiwilligkeit oder Formerfordernisse für die Einwilligung zu grübeln, springt den Nutzer die Unzulässigkeit der Einverständniserklärung förmlich an. Schweigen oder Untätigkeit erzeugt nur in Ausnahmefällen rechtliche Bindungen. Datenschutzrechtlich lässt Erwägungsgrund 32 der DS-GVO ausdrücklich keinen Zweifel daran, dass es so wie Twitter es macht, nicht geht. Der Verstoß gegen Art. 6 und 7 DS-GVO, die die Anforderungen an Einwilligungen regeln, ist offensichtlich. Er findet zudem millionenfach statt. Wer als Betreiber eines Onlinedienstes behauptet, ihm seien fundamentale Grundsätze des europäischen Vertrags- und Datenschutzrechts nicht geläufig, der sollte sich bald eines Besseren belehren. Verstöße gegen Art. 6 und 7 DS-GVO sind nämlich bußgeldbewehrt. Und zwar mit bis zu 4% des Vorjahresumsatzes des Unternehmens. Legt man die gut 2,2 Milliarden US-Dollar zugrunde, die Twitter 2015 weltweit umgesetzt hat, dann hat man eine Berechnungsgrundlage. Für die genaue Ermittlung des Bußgeldes gibt die DS-GVO eine Leitlinie. Die Geldbuße muss „im Einzelfall wirksam, verhältnismäßig und abschreckend" sein. Konkret kommt es etwa auf die Schwere und Dauer des Verstoßes, den Grad des Verschuldens oder privilegierend darauf an, ob der Anbieter sich an akzeptierte Verhaltensregeln hält oder gar zertifiziert ist. So nachhaltig, wissend, nachweislich und robust, wie Twitter per Mail europäisches Datenschutzrecht 2016 verletzt hat, könnte die Aufsicht dann erwägen, ob man den Verstoß milde bei 1% und gut 22 Millionen US-Dollar ansetzt oder, ob man doch auf abschreckende 4 %, also gut 88 Millionen US-Dollar zusteuern muss. Wegen der Umrechnung in Euro, mag die Summe etwas sinken. Alternativ kann die Aufsicht nach Art. 83 DS-GVO ein Bußgeld bis 20 Millionen Euro verhängen, wenn der Betrag gemessen am Umsatz höher ist. Wenn Twitter seine Einwilligungen weltweit so einholt wie in Deutschland, dann kann das Unternehmen die Aufsicht bei Verstößen in Europa nicht einmal davon überzeugen, dass für die Berechnung des Bußgeldes nur der Umsatz in Europa zugrunde zu legen ist. Erwägungsgrund 150 legt nämlich nahe, dass der Konzernumsatz zählt. So oder so. Allzu oft wird man sich Datenverwendungen ohne wirksame Einwilligungen nicht leisten können.

Professor Dr. Rolf Schwartmann

Prof. Dr. Rolf Schwartmann
Leiter der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln, Mitherausgeber der Fachzeitschrift RDV sowie Vorstandsvorsitzender der GDD e.V., Bonn

Termin	Thema	Ort	Kontakt
03.11.2016	Grundlagen der Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
03.11.2016	Hacker-Tools für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
03.11.2016	Die Datenschutz-Grundverordnung	Nürnberg	GDD e.V. und DATAKONTEXT
07.11.2016	IT-Sicherheit für Datenschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
07.–08.11.2016	Datenschutz Management – Teil 3	Berlin	GDD e.V. und DATAKONTEXT
10.11.2016	Verfahrensverzeichnis, Verarbeitungsübersicht, Vorabkontrolle	Stuttgart	GDD e.V. und DATAKONTEXT
16.11.2016	35. RDV-Forum	Köln	GDD e.V. und DATAKONTEXT
17.–18.11.2016	40. DAFTA	Köln	GDD e.V. und DATAKONTEXT
21.–23.11.2016	Das SAP-System für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
22.11.2016	Repetitorium GDDcert.	Köln	GDD e.V. und DATAKONTEXT
24.11.2016	Kontrolle von Auftragnehmern im Rahmen der Auftrags-datenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
29.11.2016	Die Datenschutz-Grundverordnung	Münster	GDD e.V. und DATAKONTEXT
30.11.2016	Big Data-Analysen und der Datenschutz	Köln	GDD e.V. und DATAKONTEXT
28.11.–02.12.2016	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
05.12.2016	Pflichten bei Datenpannen – Wie Sie das Haftungsrisiko für Ihr Unternehmen reduzieren können	Köln	GDD e.V. und DATAKONTEXT
07.12.2016	ISO 27001 und Datenschutz	Köln	GDD e.V. und DATAKONTEXT
07.12.2016	SAP-Funktionen für den Datenschutz	Köln	GDD e.V. und DATAKONTEXT
12.12.2016	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert.)	Köln	GDD e.V. und DATAKONTEXT
30.–31.01.2017	GDD-Winter-Workshop	Garmisch-Partenkirchen	GDD e.V. und DATAKONTEXT
14.02.2017	Datenschutz und Videoüberwachung – Was geht und was geht nicht?	Köln	GDD e.V. und DATAKONTEXT
15.02.2017	Personalprozesse datenschutzkonform organisieren	Köln	GDD e.V. und DATAKONTEXT
13.–17.02.2017	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Bonn	GDD e.V. und DATAKONTEXT
21.02.2017	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
22.–23.02.2017	3. Göttinger Forum IT-Recht	Göttingen	Institut für Wirtschafts-recht der Universität Göttingen, www.goettingen-itrecht.de

DATAKONTEXT GmbH, Telefon: 0 22 34/9 89 49 40

Aufsätze

Pascal Tavanti

Datenverarbeitung zu Werbezwecken nach der Datenschutz-Grundverordnung (Teil 1)[1]

Ab dem 25.05.2018 ist die Datenschutz-Grundverordnung (DS-GVO)[2] „in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat" (Art. 99 Abs. 2). Damit werden in absehbarer Zeit für alle Bereiche des Wirtschaftslebens neue Regeln beim Datenschutz zu beachten sein, unter anderem auch für die Unternehmen der Werbewirtschaft. Die jeweils zuständigen – nach der Terminologie der DS-GVO die „federführenden" – Aufsichtsbehörden (Art. 56), die nationalen Gerichte (Art. 79)[3] sowie Organisationen im Sinne von Art. 80[4] werden die Verordnung anzuwenden haben. Um der Umsetzung der neuen Vorgaben Nachdruck zu verleihen, sieht die DS-GVO mehr und zugleich empfindlich geschärfte Sanktionen vor.[5] Dies ist Anlass genug, sich mit dem werbewirtschaftlichen Datenschutz nach der DS-GVO näher zu befassen. Der Beitrag thematisiert die Grundlagen: Welche Regelungen sind heranzuziehen und was ist hierbei zu beachten? Was ist neu? Inwiefern besteht Kontinuität zwischen den bislang einschlägigen Regelungen in Deutschland, insbesondere in Bezug auf § 28 Abs. 3 ff., § 29 BDSG und den §§ 12 ff. TMG auf der einen und der DS-GVO auf der anderen Seite? Was ist zwar anders formuliert, substantiell aber unverändert? Eine Übersicht für Praktiker.

I. Ausgangslage und Grundbedingungen der Rechtsanwendung unter der DS-GVO

Die DS-GVO besteht aus 99 Artikeln, die durch 173 Erwägungsgründe (ErwG) erläutert und spezifiziert werden.[6] Erste Einschätzungen sprechen davon, die DS-GVO sei erheblich „unterkomplex", weil bezogen auf sämtliche materielle datenschutzrechtliche Fragen, für die im deutschen Datenschutzrecht bislang „tausende von Vorschriften bestehen", nunmehr lediglich „45 Artikel des materiellen Datenschutzes" zur Verfügung stünden.[7] Ob die Breite und Komplexität des Sachgebiets Datenschutz (insgesamt) tatsächlich so eklatant unterschätzt wurde, sei hier dahingestellt. Tatsache ist, dass die DS-GVO spezifische Erlaubnistatbestände zur Datenverarbeitung zwecks Werbung nicht kennt, den Begriff „Direktwerbung" im verfügenden Teil lediglich punktuell, nämlich beim Widerspruchsrecht (Art. 21 Abs. 2, 3), aufgreift und die Thematik im Rahmen der Erwägungsgründe ebenfalls nur punktuell, wenngleich auch in bedeutsamer Weise, bedenkt.[8] Verglichen mit den kleinteiligen Ausdifferenzierungen, die die Regelungen zum Datenumgang zu werbewirtschaftlichen Zwecken nach der BDSG-Novelle II[9] aus dem Jahr 2009 erfahren haben, ist dies natürlich – neutral formuliert – eine veritable Abstraktion. Verglichen mit der EU-Datenschutzrichtlinie (DSRL)[10] scheint vorstehender Befund aber bereits weniger dramatisch.[11]

1 Teil 1 thematisiert den relevanten Normenbestand, die für die werbewirtschaftliche Datenverarbeitung grundlegenden Prinzipien und die einwilligungsbasierte Datenverarbeitung. Teil 2 (RDV 6/2016) umfasst die Datenverarbeitung im Rahmen rechtsgeschäftlicher Verhältnisse, aufgrund der Interessenabwägung und ausgewählte Problemlagen.

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG, ABl. L 119 v. 4.5.2016. Alle Artikel und Erwägungsgründe (ErwG) ohne Gesetzesangabe beziehen sich auf die DS-GVO.

3 Wobei die letztlich verbindliche Interpretation der DS-GVO nach Maßgabe des Vorabentscheidungsverfahrens dem EuGH obliegt, Art. 267 Abs. 1 AEUV. Bei entscheidungserheblichen Rechtsfragen sind sämtliche deutschen Gerichte angehalten, den EuGH anzurufen und bis zu dessen Entscheidung das eigene Verfahren ruhen zu lassen. Unterbleibt ein solches Vorlageverfahren, ist für betroffene Personen, Verantwortliche oder Auftragsverarbeiter der Weg zum BVerfG verschlossen, vgl. Schwartmann, RDV 2015, 55.

4 Funktional vergleichbar mit den bereits seit dem 24.2.2016 erweiterten datenschutzrechtlichen Rechtsdurchsetzungsbefugnissen anspruchsberechtigter Stellen nach dem Unterlassungsklagegesetz (UKlaG), BGBl. I Nr. 8 vom 23.02.2016, S. 233ff.

5 Spindler DB 2016, 946.

6 Rechtsakte der EU sind nach Art. 296 Abs. 2 AEUV mit einer Begründung zu versehen. Anders als die Gesetzesbegründung bei deutschen Gesetzen, die als Teil des parlamentarischen Verfahrens betrachtet wird, ist die Begründung in Gestalt der ErwG Teil des Rechtsakts selbst und unterliegt als wesentliche Förmlichkeit des Rechtsakts der gerichtlichen Kontrolle (Art. 263 Abs. 2 AEUV). Wenngleich aus den ErwG als solche keine verbindlichen Rechtsfolgen resultieren, sind sie bei der Auslegung des verfügenden Teils höchst bedeutsam. Der EuGH greift hierauf regelmäßig im Rahmen seiner stärker systematischen und teleologischen Methoden verpflichteten Auslegung des Unionsrechts zurück.

7 Roßnagel, Stellungnahme zum Fachgespräch zur DS-GVO im Bundestagsausschuss Digitale Agenda, S. 2, abrufbar unter: http://isi.fraunhofer.de/forum-privatheit-de/aktuelles/aktuelles_dokumente/Stellungnahme-zu-Fragen-des-Ausschusses-digitale-Agenda.pdf .

8 ErwG 47 a.E. „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden." Verglichen mit anderen Verarbeitungszwecken ist dies eine materiell bedeutsame, weil für den Erlaubnistatbestand der Interessenabwägung nach Art. 6 Abs. 1 lit. f unmittelbar abwägungsrelevante, Determinante, näheres unter Teil 2. Weitere Erwähnungen in ErwG 58 (Transparenz der Datenverarbeitung und Information der Betroffenen), ErwG 70 (Widerspruchsrecht).

9 Gesetz zur Änderung datenschutzrechtlicher Vorschriften v. 14.08.2009 (BGBl. I, S. 2814).

10 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 v. 23.11.1995, S. 31.

11 Werbung wird dort lediglich erwähnt in Art. 14 lit. b: Widerspruchsrecht gegenüber Direktwerbung, ErwG 30: Mitgliedsstaaten können im Rahmen der Richtlinienvorgaben nähere Bedingungen festlegen, unter denen Daten an Dritte zwecks Werbung weitergegeben werden; sowie ErwG 70.

1. Der (voraussichtliche) Normenbestand ab dem 25.5.2018

Entscheidende Bedeutung kommt neben der Aufhebung der DSRL der geänderten Regelungstechnik, mithin der Verabschiedung einer EU-Verordnung zu (Art. 94 Abs. 1). Die DS-GVO ist, auch wenn sie als „Datenschutz-Grundverordnung" bezeichnet ist, wie jede EU-Verordnung in allen Teilen verbindlich, Art. 288 Abs. 2 AEUV. Damit ist sie Teil der deutschen Rechtsordnung und beansprucht unmittelbare Geltung. Mit Wirksamwerden der DS-GVO werden ihre Regelungen unmittelbar geltendes Recht, allerdings ohne das BDSG und die datenschutzrechtlichen Spezialgesetze automatisch außer Kraft zu setzen. Die Regelungen der DS-GVO treten an die Stelle all jener nationalen Rechtsnormen, die bezogen auf den Anwendungsbereich der DS-GVO (Art. 2 DS-GVO) den neuen Vorgaben widersprechen (sog. Anwendungsvorrang). Die damit normativ geschärfte europaweite Vollharmonisierung des Datenschutzrechts[12] ersetzt die aus Sicht der EU nicht erfolgreiche, weil lediglich zielbezogene, Vollharmonisierung nach der DSRL.[13] Dies soll zu mehr Rechtssicherheit, zu einer Stärkung der Betroffenenrechte und zur Förderung des gemeinsamen Marktes beitragen.[14]

Damit sind die gesetzgeberischen Schritte im Hinblick auf den werbewirtschaftlichen Datenschutz nach BDSG und Spezialgesetzen vorgegeben und der weiteren Betrachtung zugrunde zu legen: Der deutsche Gesetzgeber wird, um den inhaltlich zwingend erforderlichen Gleichlauf zwischen EU-Recht und nationalen Normen gesetzestechnisch herzustellen, bis zum 25.5.2018 eine umfassende Rechtsbereinigung vornehmen. Diese wird, bezogen auf die materiellen und formalen Vorgaben beim werbewirtschaftlichen Datenschutz, zur Aufhebung sämtlicher bislang einschlägiger Regelungen im BDSG (§ 28 Abs. 3 ff BDSG; § 29 BDSG) führen. Denn zentrale Tatbestandmerkmale von § 28 Abs. 3 BDSG, insbesondere die Begrenzung auf bestimmte Datenkategorien in § 28 Abs. 3 S. 2 BDSG („Listenprivileg"), kennt die DS-GVO schlichtweg nicht.[15]

Die Regelungen des Gesetzes gegen den unlauteren Wettbewerb (UWG), insbesondere die im werbewirtschaftlichen Bereich neben der datenschutzrechtlichen Betrachtung immer mit zu bedenkenden Verbote nach § 7 UWG, werden bestehen bleiben. Letztere beruhen auf Art. 13 der weiterhin geltenden und somit unverändert umzusetzenden Richtlinie über den Datenschutz in der elektronischen Kommunikation (im Folgenden: ePrivacy-RL).[16] Allerdings ist zu beachten, dass Verweise auf die ab Wirksamkeit der DS-GVO aufgehobene DSRL als Verweise auf die Grundverordnung gelesen und entsprechend interpretatorisch nachvollzogen werden müssen, Art. 94 Abs. 2 S. 1. Bedeutsam ist dies u.a. für das Verständnis der Einwilligung in Art. 13 ePrivacy-RL und damit auch für § 7 UWG.[17]

Für die datenschutzrechtlichen Bestimmungen im vierten Abschnitt des TMG gilt Folgendes: Es ist zu erwarten, dass diese ebenfalls nahezu vollständig aufgehoben werden. Die den Erlaubnistatbeständen nach den §§ 12 ff TMG zugrundeliegende datenschutzrechtliche Trennung in Bestands-, Nutzungs- und Inhaltsdaten und die spezifisch telemedienrechtliche Erlaubnisregel des § 15 Abs. 3 TMG findet keine Entsprechung in der DS-GVO.[18] Die datenschutzrechtlichen Vorgaben der ePrivacy-RL bleiben indes erhalten, so dass auch der entsprechende Umsetzungsbefehl für den deutschen Gesetzgeber ebenfalls fortbesteht, wobei Art 95 diese Parallelgeltung von Richtlinie und DS-GVO weiter ausgestaltet: „Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen". Für das positiv-rechtliche Schicksal des derzeitigen telemedienrechtlichen Datenschutzes ist diese Bestimmung aber ohne Bedeutung. Die datenschutzrechtlichen Bestimmungen des TMG können als bereichsspezifische Umsetzung der zum 25.5.2018 aufgehobenen DSRL interpretiert werden, nicht jedoch als Umsetzung der ePrivacy-Richtlinie.[19] Die Normen des TMG sind daher – als Konsequenz des auch für Dienste im Sinne des TMG umfassenden Geltungsanspruchs bzw. Anwendungsvorrangs der DS-GVO – zum 25.5.2018 aufzu-

12 Nach Art. 3 Abs. 2 gilt das datenschutzrechtliche Marktortprinzip, wonach die GVO auch dann Anwendung findet, wenn personenbezogene Daten von Bürgern, die sich in der EU „befinden", durch einen nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter verarbeitet werden und diese Datenverarbeitung im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen, auch unentgeltlichen (werbefinanzierten), erfolgt. Ebenso bereits zuvor EuGH, Urteil v. 13.05.2014, C-131/12 – Google Spain; vgl. auch EuGH, Urteil v. 01.10.2015, C-230/14 – Weltimmo.

13 Vgl. Dammann, ZD 2016, 310, 314, der zugleich aber auch auf die recht umfangreichen mitgliedstaatlichen Regelungsbefugnisse („Öffnungsklauseln") hinweist, wenngleich diese im werbewirtschaftlichen Kontext kaum Bedeutung erlangen sollten.

14 S. ErwG 7, 11.

15 Zur damit hinfälligen Frage nach der Richtlinienkonformität der durch die BDSG-Novelle II modifizierten Regelungen vor dem Hintergrund des Vollharmonisierungsansatzes der DSRL vgl. Hoeren, RDV 2009, 95 ff; Drewes, ZD 2012, 114. Zum Vollharmonisierungskonzept der DSRL, s. EuGH, Urt. v. 24.11.2011 – Rs. 468/10 – ASNEF", RS. 469/10 – FECEMD, Slg. 2011, I-12181 Rn. 29 ff. Inwiefern außerhalb des werbewirtschaftlich relevanten Kontextes gewisse Bestimmungen punktuell erhalten bleiben werden, z.B. § 28 a BDSG, gilt es abzuwarten.

16 RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation v. 12.7.2002, geändert durch RL 2009/136/EG zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz v. 25.11.2009 ABl. L 337/1.

17 Zu den Vorgaben für die Einwilligung nach der DS-GVO, s. unten III, 2.

18 Inwiefern der Regelungsgehalt von § 15 Abs. 3 TMG nach den Bestimmungen der DS-GVO erhalten bleiben kann, s. unten Teil 2.

19 Der Anwendungsbereich der Richtlinie umfasst gemäß Art. 3 Abs. 1 ePrivacy-RL Dienste, die öffentlich zugängliche elektronische Kommunikationsdienste in öffentlichen Kommunikationsnetzen anbieten, mithin Dienste i.S.v. § 3 Nr. 24 TKG. Das TMG ist für diese Dienste aber nahezu vollständig nicht anwendbar, § 1 Abs. 1 TMG. Zutreffend verweisen Nebel/Richter, ZD 2012, 407 f und Keppeler, MMR 2016, 781 deshalb auch darauf, dass die Vorgaben der ePrivacy-RL im TKG umgesetzt wurden, weshalb die §§ 91 TKG, nicht aber §§ 11 TMG bestehen bleiben können. Die Kritik der Aufsichtsbehörden und von Teilen der Literatur an der deutschen Umsetzungsgesetzgebung zur ePrivacy-RL setzt sich hiermit nicht auseinander, vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Verfolgung des Nutzungsverhaltens im Internet v. 5.2.2015; Schmidt/Babilon, K&R 2016, 86 ff.

heben.[20] Praxisrelevante Fragestellungen ergeben sich allerdings für die werbewirtschaftlich bedeutsame Regelung in Art. 5 Abs. 3 ePrivacy-RL. Diese Vorgabe ist für den nationalen Gesetzgeber über den 25.05.2018 hinaus beachtlich, wenngleich der Streit um den eigentlichen Umsetzungsbefehl der Norm auch dann nicht beigelegt sein dürfte.[21] Mit der DS-GVO werden sogar weitere Facetten hinzugefügt.[22] Vor diesem Hintergrund verwundert es nicht, dass ErwG 173 davon spricht, die Richtlinie 2002/58/EG „einer Überprüfung" zu unterziehen, sobald die „Verordnung angenommen worden ist, [...] um insbesondere die Kohärenz mit der Verordnung zu gewährleisten". Die EU-Kommission plant, dem Vernehmen nach, noch im Jahr 2016 einen Vorschlag zur Novellierung der ePrivacy-Richtlinie vorzulegen. Insofern steht die Bestandsaufnahme für den telemedienrechtlichen Datenschutz auch unter dem Vorbehalt der weiteren Rechtsentwicklung auf EU-Ebene.[23] Die EU-Kommission ist gut beraten, neben der Evaluierung der Richtlinie auch die Leistungsfähigkeit der DS-GVO für die anstehenden Sachfragen zu untersuchen, um den Akteuren – Betroffene, Verantwortliche, Aufsicht und Justiz – eine unklare oder gar überflüssige Gesetzgebung zu ersparen. Die DS-GVO hat nach über vier Jahren intensiver Diskussion den Anspruch, das gesamte Datenschutzrecht für den nicht-öffentlichen Bereich umfassend unmittelbar europäisch zu regeln.

2. Bewertung

Im Unterschied zu anderen Rechtsgebieten, zum Beispiel dem Verbraucherschutz- und Wettbewerbsrecht bzw. dem Recht der unfairen Geschäftspraktiken (bei B2C-Verhältnissen), bei denen die EU-Gesetzgebung einen Mix aus allgemeiner oder sektoraler Gesetzgebung, hauptsächlich in Gestalt von Richtlinien und erläuternden (unverbindlichen) Beschlüssen und Mitteilungen verfolgt (und offenbar fortsetzen und ausbauen will)[24], ist die Regulierungstiefe beim materiellen Datenschutzrecht von der DSRL zur DS-GVO keinesfalls gestiegen. Während der richtliniengeleitete nationale Normenbestand im Verbraucherschutz- und Wettbewerbsrecht immer umfänglicher und teilweise auch unübersichtlicher ausfällt[25], wird die nationale Gesetzgebung für den werbewirtschaftlichen Datenschutz infolge des Anwendungsvorrangs der DS-GVO nahezu vollständig kassiert. Die Praxis muss damit ab dem 25.05.2018 auch für ganz grundlegende Rechtsfragen auf die allgemeinen Konzepte, Generalklauseln und unbestimmten Rechtsbegriffe der DS-GVO zurückgreifen. Allerdings ist die DS-GVO beim materiellen Datenschutz weitgehend strukturkonservativ. Das grundlegende Prinzip bleibt: Die Verarbeitung personenbezogener Daten steht unter Verbot mit Erlaubnisvorbehalt[26], und auch die Erlaubnisnormen – jedenfalls für den werbewirtschaftlichen Kontext – stammen aus dem Arsenal bislang bekannter Kategorien (Einwilligung, Vertrag, Interessenabwägung). Inwiefern die spezifische Ausformung und Anwendung der im Prinzip bekannten Grundsätze infolge der langjährigen Rechtstraditionen der jeweiligen EU-Mitgliedstaaten – in Deutschland etwa in Gestalt des sogenannten „Listenprivilegs" (§ 28 Abs. 3 S. 2 BDSG), das weiterhin in den Köpfen der Akteure aufbewahrt sein dürfte – fortlebt oder gar in die DS-GVO hineingetragen wird, ist für die Erreichung der Ziele der DS-GVO von entscheidender Bedeutung. Angemessen und rechtlich erfolgversprechend kann hier nur eine Auslegung der DS-GVO sein, die diese als eigenständige autonome Rechtsquelle betrachtet und sie so auch interpretiert.[27]

II. Grundprinzipien des werbewirtschaftlichen Datenschutzes nach DS-GVO

Art. 5 Abs. 1 DS-GVO legt allgemein gültige Grundsätze für sämtliche in Art. 4 Nr. 2 umfassend definierten Datenverarbeitungstatbestände fest. Diese Grundsätze, als solche bereits aus Art. 6 DSRL bekannt, sind im Zusammenhang mit den jeweiligen Erlaubnistatbeständen und den weiteren Verpflichtungen für den Verantwortlichen oder Auftragsverarbeiter heranzuziehen und interpretatorisch zu verwerten. Auf dieser Basis erfolgen im Vergleich zum deutschen Recht eine Reihe von Neujustierungen: in Bezug auf die Anforderungen und Bedingungen für wirksame Einwilligungen[28], zur Thematik der werbewirtschaftlich verfügbaren Datenquellen infolge des Wegfalls des Direkterhebungsgrundsatzes (§ 4 Abs. 2 BDSG) und des Listenprivilegs (§ 28 Abs. 3 S. 2 BDSG)[29], im Hinblick auf die Transparenz der Datenverarbeitung (Art. 5 Abs. 1 lit. a) unter Berücksichtigung der ausgeweiteten Informations- und Benachrichtigungspflichten nach den Art. 13, 14[30] und zur zweckändernden Datenverarbeitung (Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4)[31]. Art. 5 Abs. 2 führt zudem den Begriff der Rechenschaftspflicht des Ver-

20 Einzige Ausnahme mag § 15 Abs. 8 TMG in seiner Bedeutung für Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, sein.

21 Vgl. Art. 29-Arbeitsgruppe, Opinion 2/2010, Opinion 4/2010 und Working Document 02/2013, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf; Schmidt/Babilon, K&R 2016, 86 ff; Rauer/Ettig, ZD 2015, 255 ff; OLG Frankfurt, MMR 2016, 245.

22 In Bezug auf das Erfordernis einer Einwilligung in Art. 5 Abs. 3 ePrivacy-RL für den Fall der Speicherung von Informationen oder den Zugriff auf Informationen, die auf dem Endgerät eines Betroffenen oder Nutzers gespeichert sind, werden die Vorgaben der DS-GVO maßgeblich sein, Art. 94 Abs. 1 S.2. Allerdings muss dies wiederum mit der Vorgabe nach Art. 95 abgeglichen werden, um sicherzustellen, dass die DS-GVO keine zusätzlichen Pflichten im Sinne dieses Artikels auferlegt.

23 Soweit Änderungen bei den wettbewerbsrechtlichen Regelungen in Art. 13 ePrivacy-RL vorgenommen werden, müssen auch die entsprechenden Umsetzungen in § 7 UWG „nachziehen".

24 Zum Rechtsbestand, s. http://www.eu-consumer-law.org/ . Zur Thematik unfairer Geschäftspraktiken, s. hier: http://ec.europa.eu/consumers/consumer_rights/unfair-trade/unfair-practices/index_en.htm und zum Buquet der KOM für die weitere Maßnahmen s. http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

25 Vgl. nur die Änderungen des UWG seit 2000 bis zur letzten Überarbeitung im Jahr 2015.

26 ErwG 40; Hornung, ZD 2012, 101.

27 Was zugleich auch für das Funktionieren des Kohärenzmechanismus (Art. 60 ff), die Aufstellung von Verhaltensregeln und das Zertifizierungsverfahren (Art. 40 ff) zentral sein dürfte; zu letzten Schwartmann, RDV 2016, 68 ff.

28 Nachfolgend unter III, 2. ff.

29 Siehe unter Teil 2.

30 Siehe unter Teil 2.

31 Siehe unter Teil 2.

antwortlichen ein, der nunmehr für die Einhaltung der Grundsätze der DS-GVO „verantwortlich" ist und deren Einhaltung nachweisen können muss. Die Verpflichtung auf Rechtskonformität ist für den Verantwortlichen trotz des im Vergleich zu Art. 6 Abs. 2 DSRL geschärften Wortlauts nichts Neues und nach deutschem Rechtsverständnis selbstverständlich. Entscheidender ist, dass das Dokumentations-, Darlegungs-, Beweis- und Haftungsszenario nach der DS-GVO an vielen Stellen materiell ausgeweitet und verschärft ist und – obschon Art. 5 Abs. 2 dies überraschenderweise nicht ausformuliert – auch der Auftragsverarbeiter nunmehr eigenständiger und neben dem Verantwortlichen (Auftraggeber) gleichrangiger Normadressat der Vorgaben der DS-GVO ist.[32]

III. Die materiellen Regelungen des werbewirtschaftlichen Datenschutzes nach der DS-GVO

Zur Datenverarbeitung für werbewirtschaftliche Zwecke kommen von den in Art. 6 Abs. 1 normierten Erlaubnistatbeständen im Wesentlichen die folgenden in Betracht:

- die Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a),
- die Erforderlichkeit der Datenverarbeitung zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen (Art. 6 Abs. 1 lit. b) und
- die Erforderlichkeit der Datenverarbeitung zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (Art. 6 Abs. 1 lit. f).

1. Verhältnis der Erlaubnistatbestände zueinander

Die Einwilligung des Betroffenen und die beiden gesetzlichen Erlaubnistatbestände stehen gleichrangig nebeneinander zur Verfügung. Ein Stufenverhältnis, wonach etwa die Einwilligung gegenüber den gesetzlichen Erlaubnistatbeständen vorrangig wäre, existiert nach dem Gesetzeswortlaut und der Intention des Erlaubnisvorbehalts weiterhin nicht.[33] Die Einwilligung kann Datenverarbeitungen rechtfertigen, die nicht durch einen gesetzlichen Erlaubnistatbestand gedeckt sind, der Verantwortliche ist aber nicht gehalten, die Befugnis zur Datenverarbeitung vorrangig auf eine Einwilligung zu stützen. Datenverarbeitungen können auch bei formal unwirksamer Einwilligung sowie im Falle eines Widerrufs oder einer verweigerten Einwilligung des Betroffenen auf Grundlage eines gesetzlichen Erlaubnistatbestands zulässig sein.[34] Der Umstand der Verweigerung oder des Widerrufs einer Einwilligung fließt in diesen Fällen jedoch als Abwägungsfaktor in die Interessenabwägung nach Art. 6 Abs. 1 lit. f ein. Außerdem ist – bei Wirksamkeit der Einwilligung – der hierdurch festgelegte Befugnisrahmen insoweit beachtlich, als dass der Eindruck des Betroffenen, der Verantwortliche werde sich nur innerhalb dieses Rahmens bewegen, als schutzwürdiges Interesse bei einer Interessenabwägung nach Art. 6 Abs. 1 f ebenfalls zu berücksichtigen ist.[35]

2. Einwilligungsbasierte Datenverarbeitung

Im Vergleich zu Art. 2 lit. h DSRL ist die Legaldefinition der Einwilligung in Art. 4 Nr. 11 nur unwesentlich verändert; sie enthält weiterhin auch normative Anforderungen an die Wirksamkeit einer Einwilligung. Der Detaillierungsgrad bei den Anforderungen an eine rechtswirksame Einwilligung ist nach den Art. 7 und 8 und den für die Interpretation der Bestimmungen maßgeblichen ErwG 32 f, 38 und 42 f gegenüber der DSRL, § 4 a BDSG, und den speziellen Einwilligungsregelungen in § 38 Abs. 3, 3a, b BDSG aber merklich erhöht, wobei den Verantwortlichen nach Art. 7 Abs. 1 die Beweislast für das Vorliegen der Voraussetzungen trifft.

a) Informiertheit der Einwilligung

Die Einwilligungserteilung ist nur auf informierter Basis rechtskonform. Es gelten die aus der DSRL und dem BDSG bekannten Grundsätze, so dass die Einwilligung für den konkreten Fall und in Kenntnis der Sachlage abgegeben sein muss. Unspezifische General- und Blankoeinwilligungen sind nicht rechtmäßig. Erforderlich ist weiterhin eine konkrete Information vor Abgabe der Einwilligung, wobei der Umfang der nach der DS-GVO zu gebenden Information im Vergleich zum geltenden Recht spürbar ausgebaut ist. Nach ErwG 42 soll der Betroffene (weiterhin, s. § 4a Abs. 1 BDSG) „mindestens" über die Identität des für die Verarbeitung Verantwortlichen und über die Zwecke der Verarbeitung informiert werden. Nach ErwG 32 hat sich die Einwilligung „auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge" zu beziehen, über die folglich auch informiert werden muss: Im Rahmen der Einwilligungserklärung sollten alle zur Zweckerreichung erforderlichen Verarbeitungsphasen (vgl. Art. 4 Nr. 2 DS-GVO) aufgeführt werden. Gemäß Art. 7 Abs. 3 DS-GVO ist zudem auf die Möglichkeit und die Folgen eines Widerrufs der Einwilligung hinzuweisen. Art. 13 sieht schließlich eine Vielzahl weiterer Angaben vor, die das Informationsprogramm weiter aufladen[36] und auch bei Datenerhebungen im Zuge der Einwilligung zu beachten sind. Die Umsetzung dieser

32 In Bezug auf die Kernnorm der Auftragsdatenverarbeitung ist er bei unautorisierter Datenverarbeitung als Verantwortlicher anzusehen, Art. 28 Abs. 10. Nach Art. 82 Abs. 1 steht der Auftragsverarbeiter mit dem Auftraggeber in einer gemeinsamen, gesamtschuldnerischen Haftung gegenüber dem Betroffenen für materielle und immaterielle Schäden und ist nach Art. 83 Abs. 3, 4 bei Verstoß gegen die dort aufgeführten Bestimmungen bußgeldpflichtig. Zu diesem Paradigmenwechsel und den daraus resultierenden Konsequenzen für Auftragsgeber und -verarbeiter instruktiv Müthlein, RDV 2016, 74 ff, 77ff; Petri, ZD 2015, 305.

33 ErwG 40 und ausdrücklich für den Widerruf der Einwilligung Art. 17 Abs. 1 lit. b; zur DSRL ebenso Simitis/Dammann, EG-Datenschutzrichtlinie, Art. 7, Rz. 3.

34 Zu prüfen ist aber, ob Verweigerung oder Widerruf der Einwilligung zugleich auch als Widerspruch (Art. 21 Abs. 1, 2) zu verstehen sind.

35 Wobei hier – als Konsequenz der Regelung zu Zweckänderungen nach der DS-GVO – zwischen kompatiblen und inkompatiblen Zweckänderungen zu differenzieren ist, vgl. unten Teil 2.

36 Näher dazu unter Teil 2.

Verpflichtungen wird in bestimmten Bereichen, etwa bei Postkartenformaten, größere praktische Schwierigkeiten bereiten, allerdings zeigt die DS-GVO Lösungswege auf: Zwar wird ein Verweis auf eine Webseite zur Informationserteilung im verfügenden Teil der DS-GVO nicht explizit erwähnt, ErwG 58 sieht aber, ebenso wie für die DSRL vertreten[37], die Möglichkeit eines gestuften Informationskonzepts vor, so dass die Informationen in begründeten Fällen auch auf Webseiten zur Verfügung gestellt werden können. Kommt ein solches Verfahren zur Anwendung, ist der Betroffene sowohl hierauf als auch auf die Fundstelle der weiteren Informationen klar hinzuweisen.

b) Freiwilligkeit der Einwilligung und Kopplungsverbot

Die Einwilligung muss freiwillig, d.h. ohne jeden Zwang, abgegeben werden. Gemäß ErwG 43 gilt eine Einwilligung nicht als freiwillig abgegeben, wenn zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen „ein klares Ungleichgewicht" besteht und es deshalb in Anbetracht aller Umstände in dem speziellen Fall „unwahrscheinlich ist", dass die Einwilligung ohne Zwang abgegeben wurde. Ein solches Ungleichgewicht könne „in besonderen Fällen" bestehen, „insbesondere wenn es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde handelt".[38] Für die werbewirtschaftliche Datenverarbeitung relevanter ist ErwG 42, wonach die Einwilligung freiwillig erteilt wurde, wenn die betroffene Person eine „echte oder freie Wahl" hat und somit in der Lage ist, „die Einwilligung zu verweigern oder zurückzunehmen, ohne dadurch Nachteile zu erleiden." Damit können die zum geltenden Recht entwickelten Fallgruppen, nach denen „übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe von Daten"[39] oder das Ausnutzen einer Position der rechtlichen oder wirtschaftlichen Schwäche oder Unerfahrenheit des Einwilligenden mit dem Merkmal der Freiwilligkeit nicht vereinbar sind, weiterhin herangezogen werden. Auch die Maßgaben der wettbewerbsrechtlichen „Umfeldkontrolle" in Bezug auf die konkreten Umstände der Erlangung der Einwilligung sind weiter beachtlich.[40]

Allerdings geht die DS-GVO noch weiter. Bei der Beurteilung, ob eine Einwilligung freiwillig abgegeben wurde, muss gemäß Art. 7 Abs. 4 DS-GVO dem Umstand „in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich ist." Die Regelung wird, obwohl es sich, dogmatisch betrachtet, um eine Subsumptionsanleitung zur Prüfung des Tatbestandsmerkmals der „Freiwilligkeit" handelt, als (allgemeines) Kopplungsverbot eingeordnet, das die DS-RL nicht und das BDSG nur in eingeschränkter Form für den Bereich des Werbedatenschutzes kennt (§ 28 Abs. 3b BDSG). ErwG 43 führt dazu näher aus, dass die Einwilligung nicht als freiwillig erteilt gelte, wenn zu verschiedenen Datenverarbeitungsvorgängen nicht gesondert eine Einwilligung erteilt werden könne, obwohl dies im Einzelfall angebracht sei, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig gemacht werde, obwohl diese Einwilligung nicht erforderlich sei. Bedeutung erlangt das einwilligungsbezogene Kopplungsverbot, wenn (die verschiedenen) Datenverarbeitungen nicht bereits auf gesetzlicher Grundlage, insbesondere Art. 6 Abs. 1 lit. b, legitimiert werden können.

Das Kopplungsverbot bezweckt nicht, dem Betroffenen bei Abschluss eines Vertrages Wahl- und Gestaltungsfreiheit schlechthin in Bezug auf weitere, einwilligungsbasierte Datenverarbeitungen neben einem gesetzlichen Erlaubnistatbestand einzuräumen. Art. 7 Abs. 4 soll vielmehr bewirken, dass sich die Einwilligung in der Praxis als Ausdruck informationeller Selbstbestimmung und nicht als aufoktroyierte Fremdbestimmung darstellt. Die Grundfreiheiten und -rechte des Verantwortlichen[41] müssen demzufolge bei der Anwendung von Art. 7 Abs. 4 DS-GVO ebenso berücksichtigt werden wie alle Umstände des Einzelfalls. In diesem Sinne ist das Kopplungsverbot zwar als geschärft, aber nicht als statisch-absolut zu verstehen. Es muss in einem dem Verhältnismäßigkeitsgrundsatz entsprechendem Umfang ausgelegt und angewendet werden.[42] Konstellationen, bei denen den in Art. 7 Abs. 4 und ErwG 43 aufgeführten Umständen in „größtmöglichem Umfang Rechnung getragen" werden muss, liegen bei Monopolstellung nahe, etwa bei Verträgen im Öffentlichen Personenverkehr, in der Versorgungswirtschaft oder ggf. im Versicherungswesen oder auch bei sozialen Netzwerken. Das Kopplungsverbot greift dabei sicherlich, wenn über die Einwilligung eine dem Vertragszweck fremde und sachwidrig überschießende Datenverarbeitung legitimiert werden soll. Die Regelung muss sich aber auch bewähren, wenn für die betroffene Person entgeltfreie, weil werbefinanzierte, Inhalte und Dienstleistungen Vertragsgegenstand sind (z.B. Webmail-Dienste oder bestimmte Formen von gemischt refinanzierten Paid-Content). Die einwilligungsbasierte Datenerhebung ist hier in wirtschaftlicher Hinsicht notwendig. Als Mittel zur Erbringung der Gegenleistung ist sie, vertragstypologisch betrachtet, nachvollziehbar, zumal wenn sie mit den rechtsgeschäftlichen Abreden verbunden ist und der Erfüllung und Abwicklung der rechtsgeschäftlichen Beziehung dient, die vollständig oder teilweise entgeltlos, weil werbefinanziert ist. Auch dem Be-

37 Art. 29-Arbeitsgruppe, WP 100, abrufbar unter: http://www.cnpd.public.lu/de/publications/groupe-art29/wp100_de.pdf.

38 Zur Freiwilligkeit der Einwilligung im Arbeitsverhältnis, vgl. BAG, K&R 2015, 433.

39 BGHZ 177, 253 – Payback; Gola/Reif, Kundendatenschutz, Rz. 282 ff.

40 Vgl. BGH, GRUR 2014, 682 – Nord-Job Messe, wo der BGH zwischen der Wirksamkeit der Einwilligung und der wettbewerbsrechtlichen Beurteilung der Situation ihrer Erlangung gemäß den §§ 3, 4 Nr. 2 UWG a.F. unterscheidet (nunmehr § 3 Abs. 4, § 4 a UWG).

41 Art. 15, 16 GrCh sowie Art. 12, 14 GG.

42 Zu weitgehend daher Dammann, ZD 2016, 311, der von einem strikten Kopplungsverbot spricht, das das Potenzial habe, „Verbraucher umfassend vor Verführungssituationen zu schützen, wie sie insbesondere bei der Nutzung von Online-Diensten bestehen". Daher dürfe man gespannt sein, „wie sich die Regelung gegen das Geschäftsmodell `Service gegen Daten' durchsetze". Weder der Wortlaut noch die Teleologie von Art. 7 Abs. 4 sichern eine solche, wohl eher rechtspolitisch inspirierte, Auffassung ab, denn hierdurch würde ein quasi abstraktes Gefährdungsdelikt kreiert, bei dem der Bezugspunkt und die immanenten Begrenzungen der Regelung aus dem Blickfeld geraten.

troffenen dürfte dieser Zusammenhang bekannt sein (s. Art. 13 Abs. 1 lit. c), was für die Beurteilung der Freiwilligkeit der Einwilligung und deren Schutz vor einer zumindest mittelbaren Gefährdung – Zweck und Bezugspunkt von Art. 7 Abs. 4 – von Bedeutung ist. Vorstehende Leitlinie gilt insbesondere im Hinblick auf die leicht missverständliche Formulierung in ErwG 43 („... obwohl dies im Einzelfall angebracht ist ...“). Zwar darf die Verweigerung einer Einwilligung gemäß ErwG 42 nicht zu „Nachteilen“ für die betroffene Person führen, die Ablehnung eines Vertragsangebots außerhalb monopolartiger Strukturen ist jedoch Ausdruck von Privatautonomie, die die DS-GVO in Bezug auf die Gültigkeit und das Zustandekommen von Verträgen anerkennt. So wenig das Nichtzustandekommen eines Vertrags – jedenfalls solange das europäische Recht keinen allgemeinen Kontrahierungszwang kennt – als schlichtweg unzulässig bzw. relevanter Nachteil angesehen werden kann, so wenig kann die Notwendigkeit zur Erteilung einer Einwilligung ohne Hinzutreten besondere Umstände als nach dem Kopplungsverbot unzulässige Gestaltung angesehen werden – auch wenn der Betroffene eine andere Gestaltung im Einzelfall für angebrachter halten mag.

c) Erteilung der Einwilligung

Die DS-GVO definiert in Art. 4 Nr. 11 die Einwilligung der betroffenen Person als unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Dies umfasst schriftliche, elektronische oder mündliche Willensbekundungen gleichermaßen. Nicht mehr explizit vorgeschrieben ist bei anderer Erteilung als durch Schriftform, dass der Inhalt der Einwilligung schriftlich zu bestätigen und bei elektronischer Erklärung die Protokollierung und Abrufbarkeit der Einwilligung sicherzustellen ist (bislang §§ 28 Abs. 3 a BDSG, § 13 Abs. 2 TMG). Um die Darlegungs- und Beweislast praktisch zu gewährleisten (Art. 7 Abs. 1; ErwG 42), sind entsprechende Routinen aber unverzichtbar. Als elektronisch-digitale Willensbekundung inkludiert ErwG 32 auch das Anklicken einer Tickbox beim Besuch einer Website sowie vom Nutzer vorgenommene Privacy-Einstellungen in einem Browser oder einer App („Einstellungen für Dienste der Informationsgesellschaft“. Ungewöhnlich ist die in ErwG 32 a.E. enthaltene Vorgabe für den Fall der Aufforderung zur Abgabe der Einwilligung auf elektronischem Wege. Die Aufforderung zur Einwilligungserteilung ist hiernach zwingend („so muss“) so „einzutakten“, dass der Dienst, für den die Befugnis zur Datenverarbeitung kraft Einwilligung erteilt werden soll, nicht durch diese Aufforderung unterbrochen wird – jedenfalls nicht „unnötig“. Der Erwägungsgrund betrifft zwar die Modalitäten der Erteilung einer Einwilligung, eine sachliche Verbindung besteht aber in erster Linie mit dem Merkmal der Freiwilligkeit nach Art. 4 Nr. 11, so dass dieser in diesem interpretatorischen Zusammenhang heranzuziehen ist. Offenbar geht der ErwG davon aus, dass die Freiwilligkeit der Einwilligungserteilung gefährdet ist, wenn der Dienst hierfür unterbrochen wird („Weiterklicken“), und verlangt deshalb – mittelbar – sachliche Gründe für nämliche Unterbrechung. Denkbar sind Konstellationen, bei denen aus Gründen des Marketings entweder eine „Vorschau“ des Dienstes erfolgt oder bei denen ein Verfahren automatisierter Datenverarbeitung im Sinne von § 13 Abs. 1 S. 2 TMG, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, stattfindet, etwa beim Aufruf einer mit datengetriebener Werbung refinanzierten Webseite („Targeting“) oder bei IP-TV-Angeboten. Ob eine derart kleinteilige Vorgabe erforderlich und sinnvoll ist, scheint jedoch nicht recht durchdacht. Schließlich muss die Einwilligung nach den allgemeinen Grundsätzen der Einwilligungsdogmatik vor der (dienstbezogenen) Datenverarbeitung vorliegen.[43] Inwiefern der ErwG dazu beiträgt, pragmatische Gestaltungen zu unterstützen, etwa in Bezug auf die Datenverarbeitung mittels Cookies, bleibt abzuwarten. Das Verbot der Dienstunterbrechung resultiert streng genommen bereits unmittelbar aus Art. 7 Abs. 1. Sofern Ausnahmen hiervon denkbar sein sollen („ohne unnötige Unterbrechung“), darf der Grundsatz der vorherigen Einwilligung hierdurch nicht ausgehöhlt werden.

Auch konkludente Einwilligungen, sofern die betroffene Person im jeweiligen Kontext der Datenverarbeitung durch eine entsprechende „Verhaltensweise“ (s. ErwG 32) eindeutig signalisiert, dass sie mit der Datenverarbeitung einverstanden ist, sind möglich, beispielsweise in Gestalt des Einwerfens einer Visitenkarte in eine Box an einem Messestand. Auch Formulierungen im Header einer Webseite, wonach sich der Besucher im Zuge der weiteren Nutzung der Webseite auch mit der Verwendung von Cookies einverstanden erklärt – deren Beitrag zur Verarbeitung personenbeziehbarer Daten unterstellt – sind, sofern die weiteren Voraussetzungen für die Einwilligung erfüllt sind, insbesondere in Bezug auf die Informiertheit, hiernach denkbar.[44] Die Möglichkeit, konkludent einzuwilligen, gilt jedoch nicht für die Verarbeitung von besonderen Kategorien personenbezogener Daten im Sine von Art. 9 Abs. 1. Sofern die Datenverarbeitung in diesen Fällen nicht schon per se ausgeschlossen ist (Art. 9 Abs. 2 lit. a), muss die betroffene Person gemäß Art. 9 Abs. 2 lit. a ausdrücklich in die Verarbeitung dieser Daten, einschließlich des „Wie“ der Datenverarbeitung, einwilligen.

Allerdings führt ErwG 32 DS-GVO aus, dass Stillschweigen, standardmäßig angekreuzte Kästchen oder Untätigkeit nicht als Einwilligung gewertet werden können. Im Hinblick auf verarbeitungsrelevante Voreinstellungen bei der Inanspruchnahme von Telemedien, etwa in Browser- oder App-Konfigurationen, ist dies als Absage an deren Rechtskonformität zu werten. Ob vor diesem Hintergrund Opt-Out

43 Unbestritten, vgl. nur Gola/Schomerus, BDSG, § 4 a, Rz. 15. Für den Einsatz von Cookies, vgl. Art. 29-Arbeitsgruppe, Working Document, a.a.O. (Fn.22) S. 4.

44 Vor dem Hintergrund unterschiedlicher Interpretationen und nationaler Umsetzungen von Art. 5 Abs. 3 ePrivacy-RL ist diese Praxis bislang umstritten, vgl. Rauer/Ettig, ZD 2015, 258 mw.N. zu den jeweiligen Rechtsauffassungen der Aufsichtsbehörden in den MS der EU. Bejahend zu dieser Möglichkeit Art. 29-Arbeitsgruppe, Working Document 02/2013, S. 4.

Einwilligungen, sei es für postalisches Marketing[45] oder in Bezug auf Erhebungs- und Speichertechnologien im Internet[46], weiterhin genutzt werden können, ist damit gleichfalls überaus fraglich und nicht mehr anzuraten. Die für das postalische Direktmarketing bislang gegebenen Möglichkeiten zur Generierung datenschutzrechtlich bestandskräftiger Einwilligungen werden hierdurch spürbar eingeschränkt.[47] Das Informationspotential von Daten kann in Rechtssicherheit unter der DS-GVO bei einwilligungsbasierter Datenverarbeitung nur noch durch bejahende Handlungen des Betroffenen, das heißt bei vorformulierten Einwilligungstexten: mittels zu aktivierender Opt-In Klauseln, genutzt werden.

Damit wird die Frage aufgeworfen, inwieweit Hinweise in Vertragsabreden auf Einwilligungsklauseln – wie etwa: „Mit der vertraglichen Unterschriftserteilung wird auch eine Einwilligung erteilt" – zulässig sind. Klar ist, dass sämtliche Zwecke in der Erklärung aufgeführt werden müssen, wenn die Einwilligung mehrere Zwecke legitimieren soll. Außerdem müssen sich entsprechende Gestaltungen am Kopplungsverbot messen lassen.[48] Wird die Einwilligung der betroffenen Person durch eine schriftliche Erklärung eingeholt, die „noch andere Sachverhalte" betrifft, wie Art. 7 Abs. 2 formuliert, muss die Einwilligungserklärung „in verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache" erfolgen. Der Betroffene muss die Einwilligungserklärung also von anderen Erklärungen klar unterscheiden können. Eine solche Hervorhebungspflicht ist dem geltenden Recht aber bereits bekannt, §§ 4a Abs. 1 Satz 4, 28 Abs. 3a Satz 2 BDSG. ErwG 42 S. 2 spricht in diesem Zusammenhang von „Garantien", die sicherstellen sollen, dass „die betroffene Person weiß, in welchem Umfang sie ihre Einwilligung erteilt hat.[49] Nach alledem ist die Positionierung von (vorformulierten) Einwilligungen auch in AGB nicht ausgeschlossen, zumal die DS-GVO die Thematik in Art. 7 Abs. 2 praktisch aufgreift und detaillierte Vorgaben hierzu macht[50]. Das datenschutzrechtliche Erfordernis einer „eindeutigen bestätigenden Handlung" verlangt hier aber, dass die AGB und mit ihnen die Einwilligungserklärung positiv, etwa in Gestalt einer Klickbox, in den Geschäftsablauf eingebunden werden.[51] Denkbar sind Formulierungen, wonach etwa bei Bestellprozessen beim eCommerce „mit der Anerkennung der AGB auch eine Einwilligung erteilt wird", und der hervorgehobene Terminus „Einwilligung" direkt auf den eigentlichen Einwilligungstext verlinkt. Abgesichert werden kann hiermit aber weiterhin nur die datenschutzrechtliche Einwilligung; die wettbewerbsrechtlichen Vorgaben nach § 7 UWG für die Marketingkanäle Telefon, Fax, E-Mail und SMS sind bei AGB-Sachverhalten für die geplante werbliche Ansprache von Verbrauchern weiterhin (zusätzlich) beachtlich.[52]

d) Einwilligungen Minderjähriger

Art. 8 enthält eine dem deutschen Datenschutzrecht bislang unbekannte Vorgabe zu den Wirksamkeitsbedingungen für die Einwilligung Minderjähriger. Die Thematik als solche ist unter dem Aspekt der Voraussetzung der Einwilligungsfähigkeit bei nicht voll geschäftsfähigen Personen (§§ 106 ff. BGB) bekannt, wobei BDSG und TMG den von der DS-GVO verwendeten Begriff „Kind" nicht kennen.[53] Leitlinie bislang ist, dass auch Minderjährige je nach Verarbeitungszusammenhang und in Ansehung ihrer (altersabhängigen) Einsichtsfähigkeit in die Tragweite der zu treffenden Entscheidung bei verständlicher Information über Zweck und Folgen der Datenerhebung einwilligen können.[54] Art. 8 Abs. 1 legt nun die Altersgrenze für die Wirksamkeit selbständig erteilter Einwilligungen von Minderjährigen auf mindestens 16 Jahre fest, erlaubt aber zugleich die Absenkung durch die mitgliedsstaatliche Gesetzgebung, setzt die Schwelle allerdings beim vollendeten 13. Lebensjahr. Außerhalb dieses gemischt europäisch-nationalstaatlichen Korridors ist die Einwilligung direkt durch den Träger der elterlichen Verantwortung oder aber mit deren Zustimmung abzugeben. Allerdings gilt diese Grenzziehung nicht schlechthin, sondern nur für das „Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird". Auch wenn die betreffenden Angebote einigermaßen verlässlich bestimmt werden können[55], sind die Bedenken gegen die Regelung damit nicht ausgeräumt[56] – und die praktischen Probleme evident. Wann von einem direkten Angebot auszugehen ist, insbesondere wenn sich der Dienst als solcher an die Allgemeinheit richtet oder zumindest von jedermann tatsächlich genutzt werden kann („Facebook"), ist nicht klar. Es liegt nahe, für die Abgrenzung nicht nur auf die vertraglichen Zugangsregeln, sondern auch auf die Marketingkommunikation des Dienstes abzustellen. Sofern das

45 BGH, RDV 2008, 201 ff. – Payback; BGH, RDV 2010, 77 ff. – Happy Digits.

46 Vgl. OLG Frankfurt, MMR 2016, 245, wonach eine Opt-Out-Einwilligung zulässig ist.

47 Nach Auffassung der Art. 29-Arbeitsgruppe wurde eine Opt-Out-Einwilligung bereits in Bezug auf zu Art. 2 Buchst. h DSRL kritisch bewertet, vgl. WP 187, S. 11, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf.

48 Vgl. oben III, 2. b).

49 Vgl. auch die Orientierungshilfe des Düsseldorfer Kreises zur datenschutzrechtlichen Einwilligungserklärung in Formularen, abrufbar unter https://www.lda.bayern.de/media/oh_einwilligung.pdf.

50 Vgl. ErwG 42 S. 3, wo ausdrücklich auf die Klauselkontrolle nach den Vorgaben der RL 93/13/EWG über missbräuchliche Klauseln in Verbraucherverträgen v. 5.4.1993, ABl. L 95 v. 21.04.1993, S. 29, verwiesen wird.

51 Aus AGB-Recht ergibt sich keine explizite Pflicht zum aktiven „Ankreuzen" von AGB.

52 Vgl. hierzu instruktiv Gola/Reif, a.a.O. (Fn. 39) Rz. 372 ff. Die Zusammenfassung von (hervorgehobener) datenschutzrechtlicher Einwilligung mit anderen Vertragsregelungen in AGB mit einer Unterschrift (oder Klick) kann wegen des UWG-Erfordernisses einer spezifischen Angabe im Sinne einer dezidierten Opt-In Erklärung daher faktisch nur für die Verwendung von Adressdaten von Verbrauchern zwecks Briefwerbung genutzt werden, vgl. Anwendungshinweise des Düsseldorfer Kreises zur Werbung (Stand: Sept. 2014), S. 12.

53 Zum geltenden Recht: Taeger, in: Taeger/Gabel, BDSG, § 4 a Rz. 28; Kühling, in: Wolf/Brink, Datenschutzrecht, § 4 a Rz. 32 f.

54 Gola/Schulz, ZD 2013, 478.

55 Die Legaldefinition in Art. 4 Nr. 25 verweist wie auch sonst im sekundären EU-Recht auf Art. 1 Nr. 2 der Richtlinie 98/34/EG: Jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Hierunter fallen insbesondere: Social-Media-, e-Commerce- und Gaming-Angebote.

56 Albrecht, CR 2016, 97; zutreffend weist Frank, RDV 2016, 112, darauf hin, dass die Einwilligung nach Art. 8 Abs. 2 S. 1 GRCh stets nach Treu und Glauben zu ermöglichen ist, die Regelung also nicht nur eine Beschränkung des Verantwortlichen bedeutet, sondern auch Betroffenenrechte verkürzt.

Per-se-Verbot nach Nr. 28 zu § 3 Abs. 3 UWG mit dem vollharmonisierendes europäisches Richtlinienrecht umgesetzt wird[57], erfüllt ist, dürfte das Tatbestandsmerkmal eines direkten Angebots im Sinne von Art. 8 Abs. 1 indiziert sein. Weitere Fallkonstellationen sind jedoch denkbar. Das Wettbewerbsrecht unterbindet lediglich „die in eine Werbung einbezogene unmittelbare Aufforderung an Kinder, selbst die beworbene Ware zu erwerben oder die beworbene Dienstleistung in Anspruch zu nehmen." Für Art. 8 kommt es auf die tatsächliche Ausrichtung des Dienstes an. Um die altersmäßige Mindestgrenze(n) in Bezug auf Einwilligungserklärungen einzuhalten, respektive sicherzustellen, dass die Erklärung des Trägers der elterlichen Verantwortung vorliegt, hat der für die Verarbeitung Verantwortliche gemäß Art. 8 Abs. 2 „unter Berücksichtigung der verfügbaren Technik" angemessene Anstrengungen zu unternehmen. Es bleibt abzuwarten, wie praktische Lösungen jenseits der existierenden Altersverifikationssysteme und der Möglichkeit, ein Double-Opt-In Verfahren zur Absenderverifikation einzusetzen, aussehen werden und wie etwa die Aufsichtsbehörden diese einschätzen.[58] Eine gewisse Erleichterung resultiert jedoch daraus, dass das allgemeine Vertragsrecht der Mitgliedstaaten nach Art. 8 Abs. 3 unberührt bleibt. Ist ein Minderjähriger nach nationalem Zivilrecht zum Vertragsschluss berechtigt, ist die mit dem Vertrag verbundene Datenverarbeitung nach Art. 6 Abs. 1 Buchst. b DS-GVO auch ohne Einwilligung legitimierbar. Einer zusätzlichen datenschutzrechtlichen Einwilligung der Eltern bzw. des Minderjährigen bedarf es nicht.[59] Vollständig aufgehoben ist das Nachweisproblem in Bezug auf das erforderliche Mindestalter der einwilligenden Person damit aber natürlich nicht.

e) Widerruf der Einwilligung

Gemäß Art. 7 Abs. 3 hat die betroffene Person das Recht, die Einwilligung „jederzeit zu widerrufen". Das BDSG schweigt sich zum Widerrufsrecht bekanntlich aus, die Intervention der betroffenen Person gegen eine einmal erteilte Einwilligung gehört aber zum gesicherten Bestand des Datenschutzrechts. Auch wenn sich die Bestimmungen zum Widerrufsrecht nach der DS-GVO größtenteils auf bekanntem Terrain bewegen[60], sind einige Spezifikationen und Abweichungen zu verzeichnen. Die wichtigste lautet: Das Widerrufsrecht ist nicht an das Vorliegen besonderer Voraussetzungen geknüpft, und zwar auch dann nicht, wenn die Datenverarbeitung bereits stattgefunden hat.[61] Die Ausübung des Widerrufs muss „so einfach wie die Erteilung der Einwilligung" sein; sie ist gegenüber dem Verantwortlichen zu erklären und (weiterhin) an keine besondere Form gebunden. Auf das Widerrufsrecht ist spätestens zum Zeitpunkt der Einholung der Einwilligung, jedoch vor deren Abgabe, hinzuweisen, Art. 7 Abs. 3 S. 2. Bislang hat sich dies explizit nur aus § 13 Abs. 3 TMG ergeben. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch den Widerruf nicht berührt. Der Widerruf wirkt weiterhin ex nunc und betrifft ausschließlich die Datenverarbeitungsbefugnis des Verantwortlichen. Wird der Widerruf ordnungsgemäß ausgeübt, resultieren hieraus regelmäßig weitere, bereits etablierte, Betroffenenrechte, insbesondere das Recht auf Datenlöschung (Art. 17). Etwaige vertragliche Verpflichtungen bleiben hiervon jedoch unberührt, was für werbefinanzierte Dienste von praktischer Bedeutung ist: Ist die Einwilligung zur Datenverarbeitung Bestandteil der Gegenleistung der betroffenen Person, führt diese schuldrechtliche Verpflichtung nicht zur Unzulässigkeit oder Unwirksamkeit des Widerrufs.[62] Dem Vertragspartner stehen in diesem Fall aber neben dem Leistungsverweigerungsrecht nach § 320 BGB die Rechtsbehelfe gemäß den §§ 313, 314 Abs. 1, 2 BGB zu, also praktisch das Recht zur außerordentlichen Kündigung des Vertrags. Freilich ist, datenschutzrechtlich betrachtet, der Rückgriff auf die gesetzlichen Erlaubnistatbestände in Art. 6 Abs. 1 lit. b und f für zukünftige Datenverarbeitung auch im Widerrufsfall nicht verwehrt.[63] Die inhärenten Grenzen dieser Befugnisse sind in diesem Fall, etwa wenn zugesichert wurde, ausschließlich aufgrund und im Rahmen einer Einwilligung Daten zu verarbeiten, aber zu beachten.[64]

f) Rechtsfolgen bei Verstößen gegen die Erfordernisse der DS-GVO

Art. 7 Abs. 2 S. 2 bestimmt, dass „Teile der Erklärung" – gemeint ist die Einwilligungserklärung – nicht verbindlich sind, „wenn sie einen Verstoß gegen diese Verordnung darstellen." Bezugspunkt der Vorschrift sind Verstöße inhaltlicher oder formaler Natur gegen die vorstehend einwilligungsspezifischen Vorgaben der DS-GVO, wobei diese natürlich auch relevant sind, wenn die Einwilligung nicht durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, erfolgt (§ 7 Abs. 1 S. 1). Ist eine Einwilligung hiernach vollumfänglich unwirksam und stehen keine anderen Erlaubnistatbestände zur Verfügung, ist die Datenverarbeitung unzulässig; die darüber erhobenen Daten sind zu löschen, Art. 17 DS-GVO. Inwiefern teilweise fehlerhaft eingeholte Einwilligungen unwirksam sind, ist anhand der Um-

57 Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11.05.2005 über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates, ABl. L 149 vom 11.6.2005, S. 22; berichtigt im ABl. L 253 vom 25.09.2009, S. 18.

58 Gola/Schulz, a.a.O. (Fn.57), 480.

59 Gola/Schulz, a.a.O.

60 Zum Widerrufsrecht allgemein, Gola/Schomerus, BDSG, § 4a Rz. 17 ff.

61 Nach überwiegender Auffassung zum deutschen Datenschutzrecht kann der Widerruf hier nur unter Berücksichtigung von Treu und Glauben erfolgen, insbesondere, wenn die für die Erteilung der Einwilligung maßgeblichen rechtlichen oder tatsächlichen Gründe weggefallen sind oder sich wesentlich geändert haben, Gola/Schomerus, a.a.O. (Fn. 63), Rz. 18. Auch wenn die DS-GVO in Art. 5 Abs. 1 lit a die Datenverarbeitung unter Treu und Glauben stellt, wird man angesichts des jederzeitigen und damit unbedingten Widerspruchsrechts keine Einschränkung mehr annehmen können.

62 So bislang wohl Gola/Reif, a.a.O. (Fn. 39) Rz. 833 m.w.N. Spindler, DB 2016, 940, spricht für die Rechtslage nach der DS-GVO davon, die Einwilligung müsse „wieder erteilt werden", was jedoch nicht recht überzeugt, denn damit würde das nach Art. 7 Abs. 3 „jederzeitige" und damit praktisch unabdingbare Widerrufsrecht im Ergebnis ausgehebelt.

63 Umkehrschluss aus Art. 17 Abs. 1 lit. b.

64 S. oben III, 1.

stände des jeweiligen Einzelfalls zu entscheiden.[65] Gegen eine automatische „Infizierung" der rechtswirksamen Bestandteile einer Einwilligungserklärung durch unwirksame Bestandteile, etwa bei unvollständiger Information, spricht der Gesetzeswortlaut von Art. 7 Abs. 2 S. 2 („Teile der Erklärung sind dann nicht verbindlich, wenn … "). Maßgebliche Kriterien sind die Art des Verstoßes und der Wille der betroffenen Person unter Berücksichtigung ihres Wissenstands.

g) Zum Schicksal von Alteinwilligungen

Mit Wirksamwerden der DS-GVO am 25.05.2018 müssen sich sämtliche Datenverarbeitungen an den neuen Vorgaben messen lassen. Fraglich ist, wie Alteinwilligungen, die rechtmäßig vor dem Stichtag erlangt wurden, einzuschätzen sind. Art. 96 trifft eine Regelung lediglich für die Fortgeltung internationaler datenschutzrechtlicher Abkommen, sagt aber nichts zur Zulässigkeit von Alteinwilligungen ab dem Wirksamkeitsdatum der DS-GVO. Spezifische Aussagen zur der Thematik trifft allerdings ErwG 171, S. 3.[66] Einwilligungen, die noch nach altem Recht eingeholt wurden, bleiben hiernach unter bestimmten Bedingungen weiterhin wirksam. Bezugspunkt sind Einwilligungen „gemäß der DSRL", also solche, die den Vorgaben des BDSG und TMG entsprechen.[67] Für diese ist es „nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung (dazu) erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen [der DS-GVO] entspricht". In diesem Rahmen besteht Bestandsschutz und fortdauernde Verarbeitungsbefugnis. Wollte die DS-GVO nur solchen Einwilligungen „Bestandsschutz" attestieren, die vollumfänglich nach dem Recht der DS-GVO eingeholt wurden, wären die expliziten Ausführungen zur Einwilligung in ErwG 171, S. 3 überflüssig. Damit dem Erwägungsgrund also überhaupt Bedeutung zukommt, müssen die Begriffe „Art" und „Bedingungen" ernst genommen und einschränkend ausgelegt werden. Mit „Bedingungen" gemeint sind demnach die materiellen Kernbestandteile einer Einwilligung. Sind Einwilligungen nach den Vorgaben des bisher geltenden Rechts freiwillig und hinsichtlich der wesentlichen Umstände informiert eingeholt worden, entsprechen sie den Bedingungen der DS-GVO, und es kann vertreten werden, dass sie nach Wirksamwerden der DS-GVO weiterhin gelten. Die Nichtbeachtung einzelner allgemeiner, die Informiertheit der Einwilligung im Kern nicht betreffender formeller Informationspflichten, sollte Alteinwilligungen hingegen nicht unwirksam werden lassen. Bei der Abgrenzung, die wohl nur im jeweiligen Einzelfall überzeugend geleistet werden kann, besteht Rechtsunsicherheit. Wegen der Rechtsfolgen einer unzulässigen Datenverarbeitung, die nach der DS-GVO erheblich geschärft sind, und den erweiterten Durchsetzungsbefugnisse von Aufsichtsbehörden und qualifizierten Stellen (nach dem UKlaG), sollten Einwilligungen daher möglichst frühzeitig ab Inkrafttreten der DS-GVO nur noch nach ihren Maßgaben der eingeholt werden. Bei rein formellen Pflichten, wie dem Hinweis auf das bestehende Widerrufsrecht nach Art. 7 Abs. 3 DS-GVO, bietet sich eine Nachinformation der betroffenen Person an.

IV. Fazit (Teil 1)

Die weitreichende Geltung der mit Anwendungsvorrang ausgestatteten DS-GVO hat zur Folge, dass die materiellen datenschutzrechtlichen Vorgaben für die Werbewirtschaft ab dem 25. Mai 2018 nicht mehr im nationalen Datenschutzrecht, sondern durch die DS-GVO geregelt werden. Für den werbewirtschaftlichen Datenschutz bei Telemedien wird es darauf ankommen, wie die Überarbeitung der ePrivacy-RL ausfällt. Mit der DS-GVO werden die Wirksamkeitsanforderungen für den Erlaubnistatbestand der Einwilligung stärker akzentuiert. Sofern verschiedene Datenverarbeitungen nicht auf einen gesetzlichen Erlaubnistatbestand gestützt werden können, will das Unionsrecht die Freiwilligkeit der Einwilligung durch das neu formulierte Kopplungsverbot absichern. Die Stärkung der informationellen Privatautonomie des Betroffenen geht aber nicht so weit, dass diesem die rechtsgeschäftliche Wahl und Gestaltungsfreiheit einseitig zugewiesen wird. Das Kopplungsverbot muss immer – auch und gerade bei werbefinanzierten Geschäftsmodellen – in einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Weise angewendet werden. Die Einwilligung muss auf informierter Basis erteilt werden, wobei das Informationsprogramm mit der DS-GVO ausgeweitet wurde. Gestuften Informationskonzepten steht die DS-GVO aber nicht entgegen. Vorformulierte Opt-Out-Einwilligungserklärungen dürften zukünftig nicht mehr rechtswirksam sein; alternative Gestaltungsmöglichkeiten, auch in AGB, sind aber denkbar. Von den Bordmitteln der DS-GVO erfasst ist auch die Möglichkeit zur konkludenten Einwilligung. Pragmatische Gestaltungen im Bereich der digitalen Datenverarbeitung zu Werbezwecken, etwa bei Cookies, können damit rechtskonform aufgesetzt werden. Die DS-GVO setzt eine neue Untergrenze für die Einwilligungsfähigkeit von Minderjährigen bei bestimmten Online-Sach-verhalten. Die Befolgung der Regelung wird Unternehmen in tatsächlicher

65 Gegen eine vollumfängliche Unwirksamkeit bislang Kühling, in: Wolf/Brink, Datenschutzrecht, § 4 a Rz. 43; a.A. Simitis, in: Simitis, BDSG, § 4a Rz. 76.

66 Die Grundregel für sonstige Verarbeitungen, die zum Zeitpunkt der Anwendung der DS-GVO (ab 25.5.2018) begonnen haben, lautet gemäß ErwG 171, S. 2 dagegen, dass „diese innerhalb des zweijährigen Zeitraums ab ihrem Inkraftreten (am 25.05.2016) „mit ihr in Einklang gebracht werden."

67 Wobei die Einwilligung noch „aktiv" sein, d.h. zum Wirksamkeitszeitpunkt der DS-GVO noch rechtliche Gültigkeit beanspruchen muss. Diese Frage ist nach nationalem Recht umstritten. Die deutschen Aufsichtsbehörden neigen unter Verweis auf (die nicht gefestigte) Rsp. zur Werbeeinwilligung nach § 7 UWG offenbar zu der Ansicht, dass Einwilligungen durch Zeitablauf ihre Gültigkeit verlieren, wobei eine Frist hierfür nicht benannt wird, vgl. Anwendungshinweise des Düsseldorfer Kreises zur Werbung (Stand: Sept. 2014), S. 5; hiergegen mit überzeugenden Argumenten: Schulz, CR 2012, 688; Schirmbacher/Schätzle, WRP 2014, 1148. Wie sich die DS-GVO zu der Frage, die auch jenseits der Altfallproblematik Bedeutung hat, verhält, ist nicht ausdrücklich geregelt. Da die Datenverarbeitung gemäß Art. 5 Abs. 1 lit a „nach Treu und Glauben in einer für die betroffene Person nachvollziehbaren Weise" erfolgen muss, spricht viel dafür, dass entgegen der bisherigen Ansicht der Aufsichtsbehörden zwar kein generelles Erlöschen (nach bestimmten Zeitablauf) anzunehmen ist, dass aber ein werbendes Unternehmen sich nicht mehr auf die Einwilligung berufen kann, wenn die Befugniserteilung im konkreten Einzelfall unter Berücksichtigung des Willens des Einwilligenden „erkaltet" ist, insbesondere bei Zweckerreichung.

Hinsicht Probleme bereiten. Für das ex nunc wirkende zwingende Widerrufsrecht gelten zukünftig keine Einschränkungen mehr – auch wenn die Datenverarbeitung bereits stattgefunden hat. Alteinwilligungen, erfahren Bestandsschutz: Eine erneute Einwilligung ist nicht erforderlich, wenn die Alteinwilligung den wesentlichen Bedingungen der DS-GVO entspricht. Unternehmen sind indes gut beraten, bereits vor der Verbindlichkeit der DS-GVO die neuen Maßgaben zu beachten.

Pascal Tavanti
Jahrgang 1971, Fachanwalt für gewerblichen Rechtsschutz, Fachanwalt für Urheber- und Medienrecht, Partner der Scheuermann Westerhoff Strittmatter GbR, Standort Berlin, Mitglied des Ausschusses „Gewerblicher Rechtsschutz" der Bundesrechtsanwaltskammer, Lehrbeauftragter an der Universität Potsdam, nebenamtlicher Prüfer beim Justizprüfungsamt Berlin-Brandenburg.

Prof. Dr. Rolf Schwartmann/Steffen Weiß

Ko-Regulierung vor einer neuen Blüte: Impulse für datenschutzspezifische Zertifizierungsverfahren und Verhaltensregelungen (2. Teil Verhaltensregeln)

Was der nationale Gesetzgeber über § 9a und 38a BDSG über Jahre in die Wege zu leiten versuchte, wird mittels der EU-Datenschutz-Grundverordnung (DS-GVO) Wirklichkeit: Das künftige EU-Recht sieht einen Abschnitt zu Verhaltensregeln und Zertifizierung (Art. 40-43) vor. Hierdurch wird Verbänden und anderen Vereinigungen die Möglichkeit eingeräumt, Verhaltensregeln auszuarbeiten, zu ändern oder zu erweitern, um Datenschutzanwendungen in verschiedener Hinsicht zu präzisieren. Diese Verhaltensregeln können von der Kommission für allgemeingültig erklärt werden (Art. 40 Abs. 9). Inwieweit Verhaltensregeln von Datenschutz-Zertifizierungsverfahren abzugrenzen sind, ist ebenso von Interesse wie Formen ihrer Umsetzung. Die Fokusgruppe Datenschutz der Plattform 6 „Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft" des Nationalen IT-Gipfels möchte Leitlinien für die Pseudonymisierung personenbezogener Daten, als besonders praxisrelevanten Bereich für eine Datenschutzanwendung, definieren, die in eine eigene Verhaltensregel im Sinne der DS-GVO münden können.

I. Einleitung

Im Gegensatz zu den Zertifizierungsverfahren im Datenschutz haben die Verhaltensregeln bereits über Art. 27 Einzug in die EU-Datenschutzrichtlinie 95/46/EG (EU-Datenschutzrichtlinie) gehalten, um eine ordnungsgemäße Durchführung der einzelstaatlichen Vorschriften nach Maßgabe der Besonderheiten eines einzelnen Bereichs zu berücksichtigen. Entsprechend sieht § 38a BDSG vor, dass Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten können. Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

Die DS-GVO knüpft an die Impulse der EU-Datenschutzrichtlinie an und schafft über Art. 41-42 gesetzliche Grundlagen für die Erarbeitung, Änderung oder Erweiterung von Verhaltensregeln. Art. 40 Abs. 1 DS-GVO enthält dabei – wie schon sein Pendant für die Zertifizierung – den Appell an Mitgliedstaaten, Aufsichtsbehörden, Datenschutzausschuss und Kommission, die Ausarbeitung solcher Verhaltensregeln nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstununternehmen sowie kleinen und mittleren Unternehmen zu fördern. Wie bereits im Zuge der Analyse der Zertifizierungsverfahren[1] sollen zunächst bestehende Ansätze für Verhaltensregeln dargestellt werden, bevor eine vertiefte Darstellung nach der DS-GVO und Möglichkeiten ihrer Umsetzung erfolgt.

II. Bestehende Ansätze für Verhaltensregeln

Initiativen hinsichtlich der Erarbeitung von Verhaltensregeln, auch als „Code of Conduct" bezeichnet, bestehen auf

1 Schwartmann/Weiß, RDV 2016, 68.

europäischer Ebene, allerdings kann deren Verbreitung als gering eingestuft werden. So widmete sich die International Air Transportation Association (IATA) früh nach Gültigkeit der EU-Datenschutzrichtlinie den einheitlichen Regeln im Datenschutz bei den grenzüberschreitenden Datenflüssen im internationalen Luftverkehr bei der Beförderung von Personen und Fracht. Allerdings wurde dieses Dokument nie als Verhaltenskodex im Sinne des Art. 27 Abs. 3 der EU-Datenschutzrichtlinie finalisiert und kam damit nicht über das Stadium einer Vorlage für die Erstellung von Verhaltensregeln hinaus.[2] Weiter gediehen ist der Vorstoß der Federation of European Direct and Interactive Marketing (FEDMA), verbindliche Verhaltensregeln aufzustellen. So postuliert der „European Code of Practice for the use of personal data in direct marketing"[3] Regeln für einen Umgang mit personenbezogenen Daten beim Direktmarketing, die nach Auffassung der Artikel-29-Datenschutzgruppe als im Einklang mit der EU-Datenschutzrichtlinie bzw. der Richtlinie 2002/58/EG anzusehen sind.[4] Ferner ermöglichten die Regeln einen hinreichenden und zu fordernden Mehrwehrt.[5] Auch dem Bereich des Direktmarketings zuordnenbar ist das IAB Europe EU Framework for Online Behavioural Advertising[6], das jedoch nie den Grad einer gemeinschaftlich anerkannten Verhaltensregel erlangt hat.[7] Auch der in jüngerer Vergangenheit entwickelte Code of Conduct der Cloud Select Industry Group (C-SIG), der sich mit einheitlichen Vorgaben für den Datenschutz beim Cloud Computing befasst, konnte die europäische Hürde der Artikel 29-Datenschutzgruppe aufgrund rechtlicher Bedenken sowie mangelndem Mehrwehrt noch nicht nehmen.[8]

Auf nationaler Ebene ist der Code of Conduct der Versicherungswirtschaft („Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft") hervorzuheben[9], der unter Federführung des Gesamtverbands der Deutschen Versicherungswirtschaft e.V. (GDV) und im Einvernehmen mit den Mitgliedsunternehmen entwickelt wurde. Diesen Verhaltensregeln liegt nicht nur die Zustimmung der zuständigen Aufsichtsbehörden der Mitgliedsverbände des GDV zugrunde, sondern auch die Genehmigung des Berliner Beauftragten für Datenschutz und Informationsfreiheit als die für den GDV zuständige Aufsichtsbehörde gemäß § 38a BDSG. Die Verhaltensregeln sollen den bestehenden rechtlichen Rahmen ergänzen und konkretisieren und Gewähr bieten, dass Datenschutz- und Datensicherheitsbelange bei der Gestaltung und Bearbeitung von Produkten und Dienstleistungen berücksichtigt werden. Um die Datenverarbeitung aller beigetretenen Unternehmen zu regeln, sind sie möglichst allgemeingültig formuliert[10]. Sollen Verhaltensregeln daher für möglichst viele beitretende Organisationen gelten, dürfte ein konkreter Anforderungskatalog bezüglich technisch-organisatorischer Maßnahmen beispielsweise schwierig umzusetzen sein.

Als jüngeres Beispiel einer genehmigten Verhaltensregel dient der GeoBusiness Code of Conduct – Verhaltensregel zur Geodatennutzung durch Wirtschaftsunternehmen[11], ein von der Selbstregulierung in der Informationswirtschaft (SRIW e. V.) beantragter Verhaltenskodex, damit die wirtschaftliche Nutzung von Geodaten öffentlicher Stellen durch Unternehmen nach einer anerkannten Selbstverpflichtungserklärung für den Umgang mit den Geodaten erfolgen kann. Charakteristisch für den Kodex ist der verpflichtende Einsatz eines Datenschutzmanagementsystems sowie angemessener technisch-organisatorischer Maßnahmen. Die überschaubare Anzahl von Verhaltensregeln auf nationaler und europäischer Ebene sowie zahlreiche gescheiterte Initiativen zeigen, dass der bestehende Rahmen für solche Instrumente der Selbstregulierung noch nicht Anreiz genug ist bzw. es an Rechtsklarheit bei der Erstellung und Anwendung mangelt.

III. Verhaltensregeln nach der DS-GVO

1. Rechtlicher Rahmen

Telos der „Verhaltensregeln 2.0" in der DS-GVO ist die Präzisierung der Anwendung der rechtlichen Vorgaben, resultierend aus den oftmals zu findenden generalklauselartigen Formulierungen. Art. 40 Abs. 2 DS-GVO bietet dabei eine nicht abschließende Liste für mögliche Präzisierungen durch Verbände oder andere Vereinigungen, so unter anderem bezüglich einer fairen und transparenten Verarbeitung, berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen, den Betroffenenrechten, der Datensicherheit, der Übermittlung personenbezogener Daten an Drittländer und der Pseudonymisierung. Verantwortliche und Auftragsverarbeiter mit ausschließlichem Sitz in einem Drittland, die nicht in den Anwendungsbereich der DS-GVO fallen, mithin weder Betroffenen in der EU Waren oder Dienstleistungen anbieten oder deren Verhalten in der EU beobachten, können sich genehmigten und für allgemeingültig erklärten Verhaltensregeln unterwerfen, um eine Garantie für die Übermittlung personenbezogener Daten in das jeweilige Drittland zu bieten (vgl. Art. 40 Abs. 3 S. 1 DS-GVO). Wie bereits die Zertifizierungsverfahren, erfordern auch die Verhaltensregeln die Überwachung der Einhaltung

2 Vgl. Artikel 29-Datenschutzgruppe, WP 49, S. 3.

3 Http://www.fedma.org/fileadmin/documents/SelfReg_Codex/FEDMA-CodeEN.pdf

4 Artikel 29-Datenschutzgruppe, WP 174, S. 3.

5 Artikel 29-Datenschutzgruppe, WP 174, S. 4: „Der vorgelegte Kodex muss ausreichende Qualität und Kohärenz aufweisen und ausreichenden Mehrwert liefern, insbesondere muss er ausreichend auf die spezifischen Fragen und Probleme des Datenschutzes in der Organisation oder dem Sektor ausgerichtet sein, für die er gelten soll, und für diese Fragen und Probleme ausreichend klare Lösungen bieten."

6 Http://www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf.

7 Zu den Gründen siehe auch Artikel 29-Datenschutzgruppe, WP 188.

8 Artikel 29-Datenschutzgruppe, WP 232.

9 GDV, Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft, abrufbar unter http://www.gdv.de/wp-content/uploads/2013/03/GDV_Code-of-Conduct_Datenschutz_2012.pdf.

10 S. GDV a.a.O., S. 2.

11 Http://www.geobusiness.org/GEOBUSINESS/Redaktion/DE/Downloads/geobusiness-code-of-conduct.pdf.

ihrer Bestimmungen, was die Frage nach der Abgrenzbarkeit der beiden Instrumente aufwirft (vgl. II. 4.). Der beispielhafte Katalog möglicher Präzisierungen zeigt, dass Verhaltensregelungen über die Impulse der Kommission[12] hinausgehen können. Denkbar sind damit auch Verhaltensregelungen für Auftragsdatenverarbeiter[13] ebenso wie für gemeinsam für die Verarbeitung Verantwortliche beispielsweise. Die als redaktionelles Versehen einzustufende Begrenzung auf verantwortliche Stellen in Art. 27 Abs. 2 der EU-Datenschutzrichtlinie bzw. § 38 Abs. 1 BDSG entfällt unter der DS-GVO, die Auftragsverarbeiter ausdrücklich in den Geltungsbereich der Verhaltensregeln mit einbezieht (Art. 40 Abs. 2 S. 1 DS-GVO). Verhaltensregeln sollen überdies den besonderen Risiken einer Verarbeitung Rechnung tragen, die als wahrscheinlich gelten (ErwG 98 S. 2). Der risikoorientierte Ansatz ist dabei ein prägendes Merkmal der DS-GVO. Inhaltliche Anforderungen an Verhaltensregeln stellt die DS-GVO im Übrigen nicht.

2. Überwachung

Art. 40 Abs. 4 DS-GVO enthält den unabdingbaren Appell, Verfahren für eine Überwachung der Verhaltensregeln vorzusehen. Eine Konkretisierung der Vorgaben an eine Überwachung erfolgt in Art. 41 DS-GVO, wobei sich diese an die überwachende Stelle richten, die bei der zuständigen Datenschutz-Aufsichtsbehörde zu akkreditieren ist.

Entweder die die Verhaltensregeln erlassende Organisation selbst oder eine unabhängige und fachkundige Stelle überwacht die Einhaltung der Verhaltensregeln (Art. 41 Abs. 1 DS-GVO). Die Akkreditierung ist – wie schon im Rahmen der Zertifizierungsverfahren – mit der Erfüllung besonderer Anforderungen verbunden. Fachkunde, Unabhängigkeit, eine regelmäßige Überprüfung der Einhaltung und Anwendung der Vorgaben der Verhaltensregeln werden dabei ebenso gefordert wie das Vorhandensein eines transparenten Umgangs mit Beschwerden und ein Ausschluss von Interessenskonflikten. Ferner ist die Anwendbarkeit der Verhaltensregeln beim Verantwortlichen oder Auftragsverarbeiter zu prüfen. Ob hiermit eine realistische Möglichkeit der Umsetzung vorgesehen ist oder gar eine besondere Praxistauglichkeit der Regeln gefordert wird, ergibt sich aus dem Gesetzeswortlaut nicht unmittelbar. Aus Gründen der gewünschten Verbreitung von Verhaltensregeln auf europäischer Ebene werden auch strengere Vorgaben als die in der DS-GVO geforderten formuliert werden könnten, so lange diese bei den Datenverarbeitern in irgend einer Form angewendet bzw. umgesetzt werden können. Die Differenzierung zwischen Einhaltung und Anwendung zeigt auch, dass ein Datenverarbeiter sein Handeln an den Verhaltensregeln auszurichten hat. Hier wird wiederum der Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO Rechnung zu tragen sein, die über eine bloße Einhaltung gesetzlicher Vorgaben hinausgeht und eine nachvollziehbare Anwendung solcher Anforderungen fordert. Im Übrigen werden keine besonderen Vorgaben an die Form der Überwachung gestellt. Folglich wäre der Einsatz von Fragebögen wie im Rahmen des EU-U.S. Privacy Shield ebenso denkbar, wie die Durchführung von Vor-Ort-Kontrollen. Durch die Gleichschaltung mit den Anforderungen an eine zu akkreditierende Stelle bei den Zertifizierungsverfahren wird ersichtlich, dass Brüssel im Rahmen der überwachenden Stelle keine „Zertifizierung light" bezweckte.

3. Anerkennung durch die Aufsicht

Ein entwickelter Kodex ist der Aufsichtsbehörde vorzulegen, die für den Verband bzw. die Vereinigung gem. Art. 55 DS-GVO zuständig ist. Die weitere Ausgestaltung des Verfahrens auf nationaler Ebene, bedingt durch eine föderale Struktur, wird durch die DS-GVO nicht beantwortet. Hier wären ergänzende Regelungen, wie die Zusammenarbeit zwischen den Aufsichtsbehörden der Länder – immerhin sollen Verhaltensregeln eine breite Verbreitung genießen – wünschenswert. Die zuständige Behörde prüft sodann den Kodex auf Vereinbarkeit mit der DS-GVO. Ist dies der Fall und enthalten die Verhaltensregeln ausreichende Garantien, erfolgt eine Aufnahme in das Verzeichnis für Verhaltensregeln bei der Aufsicht und eine Veröffentlichung (Art. 40 Abs. 6 DS-GVO).

Sobald mit den erarbeiteten Regeln erhebliche Auswirkungen für eine bedeutende Zahl Betroffener in mehreren Mitgliedstaaten einhergehen, ist vor der Genehmigung das Kohärenzverfahren gem. Art. 63 zu durchlaufen (Art. 40 Abs. 7 DS-GVO). Hierbei gibt der Europäische Datenschutzausschuss seine Stellungnahme ab, ob der Kodex im Einklang mit der DS-GVO steht und die geforderten Garantien bietet. Auch hierbei wird nach erfolgter Anerkennung über ein öffentlich zugängliches Register Transparenz gewahrt (Art. 40 Abs. 11 DS-GVO). Rechtsfolgen einer Anerkennung durch die zuständige Aufsicht – mit oder ohne Einbeziehung des Europäischen Datenschutzausschusses – werden durch die DS-GVO nicht formuliert.

4. Abgrenzung zu Zertifizierungsverfahren

Während die Verhaltensregeln hinsichtlich einer ordnungsgemäßen Anwendung beitragen (Art. 40 Abs. 1 DS-GVO), sollen Zertifizierungsverfahren einen Nachweis für die Einhaltung der DS-GVO erbringen (Art. 42 Abs. 1 DS-GVO). Der europäische Gesetzgeber verfolgt daher grundsätzlich zwei unterschiedliche Ziele: Zum einen sollen Unklarheiten bei der Anwendung der DS-GVO mithilfe der Verhaltensregeln beseitigt werden. Hierdurch bedient man sich entsprechender Initiativen von Verbänden und Vereinigungen. Die Zertifizierungsverfahren hingegen zielen auf einen Nachweis einer nach der DS-GVO ordnungsgemäßen Datenverarbeitung ab. D.h. hier wird der Versuch unternommen, Datenschutzkonformität sichtbar zu machen, um das Vertrauen in eine Datenverarbeitung zu stärken – ein wichtiger Leitgedanke der DS-GVO gegenüber Verantwortlichen und Betroffenen. Dieses Sichtbarmachen zeigt sich im Rahmen der Zertifizierungsverfahren auch dadurch, dass ein Verantwortlicher

12 Vgl. Artikel 38 des Entwurfs der Kommission KOM (2012) 11 endgültig.

13 So beispielsweise der Datenschutzstandard für Auftragsdatenverarbeiter „DS-BvD-GDD-01".

oder Auftragsverarbeiter gegenüber der Prüfstelle alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung zu stellen und ihr den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten zu gewähren hat (Art. 42 Abs. 6 DS-GVO). Die Verhaltensregeln hingegen werden nicht durch den Gedanken attestierter Rechtskonformität getragen. Sie wollen einer Rechtsunsicherheit begegnen und konkrete Szenarien durchleuchten. Anforderungen an die Überprüfbarkeit von Datenverarbeitern sind dort nicht enthalten. Hinsichtlich der Rechtsfolgen genehmigter Verhaltensregeln, denen sich ein Verantwortlicher oder Auftragsverarbeiter unterwirft, bedarf es keiner Klarstellung, dass solche Stellen weiterhin vollumfänglich zur Einhaltung der DS-GVO verpflichtet sind, immerhin möchten diese zu ihrer ordnungsgemäßen Anwendung beitragen. Allerdings sollen eingehaltene Verhaltensregeln bei der Verhängung einer Geldbuße durch eine Aufsichtsbehörde berücksichtigt werden (Art. 83 Abs. 2 Buchst. j), was als Anreiz für eine Erarbeitung verstanden werden sollte.

Trotz der unterschiedlichen Zielsetzung liegt beiden Instrumenten ein gemeinsamer Gedanke zugrunde: Es bedarf eines Anforderungskatalogs – im besten Fall auch bei der Zertifizierung öffentlich zugänglich –, um Hinweise für eine datenschutzkonforme Umsetzung der DS-GVO zu geben. Im Sinne eines gestuften Modells wären die Verhaltensregeln als wichtige Grundlage für ein Zertifizierungsverfahren zu sehen. Auf Basis dieses Anforderungskatalogs würden dann Anforderungen an das Verfahren um Überwachung und Durchsetzung formuliert werden. Die besondere Wertigkeit von Zertifizierungsverfahren manifestiert sich in der DS-GVO jedoch hauptsächlich in Gestalt der getroffenen Aussagen der unabhängigen Prüfer hinsichtlich der Datenschutzkonformität der Datenverarbeitung. Denn sowohl bei den Zertifizierungsverfahren als auch bei den Verhaltensregeln werden Anforderungen an die überwachende Stelle gestellt, die im Kern deckungsgleich sind. Hier wäre es wünschenswert, die besondere Bedeutung der Zertifizierung durch strengere Vorgaben an die Zertifizierungsstelle hervorzuheben, beispielsweise durch die Formulierung besonderer Anforderungen an eingeschaltete Prüfer oder die Definition eindeutiger Kriterien für mögliche Interessenskonflikte von Prüfer und Zertifizierungsstelle sowie die Veröffentlichung der Prüfkriterien zugunsten der Allgemeinheit.

5. Rolle der Kommission

Die Kommission wird erst spät in die Prüfung bzw. Genehmigung von Verhaltensregeln einbezogen. Primäre Anlaufstelle bleibt die zuständige Aufsichtsbehörde, die mit ihrer Fachkunde eine Genehmigungsfähigkeit solcher Regeln aussprechen kann. Betreffen Verhaltensregeln mehrere Mitgliedstaaten, legt die genehmigende Aufsicht diese Regeln dem Datenschutzausschuss im Rahmen des Kohärenzverfahrens nach Art. 63 DS-GVO vor. Erst wenn der Datenschutzausschuss die Regeln als im Einklang stehend mit der DS-GVO sieht bzw. diese ausreichende Garantien für einen Drittlandstransfer bieten (Art. 40 Abs. 3), leitet er seine Stellungnahme an die Kommission weiter. Sie kann sodann – muss aber nicht – im Rahmen eines Durchführungsakts[14] beschließen, dass die Verhaltensregeln allgemeine Gültigkeit in der Union besitzen sollen. Welche Inhalte einer Verhaltensregel die Kommission zu einer Erhebung hin zu einer Allgemeingültigkeit veranlassen könnten, ergibt sich aus der DS-GVO nicht. Bei der Entscheidungsfindung ist das Ausschussverfahren nach Art. 93 Abs. 2 DS-GVO vorgesehen, das gemäß der Vorgaben der Verordnung (EU) Nr. 182/2011 durch die Mitgliedstaaten kontrolliert wird. Dies umfasst jedoch kein transparentes Verfahren für die Öffentlichkeit, was bereits in der Entscheidungsfindung zum EU-U.S. Privacy Shield zu einer eingeschränkten Nachvollziehbarkeit geführt hat. Hierbei wären transparente Gründe für eine Allgemeingültigkeit wünschenswert.

Die (Rechts)folgen einer Allgemeingültigkeit werden weder in der DS-GVO noch im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) normiert. Grundsätzlich sollen Durchführungsrechtsakte, in deren Bahnen die Entscheidung über eine Allgemeingültigkeit erfolgt, einheitliche Bedingungen für bindende Rechtsakte der EU schaffen. Ihnen ist kein Gesetzgebungsakt immanent. Ob ein Verstoß gegen für allgemeingültig erklärte Verhaltensregeln damit gleichzeitig einen Verstoß gegen die DS-GVO bedeutet, ist damit noch ungeklärt. Die Klärung dieser Frage wird im Zuge einer Einzelfalluntersuchung einer Verhaltensregel erfolgen müssen, nämlich ob diese den Rahmen der DS-GVO konkretisiert – was dann für einen Verstoß sprechen würde – oder ob gar strengere Vorgaben festgelegt wurden, was dann wiederum nicht zwingend für einen Verstoß sprechen muss.

IV. Anforderungen an Verhaltensregeln

Die DS-GVO hält sich mit der Formulierung konkreter Anforderungen an Verhaltensregeln weitestgehend zurück. Der gewünschte Beitrag zur ordnungsgemäßen Anwendung der DS-GVO wird in Art. 40 Abs. 2 DS-GVO lediglich dergestalt ergänzt, dass Vorschläge für mögliche Präzisierungen gemacht werden. Diese Vorschläge sind beispielhafter Natur und enthalten keine inhaltlichen Anforderungen an eine Verhaltensregel.

Es liegt folglich nahe, den Blick über die DS-GVO hinaus zu richten, um Hinweise für konkrete Anforderungen an Verhaltensregeln zu erhalten. Hier helfen zunächst Aussagen der Artikel-29-Datenschutzgruppe bei der Beurteilung erarbeiteter Verhaltensregeln (vgl. II.). Im Übrigen enthält die Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt in Art. 37 wie schon die DS-GVO – die allgemeine Aufforderung an Mitgliedstaaten, in Zusammenarbeit mit der Kommission begleitende Maßnahmen vorzunehmen, um insbesondere Berufsverbände, -organisationen und -vereinigungen zu ermutigen, auf Gemeinschaftsebene im Einklang mit dem Gemeinschaftsrecht Verhaltenskodizes auszuarbeiten. Darüber hinaus werden über Erwägungsgrund 114 the-

14 Zu den Durchführungsrechtsakten Schwartmann/Weiß, RDV 2016, 68, 72.

matische Vorschläge für Verhaltensregeln im Dienstleistungssektor gemacht, so sollten je nach Art der einzelnen Berufe Bestimmungen über die kommerzielle Kommunikation in den reglementierten Berufen sowie die Standesregeln der reglementierten Berufe enthalten sein, die insbesondere die Wahrung der Unabhängigkeit, der Unparteilichkeit und des Berufsgeheimnisses gewährleisten. D.h. hier wird ein ähnlicher Ansatz wie bei der DS-GVO verfolgt, indem mögliche Themen für eine Verhaltensregel vorgeschlagen werden. Die Generaldirektion für Dienstleistungen der Europäischen Union hat in diesem Zusammenhang kleinere Hinweise für inhaltliche Rahmenbedingungen von Verhaltensregeln veröffentlicht, um dem Förderungsgedanken des Art. 37 der Richtlinie 2006/123/EG nachzukommen und diesen weiter zu konkretisieren.[15] Den Ausgangspunkt der Ausführungen bildet die ebenso wichtige wie selbstverständliche Feststellung, dass Verhaltensregeln im Einklang mit Europäischem Recht stehen müssen. Aus Sicht des Datenschutzes bedeutet dies, dass solche Regeln sich an Art. 7 und 8 der EU-Grundrechtecharta sowie Art. 16 des Vertrags über die Arbeitsweise der EU (AEUV) ebenso zu messen haben werden wie an der DS-GVO als sekundärem Recht. Ein Unterschreiten der gesetzlichen Anforderungen wird sich mit dem Wortlaut des Art. 40 abs. 2 DS-GVO nicht vereinbaren lassen. Verbände und andere Vereinigungen sollten jedoch nicht daran gehindert sein, strenge Anforderungen in ihren Verhaltensregeln zu formulieren. So besagt bereits Erwägungsgrund 115 der Richtlinie 2006/123/EG, dass die Mitgliedstaaten nicht daran gehindert sind, im Einklang mit dem Gemeinschaftsrecht rechtliche Maßnahmen im Zuge der Erarbeitung von Verhaltensregeln zu erlassen, oder die nationalen Berufsverbände, einen stärkeren Schutz in ihren nationalen Verhaltenskodizes vorzusehen. Die Vereinbarkeit mit europäischem Recht ist dabei stets zu berücksichtigen.[16]

Mit Blick auf die Aufsichtsbehörden für den Datenschutz auf nationaler Ebene ergeben sich weitere Erkenntnisse für die Erarbeitung von Verhaltensregeln. So genügt es nach Auffassung des Hessischen Datenschutzbeauftragten im Zuge der Prüfung von Verhaltensregeln eines Sportverbandes nicht, den Wortlaut der einschlägigen datenschutzrechtlichen Regelungen wiederzugeben.[17] Vielmehr müsse ein „Mehrwert" gegeben sein, d.h. die Verhaltensregel muss die abstrakten gesetzlichen Regelungen branchenspezifisch bzw. kontextbezogen konkretisieren, so dass typische Anwendungsfälle in dem betreffenden Bereich erläutert sind. Eine im Übrigen selbstverständliche Klarstellung, die im in Art. 40 Abs. 2 DS-GVO formulierten Präzisierungsgedanken ihr Pendant findet.

V. Möglichkeiten der Ausgestaltung nach der DS-GVO

Gemäß des in der DS-GVO verfolgten Konkretisierungsansatzes bei den Verhaltensregeln muss der jeweilige Regelungskatalog in der Lage sein, die teilweise generischen Anforderungen der DS-GVO zu präzisieren. Dass damit ein Mehrwehrt verbunden sein muss, ergibt sich aus dem Gesetzestext nicht unmittelbar, wird jedoch aufgrund der Äußerungen der Artikel-29-Datenschutzgruppe, der nationalen Aufsichtsbehörden sowie dem Sinn und Zweck solcher Regeln unumgänglich sein. Ferner müssen die Regeln im Einklang mit der DS-GVO stehen, was gerade bei strittigen Sachverhalten und dem Wirken des neuen Datenschutz-Regimes auf europäischer Ebene ab dem 25.05.2018 eine Herausforderung darstellen wird.

Um eine wichtige Vorarbeit für neue Verhaltensregeln zu leisten und die Bedeutung solcher Präzisierungen der DS-GVO aus Sicht des Datenschutzes zu stärken, hat sich die Fokusgruppe Datenschutz im Rahmen des Nationalen IT-Gipfels der Thematik zugewendet.[18] Im Sinne des gesetzgeberischen Auftrags nach einer Präzisierung wurde die Pseudonymisierung personenbezogener Daten als Szenario ausgewählt, das auch einen ausreichenden Mehrwert für Datenverarbeiter bieten kann. Die Bedeutung der Pseudonymisierung für die Wirtschaft ergibt sich an zahlreichen Stellen der DS-GVO selbst. Zum einen hat die Pseudonymisierung überhaupt Einzug in das europäische Regelwerk gehalten, was mit Blick auf bestehende Datenschutzgesetze der Mitgliedstaaten keine Selbstverständlichkeit ist. Denn weder die EU-Datenschutzrichtlinie noch die Konvention Nr. 108 kennen diese Art des Datums, im Gegensatz zum anonymen Datum in Abgrenzung zur persönlichen Information. Auch im internationalen Kontext hat die Pseudonymisierung bis dato nicht die Bedeutung erlangt, die sie einzunehmen in der Lage ist. Gerade hier werden wichtige Abgrenzungen zu anonymen Daten, im Kontext US-amerikanischer Datenverarbeiter auch als „none personally identifiable information (non-PII)" referenziert, vorgenommen werden müssen.

Neben der Begriffsdefinition des Art. 4 Abs. 5 DS-GVO als eine Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen zum Schutz vor Re-Identifizierung unterliegen, fördert die DS-GVO die Pseudonymisierung durch eine Ermächtigungsfunktion. Art. 6 Abs. 4 DS-GVO ermöglicht die Zweckänderung einer Datenverarbeitung ohne gesonderte Einwilligung des Betroffenen, vorausgesetzt der neue Zweck ist mit dem der ursprünglichen Datenerhebung vereinbar. Im Rahmen der „Kompatibilitätsprüfung" hat der Verantwortliche Garantien

15 Directorate-General for Internal Market and Services, Enhancing the quality of service in the Internal Market: The role of European codes of conduct, abrufbar unter http://ec.europa.eu/internal_market/services/docs/services-dir/codeconduct/the_role_of_european_codes_of_conduct_en.pdf.

16 Vgl. Directorate-General for Internal Market and Services a.a.O., S. 11.

17 31. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten vom 11.12.2003, Ziff. 4.

18 Http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/NationalerIT-Gipfel/Plattform-Sicherheit-Schutz-Vertrauen/plattform-sicherheit-schutz-vertrauen_node.html.

zu berücksichtigen, die auch in einer Verschlüsselung oder Pseudonymisierung liegen können (vgl. Art. 6 Abs. 4 Buchst. e DS-GVO). Damit hat die Pseudonymisierung als zunächst technisch-organisatorische Maßnahme unmittelbare Auswirkungen auf die Zulässigkeit einer Datenverarbeitung, so beispielsweise im Zuge einer Big Data Anwendung.

Neben der erwähnten Ermächtigungsfunktion fällt der Pseudonymisierung eine besondere Schutzfunktion zugunsten des Betroffenen zu, die seine unmittelbare Identifizierung verhindert. Entsprechend sind Pseudonyme technisch-organisatorisch zu schützen, wobei ihre Aufhebung zu einer Verletzung des Schutzes personenbezogener Daten im Sinne der Art. 33 und 34 DS-GVO führt (vgl. ErwG 75). Wertvolle Hinweise, wie eine technisch-organisatorische Absicherung vonstatten gehen kann, finden sich bereits in einem White Paper[19] der European Privacy Advisory Group (EPAG) zu sog. „Key-Coded Data", die den Pseudonymen gleichgesetzt werden. Hierbei wird auch betont, dass die Einbindung eines vertrauensvollen Dritten hinsichtlich der Pseudonymisierung der Daten bzw. der Speicherung des Schlüssels zum Entschlüsseln des jeweiligen Pseudonyms nicht von der Implementierung technisch-organisatorischer Maßnahmen entbindet, zumal eine Verknüpfung von erhobenen Klardaten und den Pseudonymen nicht auszuschließen ist. Hinweise hinsichtlich adäquater technischer Mittel für die Pseduonymisierung finden sich im besagten White Paper nicht, was durch die Komplexität solcher Verfahren sowie deren Abhängigkeit von den zugrunde liegenden Klardaten erklärt werden kann. Nichtsdestotrotz möchte die Fokusgruppe auch mögliche Werkzeuge für eine Pseudonymisierung evaluieren. Hierbei können Pseudonymisierungstechniken aus der IT-Sicherheit, so beispielsweise im Bereich des Abuse Managements, von Telekommunikationsanbietern genutzt werden. Die im Frühjahr begonnene Tätigkeit der Fokusgruppe soll bis zum Nationalen IT-Gipfel 2017 beendet sein.

VI. Fazit

Verhaltensregeln und Zertifizierungsverfahren verfolgen unterschiedliche Zielsetzungen, haben aber eine gemeinsame und wichtige Basis, die die Frage nach Vor- und Nachteilen in den Hintergrund treten lässt: Ein Prüfkatalog, der Hinweise für eine Umsetzung der DS-GVO liefert und der zuständigen Aufsicht vorzulegen ist. Stellen, die ihren Schwerpunkt auf einer Nachweisbarkeit ihrer rechtskonformen Datenverarbeitung legen, werden die Mühen eines Prüfverfahrens durch unabhängige Prüfer nicht scheuen. Entsprechend werden Dienstleister auf dem Markt ihre Leistung als Zertifizierungsanbieter gestalten, möchten sie eine vertrauenswürdige Aussage hinsichtlich einer datenschutzkonformen Datenverarbeitung eines Verantwortlichen oder Auftragsverarbeiters treffen wollen. Verbände oder Vereinigungen, die Datenverarbeiter vertreten, werden hingegen bemüht sein, ihren Mitgliedern Unterstützung bezüglich der konkreten Umsetzung der gesetzlichen Vorgaben zu geben oder gar das gesetzliche Schutzniveau zu steigern, was nicht nur bei Verarbeitungen „kritischer" Daten interessant sein dürfte, sondern aufgrund der allgemeinen Formulierungen der DS-GVO mit Blick auf eine notwendige Rechtssicherheit für Datenverarbeiter zwingend notwendig sein wird. Zu bemängeln ist der fehlende Mut des europäischen Gesetzgebers, den Förderungsgedanken von Zertifizierungsverfahren und Verhaltensregeln mit weiteren gesetzgeberischen Maßnahmen als der Berücksichtigung im Rahmen der Verhängung von Geldbußen zu unterstützen. Hier wäre die Formulierung konkreter Rechtsfolgen ebenso denkbar gewesen wie eine verstärkte Integration der Datenschutz-Aufsicht bereits in der Entwicklungsphase von Verhaltensregeln oder Prüfkatalogen von Zertifizierungsverfahren. Nichtsdestotrotz sind verstärkte Initiativen für solche Verfahren nach Anwendung der DS-GVO zu erwarten – immerhin werden diese nun auf einem einheitlichen Recht basieren und Millionen von Verantwortlichen und Auftragsverarbeitern in der EU betreffen können.

Prof. Dr. Rolf Schwartmann
Leiter der Kölner Forschungsstelle für Medienrecht an der Fachhochschule Köln, Mitherausgeber der Fachzeitschrift RDV sowie Vorstandsvorsitzender der GDD e.V., Bonn. Er ist Mitglied der Plattform „Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft" im Rahmen des nationalen IT-Gipfels der Bundesgierung und leitet dort die Fokusgruppe Datenschutz.

Steffen Weiß, LL.M.
Repräsentant Internationales bei der GDD und aktiver Mitarbeiter des europäischen Datenschutz-Dachverbands CEDPO. Er ist Mitglied der Plattform „Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft" im Rahmen des Nationalen IT-Gipfels und engagiert sich dort u.a. in der Fokusgruppe Datenschutz. Er studierte Rechtswissenschaften an der Universität Heidelberg und erlangte den akademischen Grad des Master of Laws über seine Teilnahme am European Legal Informatics Study Programme mit Stationen in Hannover und Buenos Aires. Vor seiner Tätigkeit bei der GDD war er Berater in Sachen Datenschutz für öffentliche und nicht-öffentliche Stellen. Er hält regelmäßig Vorträge zu datenschutzrechtlichen Themen auf nationalem und internationalem Terrain. Ferner ist er seit 2015 Lehrbeauftragter für Datenschutz an der FH Wedel.

19 Http://www.epag-thinktank.eu/docs/whitepapers/EPAG_Whitepaper_Key_Coded_Data.pdf.

Joerg Heidrich/Dr. Christoph Wegener/Brian Scheuch

Prüfungspflichten beim Verbot der Nutzung von Internet und E-Mail im Unternehmen

Die Abgrenzung zwischen der Erlaubnis und dem Verbot einer privaten Nutzung von Internet und E-Mail am Arbeitsplatz beschäftigt die juristische Literatur seit vielen Jahren. Einigkeit besteht darüber, dass es dem Arbeitgeber frei steht, die Privatnutzung zu verbieten, um die Arbeitsleistung seiner Mitarbeiter überwachen zu können. Weitgehende Einigkeit besteht auch darüber, dass im Falle der Anordnung eines solchen Verbots eine Pflicht entsteht, dessen Einhaltung zu kontrollieren. Wie allerdings genau diese Kontrolle unter datenschutzrechtlichen Bedingungen aussehen muss und kann, ist bislang nur wenig behandelt worden. Der nachfolgende Beitrag hat sich die entsprechende juristische Diskussion zum Ziel gesetzt und will gleichzeitig rechtskonforme Leitlinien zur Durchführung der notwendigen Kontrollen aufstellen.

I. Überwachung von E-Mail- und Internetverkehr

Die Überwachung des E-Mail- und Internetverkehrs der Arbeitnehmer ist ein hoch sensibles und zugleich juristisch umstrittenes Thema. Um zu prüfen, ob und unter welchen Voraussetzungen der Arbeitgeber die digitale Kommunikation seiner Mitarbeiter überwachen darf, ist es nach h.M. notwendig zu differenzieren, ob die private Nutzung der geschäftlichen E-Mail und Internetanbindung ausdrücklich erlaubt ist, der Arbeitgeber diese möglicherweise geduldet oder ausdrücklich verboten hat.[1]

1. Erlaubnis einer privaten Nutzung

Ausgangspunkt ist dabei zunächst die ausdrückliche Erlaubnis einer privaten Nutzung von E-Mail und Internet am Arbeitsplatz. Dabei ist inzwischen vor allem die Frage nach der Einstufung des Arbeitgebers als E-Mail- und Access-Providers i.S. eines Diensteanbieters nach TKG umstritten.

a) Aktuelle Rechtslage

Nach noch immer weitverbreiteter Ansicht – insbesondere auch der Datenschutzbehörden[2] – hat die Erlaubnis der Privatnutzung zur Folge, dass der Arbeitgeber als Diensteanbieter im Sinne des TKG anzusehen ist.[3] Dies hätte insbesondere zur Folge, dass dieser damit auch dem Fernmeldegeheimnis nach § 88 TKG unterliegt – mit den entsprechend weitreichenden Konsequenzen. Danach wäre eine Überwachung der E-Mails und des Internetverkehrs ohne zusätzliche Vereinbarungen grundsätzlich verboten.[4] Eine Klassifizierung des Arbeitgebers als Diensteanbieter im Sinne des Telemediengesetzes (TMG), insbesondere nach § 2 Abs. 1 Nr. 1 TMG, scheidet dagegen in den allermeisten Fällen aus[5] und kommt nur für vom Arbeitgeber selbst betriebene oder in dessen Auftrag gehostete Webdienste[6], etwa betriebliche Webmail-Portale, in Betracht.

b) Tendenz der aktuellen Rechtsprechung der Arbeitsgerichte

Die neuere Rechtsprechung im Bereich des Arbeitsrechts tendiert jedoch dahin, den Arbeitgeber nicht als Diensteanbieter im Sinne des TKG zu klassifizieren. So vertreten das LAG Niedersachsen und das LAG Berlin-Brandenburg explizit die Auffassung, dass § 88 TKG deshalb keine Anwendung findet, da der Arbeitgeber schon kein Diensteanbieter im Sinne des TKG ist.[7] Die Urteile begründen dies jedoch nur sehr unzureichend: In der Entscheidung des LAG Niedersachsen fehlt dazu jegliche Begründung, das LAG Berlin-Brandenburg führt in seiner Entscheidung immerhin aus, dass der Arbeitgeber keine geschäftsmäßige Telekommunika-

1 Stamer/Kuhnke, in: Plath, BDSG, § 32, Rn. 79; Seifert, in: Simitis, BDSG, § 32 Rn. 90.

2 Vgl. etwa: Datenschutzkonferenz, Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, Stand: Januar 2016.

3 De Wolf, NZA 2010, 1206; Vietmeyer/Byers, MMR 2010, 807, 808; Fischer, ZD 2012, 265, 266; Frings/Wahlers, BB 2011, 3126, 3130; Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, TKG, § 88 Rn. 18; Seifert, in: Simitis, BDSG, § 32, Rn. 92; Zoll, in: Taeger/Gabel BDSG, § 32, Rn. 43; Forst, in: Auernhammer, BDSG, § 32, Rn. 67; Nägele/Meyer, BB 2004, 312, 314; Mengel, BB 2004; Lindemann/Simon, BB 2001, 1950, 1953; Wedde, in: DKWW, BDSG § 32, Rn. 115ff.; Däubler, Gläserne Belegschaft, Rn. 366 ff.; Gola/Wronka, Handbuch, Rn. 1188 ff. Andere Auffassung: Stamer/Kuhnke in: Plath, BDSG, § 32, Rn. 113; Diercks, K&R, 2014, 5; Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 220 ff.; Schimmelpfennig/Wenning, DB 2006, 2290, 2292 ff.; Haußmann/Krets, NZA 2005, 259, 260; wohl auch Grobys, BB 2003, 682, 683.

4 Seifert, in: Simitis, BDSG, § 32, Rn. 92; Mengel, BB 2004, 1445 (1450); Hanau/Hoeren, S. 41 f.; De Wolf, NZA 2010, 1206; Vietmeyer/Byers, MMR 2010, 807, 808.

5 In einigen Leitfäden zur privaten Nutzung von Internet und E-Mail am Arbeitsplatz wird eine mögliche Anwendbarkeit des TMG nicht differenziert genug betrachtet. Völlig gegenteiliger Ansicht sind bspw. Polenz/Probst, „Private und dienstliche Internet- und E-Mail-Nutzung", ULD Schleswig-Holstein, 2014, online unter https://www.datenschutzzentrum.de/internet/private-und-dienstliche-internetnutzung.pdf verfügbar (Stand: 12. September 2016).

6 Für (auf Proxy-Servern) temporär zwischengespeicherte Inhalte kommt unter Umständen auch eine Anwendung des TMG in Betracht, da hier je nach Konfiguration des Proxy neben der Übertragungsleistung die Speicherung der Daten in den Vordergrund tritt.

7 LAG Berlin-Brandenburg, Urteil vom 16.02.2011 – 4 SA 2132/10; LAG Niedersachsen Urteil vom 31.05.2010 – 12 Sa 875/09.

tionsdienstleistung erbringt oder an einer solchen mitwirkt. Weiter detailliert begründet wird diese Ansicht jedoch nicht.

§ 3 Nr. 10 TKG definiert die geschäftsmäßige Erbringung einer Telekommunikationsdienstleistung als ein nachhaltiges Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. Nach richtiger Auffassung sind Mitarbeiter bei erlaubter privater Internetnutzung als Dritte im Verhältnis Arbeitgeber und Arbeitnehmer anzusehen, da die private Nutzung gerade nicht mehr in die Sphäre des Arbeitgebers fällt.[8] Auch stellt § 3 Nr. 10 TKG klar, dass es auf eine etwaige Gewinnerzielungsabsicht gerade nicht ankommt, sondern ein dauerhaftes Angebot ausreicht.

Doch auch wenn man eine andere Meinung vertreten[9] sollte und das TKG daher keine Anwendung finden würde, wäre die individuelle Überwachung der E-Mail- und Internetnutzung bei erlaubter privater Nutzung größtenteils unzulässig. Denn sollte das TKG keine Anwendung finden, so wäre man an die Voraussetzungen des § 32 BDSG gebunden.[10] Entscheidend ist demzufolge, dass eine Abwägung der gegenseitigen Interessen vorgenommen wird. Bei einer erlaubten privaten Internetnutzung wird in den allermeisten Fällen das Interesse des Arbeitnehmers überwiegen, der die geschäftliche E-Mail-Adresse und den Internetzugang auf Basis einer Erlaubnis, im Vertrauen auf die Wahrung seiner Privatsphäre, privat genutzt hat. Das Interesse eines Arbeitgebers an der Kontrolle seiner Mitarbeiter muss innerhalb der Abwägung dann zurückstehen.

2. Duldung einer privaten Nutzung

Einigkeit besteht darüber, dass eine Nichtregelung der hier im Raum stehenden Nutzung nicht automatisch dazu führt, dass die Privatnutzung dadurch erlaubt wird. Im Gegenteil ist im Einklang mit der Rechtsprechung der Arbeitsgerichte davon auszugehen, dass eine Nichtregelung erst einmal zu einem Verbot führt.[11] Weitgehend ungeklärt ist jedoch immer noch die Frage, ob und an welchem Punkt eine geduldete Privatnutzung zur Folge hat, dass der Arbeitgeber als Diensteanbieter im Sinne des TKG anzusehen ist und somit § 88 TKG Anwendung findet.[12]

Entscheidend ist dabei, ob aus einer Duldung der Privatnutzung eine betriebliche Übung entstehen kann. Eine betriebliche Übung liegt nach ständiger Rechtsprechung des BAG bei einem gleichförmigen und wiederholten Verhalten des Arbeitgebers vor, das geeignet ist, vertragliche Ansprüche auf eine Leistung oder eine sonstige Vergünstigung zu begründen.[13] Insbesondere muss der Arbeitnehmer aus dem Verhalten des Arbeitgebers schließen dürfen, ihm werde die Leistung oder Vergünstigung auch künftig gewährt.[14] Maßgebend ist, ob man aus dem Verhalten des Arbeitgebers, unter Berücksichtigung von Treu und Glauben, auf eine Bindungswirkung des Arbeitgebers schließen durfte. Eine betriebliche Übung wird man demnach nicht annehmen können, wenn der Arbeitgeber keine Kenntnis von einer privaten E-Mail- und Internetnutzung hat.[15]

Offen bleibt daher die Frage, ob eine betriebliche Übung bei Kenntnis und Duldung des Arbeitgebers hinsichtlich der privaten E-Mail- und Internetnutzung entstehen kann. Dabei stellt sich die Frage, ob bei einer reinen Duldung und Nichtsanktionierung überhaupt eine Leistung oder eine Vergünstigung seitens des Arbeitgebers gewährt wird. Nach verbreiteter Ansicht entsteht bei einer reinen Duldung keine betriebliche Übung, da es sich bei der Duldung lediglich um Annehmlichkeiten handelt und gerade nicht um eine aktive Leistung oder Vergünstigung des Arbeitgebers.[16] Denn bei einer bloßen Duldung und Nicht-Sanktionierung könne der Arbeitnehmer schon keine Erwartung haben, die Leistung komme ihm auch künftig zugute. Das hätte zur Folge, dass bei einer Kenntnis und Duldung der privaten E-Mail- und Internetnutzung das TKG grundsätzlich keine Anwendung finden würde.

Diese Ansicht überzeugt jedoch nicht. Denn die – wenn auch stillschweigende – Gestattung der Privatnutzung der betrieblichen E-Mail und Internetanbindung bietet sehr wohl einen faktischen und sogar geldwerten Vorteil, da die Zugriffsvolumina im Rahmen der Smartphone-Tarife, die der Mitarbeiter alternativ nutzen müsste, immer noch begrenzt und Nachkäufe entsprechend kostspielig sind. Wenn der Mitarbeiter aber stattdessen die betriebliche Infrastruktur nutzen kann, werden diese Volumina nicht reduziert. Zu berücksichtigen ist zudem das Zeitbudget, welches dem Mitarbeiter durch die Duldung ggf. zugestanden wird. Daher kann im Fall einer stillschweigenden Gestattung der Privatnutzung durchaus eine betriebliche Übung folgen.[17] Diese kann aber nur dann vorliegen, wenn in der „Duldung" der im Betrieb üblichen Privatnutzung durch den Arbeitgeber ein rechtsgeschäftlicher Erklärungswert liegt, der voraussetzt, dass der Arbeitgeber eindeutige Kenntnisse von der Privatnutzung hat.[18]

3. Verbot einer privaten Nutzung

Dem Arbeitgeber steht es frei, die private Nutzung von Internet und E-Mail am Arbeitsplatz ganz oder teilweise zu verbieten. Eine derartige Untersagung kann sowohl vertrag-

8 Fetzer, in: Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl. 2015, § 3, Rn. 27, m.w.N.

9 So etwa: Stamer/Kuhnke in: Plath, BDSG, § 32, Rn. 113; Diercks, K&R, 2014, 5; Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 220 ff.; Schimmelpfennig/Wenning, DB 2006, 2290 (2292 ff.); Haußmann/Krets, NZA 2005, 259 (260); wohl auch Grobys, BB 2003, 682, 683.

10 So auch: Zöll, in: Taeger/Gabel, BDSG, § 32, Rn. 43.

11 Stamer/Kuhnke, in: Plath, BDSG, 32 BDSG Rn. 89., m.w.N.

12 Zöll, in: Taeger/Gabel, BDSG, § 32, Rn. 43 m.w.N.

13 BAG, Urteil vom 11.11.2014, Az.: 3 AZR 849/11, Rn. 54

14 BAG, Urteil vom 19.05.2016 – 3 AZR 131/15 – Rn. 45.

15 So im Ergebnis auch: LAG Berlin-Brandenburg, Urteil v. 14.01.2016, Az. 5 Sa 657/15, online abrufbar unter http://tlmd.in/u/1681

16 Waltermann, NZA 2007, 529; Stamer/Kuhnke, in: Plath, BDSG, § 32, Rn. 92; Zöll, in: Taeger/Gabel, BDSG, § 32, Rn. 43; BAG, NZA 1998, 423 (424). Andere Auffassung: Barton, NZA 2006, 460 (461); Fleischmann, NZA 2008, 1397 (1397 f.); Küttner/Kreitner, Internet-, Telefonnutzung Rn. 4.

17 So auch: Landesbeauftragte für Datenschutz Baden-Württemberg, Dienstliche und private E-Mail- und Internet-Nutzung am Arbeitsplatz, Stand: Juni 2012

18 LAG Berlin-Brandenburg, Urteil v. 14.01.2016, Az. 5 Sa 657/15, online abrufbar unter http://tlmd.in/u/1681

lich als auch über eine Betriebsvereinbarung erfolgen. Sofern die private Nutzung ausdrücklich untersagt ist, richtet sich die Zulässigkeit einer solchen Überwachung entweder nach den Regelungen, die durch eine Einwilligung gemäß § 4 Abs. 1 BDSG getroffen wurden, oder, falls es an einer konkreten Einwilligung fehlt, nach den Vorgaben in § 32 BDSG.[19]

a) Einwilligung in die Überwachung

Lange Zeit war die Frage, ob es eine freiwillige datenschutzrechtliche Einwilligung im Rahmen eines Arbeitsverhältnisses geben kann, höchst umstritten.[20] Das Bundesarbeitsgericht hat jedoch inzwischen klargestellt, dass dies sehr wohl möglich ist.[21] Es steht dem Arbeitnehmer also grundsätzlich frei, in die E-Mail- und Internet-Überwachung und damit in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten einzuwilligen.[22] Unzweifelhaft muss die Einwilligung bereits im Voraus, d.h. vor einer erstmaligen Nutzung des geschäftlichen E-Mail- und Internetzugangs, erfolgen. Insofern ist es sinnvoll, neue Mitarbeiter schon bei der Einstellung eine entsprechende Vereinbarung unterschreiben zu lassen, die auch die Überwachung regelt.

b) Betriebsvereinbarung

Ist ein Betriebsrat vorhanden, so ist in den meisten Fällen der Abschluss einer Betriebsvereinbarung[23] hinsichtlich der Art und des Umfangs der Überwachung der Internet- und E-Mail-Kommunikation das Mittel der Wahl. Eine Betriebsvereinbarung kann dann als besondere Rechtsvorschrift nach § 4 Abs. 1 BDSG angesehen werden, wenn die Datenerhebung, -verarbeitung und -nutzung hinreichend präzise innerhalb des Erlaubnisumfangs gesetzlicher Bestimmungen geregelt wird und sie das gesetzliche Schutzniveau von TKG/TMG und BDSG nicht unterschreitet.[24] Die Empfehlung zum Abschluss einer Betriebsvereinbarung gilt grundsätzlich unabhängig davon, ob die Privatnutzung erlaubt werden soll oder nicht: Im ersten Fall ist die Betriebsvereinbarung konstitutiv und bildet den Rahmen für die gesonderten Einwilligungserklärungen der nutzungswilligen Beschäftigten; im zweiten Fall ist sie deklaratorischer Natur und konkretisiert die datenschutzrechtlichen Bestimmungen des BDSG.[25] Inhaltlich sollten vor allem die Fragen des Zugriffs, der Protokollierung, Auswertung und verfahrensmäßigen Durchführung von Kontrollen sowie die möglicher Sanktionen bei Verstößen gegen die Vorgaben eindeutig geregelt werden.

c) Keine Einwilligung

Sofern keine Einwilligung der Betroffenen vorliegt, richtet sich die Zulässigkeit solcher Maßnahmen grundsätzlich nach § 32 BDSG.[26] Diese Vorschrift rechtfertigt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zum Zwecke eines Beschäftigungsverhältnisses. Zur Begründung eines Beschäftigungsverhältnisses fehlt es i.d.R. an der Notwendigkeit einer E-Mail- und Internetüberwachung. Für die Durchführung des Beschäftigungsverhältnisses kann eine E-Mail- und Internetüberwachung aber durchaus erforderlich sein, etwa, wenn, wie im vorliegenden Fall, eine Kontrolle der privaten Nutzung notwendig ist.

Es ist demzufolge eine Abwägung der gegenseitigen Interessen erforderlich. Man wird annehmen können, dass das Interesse des Arbeitgebers, zumindest bei ausgeschlossener privater Nutzung, regelmäßig überwiegen wird.[27] Arbeitgeber haben grundsätzlich ein Interesse daran, die Arbeit ihrer Mitarbeiter[28] und etwaige Verstöße gegen die Geheimhaltungspflicht von Geschäftsgeheimnissen zu überprüfen.

d) Tendenz der aktuellen Rechtsprechung

Der EGMR hat kürzlich entschieden, dass es dem Arbeitgeber gestattet ist, private Chatprotokolle seiner Arbeitnehmer zu überwachen, sofern die private Internetznutzung ausdrücklich ausgeschlossen wurde.[29] In dem vom EGMR zu entscheidenden Fall hatte der Arbeitnehmer einen Messenger auf Wunsch des Arbeitgebers installiert und genutzt, um mit Kunden zu kommunizieren. Die private Nutzung des Messengers wurde jedoch unstreitig verboten. Auch informierte der Arbeitgeber den Mitarbeiter darüber, dass die Nutzung des Messengers überwacht wird. Die Ausführungen zur privaten Nutzung von E-Mail und Internet am Arbeitsplatz sind daher grundsätzlich auch auf dienstlich benutzte Messenger übertragbar. Sofern solche Messenger ausnahmslos privat genutzt werden, ist eine Inhaltskontrolle grundsätzlich unzulässig, da sich anhand der Zeitstempel in den entsprechenden Protokollen schon auswerten lässt, wie viel Arbeitszeit der Mitarbeiter mit dem entsprechenden Messenger verbracht hat.

4. Zwischenergebnis

Nach der aktuellen Rechtslage hat der Arbeitgeber bei untersagter privater Nutzung oder bei Einwilligung des Betroffenen das Recht, die E-Mails und die Internetkommunikation seiner Arbeitnehmer zu überwachen. Gestattet der Arbeitgeber jedoch eine private Nutzung, so scheidet eine Überwachung der E-Mails und des Internetverkehrs regelmäßig aus, sofern diese nicht explizit mit den Mitarbeitern oder per Betriebsvereinbarung vereinbart wurde.

19 Diercks, K&R 2014,1; Hoppe/Braun, MMR 2010, 80.

20 Stamer/Kuhnke, in: Plath, BDSG, 32 BDSG Rn. 87.

21 BAG, Urteil vom 11.12.2014 – 8 AZR 1010/13.

22 Kilian/Heussen, Computerrecht, 32. Ergänzungslieferung 2013, Rn. 14.

23 Die Ausführungen in diesem Beitrag gelten im Falle der Anwendbarkeit des entsprechenden Landespersonalvertretungsgesetzes (LPersVG) bzw. des Bundespersonalvertretungsgesetzes (BPersVG) analog für etwaige zu treffenden Dienstvereinbarungen unter Beteiligung des zuständigen Personalrats.

24 Schrader/Mahler, NZA-RR 2016, 57; Brink, ZD 2015, 295

25 Brink, ZD 2015, 295

26 Stamer/Kuhnke, in: Plath, BDSG, 32 BDSG Rn. 81; De Wolf, NZA 2010, 1206 (1208); Hoppe/Braun, MMR 2010, 80.

27 Hoppe/Braun, MMR 2010, 81; Härting, in: Härting, Internetrecht, 5. Aufl. 2014, B. Datenschutzrecht Rn. 349.

28 Gräfin v. Brühl/Sepperer, DSRITB 2014, 513.

29 Europäischer Gerichtshof für Menschenrechte, Urteil vom 12.01.2016, Az. 61496/08.

II. Änderungen nach Einführung der DS-GVO

Die DS-GVO enthält keine rechtsgestaltende Regelung zum Beschäftigtendatenschutz. Art. 88 der Verordnung enthält eine Öffnungsklausel, wonach Mitgliedsstaaten Rechtsvorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext erlassen dürfen. Insoweit ist davon auszugehen, dass § 32 BDSG, als bereits im BDSG enthaltene spezielle Regelung für den Bereich des Beschäftigtendatenschutzes, erhalten bleibt.[30] Größere Änderungen sind in den hier relevanten Bereichen nicht zu erwarten.[31]

III. Anforderungen und Gestaltung der betrieblichen Mitbestimmung

Datenschutzrechtliche Bestimmungen werden durch die Beteiligungsrechte des Betriebsrats ergänzt, die im BetrVG festgelegt sind und zu denen auch die Einhaltung des Datenschutzes im Unternehmen bezüglich der Mitarbeit zählt. Bei Einführung und Änderung von IT-Systemen hat der Betriebsrat allgemeine Informationsrechte nach § 80 BetrVG und Beteiligungsrechte u.a. nach §§ 90 ff BetrVG. Zu diesem Zweck muss der Arbeitgeber dem Betriebsrat rechtzeitig die erforderlichen Unterlagen vorlegen.[32] Dies gilt insbesondere dann, wenn es sich bei neu einzuführenden IT-Systemen oder -Prozessen um solche handelt, die eine „technische Kontrolleinrichtung“ nach § 87 Abs. 1 Nr. 6 BetrVG darstellen.

Nach Ansicht des LAG Hamm unterliegt das betriebliche Verbot der Privatnutzung der Internet- und E-Mailnutzung im Unternehmen nicht allein dem Mitbestimmungsrecht des Betriebsrats.[33] Dies ergibt sich bereits daraus, dass diese Maßnahme lediglich der Ordnung des Betriebs dient, da es um eine arbeitgeberseitige Anordnung zur Nutzung der Betriebsmittel durch die Mitarbeiter geht. Dies gilt aber nur für die eigentliche Entscheidung zum Verbot, nicht deren Durchführung.

Denn „Überwachung“ im Sinne des § 87 BetrVG ist ein Vorgang, durch den Informationen über das Verhalten oder die Leistung des Arbeitnehmers erhoben und aufgezeichnet werden, um sie auch späterer Wahrnehmung zugänglich zu machen.[34] Die Informationen müssen auf technische Weise ermittelt und dokumentiert werden, so dass sie zumindest für eine gewisse Dauer verfügbar bleiben und vom Arbeitgeber herangezogen werden können.[35] Die Einbindung in eine von dem einzelnen Mitarbeiter nicht beeinflussbare Überwachungstechnik kann zu erhöhter Abhängigkeit führen und damit die freie Entfaltung seiner Persönlichkeit hindern.[36]

Aus diesen Gründen ist der Betriebs- bzw. Personalrat vorab über geplante Maßnahmen zu informieren, die der Überwachung der Mitarbeiter im Rahmen der Internet- oder E-Mail-Nutzung dienen. Die Einführung derartiger Maßnahmen ist mitbestimmungspflichtig nach § 87 Abs. 1 Nr. 6 BetrVG.[37] Auch bei der Ausführung der Überwachung sollte der Betriebsrat entsprechend berücksichtigt werden und ggf. zu einer Einsichtnahme in E-Mail- oder Web-Protokolle herangezogen werden.

IV. Technische Gestaltung der notwendigen Kontrollmaßnahmen

Um der sich aus einem möglichen Verbot der Internet- und E-Mail-Dienst-Nutzung ergebenden Kontrollpflichten wirksam nachkommen zu können, ist die Protokollierung der Internet- und E-Mail-Nutzung durch die Mitarbeiter ein essentieller Bestandteil. Zudem können aus dieser Quelle auch die Daten extrahiert werden, die für das Führen und Aktualisieren von Filterlisten (so genannten „Blacklists“) als zusätzliche, „proaktive“ Maßnahme im Rahmen eines (teilweisen) Verbots benötigt werden.

1. Umsetzung der Protokollierung

Aus technischer Sicht ist dabei zunächst zu klären, wo, wie und in welchem Umfang Protokolldaten angelegt werden oder bereits vorhanden sind. Zur Ausgestaltung der entsprechenden Maßnahmen hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (kurz: ULD) im Jahre 2014 mit seiner Empfehlung einen ersten Grundstein gelegt.[38] Das dort in Abschnitt 5 erläuterte „Eskalierte Stufenmodell“ hat mittlerweile – in abgewandelter Form – auch Berücksichtigung in der „Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“[39] bzw. in die darin verfügbaren Muster für entsprechende Betriebsvereinbarungen gefunden.[40] Die nachfolgende Darstellung orientiert sich an diesen Vorgaben, die im Wesentlichen folgendes Schema vorsehen:

30 Brink/Düwel, NZA 2016, 665.

31 Dazu: Marquardt/Sörup, ArbRAktuell 2016, 103; Brink/Düwel, NZA 2016, 665.

32 Conrad, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, Rn. 299.

33 LAG Hamm, MMR 2006, S. 700.

32 LAG Düsseldorf, NZA-RR 2015, 355.

35 BAG, NZA 2014, 439; BAGE NJW 2004, 1756.

36 BAG, NZA 2014, 439.

37 Für E-Mail: BAG, NZA 2009, 1218; Dann/Castell, NJW 2008, 2945; Ernst, NZA 2002, 585; Fülbier/Splitgerber, NJW 2012, 1995; Kömpf/Kunz, NZA 2007, 1341; Raffler/Hellich, NZA 1997, 862. Für Internet: Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 26 ff.; Kömpf/Kunz, NZA 2007, 1341.

38 Polenz/Probst, „Private und dienstliche Internet- und E-Mail-Nutzung“, ULD Schleswig-Holstein, 2014, online unter https://www.datenschutzzentrum.de/internet/private-und-dienstliche-internetnutzung.pdf verfügbar (Stand: 12. September 2016).

39 Online bspw. unter http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/02/OH_E-Mail_Internet_Arbeitsplatz.pdf verfügbar (Stand: 12. September 2016).

40 Einen weiteren, wenngleich weniger detaillierten und zudem deutlich älteren Leitfaden hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (kurz: BfDI) bereits im Jahre 2008 veröffentlicht; er ist unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenInternetAmArbeitsplatzneu.html online verfügbar (Stand: 12.09.2016).

a) Anonyme bzw. pseudonyme Protokollierung an zentraler Stelle

Jeglicher Überwachung muss zunächst zwingend nicht nur eine umfangreiche Bestandsaufnahme, sondern auch eine Einbeziehung der zuständigen Mitarbeiter vorausgehen. Nach Abstimmung der Maßnahmen und Vorgehensweisen mit den zu beteiligenden Stellen und einer angemessenen Aufklärung aller Mitarbeiter über das Vorgehen sieht diese erste Stufe zunächst eine Protokollierung an zentraler Stelle und ohne Personenbezug vor.

Für Unternehmen, die aufgrund ihres Tätigkeitsbereichs das Internet weniger intensiv nutzen, kann dabei schon eine Auswertung rein auf Basis der im Beobachtungszeitraum übertragenen Datenmengen zielführend und unter Umständen sogar ausreichend sein. In diesem Fall ist dann so bereits eine einfache Statistik – d.h. ohne konkrete Erfassung der genutzten Internet- bzw. E-Mail-Server – des Internetverkehrs ausreichend, um auf eine übermäßige Nutzung der Internets bzw. des E-Mail-Dienstes durch die Mitarbeiter schließen zu können. Der Vorteil dieser Lösung liegt vor allem im bestmöglichen Ausschluss eines Personenbezugs, wesentlicher Nachteil ist die fehlende Möglichkeit der Beurteilung einer möglichen privaten Nutzung anhand der Inhaltsdaten.

In der Regel wird man daher auch „inhaltliche Aspekte" i.S. der genutzten Web- bzw. E-Mail-Server in der Analyse berücksichtigen müssen, um sinnvoll entscheiden zu können, ob es sich eher um eine dienstliche oder tatsächlich doch um eine private Nutzung handelt. In diesem Fall kommen aus technischer Sicht vor allem vorhandene Web- bzw. E-Mail-Proxy-Server als Stelle der Protokollierung in Frage. Diese haben aufgrund ihrer zentralen Funktion den Vorteil, entsprechend große Mengen an Daten aggregieren und somit einen Personenbezug bestmöglich ausschließen zu können. Sind entsprechende Proxies nicht vorhanden, können die Protokolldateien grundsätzlich auch auf den jeweils zuständigen Gateways erzeugt werden.

In allen Fällen ist allerdings darauf zu achten, dass die Protokollierung streng datenschutzfreundlich konfiguriert bzw. gestaltet werden kann.[41] Dies betrifft neben der Zweckbestimmung zum einen die Speicherdauer, zum anderen auch die Art und Weise, wie die Protokolldaten aggregiert bzw. gefiltert werden können. Zahlreichen auf dem Markt befindlichen Produkten fehlen entsprechende Konfigurationsmöglichkeiten, so dass hier ggf. selbst generierte Filter nachgeschaltet werden müssen, um die notwendige Anonymität bzw. Pseudonymität zu erreichen.

Im Falle des Internet-Zugriffs muss bspw. auch bedacht werden, dass insbesondere auch ein aufgerufener Uniform Resource Locator (kurz: URL) entsprechenden Personenbezug beinhalten kann, etwa durch das Vorhandensein des Namens des Mitarbeiters in dem aufgerufenen URL. Um einen Personenbezug in dieser Stufe bestmöglich ausschließen zu können, sollte die Protokollierung daher vorzugsweise nur anhand der Domain erfolgen.[42] Ist eine Anonymisierung der Protokolldaten nicht vollständig umsetzbar, so kann die Nutzung der Protokolldaten insbesondere im Falle der E-Mail-Kommunikation problematisch sein, da dann auch Dritte außerhalb des Unternehmens, die E-Mail-Kommunikationspartner, mit betroffen sind. Dies ist umso mehr für „gemischte Lösungen" relevant, bei denen zum Beispiel die Privatnutzung zwar erlaubt, eine Überwachung jedoch gleichwohl vereinbart wurde. Denn sollte der Arbeitgeber als Diensteanbieter i.S. des TKG zu klassifizieren sein, sind § 88 TKG bzw. § 100 TKG maßgeblich, und eine Speicherung zu anderen als den dort genannten Zwecken ist nicht zulässig.[43]

Eine gern genutzte Möglichkeit, den Personenbezug – in diesem Fall den der Protokolldaten – auszuschließen, zumindest aber zu erschweren, ist die Bildung von Gruppen. Diese Möglichkeit, die auch in der Orientierungshilfe der Datenschutzkonferenz genannt wird, setzt im konkreten Anwendungsfall aber i.d.R. eine technische Unterstützung voraus. Denn im Falle der Protokollierung der Internetnutzung sind die IP-Adressen der anfragenden Mitarbeiter-PCs, im Falle der Nutzung des E-Mail-Dienstes die von Mitarbeitern verwendeten E-Mail-Adressen bzw. Zugangskennungen zum E-Mail-Server nun in entsprechende Gruppen einzuordnen. Dabei ist vor allem zu beachten, dass die Größe einer Gruppe so gewählt ist, dass eine spätere Identifizierung von einzelnen Mitarbeitern ausgeschlossen wird. Während dies gerade bei kleinen Organisationen ein Problem darstellen kann, da die Gruppen hier schnell zu klein werden, müssen bei größeren Organisationen passende Möglichkeiten gefunden werden, die Gruppen überhaupt sinnvoll organisieren zu können.

Als Grundlage für eine Gruppierung können auch die einzelnen Organisationseinheiten wie Abteilungen innerhalb des Unternehmens genutzt werden, allerdings wird dies bei kleinen Organisationen regelmäßig allein an einer zu kleinen daraus resultierenden Gruppengröße scheitern. Eine weitere Möglichkeit besteht in einer möglichst gleichförmigen Gruppierung der von der Organisation verwendeten IP-Adressen (bspw. durch simples Aufteilen der/des genutzten Netzsegmente/s) bzw. E-Mail-Konten. Sinnvoll wäre beispielsweise ein simples, ggf. alphabetisches Aufteilen in gleich große Gruppen.

Vorgaben zu einer aufgrund einer möglichst ausgeschlossenen Re-Identifizierung notwendigen Mindestgröße sollten neben der reinen Anzahl der Gruppenmitglieder[44] aber auch berücksichtigen, wie stark die einzelnen IP-Adressen bzw. E-Mail-Konten an der Kommunikation teilnehmen. Besteht bspw. eine Gruppe aus mehreren IP-Adressen von Mitarbeiter-PCs, und alle bis auf einen der betroffenen Mitarbeiter sind für zwei Wochen im Urlaub, so wird deutlich, dass sich die Protokolldaten nunmehr allein auf den verbliebenen

41 Heidrich/Wegener, MMR 2015, 487

42 Auch in diesem Fall ist ein möglicher Personenbezug natürlich nicht vollständig auszuschließen, bspw. wenn ein Mitarbeiter eine eigene Domain mit seinem Namen als Bestandteil der Domain (also i.S.v. www.mitarbeitername.example.com) registriert hat.

43 Vgl. dazu auch Heidrich/Wegener, MMR 2015, 487.

44 Im Beispiel ist dies die Anzahl an IP-Adressen bzw. E-Mail-Konten pro Gruppe.

Mitarbeiter beziehen. Um mögliche negative Konsequenzen – bspw. im Rahmen einer nicht-Verwertbarkeit von Protokolldaten – idealerweise auszuschließen, ist das Vorgehen bei der Gruppierung daher bereits im Vorfeld sorgfältig zu planen.

Aufgrund der in den vorstehenden Abschnitten beschriebenen Probleme erscheint auf den ersten Blick eine Protokollierung und Analyse auf Basis der reinen „Datenmengen" die bestmögliche Variante. Allerdings wird dies in der Vielzahl der Fälle und insbesondere für den Anwendungsfall der Pflege der Blacklists nicht ausreichend sein, so dass auch Inhaltsdaten mit in die Protokollierung einbezogen werden müssen. Bereits im Vorfeld ist dann aber zu prüfen, ob die Anonymität bzw. Pseudonymität überhaupt angemessen sichergestellt werden kann. Im Zweifel ist der Kontrollpflicht des Arbeitgebers Vorrang einzuräumen, dann sind allerdings entsprechend kompensierende Maßnahmen zu treffen, bspw. indem der Zugriff auf die Protokolldaten strikt reglementiert wird.

b) Personenbezogene Protokollierung an zentraler Stelle

Sofern die erste Stufe keine gravierenden Verstöße gegen die Vorgaben zeigt, kann die weitere Überwachung unterbleiben. Steht dagegen auf Basis der Analyse der in der vorangehenden Stufe gewonnenen Daten fest, dass die Mitarbeiter sich nicht an die Vorgaben halten, steht nach entsprechender Benachrichtigung der Mitarbeiter als nächste Stufe eine personenbezogene Protokollierung an zentraler Stelle an.

Dabei ist allerdings wesentliche Voraussetzung, dass eben nicht eine Protokollierung der Internet- bzw. E-Mail-Nutzung von allen Mitarbeitern erfolgt. Eine entsprechende Vorauswahl ist bspw. durch die bereits erläuterte Gruppenbildung bei der anonymen bzw. pseudonymen Protokollierung an zentraler Stelle zu realisieren. Ist eine entsprechende Gruppierung nicht sinnvoll durchführbar – bspw. weil der dafür notwendige administrative Aufwand als für zu hoch erachtet wird – so scheidet eine personenbezogene Protokollierung regelmäßig aus.[45] Alternativ kommt hier dann eine stichprobenartige Kontrolle aller Mitarbeiter in Betracht.

Im Zuge der in dieser Stufe durchgeführten Protokollierung ist zudem ebenfalls zu beachten, dass im Rahmen der Protokollierung des E-Mail-Dienstes aus den oben dargelegten Gründen keine Erhebung von E-Mail- und IP-Adressen der E-Mail-Kommunikationspartner stattfindet. Einfacher gestaltet sich die Protokollierung der Internetnutzung: Sinn und Zweck dieser Stufe der Protokollierung ist es ja gerade, einen Personenbezug zu dem/den entsprechenden Mitarbeiter/n herzustellen. Daher müssen die aufgerufenen URL in diesem Fall nicht weiter anonymisiert werden.

c) Personenbezogene Kontrolle auf den Mitarbeiter-PCs

Als letzte Stufe der Kontrolle sieht die Orientierungshilfe der Datenschutzkonferenz unangekündigte Überprüfungen der Protokolldaten auf den PCs der über die personenbezogene Protokollierung als "Verursacher" identifizierten Mitarbeiter vor. Diese Stufe wird insbesondere zur Beweissicherung im arbeitsrechtlichen Umfeld und/oder zur Aufdeckung von Straftaten genutzt werden und ist nicht zwingend erforderlich. Während die Mitarbeiter bei einer Protokollierung der Internet- und E-Mail-Nutzung an zentraler Stelle im Vorhinein über die Maßnahmen zu informieren sind, setzt die Orientierungshilfe dies bei der Protokollierung auf den PCs der Mitarbeiter nicht voraus.

Aus technischer Sicht sind für die Protokollierung in dieser Stufe insbesondere die Zugriffsprotokolle des auf dem Mitarbeiter-PC befindlichen Internet-Browsers bzw. E-Mail-Clients relevant. Ein interessanter Aspekt – insbesondere im Falle der Gestattung einer privaten Nutzung in angemessenem Umfang – ist die Frage, wie eine solche Protokollierung dann überhaupt eingerichtet wird und welchen Zugriff ein Administrator dabei potentiell auf private Daten eines Mitarbeiters nehmen kann. Da die Mitarbeiter i.d.R. nicht in den Prozess der Aktivierung einer entsprechenden Protokollierung eingebunden sein werden, ist für die Einrichtung derselben technisch sicherzustellen, dass der Administrator über die dazu notwendigen Kennwörter verfügt, bspw. um eine pre-Boot Authentification und/oder eine verschlüsselte Systemplatte frei schalten zu können.

Um bei der Einrichtung einen Zugriff – insbesondere den versehentlichen – auf private Daten eines Mitarbeiters bestmöglich zu vermeiden, scheint es zudem ratsam, im Vorfeld entsprechende Regelungen festzulegen, wo die Mitarbeiter ihre privaten Dokumente abspeichern sollen. Zudem sollte die Einrichtung – auch zur Vermeidung von späteren Missverständnissen – generell nur mit mindestens vier Augen und unter Beteiligung des Betriebs- bzw. Personalrats und dem/der betrieblichen Datenschutzbeauftragten durchgeführt werden.

2. Berücksichtigung spezieller Personen bzw. Personengruppen

Insbesondere für die Personen bzw. Personengruppen, die aufgrund ihrer Tätigkeit einer besonderen Vertraulichkeit unterliegen, bspw. die Mitglieder des Betriebs- bzw. Personalrats, den Suchtbeauftragten, Betriebsarzt oder den/die betrieblichen Datenschutzbeauftragte, darf eine Protokollierung, wie bisher beschrieben, nicht durchgeführt werden.[46] Selbiges gilt auch für die schutzwürdigen Belange derjenigen, die als Kommunikationspartner mit diesen Stellen Kontakt aufnehmen, bspw. Mitarbeiter, die den Betriebs- bzw. Personalrat wegen einer Personalangelegenheit anrufen oder auch externe Personen, die den/die BDSB im Rahmen eines Auskunftsersuchens kontaktieren.

Aus praktischer Sicht erscheint es dazu dringend geboten, diesen Sachverhalt bereits angemessen bei der Konzeption und Implementierung der IT zu berücksichtigen. So

45 So auch die Orientierungshilfe der Datenschutzkonferenz, die – allerdings fehlerhaft – § 32 Abs. 1 Satz 2 als Begründung anführt.

46 Seifert, in: Simitis, BDSG, § 32, Rn. 91. Auch im Falle der Anwendbarkeit des Geheimschutzhandbuches wäre zu prüfen, ob und ggf. wie hier eine Protokollierung und etwaige Kontrollen durchzuführen sind.

lässt sich sicherstellen, dass für die betreffenden Personen bzw. Personengruppen eigene, fest zugeordnete IP-Adressbereiche bzw. entsprechende Funktionspostfächer definiert werden, die dann vollständig von der Protokollierung ausgenommen werden. Ein Ausschluss vor der eigentlichen Protokollierung ist – wenngleich wünschenswert – aufgrund der verwendeten IT nicht immer realisierbar, kann aber durch ein Ausfiltern der entsprechenden Daten vor einer Auswertung kompensiert werden.

V. Fazit

Da bislang noch keine höchstrichterliche Rechtsprechung zu dieser Thematik existiert, ist es für Arbeitgeber, die die E-Mail-Kommunikation und Internetnutzung ihrer Arbeitnehmer überwachen möchten, grundsätzlich ratsam, die private Internet- und E-Mail-Nutzung zu untersagen. Gerade wenn Mitarbeiter aufgrund einer Erkrankung längerfristig nicht tätig sind, hat der Arbeitgeber ein besonderes Interesse daran, sich über den aktuellen Sachstand etwaiger Bearbeitungen der E-Mails zu informieren. Zu berücksichtigen ist dabei, dass eine angemessene und dokumentierte Kontrolle und Sanktionierung bei Verstößen notwendig ist, um eine betriebliche Übung und damit i.d.R. unkontrollierbare private Nutzung durch die Mitarbeiter zu vermeiden.

Um eine möglicherweise für beide Seiten zufriedenstellende Lösung zu schaffen, könnte der Arbeitgeber seinen Mitarbeitern aber dadurch entgegenzukommen, die Internetkommunikation für private Zwecke zu gestatten, damit Arbeitnehmer so auf ihre private E-Mail-Adresse zugreifen können, so dass diese erst gar nicht darauf angewiesen sind, die geschäftlich E-Mail-Adresse für private Zwecke zu nutzen. So hat Arbeitgeber insbesondere die Möglichkeit, auf die E-Mails seiner Mitarbeiter zuzugreifen, falls diese längerfristig abwesend sein oder dauerhaft ausscheiden sollten.

In jedem Fall gebietet sich eine detaillierte Regelung der Rechte der Arbeitnehmer und der Kontrollbefugnisse des Arbeitgebers, je nach Fallkonstellation entweder durch Individualvereinbarungen und/oder eine Betriebsvereinbarung. Insbesondere die technische Ausgestaltung der Kontrollmaßnahmen sollte im Vorfeld klar definiert und entsprechend dokumentiert sein. Zudem sollten die bereits bestehenden Geschäftsprozesse und die dazu notwendige IT in der Organisation bereits bei der Entscheidung für oder gegen eine (teilweise) private Nutzung von E-Mail und Internet am Arbeitsplatz berücksichtigt werden, um unliebsame Überraschungen bei der technischen Ausgestaltung der ggf. notwendigen Kontrollmaßnahmen zu vermeiden.

Joerg Heidrich
ist seit 2001 als Justiziar und Datenschutzbeauftragter der Heise Medien GmbH & Co. KG sowie als Rechtsanwalt in Hannover tätig. Er ist Fachanwalt für IT-Recht, zertifizierter Datenschutzbeauftragter (TÜV) und Sachverständiger für IT-Produkte (ULD SH/rechtlich).

Dr. Christoph Wegener (CISA, CISM, CRISC)
ist von der GDD und dem TÜV Nord zertifizierter Datenschutzbeauftragter und seit 1999 als freier Berater mit der wecon.it-consulting in den Themen Informationssicherheit und Datenschutz tätig.

Brian Scheuch
ist Rechtsreferendar beim Oberlandesgericht Celle und juristischer Mitarbeiter bei Heise Medien. Er studierte Rechtswissenschaften an der Universität Leipzig und Universität Hannover. An der Universität Hannover belegte er den Schwerpunkt IT-Recht & Geistiges Eigentum.

Kurzbeiträge

Die EU-Datenschutz-Grundverordnung in der Umsetzung: Eine Diskussion über Chancen und Herausforderungen

Dr. Dirk Bornemann und Lennart Wetzel, München/Berlin*

Die Verabschiedung der Europäischen Datenschutz-Grundverordnung (DS-GVO) stellt vor dem Hintergrund eines zunehmenden globalen Wettbewerbsdrucks und der Notwendigkeit, den Wirtschafts- und Innovationsstandort Europa langfristig zu stärken, zweifelsohne einen bedeutenden Fortschritt für mehr Rechtssicherheit in Fragen des Datenschutzes in Europa dar. Im Rahmen der Umsetzung und Anwendung der DS-GVO wird sich jedoch auch zeigen, inwiefern die hochgesteckten Ziele Harmonisierung, Wettbewerbsangleichung und Modernisierung tatsächlich in ihrer Gänze erfüllt werden können und sich im Idealfall auf diese Weise ein rechtlicher Orientierungsrahmen für Individuen und Unternehmen etabliert, der eine vernünftige Balance zwischen dem Bedürfnis nach Sicherheit, verfassungsrechtlich verankerten Privatsphäre- und Freiheitsrechten sowie Innovationsförderung und offenen Märkten gewährleistet. Um dies zu erreichen, gilt es, schnellstmöglich die noch offenen Fragen hinsichtlich nationaler Auslegungsspielräume und den neuen Herausforderungen des digitalen Zeitalters zu diskutieren und umfassende Empfehlungen zu formulieren, an denen sich Verantwortliche und Auftragsverarbeiter, aber auch Behörden und Gerichte orientieren können. Der folgende Artikel versucht in diesem Zusammenhang einen ersten Beitrag zu leisten.

Die Notwendigkeit einer zeitgemäßen Datenpolitik

„Es war die beste Zeit, es war die schlechteste Zeit. Es war das Zeitalter der Weisheit, es war das Zeitalter der Torheit…" – mit diesen Worten beginnt Charles Dickens seinen Roman „A Tale of Two Cities" (Eine Geschichte aus zwei Städten). Eine Erzählung, die zu einem Zeitpunkt entstand, indem sich Europa und die Welt durch die voranschreitende industrielle Revolution inmitten einer tiefgreifenden und dauerhaften Umgestaltung der wirtschaftlichen und sozialen Verhältnisse, der Arbeitsbedingungen und Lebensumstände befand. Zwar erleben wir in diesen Tagen die mittlerweile vierte Phase der industriellen Revolution, doch sind die dadurch entstehenden wirtschaftlichen und sozialen Veränderungen nicht weniger tiefgreifend als vor mehr als 150 Jahren.

Maßgeblich geprägt wird der technologische Fortschritt im Jahr 2016 durch Cloud-Computing, das Internet der Dinge, Maschinelles Lernen und Big Data. Diese neue Generation digitaler Technologien verändert die Art, wie Produkte und damit verbundene Dienstleistungen entwickelt, hergestellt und vermarktet werden, nachhaltig und ermöglicht immer innovativere Geschäftsmodelle. Da Datenverarbeitung im Zeitalter der Globalisierung zunehmend international erfolgt und Netzinfrastrukturen weltweit verbunden sind, kann Datenschutz nicht mehr durch die territorial beschränkte Gesetzgebung einzelner Staaten reguliert werden, sondern braucht klare und harmonisierte internationale Regeln.

Die Notwendigkeit der Etablierung eines kohärenten internationalen Rechtsrahmens hat sich seit den Enthüllungen durch Edward Snowden im Rahmen der NSA-Affäre noch einmal verstärkt. Gerade innerhalb Europas ist eine Sensibilisierung hinsichtlich des Schutzes personenbezogener Daten und technologischer Sicherheit zu beobachten, die die Gefahr einer digitalen Vertrauenskrise endgültig real gemacht hat. Die Sicherstellung von Vertrauen in digitale Dienste und Plattformen ist somit zu einer dringlichen gesellschaftspolitischen Aufgabe geworden, die es auf nationaler sowie europäischer Ebene gleichermaßen zu bewältigen gilt. Gleiches gilt für die Gewährleistung eines innovationsfördernden Datenschutzniveaus in Europa.

Mit der im Mai 2015 von der Europäischen Kommission veröffentlichten „Strategie für einen digitalen Binnenmarkt für Europa" hat sich Europa glücklicherweise bewusstgemacht, dass man im Kontext der digitalisierten Welt nur ein Teil eines globalen Marktes ist. Vor diesem Hintergrund verkörpert der digitale Binnenmarkt eine absolute Notwendigkeit, um auf globaler Ebene Schritt halten und eine hohe Innovationskraft der EU-Mitgliedstaaten langfristig gewährleisten zu können. Gelingen kann die Umsetzung dieses ehrgeizigen politischen Ziels allerdings nur innerhalb kohärenter und zeitgemäßer rechtlicher Rahmenbedingungen.

Die Verabschiedung der DS-GVO ist ein wichtiger Schritt zu mehr Rechtssicherheit in Europa

Die Verabschiedung der Europäischen Datenschutz-Grundverordnung (DS-GVO) stellt vor den genannten Hintergrün-

* Der Autor Dr. Dirk Bornemann ist seit 2006 als promovierter Jurist bei Microsoft tätig, von 2010 an als Leiter der Rechtsabteilung. Er ist Mitglied der Geschäftsleitung und Assistant General Counsel für Deutschland, Österreich und die Schweiz.

Der Autor Lennart Wetzel ist seit November 2014 Government Affairs Manager bei Microsoft Deutschland.

den einen bedeutenden Fortschritt für mehr **Rechtssicherheit** in Fragen des Datenschutzes im europäischen Raum dar. Durch die direkte Gültigkeit der DS-GVO in allen EU-Mitgliedsstaaten soll zukünftig gewährleistet sein, dass das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten unionsweit gleichmäßig und einheitlich ist.

Im Idealfall etabliert sich auf diese Weise ein rechtlicher Orientierungsrahmen für Individuen und Unternehmen, der eine vernünftige Balance zwischen dem Bedürfnis nach Sicherheit, verfassungsrechtlich verankerten Privatsphäre- und Freiheitsrechten sowie Innovationsförderung und offenen Märkten gewährleistet, sowie klare und harmonisierte datenschutzrechtliche Bestimmungen beinhaltet, von denen Industrie und Verbraucher gleichermaßen profitieren.

Man muss sich in diesem Kontext dessen bewusst sein, dass insbesondere Unternehmen der Digitalwirtschaft ein gewisses Maß an Flexibilität benötigen, um Innovationen und neue Lösungen für den Datenschutz entwickeln zu können. Dieser Herausforderung, die richtige Balance zwischen dem Schutz personenbezogener Daten der europäischen Verbraucher und der gleichzeitigen Förderung technologischer Innovationen zu finden und damit ein zukunftsfähiges rechtliches Fundament zu schaffen, nimmt sich die DS-GVO an. Dabei reicht es nicht aus, die Verordnung zügig umzusetzen, vielmehr gilt es, von Anfang an neben den bereits beschriebenen Vorteilen der neuen Gesetzgebung auch die noch ungeklärten Fragen und neuen Herausforderungen für Wirtschaftsunternehmen sowie die zukünftige Rolle der nationalen Datenschutzbehörden offen zu diskutieren.

Die DS-GVO in der Praxis: Herausforderungen und Chancen für Unternehmen

Der Datenschutz wurde in Europa bisher maßgeblich durch die EU-Datenschutzrichtlinie 95/46/EG geregelt, welche in nationale Gesetze umgesetzt wurde und sich in Deutschland primär im Bundesdatenschutzgesetz (BDSG) wiederfindet. Die Richtlinie stammt aus dem Jahr 1995 und spiegelt entsprechend viele technologische Entwicklungen nicht mehr wider. Insgesamt werden Unternehmen für die von ihnen gespeicherten personenbezogenen Daten zukünftig stärker verantwortlich gemacht. Dies impliziert die Notwendigkeit, rechtzeitig umfassende neue Prozesse und Strukturen zu schaffen, um den Vorgaben der DS-GVO zu entsprechen.

In diesem Zusammenhang ist vor allem das neueingeführte **„Recht auf Vergessenwerden"** (Kap. 3 Art. 17 DS-GVO) zu nennen, welches jeder Person einen Anspruch auf Löschung ihrer personenbezogenen Daten einräumt. Diese sich aus der neuen Verordnung ergebenden Pflichten zur Löschung von Daten sind umfassender als jene, die bislang unter dem BDSG Geltung haben. Kommt ein Verantwortlicher seinen Löschungspflichten nicht nach, kann dies mit Bußgeldern in Höhe von bis zu 4 Prozent des Jahresumsatzes sanktioniert werden. Für Unternehmen wird es daher zukünftig entscheidend sein, jene veränderten Anforderungen in ihren Löschkonzepten präzise abzubilden, um künftig nachweisen zu können, dass sie die Vorgaben der DS-GVO einhalten.

Die zusätzlichen Anforderungen für Unternehmen zeigen sich auch in den in der DS-GVO verankerten, umfassenden **Melde-und Benachrichtigungspflichten** (Kap. 4 Art. 33 und 34 DS-GVO) sowie der erweiterten Haftung für **Verantwortliche und Auftragsdatenverarbeiter** (Kap. 8 Art. 82 Abs. 1 DS-GVO). In diesem Zusammenhang zeichnet sich ab, dass zukünftig auch die Nutzung von Cloud-Angeboten durch die Mitarbeiter in die Verantwortung der Unternehmen fallen wird. Wenn sie etwa personenbezogene Daten bei Cloud-Dienstleistern ablegen oder auf diesem Weg mit anderen austauschen, kann dafür in Zukunft das Unternehmen in die Pflicht genommen werden, und zwar selbst dann, wenn es sich um keine offiziell genehmigte Nutzung, sondern um eine Form der „Schatten-IT" handelt. Das gilt im Übrigen auch für mobile Endgeräte wie Notebooks, Tablets oder Smartphones, die von den Mitarbeitern mit nach Hause genommen werden. Unternehmen sollten daher nach Wegen suchen, den Zugriff auf nicht-autorisierte Dienste beispielsweise über entsprechende Filterregeln zu unterbinden und strikte Regelungen für den Umgang mit personenbezogenen Daten auf privat genutzten Geräte zu formulieren. Bei den von Unternehmen eingesetzten Cloud-Diensten sollte zudem überprüft werden, ob sie den Vorschriften der DS-GVO entsprechen.

Die Vergangenheit hat zudem immer wieder gezeigt, dass datenschutzrechtliche Verpflichtungen nur in dem Umfang wirksam sind, in dem sie auch tatsächlich durchgesetzt werden. Bei Verstößen gegen die Bestimmungen der DS-GVO drohen daher nach Art. 83 (Kap. 8 DS-GVO) Strafen von bis zu vier Prozent des globalen Jahresumsatzes. Zudem drohen an Verstößen gegen die DS-GVO beteiligten Personen Geldstrafen von bis zu 20 Millionen Euro. Der **Bußgeldrahmen** der DS-GVO liegt damit deutlich über dem des BSDG, welches bislang Strafzahlungen in Höhe von maximal 300.000 Euro festlegte. Dies ist ein deutliches Signal dafür, dass Verstöße gegen den Datenschutz ernst zu nehmen sind. Zudem ist es durchaus vertretbar, Unternehmen, welche die Ihnen anvertrauten Daten nicht angemessen sichern und schützen, durch empfindliche Strafen zu maßregeln und erweiterte Kontrollmechanismen zu implementieren – so lange ihnen durch die Umsetzung und Auslegung der im Rahmen der DS-GVO verabschiedeten Neuregelungen eine zeitgemäße Möglichkeit gegeben wird, Innovationspotenziale ausschöpfen zu können und flexible sowie den jeweiligen Umständen angemessene Datenschutzlösungen zu entwickeln.

Niederlassungsprinzip/Marktortprinzip – eine verpasste Chance auf „Wettbewerbsgleichheit"?

Durch die DS-GVO wird der geografische Geltungsbereich des europäischen Datenschutzrechts bedeutend ausgeweitet. Basierend auf dem **„Niederlassungsprinzip"** legt die DS-GVO fest, dass ihre Bestimmungen Anwendung auf die Verarbeitung personenbezogener Daten finden, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbei-

ters in der Union erfolgt. Das **„Marktortprinzip"** erweitert diese Bestimmung und legt fest, dass der europäische Datenschutz für alle Unternehmen gelten soll, die sich an europäische Verbraucher wenden – unabhängig davon, wo sich der jeweilige Firmensitz befindet. Dies umfasst die Vorgaben der DS-GVO in Bereichen der Datensicherheit, der Zulässigkeit der Datenverarbeitung, die Rechte betroffener Personen sowie Aufsichts-und Zertifizierungsfragen. Ziel dieser Erweiterung ist es, mehr Wettbewerbsgleichheit auf dem europäischen Markt von Anbietern innerhalb und außerhalb der Europäischen Union herzustellen und die Wahrnehmung von Betroffenenrechten zu vereinfachen. Beides wird nur zu Teilen erreicht.

Zum einen führt die Zweckbegrenzung dieses Prinzips dazu, dass bestimmte Datenverarbeitungen von Personen, die sich in der Europäischen Union aufhalten, in den Anwendungsbereich fallen und andere nicht. Dies wird mit großer Wahrscheinlichkeit zu problematischen Abgrenzungsfragen führen und untergräbt die intendierte Rechtsklarheit. Zum anderen unterliegt die Beschränkung des Anwendungsbereichs der durch die DS-GVO geregelten Betroffenenrechte weiterhin den Mitgliedsstaaten, *„sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt (Kap. 2 Abschnitt 5 Art. 23 DS-GVO)"*. Jene Beschränkungen reichen vom Schutz der „Rechte und Freiheiten betroffener Personen", den „Kategorien personenbezogener Daten", den Zwecken ihrer Verarbeitung bis hin zum „Schutz der nationalen Sicherheit". Der Umfang der Beschränkungen, wie auch die abstrakte Formulierung, wann diese zum Tragen kommen, werden in vielen Fällen eine weitergehende, von der Pfadabhängigkeit mitgliedstaatlicher Rechtsauslegungen geprägte Interpretation durch nationale Gerichte notwendig machen, um die durch das „Marktortprinzip" festgelegten Regelungen vollziehen zu können. Dies wird aller Voraussicht nach zwischen den Mitgliedsstaaten zu erheblichen Unterschieden in der Anwendung der Verordnung führen. Zwar könnte man dieser These entgegensetzen, dass der im Rahmen der DS-GVO eingeführte Europäische Datenschutzausschuss (Kap. 7 Artikel 66 DS-GVO) künftig dafür sorgen wird, dass die Verordnung einheitlich angewandt wird. Dessen Beschlüsse sind allerdings für Gerichte nicht bindend, sondern können bestenfalls als Empfehlungen dienen, da die DS-GVO nur vonseiten des Europäischen Gerichtshofes abschließend ausgelegt werden kann. Somit droht ein fragmentierter Rechtsrahmen anstelle harmonisierter Wettbewerbsbedingungen, der den bereits existierenden Nachteilen im internationalen Vergleich nur schwer entgegenwirken werden kann.

Eine größere Rolle für die Europäischen Datenschutzbehörden

Um die Gefahr des Wettbewerbsnachteils für Europa durch fehlende Kohärenz in der Rechtsumsetzung größtmöglich einzudämmen, wird es zukünftig vor allem auf die effektive Zusammenarbeit der nationalen Datenschutzbehörden ankommen, deren Aufgabenbereich durch die DS-GVO und den im EU-U.S. Privacy Shield verankerten zusätzlichen Prüfungsrechten erheblich ausgeweitet wird. Ein europaweites System der Datenschutzaufsicht soll jene einheitliche Rechtsdurchsetzung im Datenschutz zukünftig gewährleisten (**„One-Stop-Shop"**). Dabei sollen betroffene Personen weiterhin ihre lokale Datenschutzaufsichtsbehörde kontaktieren können. Diese wendet sich daraufhin an die für das jeweilige Unternehmen zuständige Datenschutzaufsichtsbehörde, welche dann in Absprache mit den anderen Aufsichtsbehörden eine europaweit einheitliche Entscheidung fällt. Auch Unternehmen selbst wenden sich entsprechend diesem Prinzip an die Datenschutzbehörde, in deren Zuständigkeitsbereich der Hauptsitz ihres Unternehmens fällt. Dies hat den positiven Effekt, dass Unternehmen in Datenschutzfragen nur noch mit ihrer eigenen zuständigen Behörde in Kontakt treten müssen und nicht mehr mit potenziell konfligierenden Behördenaussagen konfrontiert sind. Ferner sind die nationalen Datenschutzbehörden nun auch mit der Aufgabe der „Öffentlichkeitsarbeit" betraut. Dabei sollen sie die Bevölkerung beispielsweise für Risiken im Zusammenhang mit der Datenverarbeitung sensibilisieren. Außerdem fällt die Aufklärung von Unternehmen nun in den Aufgabenbereich der Datenschutzbehörden. Darüber hinaus sollen die Datenschutzbehörden zukünftig selbst die Nutzung von Standardvertragsklauseln innerhalb von Verträgen zwischen Service-Providern und Kunden überprüfen können, so dass schneller Rechtssicherheit für beide Seiten erlangt werden kann.

Da die deutschen Datenschutzbehörden leider in der Vergangenheit nur in Ausnahmefällen dafür sorgen konnten, ein länderübergreifendes, homogenes Datenschutzniveau in Deutschland herzustellen, sollte ihre gegenwärtige Organisationsstruktur hinsichtlich der durch die DS-GVO hinzugewonnen Kompetenzen auf den Prüfstand gestellt werden. Nur durch eine effiziente und agile Zusammenarbeit wird es zukünftig möglich sein, eine starke und zeitgemäße Position innerhalb Europas zu vertreten. Hierunter fällt auch die ausreichende Berücksichtigung von Innovationspotenzialen neuer Geschäftsmodelle im Rahmen von Abwägungsentscheidungen. Die Verankerung formeller Anhörungsverfahren zu den unternehmerischen und industriellen Interessen könnte an dieser Stelle ein Schritt in die richtige Richtung sein.

Zweckänderungen und Vereinbarkeit: Warum Datensparsamkeit nicht mehr zeitgemäß ist

Die DS-GVO führt das bisherige Grundprinzip fort, wonach jede Datenverarbeitung verboten ist, solange es keine gesetzliche Erlaubnisnorm gibt oder die betroffene Person nicht eingewilligt hat (sog. „Verbot mit Erlaubnisvorbehalt"). Bislang galten, basierend auf dem BDSG, zudem die Prinzipien der Zweckbindung und Datensparsamkeit. Hiernach dürfen Daten nur für einen zuvor bestimmten Zweck und auch nur solange verarbeitet werden, bis dieser Zweck der Datenverarbeitung erlischt – anschließend sind perso-

nenbezogene Daten zu löschen. Laut DS-GVO soll die Verarbeitung personenbezogener Daten zu einem anderen Zweck als dem ihrer Erhebung zukünftig jedoch unter bestimmten Voraussetzungen zunächst zulässig sein. Basierend auf der DS-GVO wäre solch eine Zweckänderung künftig zulässig, sofern die betroffene Person in eine solche Zweckänderung eingewilligt hat und sie mit dem ursprünglichen Zweck „vereinbar" ist. Bereits jetzt kann festgehalten werden, dass diese Änderungen mit Blick auf den technologischen Fortschritt der letzten Jahre nicht weit genug greifen und das Prinzip der Datensparsamkeit grundsätzlich fortgeführt wird.

Ein zeitgemäßer Datenschutz erfordert die Schaffung eines Ordnungsrahmens für eine mehr und mehr digitalisierte Welt, der die Persönlichkeitsrechte der Menschen schützt und gleichzeitig innovative Methoden der Datenverarbeitung ermöglicht. Man hätte daher erwarten können, dass im Rahmen der DS-GVO konkrete Richtlinien etabliert werden, die sich insbesondere den bisher ungeklärten Fragen rund um die Themen Industrie 4.0 und Big Data annehmen, um die daraus entstehenden Geschäftsmodelle auf ein solides Fundament zu stellen. Leider wurde diese Chance nicht in einem wünschenswerten Maße genutzt.

Grundsätzlich geht es dabei nämlich um folgendes Problem: „Big Data"-Analysen haben das Ziel, durch die Zusammenführung und Auswertung großer Datenmengen aus unterschiedlichen Anwendungs- und Lebensbereichen vorher nicht bekannte Muster zu entdecken. Dies impliziert in der Regel, dass jene Daten aus ihren ursprünglichen Zusammenhängen gerissen werden und der ursprünglich vorgesehene Verarbeitungszweck damit seine Gültigkeit verliert. Big Data-Analysen mit Personenbezug kommen heutzutage im Gesundheitswesen, der Verkehrslenkung, in der Forschung oder bei der Energieversorgung zum Einsatz.

Der Datenschutz steht diesem Ansatz in seinen Grundsätzen entgegen. Ihm zufolge ist der Umgang mit personenbezogenen Daten nur dann erlaubt, wenn von vornherein Einwilligungen oder Verträge vorliegen, die eine eindeutige Transparenz über Umfang und Zweck der Datenverarbeitung garantieren. Darüber hinaus spielt es für den Datenschutz keine Rolle, ob die aus der Analyse von Massendaten gewonnen Informationen auch Aussagen über bestimmte Personen treffen und damit auch nicht, auf welche expliziten Informationen es dem Datenverarbeiter ankommt. So mag beispielsweise der Automobilhersteller durch moderne Datenanalysen einzig beabsichtigen, seine Fahrzeuge und deren Probleme in Zukunft besser verstehen zu können. Gemäß den Prinzipien des Datenschutzes werden diese Daten jedoch in den meisten Fällen auch Aussagen über die Fahrzeugnutzer treffen. Unter diesen Umständen bezieht der Datenschutz auch jene Informationen mit ein, die aus datenschutzrechtlichen Gesichtspunkten eigentlich irrelevant sein sollten, wie beispielsweise Verkehrsdaten oder Informationen zum Verschleißverhalten bestimmter Fahrzeugmodelle. Die DS-GVO hätte nun an dieser Stelle Kriterien einführen können, die die Bestimmung der Personenbeziehbarkeit sowie die Beurteilung der Zulässigkeit der Datenverarbeitung vereinfachen und für alle Beteiligten transparenter machen würden. Bedauerlicherweise bleibt es aber fraglich, ob die neue Verordnung (Art. 6 Abs. 4 DS-GVO) diese Anforderungen erfüllen kann und sich darauf aufbauend eine innovationsfreundliche Auslegung des Prinzips der Zweckbindung entwickeln wird.

Innovationsfreundlichkeit darf in diesem Zusammenhang nicht bedeuten, dass Unternehmen mit personenbezogenen Daten machen können, was sie wollen. Um Europa jedoch nicht langfristig von der technologischen Entwicklung abzukoppeln, ist es unabdinglich, einen pragmatischen Ansatz zu etablieren, der innovative Datenanalysen möglich macht und gleichzeitig Missbrauchspotenziale dort bekämpft, wo sie vorhersehbar sind oder tatsächlich auftauchen. Des Weiteren kann es sogar schon hilfreich sein, die Öffentlichkeit gezielt über die Nutzungspotenziale von Big Data aufzuklären und einen gesellschaftlichen Diskurs über Chancen und selbstgesetzte Grenzen des Einsatzes der Technologie anzustoßen.

Datenkontrolle als neues Prinzip des Datenschutzes

Da in einer digitalisierten Welt nicht mehr die Minimierung von Daten das eigentliche Schutzziel sein kann, muss der Verbraucher dadurch geschützt werden, dass er die Kontrolle über seine Daten behält. So sollten alle Dienste und Plattformen die Daten mit Personenbezug verarbeiten, den Nutzern umfangreiche Möglichkeiten geben, die Nutzung und Weiterverarbeitung ihrer Daten in den Privacy-Settings selbst einstellen zu können. In Anbetracht der neuen technologischen Möglichkeiten im Bereich der Datenverarbeitung muss Datenschutz also bereits bei der Produktentwicklung mitgedacht werden. Das Prinzip des **„Privacy by Design"** ist in der DS-GVO nun gesetzlich verankert. Dabei ist es jedoch nicht ausreichend, dies allein auf die „Bauweise" von Produkten zu beschränken. Vielmehr sollte es verantwortungsvollen Technologieunternehmen als einer der Grundpfeiler ihrer Unternehmenskultur dienen und die Art und Weise, wie Dienstleistungen angeboten und durchgeführt werden, maßgeblich beeinflussen.

Extraterritoriale Rechtsanwendung: Es besteht weiterhin Reformbedarf

Für Unternehmen jeglicher Branchen und jeglichen Ursprungs ist es von hervorgehobener Bedeutung, in einem rechtlich sicheren Rahmen für den Transfer personenbezogener Daten operieren zu können. Gleichzeitig müssen zeitlose und nicht verhandelbare Werte und individuelle Rechte wie der Schutz der Privatsphäre auch in Anbetracht des technologischen Wandels und wachsender Datenmengen Bestand haben. Das daraus resultierende Spannungsverhältnis konnte in der Vergangenheit nur schwer aufgelöst werden und erzeugt grundlegenden Reformbedarf, welcher auch mit Inkrafttreten der DS-GVO weiterhin bestehen bleibt. Dement-

sprechend werden Datentransfers in Drittstaaten weiterhin nur zulässig sein, wenn zusätzliche Sicherheitsmechanismen dazu beitragen, ein angemessenes Datenschutzniveau zu gewährleisten, oder wenn ein solches verbindlich festgestellt wurde. Grund hierfür ist die Annahme, dass in Drittstaaten im Allgemeinen kein angemessenes Datenschutzniveau vorherrscht. Nichtsdestotrotz wurden in der neuen Verordnung einige Konkretisierungen vorgenommen, die insbesondere die Rechtsprechung des Europäischen Gerichtshofes aufgreifen und ausdrücklich auf bereits existierende Instrumentarien hinweisen, die als „geeignete Garantien" einen Datentransfer in Drittstaaten legimitieren. Zur Herstellung eines angemessenen Datenschutzniveaus wird nun explizit auf Standardvertragsklauseln, welche von der Europäischen Kommission als Modelklauseln vorgeben werden und deren Inhalt nicht abgeändert werden darf, sowie auf die als „Binding Corporate Rules" (BCR) bezeichneten, verbindlichen und selbstauferlegten Unternehmensvorschriften zum Umgang mit personenbezogenen Daten hingewiesen. Zur Heranziehung der BCRs werden in Artikel 47 der DGVO konkrete Anforderungen festgelegt, die die Umsetzung von Betroffenenrechten, Beschwerde- und Konfliktlösungsverfahren, die Haftungsübernahme im Fall von Verstößen gegen das Datenschutzrecht und die Kooperation mit Aufsichtsbehörden umfassen. Sofern die Zulässigkeit nicht über Ausnahmeregelungen hergestellt wurde und keine der gerade beschriebenen Schutzgarantien vorliegen, sollen Datenübermittlungen weiterhin zulässig sein, wenn *„die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und falls der für die Verarbeitung Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat (Kap. 5 Artikel 49 DSVGO)"*. Um für sich selbst zumindest ein ausreichendes Maß an Rechtssicherheit herstellen zu können, sind Verantwortliche also auch zukünftig darauf angewiesen, bestehende Rechtsgrundlagen im Einzelfall zu analysieren und geeignete Mechanismen zur Herstellung eines angemessenen Datenschutzniveaus abzuleiten.

Aus globaler Sicht haben die Aufhebung des „Safe Harbor"-Abkommens sowie die wachsende Problematik der extraterritorialen Anwendung nationaler Gesetze im Zusammenhang mit Anfragen von Regierungen nach Daten, die außerhalb ihrer Rechtshoheit liegen, darüber hinaus deutlich gemacht, dass das heutige internationale System des Datenschutzes auch an anderen Stellen einer dringenden Modernisierung bedarf. Insbesondere die internationalen Rechtshilfeabkommen (engl. „Mutual Legal Assistance Treaties", kurz: MLAT) müssen dringend an die Realitäten des digitalen Zeitalters angepasst werden. Microsoft sollte nicht zwischen den Stühlen stehen müssen, wenn Regierungen den Zugriff auf Nutzerdaten einfordern.

Jene Reformnotwendigkeit wurde durch die als „Warrant Case" bekannt gewordene Anfechtungsklage von Microsoft gegen einen Durchsuchungsbeschluss (warrant), der von einem amerikanischen Gericht erlassen wurde und von Microsoft die Herausgabe der Inhalte des im Rechenzentrum von Microsoft im irischen Dublin gespeicherten Emailverkehrs eines Kunden fordert, bestätigt. Im Mittelpunkt des Falls stand die Frage, ob die US-Regierung extraterritorial in ein europäisches Rechenzentrum eingreifen kann, um persönliche Kommunikationsdaten von EU-Bürgern einzufordern, ohne dabei das EU-Recht zu berücksichtigen. Microsofts Handeln gründet in diesem Zusammenhang auf einer der zentralen Verpflichtungen des Unternehmens im Bereich des Datenschutzes gegenüber seinen Nutzern – und zwar, nur dann den Forderungen einer Regierung nach Aushändigung von Nutzerdaten nachzukommen, wenn das Unternehmen rechtlich dazu verpflichtet ist. Microsoft hat sich ferner dazu verpflichtet, wo möglich (wie am Beispiel des Warrant Cases) Einspruch zu erheben, wenn Regierungen Daten in Ländern beschaffen wollen, die nicht in ihre Gerichtsbarkeit fallen. Dabei versucht Microsoft nicht, die US-Regierung – oder andere Staaten – davon abzuhalten, die notwendigen Beweismittel zur Verfolgung krimineller Aktivitäten zu erlangen. Das Unternehmen ist vielmehr der Auffassung, dass die US-Regierung bestehende internationale Mechanismen wie die vereinbaren MLAT-Verfahren für die Erlangung von Beweismitteln außerhalb der USA einhalten sollte, anstatt die US-Rechtsprechung auf Daten, die im Ausland gespeichert werden, anzuwenden und einseitig durchzusetzen. Durch die Beschaffung digitaler Informationen im Rahmen eines Durchsuchungsbeschlusses anstelle von Rechtshilfeabkommen vereitelt die US-Regierung den Zweck dieser Abkommen. Die US-Regierung widersprach der Position von Microsoft, da der Durchsuchungsbeschluss gegen Microsoft in den USA ergangen sei und sich die Daten unter der Kontrolle von Microsoft befinden würden. Sie geht davon aus, dass sie Technologieunternehmen, über die sie Rechtsgewalt hat, dazu zwingen kann, Emails von Kunden offenzulegen – unabhängig davon, wo diese Emails gespeichert sind und welche Datenschutzgesetzte vor Ort gelten. Am 14. Juli 2016 hat das US-Berufungsgericht „U.S. Court of Appeals for the Second Circuit" über die Klage von Microsoft gegen die globale Anwendbarkeit von US-Durchsuchungsbeschlüssen für E-Mails von Personen entschieden. Das Gericht entschied zugunsten von Microsoft und hob damit das Urteil der vorherigen Instanz auf.

Strafverfolgungsbehörden und Unternehmen müssen zukünftig enger zusammenarbeiten

Es sollte an dieser Stelle betont werden, dass die Einhaltung von Recht und Gesetz, wie von Microsoft im Rahmen des „Warrant Case" gefordert, nur dann legitim sein kann, wenn den Strafverfolgungsbehörden funktionsfähige Mittel zur Rechtsausübung gegeben werden. Diese Voraussetzung

wird mit dem Verweis auf die MLAT-Verfahren unter den momentanen Voraussetzungen nicht erfüllt und ruft somit einen dringenden Reformbedarf dieser und anderer Mittel hervor. Jene Reformen müssen die heutige Welt in angemessener Form widerspiegeln, anstatt sich an Technologien zu orientieren, die vor drei Jahrzehnten zur Zeit der Verabschiedung dieser Gesetze verbreitet waren. So hat Microsoft das US-Justizministerium bereits um Änderungen des bestehenden MLAT-Prozesses gebeten. Unter anderem geht es dabei um die Schaffung eines Online-Tracking-Systems für Anfragen und zur Veröffentlichung von jährlichen Statistiken über den Umfang der Rechtshilfeanfragen. Darüber hinaus müssen Strafverfolgungsbehörden gerade in Zeiten zunehmender terroristischer Bedrohungen dazu fähig sein, ihren Aufgaben effektiv nachzugehen. Eine Erneuerung der MLAT-Verfahren sollte daher verbindliche Regelungen einführen, die die internationale Herausgabe von Auskünften zu Tatverdächtigen und Anschlagsplanungen beschleunigen und damit die öffentliche Sicherheit stärken. Es ist somit notwendiger denn je, dass die Technologiebranche und die Politik konstruktiv zusammenarbeiten, um Bedürfnisse des Rechts auf Privatsphäre und der Strafverfolgung gleichermaßen weiterentwickeln zu können und die Rechte Einzelner als auch die Rechtsordnungen weltweit respektiert werden.

Es darf letztendlich nicht vergessen werden, dass dies keine Themen sind, die ausschließlich US-amerikanische Unternehmen, sondern die rechtliche Grundlage des internationalen Datenverkehrs betreffen und dadurch den Kern der gesamten europäischen Industrie berühren sowie das Vertrauen in die europäische Digitalwirtschaft in den nächsten Jahren maßgeblich beinflussen werden. Es bedarf daher eines konsistenten und einheitlichen europäischen Regelwerks, um zu vermeiden, dass ein rechtlicher Flickenteppich entsteht. Eine Gefahr, die sich unter Umständen auch zukünftig im Rahmen der Umsetzung der DS-GVO ergeben könnte.

Öffnungsklauseln: Weniger ist in diesem Fall mehr

Die neue Verordnung enthält insgesamt 70 sogenannter Öffnungsklauseln. Diese Vorschriften erlauben es den Mitgliedstaaten, für einzelne Datenverarbeitungen oder Anforderungen nationale Ausnahmeregelungen zu schaffen, etwa beim Beschäftigtendatenschutz, Fragen der Erlaubnis von Datenverarbeitungen, der Beschränkung von Betroffenenrechten oder im Gesundheitswesen.

Im Ergebnis beschränken die Öffnungsklauseln das Maß an EU-weiter Vereinigung und sind zum Teil derart abstrakt formuliert, dass die Mitgliedstaaten sie jeweils entsprechend ihrer nationalen Rechtstradition auslegen können. Zwar bleibt es abzuwarten, ob und in welcher Form die Mitgliedsstaaten von diesem Recht Gebrauch machen werden und welchen Spielraum der Europäische Gerichtshof ihnen hierfür einräumen wird, im Interesse eines tatsächlich einheitlichen europäischen Rechtsrahmens sollten die Öffnungsklauseln jedoch in so geringem Maße wie möglich genutzt werden. Dabei sollte man sich auch noch einmal vor Augen führen, dass jene Freiräume in ihrer ursprünglichen Form nur geschaffen wurden, um nationale Besonderheiten ausreichend berücksichtigen zu können. Dies sollte jedoch nur in Fällen erfolgen, die eine Vereinheitlichung des Rechtsrahmens aus allgemein verständlichen Gründen ausschließen, andernfalls besteht das Risiko der Rechtsunsicherheit und einer nachhaltigen Fragmentierung der DS-GVO.

Fazit

Es ist nicht zu bestreiten, dass die Datenschutz-Grundverordnung vor dem Hintergrund eines zunehmenden globalen Wettbewerbsdrucks und der Notwendigkeit, den Wirtschafts- und Innovationsstandort Europa langfristig zu stärken, einen bedeutenden Fortschritt darstellt. Dieser Beitrag hat jedoch auch gezeigt, dass die ausgerufenen Ziele Harmonisierung, Wettbewerbsangleichung und Modernisierung nur zu Teilen erfüllt werden. Die Defizite führen im Umkehrschluss zu einer großen Verantwortung für die EU-Mitgliedstaaten und deren Datenschutzbehörden, Unternehmen, Verbände und neu geschaffene Institutionen wie dem Europäischen Datenschutzausschuss. Nur durch eine effektive und verbindliche Zusammenarbeit über alle Ebenen hinweg kann die neue Verordnung als Orientierungspunkt fungieren, der eine vernünftige Balance zwischen dem Bedürfnis nach Sicherheit, verfassungsrechtlich verankerten Privatsphäre- und Freiheitsrechten sowie Innovationsförderung und offenen Märkten gewährleist, sowie klare und harmonisierte datenschutzrechtliche Bestimmungen beinhaltet, von denen Industrie und Verbraucher gleichermaßen profitieren.

Es gilt also schnellstmöglich, die noch offenen Fragen hinsichtlich nationaler Auslegungsspielräume und den neuen Herausforderungen des digitalen Zeitalters zu diskutieren und umfassende Empfehlungen zu formulieren, an denen sich Verantwortliche und Auftragsverarbeiter, aber auch Behörden und Gerichte orientieren können. Dies betrifft insbesondere den Umgang mit der Vielzahl von Öffnungsklauseln, weiterführenden Reformmaßnahmen im Bereich internationaler Rechtshilfeabkommen (MLAT-Verfahren) und sonstigen Regelungen des internationalen Datenverkehrs, sowie den neu eingeführten Prinzipien wie dem der datenschutzfreundlichen Produktgestaltung („Privacy by Design“) und Zertifizierungen. Darüber hinaus gilt es zu klären, ob man sich durch eine weiterhin restriktive Auslegung des Prinzips der Zweckbindung in der Datenverarbeitung tatsächlich der Gefahr aussetzten möchte, die im Rahmen des Einsatzes von Big Data-Analysen entstehenden Innovationspotenziale in Bereichen wie dem Gesundheitswesen zu vergeben und damit Europas internationale Anschlussfähigkeit langfristig zu gefährden. Nur wenn diese Fragen gelöst werden und ein pragmatischer Ansatz gefunden wird, besteht eine berechtigte Chance, kohärente und zeitgemäße rechtliche Rahmenbedingungen im Bereich des Datenschutzes in Europa nachhaltig zu etablieren.

Aus den Aktuellen Berichten der Aufsichtsbehörden (27): Kommunales

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter*

In diesem Jahr erschienen bislang 10 Tätigkeitsberichte der Landesdatenschutzbeauftragten (Rheinland-Pfalz, 25. TB vom 12.7.2016; Hessen, 44. TB vom 12.7.2016; Thüringen, Bericht 2014/15 vom 25.5.2016; Mecklenburg-Vorpommern, TB 2014/2015 vom 3.4.2016; Brandenburg, 18. TB vom 12.4.2016; Berlin, 37. TB vom 23.3.2016; Bremen, 38. TB vom 11.3.2016; Sachsen-Anhalt, 12. TB (2014/2015) vom 23.2.2016, Hamburg, 25. TB (2014/2015) vom 25.2.2016; Baden-Württemberg, 32. TB (2014/2015) vom 29.1.2016). Ausgewählt wurden nachstehend einige an die Aufsichtsbehörden herangetragenen Fragen des datenschutzgerechten Umgangs mit personenbezogenen Daten in Kommunen, wobei der ThürLfDI festhält, dass es auch bei einigen öffentlichen Stellen noch immer an den erforderlichen Grundkenntnissen zum Datenschutz und an der gebotenen Sensibilität im Umgang mit personenbezogenen Daten mangele. Nicht hinreichend bewusst sei, dass eine Erhebung personenbezogener Daten ohne Rechtsgrundlage und ohne bewusste Mitwirkung der Betroffenen einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstelle.

Datenausspähung der Bürgermeister-E-Mails

Über eine Datenausspähung durch Sichtung des E-Mail-Verkehrs des Bürgermeisters durch die Gemeindevertretung berichtet der LfD Sachsen-Anhalt (12. TB, 04-2024/03-2015, Ziff. 13.4.2). Ein Konflikt zwischen dem Bürgermeister und der Gemeindevertretung hatte letztendlich dazu geführt, dass einzelne Ratsmitglieder eine Abwesenheit des Bürgermeisters nutzten, um mehrere Beschlüsse der Gemeindevertretung herbeizuführen, nach welchen u.a. der gesamte E-Mail-Verkehr der Verbandsgemeinde durch eine IT-Firma auf einer Festplatte gesichert wurde. Diese Sicherung sollte auch genutzt werden, um speziell den E-Mail-Verkehr des Bürgermeisters und einiger anderer Beschäftigter zu sichten, um Disziplinarmaßnahmen gegen diese anzustrengen.

Nachdem die Speicherung und auch ein Datenzugriff einiger Gemeinderatsmitglieder erfolgte, wurde die Aktion gestoppt, weil die Kommunalaufsicht dem Vorhaben widersprach. Begründet wurde dies letztendlich damit, dass für den Vollzug der Beschlüsse und die Gestaltung von Rechtsbeziehungen mit Dritten in einer Kommune stets der Bürgermeister zuständig sei. Die Vertretung als Gremium kann diese Aufgabe, auch nicht durch einen Beschluss, an sich ziehen. Das bedeutet, dass die Vertretung keinen Auftrag zur Datenspeicherung hätte erteilen dürfen. Diese Befugnis stehe in Zeiten der Abwesenheit des Verbandsgemeindebürgermeisters nur seiner Stellvertreterin zu.

Der LfD bewertet den Vorfall datenschutzrechtlich wie folgt: Durch das Handeln des Gemeinderates haben einige Vertreter dieses Gremiums eine Sammlung personenbezogener Daten in die Hände bekommen, die allein der Gemeindeverwaltung zugestanden hätte. Der Gemeinderat darf nur Kenntnis von personenbezogenen Daten erhalten, welche er für Entscheidungen, für die er zuständig ist, benötigt. Damit stehe fest, dass sich ein nicht namentlich bekannter Personenkreis Zugang zu personenbezogenen Daten verschafft hatte, die er für seine Aufgabenerfüllung nicht benötigte.

Die mit der Sache befasste Staatsanwaltschaft stellte das Verfahren gegen Zahlung einer Geldbuße ein. Eine abschließende datenschutzrechtliche Beurteilung enthält der Bericht auch im Hinblick auf ein paralleles Petitionsverfahrens im Landtag von Sachsen-Anhalt noch nicht.

Der Fall wirft die generelle Frage auf, mit der sich der LfD Sachsen-Anhalt nachfolgend befasst (12. TB, Ziff. 13.4.3), in welchem Umfang welche personenbezogenen Daten dem Rat als Vertretung der Kommune durch die Kommunalverwaltung vorgelegt werden müssen. Dazu verweist der LfD auf § 10 DSG LSA, nach dem das Nutzen personenbezogener Daten nur zulässig ist zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben und für die Zwecke, für die sie erhoben worden sind. Ist eine Aufgabe eindeutig dem Hauptverwaltungsbeamten zugewiesen, darf die Vertretung diese Aufgabe nicht an sich ziehen. Jedoch darf jedes Mitglied der Vertretung nach § 45 Abs. 7 KVG LSA über einzelne Angelegenheiten der Kommune und ihrer Verwaltung Auskunft vom Hauptverwaltungsbeamten verlangen.

„Mystery-Check im Thüringer Wald“

Über von einer „kommunalen Arbeitsgemeinschaft Ferienregion“ veranlasste so genannte Mystery-Calls berichtet der ThürLfDI (11. TB Öffentlicher Bereich, 2014/2015, S. 125). Dabei wurde u.a. Zimmervermietern per Telefon oder Email vorgegaukelt, dass ein Kunde ein Zimmer mieten wolle. In Wirklichkeit sollte jedoch die Servicequalität seines Unternehmens am Telefon oder per E-Mail beurteilt werden.

Der ThürLfDI hat den festgestellten Sachverhalt wie folgt bewertet: Beim Verfahren „Mystery-Check“ wurden personenbezogene Daten im Sinne von § 3 Abs. 3 ThürDSG verarbeitet. Bei den erhobenen Daten handele es sich um personenbezogene bzw. personenbeziehbare Einzelangaben über das Kommunikationsverhalten von Inhabern und Mitarbeitern von Beherbergungsbetrieben im Sinne des § 3 Abs. 1

* Der Autor ist Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn.

ThürDSG. Eine solche Erhebung personenbezogener Daten sei gemäß § 19 Abs. 1 ThürDSG nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist.

Fraglich war im vorliegenden Sachverhalt bereits, ob es Aufgabe der Gemeindeverwaltungen als KAG-Mitglieder war, die Service-Qualität privater Beherbergungsbetriebe zu bewerten. Der Begriff „Erforderlichkeit" ist ein unbestimmter Rechtsbegriff, der im jeweiligen Einzelfall auszufüllen und zu konkretisieren ist. Die Kenntnis der Daten ist dann erforderlich, wenn die öffentliche Stelle im jeweiligen konkreten Einzelfall ihre Aufgaben nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und außerdem erst aktuell dann und nur in dem Umfang, wie es die Aufgabenerfüllung gerade in Bezug auf die betroffene Person erfordert.

Letztlich konnte die Frage, ob die Datenerhebung im vorliegenden Sachverhalt erforderlich war, jedoch offen bleiben. Denn im konkreten Fall waren die weiteren Voraussetzungen des § 19 Abs. 2 ThürDSG für eine Datenerhebung durch die KAG bzw. ihre Mitgliedskommunen nicht gegeben. Nach § 19 Abs. 2 Satz 1 ThürDSG sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben. Dies setzt voraus, dass der Betroffene an der Erhebung seiner Daten bewusst mitwirkt, d.h. dass ihm die Tatsache einer Datenerhebung und der damit verbundene Eingriff in seine Persönlichkeitsrechte bekannt sein müssen. Dies ist nicht der Fall, wenn der Anrufer suggeriert, dass er Zimmer bzw. Zimmerkontingente bei dem angerufenen Tourismusbetrieb buchen bzw. reservieren will und während dieses Gesprächs – ohne Wissen des Gesprächspartners – anhand einer Matrix mit vorab definierten Bewertungskriterien das Verhalten des Gesprächspartners des Tourismusbetriebes am Telefon bewertet. Ohne Mitwirkung des Betroffenen dürfen dessen personenbezogene Daten aber nur erhoben werden, wenn 1. dies eine Rechtsvorschrift vorsieht oder zwingend voraussetzt (§ 19 Abs. 2 Satz 1 Nr. 1 ThürDSG), 2. die erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht (§ 19 Abs. 2 Satz 1 Nr. 2 ThürDSG) oder 3. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde (§ 19 Abs. 2 Satz 1 Nr. 3 ThürDSG). In den Fällen der genannten Nr. 2 und Nr. 3 ist eine Erhebung bei Dritten nur zulässig, wenn keine Anhaltspunkte dafür vorliegen, dass überwiegend schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Im konkreten Fall war hier weder eine Rechtvorschrift im Sinne des § 19 Abs. 2 Nr. 1 ThürDSG ersichtlich, auf die diese Datenerhebung gestützt werden konnte, noch konnte angenommen werden, dass eine Verwaltungsaufgabe einen derartigen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Inhaber und Mitarbeiter der befragten Unternehmen zwingend voraussetzte bzw. erforderlich machte. Da im Ergebnis nicht erkennbar war, dass die Zulässigkeitsvoraussetzungen des § 19 Abs. 2 ThürDSG vorlagen, stellte die Erhebung und Verarbeitung von personenbezogenen Daten mittels des Verfahrens „Mystery-Check" einen Verstoß gegen datenschutzrechtliche Vorschriften dar.

Aufgrund dieser Bewertung beanstandete der ThürLfDI die rechtswidrige Erhebung und Verarbeitung personenbezogener Daten von Beherbergungsunternehmen schließlich gegenüber den für die unzulässige Datenerhebung verantwortlichen Mitgliedsgemeinden des KAG gemäß § 39 Abs. 1 Satz 1 ThürDSG. Anders wäre der Fall wohl zu beurteilen gewesen, wenn ein privatwirtschaftlichen organisiertes Fremdenverkehrsbüro die Umfrage durchgeführt hätte (vgl. zu Mystery Calls Gola, Datenschutz am Arbeitsplatz, Rn. 430 ff).

Der mitteilsame Oberbürgermeister

Als alles andere als datenschutzrechtlich „gewöhnlich" bezeichnen der ThürLfDI (11. TB (2014/2015), S. 121) eine unbefugte Veröffentlichung sensibler personenbezogener Daten durch einen Oberbürgermeister. Konkret ging es um einen leitenden Beamten der Stadt, gegen den die Staatsanwaltschaft ein strafrechtliches Ermittlungsverfahren wegen des Vorwurfs des sexuellen Missbrauchs widerstandsunfähiger Personen gemäß § 179 Abs. 5 Strafgesetzbuch geführt hatte. Hauptbelastungszeugin und mutmaßliches Opfer war eine Kollegin des Beamten. Die Staatsanwaltschaft stelle das Ermittlungsverfahren ein, da sie keine Anhaltspunkte für ein dem beschuldigtem Beamten vorgeworfenes Handeln nachweisen konnte. Die Staatsanwaltschaft hielt den Beamten deshalb für unschuldig, kommunizierte ihr Ermittlungsergebnis gegenüber der Presse und gab ansonsten keine weiteren Details ihres ermittelten Geschehensablaufs preis.

Dieses Ermittlungsergebnis der Staatsanwaltschaft kommentierte der Oberbürgermeister mit einer eigenen Pressemitteilung zu dieser Causa: Darin war unter anderem zu lesen, dass in dem genannten Ermittlungsverfahren „Aussage gegen Aussage" stehe. Ferner ließ der Oberbürgermeister darin vermelden, dass *„die Zeugenaussage der betroffenen … [Hauptbelastungszeugin] ebenso glaubwürdig sei wie die nicht zu widerlegende Behauptung von …[dem beschuldigten Beamten], es habe sich um einvernehmlichen Geschlechtsverkehr* ***unter Alkoholeinfluss*** *gehandelt"*.

Der betroffene Beamte bat den ThürLfDI um datenschutzrechtliche Prüfung der Vorgehensweise des Oberbürgermeisters, in der Pressemitteilung zu verlautbaren, dass es im Ermittlungsverfahren der Staatsanwaltschaft um einen Geschlechtsverkehr „unter Alkoholeinfluss" gegangen sei. Das Faktum „unter Alkoholeinfluss" sei weder von der Staatsanwaltschaft noch von ihm, dem Beamten selbst, in der Presse jemals genannt worden. Erst durch die Pressemitteilung des Oberbürgermeisters sei dieser Vorwurf in die Öffentlichkeit gelangt.

Die datenschutzrechtliche Prüfung durch den ThürLfDI ergab dabei Folgendes: Bei den Informationen „Geschlechtsverkehr unter Alkoholeinfluss" handelte es sich zunächst um Einzelangaben über persönliche Verhältnisse von bestimmbaren Personen und damit um personenbezogene Daten im Sinne von § 3 Abs. 1 ThürDSG.

Die Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss" durch die Pressemitteilung des Oberbürgermeisters erfolgte auch ohne Rechtsgrundlage. Denn weder war die Datenübermittlung durch § 22 Abs. 1 Nr. 1 ThürDSG

zur Erfüllung der Aufgaben des Bürgermeisters erforderlich noch durch § 22 Abs. 1 Nr. 2 ThürDSG gerechtfertigt.

Der Oberbürgermeister berief sich zwar darauf, dass er aus der „Fürsorgepflicht des Dienstherrn" gehalten war, „unabgewogene(n) Pressemitteilungen" und dem Eindruck entgegenzuwirken, dass die Opferzeugin „nachweislich gelogen habe". Aber wenn man unterstellen würde, dass eine solch weitgehende Fürsorgepflicht des Dienstherrn tatsächlich existierte, so war es gleichwohl nicht erforderlich gewesen, quasi zur Wiederherstellung der Glaubwürdigkeit der Opferzeugin das personenbezogene Datum „unter Alkoholkonsum" mit dem personenbezogenen Datum „Geschlechtsverkehr" in einen unmittelbaren Kontext zu stellen und an die Presse zu übermitteln. Denn nach dem Grundsatz der Erforderlichkeit sei von mehreren geeigneten Maßnahmen diejenige zu wählen, die den einzelnen am wenigsten beeinträchtigte. Dafür hätte es ausgereicht, wenn der Oberbürgermeister allein darauf hingewiesen hätte, dass Aussage gegen Aussage stehe. Zudem hatte der betroffene Beamte wie die Opferzeugin ein schutzwürdiges Interesse an dem Ausschluss der Datenübermittlung. Dieses bestand hier darin, die Öffentlichkeit nicht wissen zu lassen, dass es unter Alkoholeinfluss zwischen beiden zum Geschlechtsverkehr gekommen war. Denn bei dieser Information handelte es sich um ein – höchst persönliches – personenbezogenes Datum. Dieses personenbezogenes Datum ist schützenswert im Sinne von § 22 Abs. 1 Nr. 2 ThürDSG, wenn es aus objektiver Sicht unter Zugrundelegung durchschnittlicher Verhältnisse zu Nachteilen für die Betroffenen führen kann. Die Information konnte ihre Integrität bzw. ihr Ansehen beschädigen und damit zu sozialen und persönlichen Nachteilen führen. Zusätzlich war hinsichtlich der Opferzeugin zu berücksichtigen, dass durch die Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss" an die Presse der mit der Pressemitteilung des Oberbürgermeisters verfolgte Zweck, nämlich den Eindruck zu vermeiden, dass die Opferzeugin „nachweislich gelogen habe", gerade nicht zu erreichen war und daher auch insoweit Nachteile persönlicher Art für die Opferzeugin zu befürchten waren.

Die dargestellten schutzwürdigen Interessen des betroffenen Beamten und der betroffenen Opferzeugin seien im Ergebnis auch höher zu gewichten als das Interesse der Pressevertreter, Detailkenntnisse über den Sachverhalt zu erfahren, der Gegenstand des strafrechtlichen Ermittlungsverfahrens gegen den betroffenen Beamten war. Denn über die wesentlichen Gründe für die Einstellung des strafrechtlichen Ermittlungsverfahrens hatte der Pressesprecher der zuständigen Staatsanwaltschaft die Medien hinreichend unterrichtet.

Aufgrund des Ergebnisses der datenschutzrechtlichen Prüfung beanstandete der ThürLfDI gemäß § 39 Abs. 1 Satz 1 ThürDSG die rechtswidrige Datenübermittlung.

Datenerhebung mittels Mülltonne?

Erneut (zuvor 8. TB, Ziff. 5.16) hatte sich der ThürLfDI (11. TB (2014/2015) für den öffentlichen Bereich, Ziff. 5.8) mit Datenschutzproblemen bei Kommunalen Abfallentsorgungsunternehmen zu befassen. Ein Abfallwirtschaftsbetriebs (AWB) hatte an den Tonnen für Papiermüll Aufkleber angebracht, auf denen die Kunden des AWB Straßenname, Hausnummer, Postleitzahl und Ort des Abfalltonnenstandorts angeben sollten. Die Erhebung dieser Daten sollte zum einen der Überwachung und Durchsetzung des Anschluss- und Benutzungszwanges in der Abfallfraktion Papier/Pappe/Kartonagen und zum anderen einer näherungsweisen Überwachung der entsorgten Abfallmenge dienen.

Zu der zunächst vertretenen Auffassung des AWB, dass es sich bei diesen Daten nicht um personenbezogene, sondern lediglich um anonymisierte Daten handele, vermittelte der LfDI die zutreffende Klarstellung, dass Personenbeziehbarkeit der Daten vorliege, wenn ein objektiver Dritter ohne größeren Aufwand von den o. g. Daten auf die anschluss- und benutzungspflichtigen natürlichen Personen schließen konnte. Das erforderliche Zusatzwissen, d.h. die Kenntnis der Grundbucheintragung zur Bestimmung des anschluss- und benutzungspflichtigen Eigentümers, sei ohne unverhältnismäßigen Aufwand durch eine Anfrage im Grundbuchamt erhältlich. Dass sich der Recherchierende dieses Zusatzwissen erst besorgen müsse und ob seine entsprechende Absicht dafür bestehe, spiele keine Rolle.

Fraglich war sodann, ob das für die Verarbeitung bestehende Verbot mit Erlaubnisvorbehalt durch § 30 Abs. 2 Satz 1 des Thüringer Gesetzes über die Vermeidung, Verminderung, Verwertung und Beseitigung von Abfällen (ThürAbfG) durchbrochen würde. § 30 Abs. 2 Satz 1 ThürAbfG berechtigt die öffentlich-rechtlichen Entsorgungsträger, die zu ihrer Aufgabenerfüllung erforderlichen personenbezogenen Daten zu erheben, wobei sie verpflichtet sind, mittels Satzung zu regeln, bei welchen Personen oder Stellen welche personenbezogenen Daten erhoben werden sollen. Die maßgebende Satzung enthielt jedoch eine diesbezügliche Regelung nicht.

Letztendlich erklärte der AWB, dass er die AbfWS umgehend um eine Erlaubnisnorm zur Erhebung der personenbezogenen Daten der Postleitzahl, des Ortes, des Straßennamen und der Hausnummer des betreffenden Grundstückes ergänzen werde.

Keine Speicherung von Dissertationsurkunden und Scheidungsurteilen bei Meldebehörden

Am oben genannte Beispiel macht der HessDSB deutlich, dass beantragte Veränderungen im Einwohnermelderegister zwar im erforderlichen Umfang belegt werden müssen, dass dazu in der Regel für die Meldebehörde der Vermerk ausreiche, dass das entsprechende Dokument vorgelegen habe (Hess DSB, 44. TB Ziff. 4.1.4.3). Dem haben die Einwohnermeldeämter Rechnung zu tragen und nicht mehr Informationen anzufordern oder zu speichern, als dies zur Aufgabenerfüllung eines Meldeamtes erforderlich ist. Der Datenumfang der Einwohnermelderegister ist in § 3 HMG abschließend festgelegt. Über die als „Daten" bezeichneten Angaben hinaus dürfen die Meldebehörden auch die zum Nachweis der Richtigkeit erforderlichen Hinweise speichern. Hierbei handelt es sich um die Benennung von Urkunden und Nachweisen mit Bezeichnung der ausstellenden Behörde oder des Gerichts mit Aktenzeichen und Tag der Ausstellung sowie

Tag des Ereignisses. Gleichwohl ist aber auch insoweit die Erforderlichkeit nach § 11 HDSG zu beachten. Demgemäß dürfe die einfache Verfügbarkeit von Kopierern nicht dazu führen, dass mehr personenbezogene Daten im Einwohnermeldeamt gespeichert werden, als dies zur Aufgabenerfüllung erforderlich ist. Regelmäßig genügt zum Nachweis der Richtigkeit ein Vermerk darüber, dass die entsprechende Urkunde oder das Gerichtsurteil vorgelegen hat, ergänzt um die oben ausgeführten Daten. Für den Nachweis einer rechtskräftigen Scheidung gegenüber Behörden genügt der Tenor der Gerichtsentscheidung. Ebenso ist ich die Aufbewahrung einer Kopie der Dissertationsurkunde mit ihren Detailangaben (Note etc.) nicht erforderlich.

Keiner soll entkommen: Erneuter Meldedatenabgleich für den Beitragsservice der Rundfunkanstalten

Keinen Erfolg hatte der LfDI M.-V. (12. TB, 2014/2015, Öffentlicher Bereich, Ziff. 5.4.10) mit seinen unter den Aspekten der Erforderlichkeit und der Verhältnismäßigkeit geltend gemachten Bedenken gegen die 19. Änderung des Rundfunkstaatsvertrages, mit der ein erneuter Datenabgleich aller Meldedaten vorgesehen ist, um Beitragspflichtige zu ermitteln, die den Wohnsitz geändert haben oder für die eine Beitragspflicht neu entstanden ist, etwa bei Jugendlichen. Mit Inkrafttreten der 15. Änderung des Rundfunkstaatsvertrages am 1. Januar 2013 war ein erster vollständiger Meldedatenabgleich durchgeführt worden, um den Wechsel von einer gerätebezogenen Abgabe zu einem wohnungs- bzw. betriebsbezogenen Beitrag zur Finanzierung des öffentlich-rechtlichen Rundfunks zu ermöglichen. Dazu wurden die Daten des Beitragsservices der bisher Beitragspflichtigen mit den Daten aller volljährigen Personen, die bei den Einwohnermeldeämtern in Deutschland gemeldet sind, verglichen. Dabei ging es um Angaben zum Namen, Doktorgrad, Familienstand, Geburtsdatum sowie zur aktuellen und vorherigen Anschrift der Haupt- und Nebenwohnungen und zum Tag des Einzugs. Mit der 19. Änderung des Rundfunkstaatsvertrages ist nunmehr ein nochmaliger, vollständiger Meldedatenabgleich aller meldepflichtigen Personen in Deutschland vorgesehen.

Rechtsprechung

Zur Gewährung von Schmerzensgeld nach rechtswidrigem Freiheitsentzug (Ls)

(**Bundesverfassungsgericht**, Beschluss vom 29. Juni 2016 – 1 BvR 1717/15 –)

1. **Der Schutzauftrag des allgemeinen Persönlichkeitsrechts wird durch den Anspruch auf Ausgleich des immateriellen Schadens verwirklicht. Dies gilt nicht weniger, wenn auch das Grundrecht auf Freiheit der Person betroffen ist. Dass eine Geldentschädigung wegen der Verletzung immaterieller Persönlichkeitsbestandteile nach der zivilgerichtlichen Rechtssprechung nur unter der Voraussetzung einer hinreichenden Schwere und des Fehlens einer anderweitigen Genugtuungsmöglichkeit beansprucht werden kann, ist verfassungsrechtlich und auch vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte unbedenklich.**
2. **Demgemäß ist die Verletzung des Grundrechts aus Art. 2 Abs. 2 Satz 2 GG in die gebotene Gesamtschau aller Umstände des Einzelfalles einzubeziehen. Auch wenn in der mindestens achtstündigen rechtswidrigen Festsetzung des Beschwerdeführers keine nachhaltige Beeinträchtigung gesehen wird, ist die abschreckende Wirkung zu erwägen, die einer derartigen Behandlung für den künftigen Gebrauch des Rechts auf Versammlungsfreiheit zukommen kann.**

(Nicht amtliche Leitsätze)

Wahre Tatsachenbehauptungen über Vorgänge aus der Sozialsphäre sind grundsätzlich hinzunehmen (Ls)

(**Bundesverfassungsgericht**, Beschluss vom 29. Juni 2016 – 1 BvR 3487/14 –)

1. **Die Schwelle zur Persönlichkeitsrechtsverletzung wird bei der Mitteilung wahrer Tatsachen über die Sozialsphäre regelmäßig erst überschritten, wo sie einen Persönlichkeitsschaden befürchten lässt, der außer**

Verhältnis zu dem Interesse an der Verbreitung der Wahrheit steht.

2. Der Einbruch in die persönliche Sphäre darf nicht weiter gehen, als eine angemessene Befriedigung des Informationsinteresses dies erfordert. Die für den Genannten entstehenden Nachteile müssen im rechten Verhältnis zur Schwere des geschilderten Verhaltens oder der sonstigen Bedeutung für die Öffentlichkeit stehen. Auch wenn die Äußerung im Internet über einen drei Jahre zurückliegenden Rechtsstreit erfolgt führt das nicht zu einem überwiegenden Schutzinteresse.

Die falsche Einordnung einer Äußerung als Schmähkritik verkürzt den grundrechtlichen Schutz der Meinungsfreiheit (Ls)

(**Bundesverfassungsgericht**, Beschluss vom 29. Juni 2016 – 1 BvR 2646/15 –)

1. Wegen seines die Meinungsfreiheit verdrängenden Effekts ist der Begriff der Schmähkritik von Verfassungs wegen eng zu verstehen. Schmähkritik ist ein Sonderfall der Beleidigung, der nur in seltenen Ausnahmekonstellationen gegeben ist. Die Anforderungen hierfür sind besonders streng, weil bei einer Schmähkritik anders als sonst bei Beleidigungen keine Abwägung mit der Meinungsfreiheit stattfindet. Wird eine Äußerung unzutreffend als Schmähkritik eingestuft, liegt darin ein eigenständiger verfassungsrechtlicher Fehler, auch wenn die Äußerung im Ergebnis durchaus als Beleidigung bestraft werden darf.

2. Das Grundrecht auf Meinungsfreiheit schützt nicht nur sachlich-differenzierte Äußerungen. Vielmehr darf Kritik auch pointiert, polemisch und überspitzt erfolgen. Einen Sonderfall bilden herabsetzenden Äußerungen, die sich als Formalbeleidigung oder Schmähung darstellen. In diesen Fällen ist ausnahmsweise keine Abwägung zwischen der Meinungsfreiheit und dem Persönlichkeitsrecht notwendig, weil die Meinungsfreiheit regelmäßig hinter den Ehrenschutz zurücktritt.

3. Diese für die Meinungsfreiheit einschneidende Folge gebietet es aber, hinsichtlich des Vorliegens von Formalbeleidigungen und Schmähkritik strenge Maßstäbe anzuwenden. Bedeutung und Tragweite der Meinungsfreiheit sind auch dann verkannt, wenn eine Äußerung unzutreffend als Schmähkritik eingestuft wird mit der Folge, dass sie dann nicht im selben Maß am Schutz des Grundrechts teilnimmt wie Äußerungen, die als Werturteil ohne beleidigenden oder schmähenden Charakter anzusehen sind.

(Nicht amtliche Leitsätze)

Eilanträge gegen das Vorratsdatenspeicherungsgesetz erfolglos

(**Bundesverfassungsgericht**, Beschlüsse vom 8. Juni 2016 – 1 BvO 42/15 und 1 BvR 229/16 –)

Mit der Datenspeicherung allein ist noch kein derart schwerwiegender Nachteil verbunden, dass er die Außerkraftsetzung eines Gesetzes erforderte. Darüber hinaus hat der Gesetzgeber den Abruf von Telekommunikations-Verkehrsdaten von qualifizierten Voraussetzungen abhängig gemacht, die das Gewicht der durch den Vollzug der Vorschrift drohenden Nachteile im Vergleich mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen lassen.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Beschwerdeführer begehren mit ihrem Eilantrag, die durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218; im Folgenden: Vorratsdatenspeicherungsgesetz) eingeführte Vorratsspeicherung von Telekommunikations-Verkehrsdaten zu Zwecken der öffentlichen Sicherheit außer Kraft zu setzen.

1. Ein Abruf von Telekommunikations-Verkehrsdaten – etwa gemäß § 100g Abs. 1 StPO – hatte bisher nur dann Erfolg, wenn der ersuchte Diensteanbieter die Daten zu eigenen Zwecken gespeichert hatte, etwa gemäß § 97 Telekommunikationsgesetz (im Folgenden: TKG) zur Entgeltermittlung und Entgeltabrechnung oder gemäß § 100 TKG zur Feststellung, Eingrenzung und Beseitigung der Störung einer Telekommunikationsanlage. Tatsächlich ist es in erheblichem Umfang vom Zufall abhängig, welche Daten bei einer Abfrage nach § 100g StPO abgerufen werden können (vgl. BTDrucks 18/5088, S. 21).

Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vom 21. Dezember 2007 (BGBl I S. 3198; im Folgenden: Gesetz zur Neuregelung der Telekommunikationsüberwachung), das in Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl Nr. L 105 vom 13. April 2006, S. 54; im Folgenden: Richtlinie 2006/24/EG), erlassen wurde, sollte dem durch eine vorsorgliche Speicherungspflicht der Telekommunikations-Verkehrsdaten durch die Diensteanbieter entgegenwirken. Es ist aus verfassungsrechtlichen Gründen nicht wirksam geworden. Mit Beschluss vom 11. März 2008 hat der Erste Senat des Bundesverfassungsgerichts dem Antrag auf einstweilige Anordnung gegen das Gesetz teilweise stattgegeben (vgl. BVerfGE 121, 1 <19 ff.>) und mit Urteil vom 2. März 2010 die §§ 113a und 113b TKG sowie § 100g Abs. 1 Satz 1 StPO, soweit danach Verkehrsdaten nach § 113a TKG erhoben werden durften, in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl I S. 3198), wegen Verstoßes gegen Art. 10 Abs. 1 GG für nichtig erklärt (vgl. BVerfGE 125, 260 <262 f., 307 ff.>). Die Große Kammer des Europäischen Gerichtshofs erklärte mit Urteil vom 8. April 2014 auf Vorabentscheidungsersuchen des Irischen High Court und des Österreichischen Verfassungsgerichtshofs

dann auch die Richtlinie 2006/24/EG für ungültig, weil der Unionsgesetzgeber beim Erlass der Richtlinie die Grenzen überschritten habe, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 der Europäischen Grundrechtecharta (GRCh) einhalten musste (vgl. EuGH, Urteil der Großen Kammer vom 8. April 2014, Digital Rights Ireland Ldt/Minister for Communications, Marine and Naturale Recourses u.a., C-293/12, C-594/12, NJW 2014, S. 2169 <2173>).

2. Das im vorliegenden Verfahren angegriffene Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten dient nach der Gesetzesbegründung erneut der Vereinheitlichung der Speicherpraxis der Erbringer öffentlich zugänglicher Telekommunikationsdienste. Es soll Unzulänglichkeiten in der Strafverfolgungsvorsorge und der Gefahrenabwehr beseitigen (vgl. BTDrucks 18/5088, S. 21 f.). Zu diesem Zweck enthält sein Art. 1 Änderungen der Strafprozessordnung und sein Art. 2 Änderungen des Telekommunikationsgesetzes. Die von den Beschwerdeführern angegriffenen Regelungen zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten finden sich in den neu geschaffenen §§ 113a bis 113g TKG, die angegriffenen Regelungen über die Erhebung der Verkehrsdaten durch die Strafverfolgungsbehörden und das dabei zu beachtende Verfahren finden sich in dem neu gefassten § 100g StPO und den neu geschaffenen §§ 101a und 101b StPO.

§ 113a Abs. 1 TKG bestimmt mit den Anbietern öffentlich zugänglicher Telekommunikationsdienste für Endnutzer den Verpflichteten der Vorratsdatenspeicherung. § 113b TKG verpflichtet die Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer sodann, bestimmte einzeln aufgeführte Verkehrs- und Standortdaten unabhängig von einem besonderen Anlass für einen bestimmten Zeitraum zu speichern und für die Nutzung durch Sicherheitsbehörden bereitzuhalten. Verkehrsdaten im Sinne des § 113b Abs. 2 und 3 TKG (z.B. Rufnummern, Datum und Uhrzeit von Beginn und Ende der Verbindung, Internetprotokoll-Adressen) müssen gemäß § 113b Abs. 1 Nr. 1 TKG für zehn Wochen gespeichert werden; die Speicherpflicht für Standortdaten nach § 113b Abs. 4 TKG (z.B. die Bezeichnungen der Funkzellen bei der Nutzung mobiler Telefondienste) beträgt demgegenüber vier Wochen (vgl. § 113b Abs. 1 Nr. 2 TKG). Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden (vgl. § 113b Abs. 5 TKG). Das Gleiche gilt gemäß § 113b Abs. 6 Satz 1 TKG für Daten, die den in § 99 Abs. 2 TKG genannten Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen.

Die Speicherung der Daten hat allgemein so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können (vgl. § 113b Abs. 7 TKG). Nach § 113b Abs. 8 TKG hat der nach § 113a Abs. 1 TKG Verpflichtete die gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach § 113b Abs. 1 TKG, irreversibel zu löschen oder die irreversible Löschung sicherzustellen. In § 113c TKG werden abschließend (vgl. § 113c Abs. 2 TKG) die zulässigen Verwendungszwecke der nach § 113b TKG gespeicherten Daten normiert. So dürfen etwa gespeicherte Daten an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b TKG genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt. Die Daten sind dabei so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 113b TKG gespeichert waren (vgl. § 113c Abs. 3 Satz 2 TKG). Ob die Behörden berechtigt sind, ein Verlangen im Sinne des § 113c TKG an den Erbringer öffentlich zugänglicher Telekommunikationsdienste zu richten, ist nicht Regelungsgegenstand von § 113c TKG, sondern bestimmt sich nach den für die Strafverfolgungs- und Gefahrenabwehrbehörden jeweils maßgeblichen Regelungen des Fachrechts (vgl. BTDrucks 18/5088, S. 40). Jedoch liegt in der Norm die grundlegende Bestimmung, für welche Zwecke die Daten verwendet werden dürfen. Sie befreit diesbezüglich die Telekommunikationsunternehmen von ihrer im Übrigen geltenden Geheimhaltungspflicht (vgl. entsprechend zur damaligen Regelung BVerfGE 125, 260 <312>). § 113d TKG sieht sodann näher bestimmte Anforderungen an die Gewährleistung der Datensicherheit vor. Der nach § 113a Abs. 1 TKG Verpflichtete hat gemäß § 113e TKG sicherzustellen, dass für Zwecke der Datenschutzkontrolle jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren der gespeicherten Daten protokolliert wird und die Protokolldaten (Zeitpunkt des Zugriffs, zugreifende Personen, Zweck und Art des Zugriffs) nach einem Jahr gelöscht werden. Gemäß § 113f Abs. 1 TKG ist seitens der Bundesnetzagentur ein Anforderungskatalog zur Gewährleistung eines besonders hohen Standards der Datensicherheit und Datenqualität zu erstellen. Die Regelung des § 113g TKG ergänzt die Vorschrift des § 109 Abs. 4 TKG und verlangt die Aufnahme spezifischer Schutzmaßnahmen in das zu erstellende Sicherheitskonzept.

§ 100g StPO regelt die Voraussetzungen für die Erhebung von Verkehrsdaten. Während in Absatz 1 die Erhebung von Verkehrsdaten geregelt wird, die aus geschäftlichen Gründen bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste gespeichert werden (§ 96 TKG), legt Absatz 2 fest, unter welchen Voraussetzungen die nunmehr durch die neue Speicherpflicht gespeicherten Daten erhoben werden dürfen: Es bedarf danach den durch bestimmte Tatsachen begründeten Verdacht einer in § 100g Abs. 2 Satz 2 StPO enumerativ und abschließend (vgl. BTDrucks 18/5088, S. 31) aufgeführten besonders schweren Straftat, die auch im Einzelfall besonders schwer wiegt. Darüber hinaus muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. § 100g Abs. 4 StPO schließt zum Schutz von Berufsgeheimnisträgern im Sinne des § 53 Abs. 1 Satz 1 Nr. 1 bis 5 StPO die Erhebung von Verkehrsdaten nach § 100g Abs. 2 StPO aus. § 101a StPO überträgt den Richtervorbehalt des § 100b Abs. 1 StPO auf die Erhebung von Verkehrsdaten nach § 100g StPO und stellt konkrete Anforderungen an die Gestaltung der Entscheidungsformel und die Begründung des Beschlusses, die einzelfallbezogen sein muss und die wesentlichen Erwägungen zu der Erforderlichkeit und Angemessenheit der Maßnahme darzulegen hat (vgl. § 101a Abs. 2 StPO). § 101a Abs. 6 StPO sieht eine Pflicht zur Benachrichtigung der Beteiligten der betroffenen Telekommunikation nach Maßgabe des § 101 Abs. 4 Satz 2 bis 5 und Abs. 5 bis 7 StPO vor. Die Regelung des § 101b StPO sieht schließlich nähere Vorgaben zur statistischen Erfassung der Erhebung von Verkehrsdaten vor.

Aus den Gründen:

Der Antrag auf Erlass einer einstweiligen Anordnung ist abzulehnen.

Nach § 32 Abs. 1 BVerfGG kann das Bundesverfassungsgericht im Streitfall einen Zustand durch einstweilige Anordnung vorläufig regeln, wenn dies zur Abwehr schwerer Nachteile, zur Verhinderung drohender Gewalt oder aus einem anderen wichtigen Grund zum gemeinen Wohl dringend geboten ist. Dabei haben die Gründe, die für die Verfassungswidrigkeit des angegriffenen Hoheitsakts vorgetragen werden, grundsätzlich außer Betracht zu bleiben, es sei denn, die Verfassungsbeschwerde erwiese sich von vornherein als unzulässig oder offensichtlich

unbegründet (vgl. BVerfGE 112, 284 <291>; 121, 1 <14 f.>; stRspr). Dies lässt sich vorliegend nicht in der für das Eilverfahren gebotenen Kürze der Zeit klären. Über den Antrag auf einstweilige Anordnung ist deshalb nach Maßgabe einer Folgenabwägung zu entscheiden. Danach sind die Folgen, die eintreten würden, wenn die einstweilige Anordnung nicht erginge, die Verfassungsbeschwerde später aber Erfolg hätte, gegen die Nachteile abzuwägen, die entstünden, wenn die begehrte einstweilige Anordnung erlassen würde, der Verfassungsbeschwerde aber der Erfolg zu versagen wäre (vgl. BVerfGE 117, 126 <135>; 121, 1 <17>; stRspr). Diese Abwägung fällt zu Ungunsten der Beschwerdeführer aus.

1. Wird die Aussetzung des Vollzugs eines Gesetzes begehrt, ist bei der Folgenabwägung ein besonders strenger Maßstab anzulegen (vgl. BVerfGE 3, 41 <44>; 104, 51 <55>; 112, 284 <292>; 121, 1 <17>; stRspr). Das Bundesverfassungsgericht darf von seiner Befugnis, den Vollzug eines in Kraft getretenen Gesetzes auszusetzen, nur mit größter Zurückhaltung Gebrauch machen, da der Erlass einer solchen einstweiligen Anordnung stets ein erheblicher Eingriff in die Gestaltungsfreiheit des Gesetzgebers ist (vgl. BVerfGE 64, 67 <69>; 117, 126 <135>; 121, 1 <17>; BVerfG, Beschluss des Ersten Senats vom 6. Oktober 2015 – 1 BvR 1571/15 u.a. –, www.bverfg.de, Rn. 13). Müssen die für eine vorläufige Regelung sprechenden Gründe schon im Regelfall so schwer wiegen, dass sie den Erlass einer einstweiligen Anordnung unabdingbar machen, so müssen sie im Fall der begehrten Außervollzugsetzung eines Gesetzes darüber hinaus besonderes Gewicht haben (vgl. BVerfGE 104, 23 <27 f.>; 117, 126 <135>; 122, 342 <361 f.>; stRspr). Insoweit ist von entscheidender Bedeutung, ob die Nachteile irreversibel oder nur sehr erschwert revidierbar sind (vgl. BVerfGE 91, 70 <76 f.>; 118, 111 <123>; BVerfG, Beschluss des Ersten Senats vom 6. Oktober 2015 – 1 BvR 1571/15 u.a. –, www.bverfg.de, Rn. 13), um das Aussetzungsinteresse durchschlagen zu lassen.

2. Nach diesen Maßstäben war der Antrag auf Erlass einer einstweiligen Anordnung abzulehnen. Eine Aussetzung der durch §§ 113a, 113b TKG angeordneten Speicherpflicht von Telekommunikations-Verkehrsdaten scheidet aus (a). Auch hinsichtlich der Regelung zur Nutzung dieser Daten für bestimmte Anlässe der Strafverfolgung ist eine vorläufige Aussetzung der angegriffenen Vorschriften nicht geboten (b).

a) Eine Aussetzung des Vollzugs von §§ 113a, 113b TKG scheidet aus.

Ein besonders schwerwiegender und irreparabler Nachteil, der es rechtfertigen könnte, den Vollzug der Norm ausnahmsweise im Wege einer einstweiligen Anordnung auszusetzen, liegt in der Datenspeicherung allein nicht.

Zwar kann die gegenüber den Verpflichteten nach § 113a TKG in § 113b TKG angeordnete umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann für staatliche Zwecke, die sich zum Zeitpunkt der Speicherung der Daten nicht im Einzelnen absehen lassen, einen erheblichen Einschüchterungseffekt bewirken, weil das Gefühl entsteht, ständig überwacht zu werden. Dieser Effekt ließe sich für die Zeit zwischen dem Inkrafttreten der Norm und der Entscheidung des Bundesverfassungsgerichts selbst dann nicht rückgängig machen, wenn die Verfassungsbeschwerde in der Hauptsache Erfolg haben sollte.

Der in der Speicherung für Einzelne liegende Nachteil für ihre Freiheit und Privatheit verdichtet und konkretisiert sich jedoch erst durch einen Abruf der Daten zu einer möglicherweise irre-

parablen Beeinträchtigung. Die Datenbevorratung ermöglicht zwar den Abruf, doch führt erst dieser zu konkreten Belastungen. Das Gewicht eines denkbaren Einschüchterungseffekts hängt dann davon ab, unter welchen Voraussetzungen die bevorrateten Daten abgerufen und verwertet werden können. Je weiter die Befugnisse staatlicher Stellen insoweit reichen, desto eher müssen die Bürgerinnen und Bürger befürchten, dass diese Stellen ihr Kommunikationsverhalten überwachen (vgl. BVerfGE 121, 1 <20>). So ist mit der Speicherung allein jedoch noch kein derart schwerwiegender Nachteil verbunden, dass er die Außerkraftsetzung eines Gesetzes erforderte. Dies gilt auch für die Speicherung der Daten von Berufsgeheimnisträgern.

Ein die Aussetzung der Speicherpflicht erfordernder besonders schwerer Nachteil ergibt sich auch nicht daraus, dass beim Short Message Service (SMS) Verkehrsdaten und Kommunikationsinhalte möglicherweise nicht getrennt werden können. Nach dem klaren Wortlaut des § 113b Abs. 5 TKG dürfen der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post auf Grund dieser Vorschrift nicht gespeichert werden. Die angegriffene gesetzliche Regelung schließt damit ein technisch bedingtes „Mitloggen" von Kommunikationsinhalten aus. Wenn dies technisch zurzeit noch nicht möglich sein sollte, rechtfertigt das nicht, sich über die Maßgabe des Gesetzes hinwegzusetzen; vielmehr sind dann zunächst die technischen Bedingungen zu schaffen, um die Speicherpflicht erfüllen zu können.

b) Eine Aussetzung des Vollzugs ist auch nicht hinsichtlich der §§ 100g, 101a und 101b StPO geboten.

aa) Allerdings liegt in dem Verkehrsdatenabruf nach § 100g Abs. 1 und 2 StPO ein schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG. Ein solcher Datenabruf ermöglicht es, weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte der Betroffenen zu erlangen, gegebenenfalls sogar begrenzte Rückschlüsse auf die Gesprächsinhalte zu ziehen. Zudem weist ein Verkehrsdatenabruf eine erhebliche Streubreite auf, da er neben der Zielperson des Auskunftsersuchens notwendigerweise deren Kommunikationspartner erfasst, also vielfach Personen, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff in ihr Grundrecht aus Art. 10 Abs. 1 GG durch ihr Verhalten nicht veranlasst haben (vgl. BVerfGE 107, 299 <318 ff.>; 121, 1 <22>).

Doch hat der Gesetzgeber mit § 100g Abs. 2 StPO den Abruf von Telekommunikations-Verkehrsdaten im Sinne des § 113b TKG von qualifizierten Voraussetzungen abhängig gemacht, die das Gewicht der dem Einzelnen und der Allgemeinheit durch den Vollzug der Vorschrift drohenden Nachteile für die Übergangszeit bis zur Entscheidung über die Hauptsache hinnehmbar und im Vergleich mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen lassen.

Maßgeblich ist hierfür die Gewichtung, die auch der Entscheidung des Bundesverfassungsgerichts über den Antrag auf einstweilige Anordnung gegen das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007 zugrunde lag (vgl. BVerfGE 121, 1 <23 f.>). Das Bundesverfassungsgericht hatte dort wegen des öffentlichen Gewichts einer wirksamen Verfolgung schwerer Straftaten solche Abrufersuchen zugelassen, die der Verfolgung von Katalogtaten im Sinne des § 100a Abs. 2 StPO dienten, wenn darüber hinaus auch die Voraussetzungen des § 100a Abs. 1 StPO vorlagen, namentlich die Tat auch im Einzelfall schwer wog und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos gewesen wäre.

Diese Voraussetzungen ergeben sich nunmehr unmittelbar aus § 100g Abs. 2 Satz 1 StPO. Danach muss ein auf bestimmte Tatsachen gestützter Verdacht einer besonders schweren Straftat vorliegen, die auch im Einzelfall besonders schwer wiegt. Nach § 100g Abs. 2 Satz 1 StPO muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der Beschuldigten darüber hinaus auf andere Weise wesentlich erschwert oder aussichtslos sein und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Daneben steht ein abschließender Katalog besonders schwerer, zur Erhebung von Verkehrsdaten ermächtigender Straftaten als Teilmenge (vgl. BTDrucks 18/5088, S. 32) der in § 100a Abs. 2 StPO aufgeführten Katalogtaten. Sie begegnen für sich genommen keinen durchgreifenden verfassungsrechtlichen Bedenken gegen die Klassifizierung als Straftaten für Maßnahmen der Telekommunikationsüberwachung (vgl. BVerfGE 129, 208 <241 f.>). Sie können vielmehr als Leitlinie dafür gelten, welche Straftaten der Gesetzgeber als so schwerwiegend bewertet, dass sie auch gewichtige Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG rechtfertigen können (vgl. BVerfGE 121, 1 <25>). Der Gesetzgeber hat den Katalog in § 100g Abs. 2 Satz 2 StPO damit auf solche Straftaten reduziert, die der Bekämpfung des Terrorismus oder dem Schutz höchstpersönlicher Rechtsgüter, insbesondere Leib, Leben, Freiheit und sexuelle Selbstbestimmung, dienen. Außerdem sollen besonders schwere Straftaten umfasst sein, bei denen die gespeicherten Verkehrsdaten nach kriminalistischer Erfahrung besonders wertvolle Dienste leisten können (vgl. BTDrucks 18/5088, S. 32). Im Unterschied zu dem Katalog in § 100a Abs. 2 StPO bilden etwa bestimmte Vermögensdelikte (z.B. §§ 263, 263a, 264 StGB) keine tauglichen Anlasstaten für eine Vorratsdatenspeicherung. Angesichts dieser Einschränkungen hat das öffentliche Strafverfolgungsinteresse grundsätzlich derartiges Gewicht, dass die Aussetzung der Vorschrift durch eine einstweilige Anordnung trotz der entgegenstehenden gewichtigen Nachteile nicht geboten ist.

bb) Auch in Blick auf §§ 101a, 101b StPO ist eine einstweilige Anordnung nicht geboten. Gemäß § 101a Abs. 1 Satz 1 in Verbindung mit § 100b Abs. 1 Satz 1 StPO steht die Erhebung von Verkehrsdaten nach § 100g StPO grundsätzlich unter Richtervorbehalt; nach § 101a Abs. 1 Satz 2 StPO findet zudem in den Fällen des § 100g Abs. 2 StPO (Erhebung von Verkehrsdaten im Sinne des § 113b Abs. 1 TKG) § 100b Abs. 1 Satz 2 und 3 StPO keine Anwendung, sodass die Staatsanwaltschaft auch bei Gefahr im Verzug die Anordnung nicht selbst treffen kann. § 101a Abs. 1 Satz 1 StPO stellt zudem spezifische Anforderungen an die Begründung einer solchen Entscheidung. Ob der Gesetzgeber mit diesen Vorgaben den verfassungsrechtlichen Anforderungen im Einzelnen gerecht geworden ist, ist im Verfahren des Eilrechtsschutzes nicht abschließend zu klären. Jedenfalls ergibt sich aus der vorübergehenden Geltung dieser Vorschriften kein besonders schwerer Nachteil, der im Rahmen der hier gebotenen Folgenabwägung eine Aussetzung des Vollzugs der angegriffenen Vorschriften verlangte.

c) Ob und gegebenenfalls in welcher Weise die Europäische Grundrechtecharta oder sonstiges Unionsrecht für die Beurteilung der angegriffenen Vorschriften Bedeutung entfaltet, ist im Hauptsacheverfahren zu entscheiden. Dass Unionsrecht dazu

verpflichten könnte, die angegriffenen Vorschriften schon im Eilverfahren im Wege der einstweiligen Anordnung außer Kraft zu setzen, ist weder substantiiert vorgetragen noch ersichtlich.

Zur Wirksamkeit eines im Rahmen eines „Cold Calls" abgeschlossenen Vertrages

(**Bundesgerichtshof**, Urteil vom 21. April 2016 – I ZR 276/14 –)

1. **Ein auf eine unzulässige Telefonwerbung gemäß § 7 Abs. 1, Abs. 2 Nr. 2 UWG gestützter Schadensersatzanspruch erfasst nur solche Schäden, die vom Schutzbereich dieser Bestimmung erfasst sind.**
2. **Gegenstand des Schutzes gemäß § 7 Abs. 1 UWG ist die Verhinderung des Eindringens des Werbenden in die Privatsphäre des Verbrauchers und die geschäftliche Sphäre, insbesondere die Ungestörtheit der Betriebsabläufe des sonstigen Marktteilnehmers; es soll verhindert werden, dass dem Verbraucher und sonstigen Marktteilnehmer Werbemaßnahmen gegen seinen erkennbaren oder mutmaßlichen Willen aufgedrängt werden. Verhindert werden soll darüber hinaus, dass die belästigende Werbung zu einer Bindung von Ressourcen des Empfängers (z.B. Zeitaufwand, Kosten für Faxpapier, Vorhaltekosten von Empfangseinrichtungen, Entsorgungskosten) führt.**
3. **§ 7 Abs. 2 Nr. 2 UWG bezweckt nicht den Schutz der Entscheidungsfreiheit der Verbraucher und sonstigen Marktteilnehmer vor Belästigungen durch Werbeanrufe.**

Sachverhalt:

Die Klägerin betreibt im Internet unter dem Domainnamen „www. '.de" ein elektronisches Branchenverzeichnis. Die Beklagte bietet in ihrem Ladengeschäft mit angeschlossenem Restaurant unter der Firma „Lebens-Kost" Bio-Produkte an. Sie verfügt über eine Internet-Homepage, auf der ihre telefonischen und postalischen Kontaktdaten aufgeführt sind.

Am 3. Mai 2013 rief ein Mitarbeiter der Klägerin von sich aus und ohne vorangegangenen Kontakt bei der Beklagten in ihrem Ladengeschäft an und bot ihr einen Eintrag in das elektronische Branchenverzeichnis der Klägerin mit einer Laufzeit von 36 Monaten (beginnend am 3. Mai 2013) zu einem Gesamtpreis von 728,28 € einschließlich Umsatzsteuer an. Die Beklagte bekundete in dem Gespräch ihr grundsätzliches Interesse an einem solchen Eintrag. Die Beteiligten kamen überein, dass es zu einem weiteren Gespräch zur Absprache der Details der Vertragsbedingungen kommen sollte. Am selben Tag rief eine Mitarbeiterin der Klägerin die Beklagte ein weiteres Mal an; dieses Gespräch wurde mit Zustimmung der Beklagten aufgezeichnet. Die Mitarbeiterin der Klägerin bezog sich auf das vorangegangene Telefonat und die hierbei grundsätzlich bereits erzielte Einigung über eine entgeltliche Eintragung zu den genannten Konditionen; dies bejahte die Beklagte. Die Beklagte bestätigte ihre bereits im ersten Gespräch mitgeteilten Firmendaten, die gewünschten Eintragungsrubriken, die Laufzeit des Vertrages und die Vergütung in Höhe von 632€ netto (728,28 € brutto), wobei eine monatliche Zahlungsweise mit Raten zu je 17€ netto (20,23 brutto) vereinbart wurde. Die Beklagte bestätigte ferner die Angaben für die Rechnungsadresse und gab an , dass sie persönlich die Inhaberin der Firma „Lebens-Kost" sei . Die Beklagte wurde darauf hingewiesen, dass die Rechnung den Gesamtbetrag der Kosten enthalten werde und dass die Allgemeinen Geschäftsbedingungen (AGB) gälten, welche auf der Internetseite der Klägerin abrufbar seien.

In den AGB der Klägerin ist in § 6 eine Vorleistungspflicht des Kunden festgelegt; ein Rücktritts – oder Widerrufsrecht sehen die Bedingungen nicht vor.

Die Beklagte hat die Rechnung der Klägerin über 728,28€ spätestens am 8. Mai 2013 erhalten, hierauf jedoch trotz einer Mahnung vom 24. Mai 2013 keine Zahlungen geleistet. Eine Eintragung der Daten des Unternehmens der Beklagten in das Branchenverzeichnis der Klägerin ist jedenfalls bis zur mündlichen Berufungsverhandlung am 1. Juli 2014 nicht erfolgt. Mit Rechtsanwaltsschreiben vom 24. Mai 2013 hat die Beklagte die Anfechtung des mit der Klägerin geschlossenen Vertrags erklärt.

Die Klägerin hat beantragt, die Beklagte zu verurteilen, an sie 728,28 € nebst Zinsen in Höhe von acht Prozentpunkten über dem Basiszinssatz seit dem 8. Juni 2013 zu zahlen; hilfsweise, die Beklagte zu verurteilen, an sie 182,07 € nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz sei dem 1. Februar 2014, und im Zeitraum von Februar 2014 bis April 2016 monatlich 20,23 € zu zahlen.

Die Beklagte ist der Klage entgegengetreten und hat hilfsweise mit einem Schadensersatzanspruch wegen eines gemäß § 7 UWG unlauteren Werbeanrufs aufgerechnet.

Das Amtsgericht hat der Klage im Umfang einer Zahlungspflicht in Höhe von 20,23 € monatlich für den Zeitraum von Februar 2014 bis April 2016 stattgegeben und die Klage im Übrigen abgewiesen. Auf die Berufung der Beklagten hat das Berufungsgericht die Klage in vollem Umfang abgewiesen (LG Bonn, Urteil vom 5. August 2014 – 8 S 46/14, juris). Mit ihrer vom Berufungsgericht zugelassenen Revision, deren Zurückweisung die Beklagte beantragt, begehrt die Klägerin die Wiederherstellung des amtsgerichtlichen Urteils.

Aus den Gründen:

A. Das Berufungsgericht hat angenommen, ein Vergütungsanspruch der Klägerin sei zwar zunächst wirksam entstanden, infolge der von der Beklagten hilfsweise erklärten Aufrechnung mit einem Schadensersatzanspruch gemäß § 823 Abs. 2 BGB in Verbindung mit § 7 Abs. 2 Nr. 2 UWG aber erloschen. Zur Begründung hat es ausgeführt:

Zwischen den Parteien sei im Rahmen des zweiten Anrufs ein Vertrag über die einmalige Einstellung der Daten des Unternehmens der Beklagten in das Branchenverzeichnis der Klägerin sowie über das Aufrechterhalten und Pflegen des Eintrags (Dienstvertrag mit werkvertraglichen Elementen) zustande gekommen. Der Vertrag sei auch wirksam. Er sei nicht wegen Verstoßes gegen ein gesetzliches Verbot (§ 134 BGB in Verbindung mit Vorschriften des Gesetzes gegen den unlauteren Wettbewerb), wegen Sittenwidrigkeit gemäß § 138 BGB oder wegen der von der Beklagten erklärten Anfechtung (§ 142 BGB) nichtig. Es greife aber die Hilfsaufrechnung der Beklagten durch. Da diese zum Erlöschen der Forderung führe, gehe diese einer etwaigen Hemmung wegen der Einrede des nicht erfüllten Vertrags nach § 320 BGB vor. Der Beklagten stehe ein Schadensersatzanspruch gemäß § 823 Abs. 2 BGB in Verbindung mit § 7

Abs. 2 Nr. 2 UW G in Höhe des Vergütungsanspruchs der Klägerin zu. § 7 Abs. 2 Nr. 2 UWG sei ein Schutzgesetz im Sinne von § 8 23 Abs. 2 BGB. Eine unzumutbare Belästigung im Sinne von § 7 Abs. 2 Nr. 2 Fall 2 UWG sei ebenfalls gegeben. Die Voraussetzungen einer mutmaßlichen Einwilligung der Beklagten in den ersten Anruf des Mitarbeiters der Klägerin seien nicht gegeben.

Die Klägerin habe nicht von einem mutmaßlichen Interesse der Beklagten am Erhalt des entgeltlichen Eintragungsangebots auf dem Telefonwege ausgehen dürfen. Der erste Anruf, auf den es allein ankomme, sei auch kausal für die Eingehung der Verbindlichkeit durch die Beklagte gewesen, so dass dieser ein Schaden in Höhe des Vergütungsanspruchs der Klägerin entstanden sei. Der Beklagten sei es wegen des wirksamen Ver tragsschlusses über die entgeltliche Eintragung nicht nach Treu und Glauben im Sinne von § 242 BGB verwehrt, sich auf den Schadensersatzanspruch zu berufen. Der Vertragsschluss beruhe auf einer von der Klägerin gezielt geschaffenen rechtswidrigen Überrumpelungssituation.

B. Die hiergegen gerichtete Revision der Klägerin ist begründet und führt zur Aufhebung des Berufungsurteils und zur Zurückverweisung der Sache an das Berufungsgericht. Entgegen der Annahme des Berufungsgerichts steht der Beklagten kein Schadensersatzanspruch zu, den sie dem wirksam entstandenen und nicht erloschenen oder in seiner Durchsetzung gehemmten Vergütungsanspruch der Klägerin entgegenhalten kann. Es kommt damit auf die vom Berufungsgericht offengelassene und in der neuen Berufungsverhandlung zu klärende Frage an, ob und gegebenenfalls für welchen Zeitraum sich die Beklagte auf die Einrede des nichterfüllten Vertrags gemäß § 320 Abs. 1 BGB berufen kann.

I. Das Berufungsgericht ist davon ausgegangen, dass sich die Beklagte gegenüber der Klägerin rechtswirksam zur Zahlung von 728,28€ einschließlich Umsatzsteuer für einen Eintrag in das elektronische Branchenverzeichnis der Klägerin mit einer Laufzeit von 36 Monaten (beginnend am 3. Mai 2013) verpflichtet hat und die Zahlungsforderung nicht durch Anfechtung der Willenserklärung der Beklagten gemäß §§ 119, 123 Abs. 1, § 142 Abs. 1 BGB erloschen ist. Diese Beurteilung nimmt die Revision als für ihren Standpunkt günstig hin.

Sie lässt auch keinen Rechtsfehler erkennen.

II. Der Beklagten steht entgegen der Ansicht des Berufungsgerichts kein Schadensersatzanspruch wegen einer unzumutbaren Belästigung im Sinne von § 7 Abs. 2 Nr. 2 UWG zu, den sie der Klageforderung gemäß § 242 BGB wegen einer sofortigen Rückgewährverpflichtung (dolo agit, qui petit, quod statim redditurus est) oder, wovon das Berufungsgericht ausgegangen ist, im Wege der hilfsweise erklärten Aufrechnung gemäß § 389 BGB entgegenhalten kann.

1. Gemäß § 7 Abs. 2 Nr. 2 UWG liegt eine unzumutbare Belästigung vor, wenn gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung mit einem Telefonanruf geworben wird.

2. Ein auf eine Verletzung dieser Bestimmung in Verbindung mit § 823 Abs. 1 BGB (vgl. zur unverlangten Zusendung von E-Mails BGH, Beschluss vom 20. Mai 2009 – I ZR 218/07, GRUR 2009, 980 Rn. 10 ff. = WRP 2009, 1246 – E-Mail-Werbung II; Urteil vom 12. September 2013 – I ZR 208/12, GRUR 2013, 1259 Rn. 15 ff. = WRP 2013, 1579 – Empfehlungs-E-Mail; zu Werbeanrufen Köhler, in: Köhler/Bornkamm UWG, 34. Aufl. § 7 Rn. 14, 119; Koch, in: Ullmann, JurisPK-UWG, 3. Aufl., § 7 Rn. 263; Leible, in: MünchKomm. UWG, 2. Aufl., § 7 UWG Rn. 40) oder § 823 Abs. 2 BGB (vgl. dazu Köhler, in: Köhler/Bornkamm a.a.O. Einl. Rn. 7.5 m.w.N.) gestützter Schadensersatzanspruch der Beklagten scheidet im Streitfall bereits deshalb aus, weil es an einem vom Schutzbereich des § 7 Abs. 2 Nr. 2 UWG erfassten Schaden fehlt.

a) Ersatzfähig ist nur der Schaden, der vom Schutzbereich der verletzten Norm erfasst ist (BGH, Urteil vom 22. September 1999 – I ZR 48/97, GRUR 2000, 226, 227 = WRP 2000, 101 – Planungsmappe; Urteil vom 4. Juli 2014 – V ZR 229/13, NJW 2014, 3727 Rn. 15 ; Köhler, in: Köhler/Bornkamm a.a.O. § 9 Rn. 1.13 ; Oetker, in: MünchKomm.BGB, 7. Aufl., § 249 Rn. 122 ff.; Palandt/Grüneberg, BGB, 75. Aufl., Vor § 249 Rn. 29). Eine Haftung besteht nur für diejenigen äquivalent und adäquat verursachten Schadensfolgen, die aus dem Bereich der Gefahren stammen, zu deren Abwendung die verletzte Norm erlassen oder die verletzte Vertragspflicht übernommen wurde (st. Rspr.; vgl. BGH, Urteil vom 26. Februar 2013 – VI ZR 116/12, NJW 2013, 1679 Rn. 12 m.w.N.).

b) Die Bestimmung des § 7 UWG, dessen Maßstäbe zur Vermeidung von Wertungswidersprüchen auch im Rahmen der Prüfung eines Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb gemäß § 823 Abs. 1 BGB zur Anwendung kommen (BGH, GRUR 2009, 980 Rn. 14 ff. – E-Mail-Werbung II; GRUR 2013, 1259 Rn. 20 – Empfehlungs-E-Mail; Köhler, in: Köhler Bornkamm a.a.O. § 7 Rn. 14; Koch, in: Ullmann, JurisPK – UWG a.a.O. § 7 Rn. 153), soll Marktteilnehmer vor einer unzumutbaren Belästigung bewahren (§ 7 Abs. 1 Satz 1 UWG). Gegenstand des Schutzes ist die Verhinderung des Eindringens des Werbenden in die Privatsphäre des Verbrauchers und die geschäftliche Sphäre, insbesondere die Ungestörtheit der Betriebsabläufe des sonstigen Marktteilnehmers; es soll verhindert werden, dass dem Verbraucher und sonstigen Marktteilnehmer Werbemaßnahmen gegen seinen erkennbaren oder mutmaßlichen Willen aufgedrängt werden (vgl. Begründung zum Regierungsentwurf UWG 2004, BT-Drucks. 15/1487, Seite 20 f.; BGH, Urteil vom 1. April 2004 – I ZR 227/01, GRUR 2004, 699, 701 = WRP 2004, 1160 – Ansprechen in der Öffentlichkeit I; Urteil vom 9. September 2004 – I ZR 93/02, GRUR 2005, 443, 444 = WRP 2005, 485 – Ansprechen in der Öffentlichkeit II ; Urteil vom 1. Juni 2006 – I ZR 167/03, GRUR 2007, 164 Rn. 8 f. = WRP 2007, 67 – Telefax-Werbung II; Urteil vom 11. März 2010 – I ZR 27/08, GRUR 2010, 939 Rn. 20 = WRP 2010, 1249 – Telefonwerbung nach Unternehmerwechsel; Urteil vom 3. März 2011 – I ZR 167/09, GRUR 2011, 747 Rn. 18 = WRP 2011, 1054 – Kreditkartenübersendung; Leible, in: MünchKomm. UWG a.a.O. § 7 Rn. 1; Köhler, in: Köhler/Bornkamm a.a.O. § 7 Rn. 2; Ohly, in: Ohly/Sosnitza, U WG, 6. Aufl., § 7 Rn. 1; Koch, in: Ullmann, JurisPK – UWG a.a.O. § 7 Rn. 3 f.; Pahlow, in: Großkomm.UWG, 2. Aufl., § 7 Rn. 1; Mehler, in: Büscher/Dittmer/Schiwy, Gewerblicher Rechtsschutz Urheberrecht Medienrecht, 3. Aufl., § 7 UWG Rn. 3). Verhindert werden soll darüber hinaus, dass die belästigende Werbung zu einer Bindung von Ressourcen des Empfängers (z.B. Zeitaufwand, Kosten für Faxpapier, Vorhaltekosten von Empfangseinrichtungen, Entsorgungskosten) führt (vgl. BGH, GRUR 2007, 164 Rn. 9 – Telefax-Werbung II; Leible, in: MünchKomm. UWG a.a.O. § 7 Rn. 1; Köhler, in: Köhler/Bornkamm a.a.O. § 7 Rn. 2; Pahlow, in: Großkomm. UWG a.a.O. § 7 Rn. 1; Schöler, in: Harte/Henning, UWG, 3. Aufl., § 7 Rn. 36). Dagegen bezweckt § 7 Abs. 2 Nr. 2 UWG nicht den Schutz der Entscheidungsfreiheit der Verbraucher und sonstigen Marktteilnehmer (Leible, in: MünchKomm. UWG a.a.O. § 7 UWG

Rn. 1; Köhler, in: Köhler/Bornkamm a.a.O. § 7 Rn. 3 ; Ohly, in: Ohly/Sosnitza a.a.O. § 7 Rn. 1; Pahlow, in: Großkomm. UWG a.a.O. § 7 Rn. 20; aA Fezer/Mankowski, UWG, 2. Aufl., § 7 Rn. 43; Mehler, in: Büscher/ Dittmer/Schiwy a.a.O. § 7 Rn. 5; Schöler, in: Harte/Henning a.a.O. § 7 Rn. 36). Das Erfordernis einer über die Belästigung hinausgehenden Beeinträchtigung der Entscheidungsfreiheit, etwa unter dem Gesichtspunkt der Überrumpelung, lässt sich dem Wortlaut der Bestimmung des § 7 UWG nicht entnehmen (vgl. Köhler, in: Köhler/Bornkamm a.a.O. § 7 Rn. 3). Die Einbeziehung der Entscheidungsfreiheit des Umworbenen in den Schutzbereich von § 7 UWG würde zudem die auch durch das Unionsrecht nahegelegten systematischen Grenzen zu § 4 a Abs. 1 Satz 2 Nr. 1 UWG verwischen (vgl. zu § 4 Nr. 1 UWG aF Leible, in: MünchKomm. UWG a.a.O. § 7 Rn. 1; Ohly, in: Ohly/Sosnitza a.a.O. § 7 Rn. 16; ders., GRUR 2016, 3, 5; Beater, WRP 2012, 6, 10 f.).

c) Vorliegend hat das Berufungsgericht keinen Schaden festgestellt, der in den Schutzbereich des § 7 Abs. 2 Nr. 2 UWG fällt.

aa) Das Berufungsgericht hat angenommen, ein ersatzfähiger Schaden der Beklagten liege in der Belastung der Beklagten durch den Vergütungsanspruch, den die Klägerin gegen die Beklagte dadurch erlangt habe, dass es zwischen den Parteien beim zweiten Telefonanruf zu einem wirksamen Vertragsschluss über den vergütungspflichtigen Eintrag in das von der Klägerin betriebene elektronische Branchenverzeichnis gekommen sei. Insoweit sei ohne Bedeutung, dass im Hinblick auf den zweiten Anruf möglicherweise eine Einwilligung der Beklagten vorgelegen habe. Entscheidend sei allein der ohne Einwilligung der Beklagten erfolgte erste Anruf, bei dem bereits sämtliche Grundlagen des späteren Vertragsschlusses gelegt worden seien. Der Vertragsschluss beruhe auf einer gezielt geschaffenen und rechtswidrigen Überrumpelungssituation durch den ersten Anruf, vor der § 7 Abs. 2 UWG gerade schützen wolle.

bb) Dem kann nicht zugestimmt werden.

(1) Der zur Belastung mit der Zahlungsverbindlichkeit führende Vertragsschluss ist nach den rechtsfehlerfrei getroffenen Feststellungen des Berufungsgerichts bei dem zweiten Telefonat erfolgt. Der zweite Anruf war jedoch durch die zuvor von der Beklagten ausdrücklich erklärte Einwilligung gedeckt, so dass insoweit die Annahme einer unerlaubten Handlung gemäß § 7 Abs. 2 Nr. 2 UWG sowie § 823 Abs. 1 BGB ausscheidet.

(2) Der Umstand, dass der erste Anruf, bei dem die Beklagte ihre Einwilligung in einen weiteren Anruf erklärt hat, möglicherweise nicht durch eine ausdrücklich erklärte oder mutmaßliche Einwilligung der Beklagten gedeckt war, führt zu keiner abweichenden Beurteilung. Entgegen der Ansicht des Berufungsgerichts gehört eine von ihm insoweit angenommene Überrumpelungssituation und die damit einhergehende Beeinträchtigung der Entscheidungsfreiheit nicht zum Bereich der Gefahren, die § 7 Abs. 2 Nr. 2 UWG verhindern will.

Es ist vom Berufungsgericht auch nicht festgestellt noch sonst ersichtlich, dass der Vertragsschluss als eine Folge der Störung der Betriebsabläufe der Beklagten durch den ersten Telefonanruf anzusehen ist.

III. Das Berufungsurteil stellt sich auch nicht aus anderen Gründen als richtig dar (§ 561 ZPO).

1. Schäden, die der Beklagten infolge eines belästigenden Eindringens in ihre geschäftliche Sphäre durch den Einsatz von Ressourcen entstanden sind und die der Klageforderung entgegengehalten werden könnten, sind vom Berufungsgericht nicht festgestellt worden.

2. Im Streitfall kommt auch kein Schadensersatzanspruch der Beklagten gemäß §§ 3, 9 UWG in Verbindung mit § 4 Nr. 1 UWG aF in Betracht. Bei der gebotenen richtlinienkonformen Auslegung dieser Bestimmung liegt eine Beeinträchtigung der Entscheidungsfreiheit der Verbraucher im Sinne von § 4 Nr. 1 UWG aF nur dann vor, wenn der Handelnde diese Freiheit gemäß Art. 8 und 9 der Richtlinie 2005/29/EG durch Belästigung, Nötigung oder durch unzulässige Beeinflussung im Sinne des Art. 2 Buchst. j der Richtlinie 2005/29/EG erheblich beeinträchtigt (vgl. BGH, Urteil vom 3. März 2011 – I ZR 167/09, GRUR 2011, 747 Rn. 26 = WRP 2011, 1321 – Kreditkartenübersendung; Urteil vom 3. April 2014 – I ZR 96/13, GRUR 2014, 1117 Rn. 26 = WRP 2014, 1301 – Zeugnisaktion; Urteil vom 19. März 2015 – I Z R 157/13, GRUR 2015, 1134 Rn. 31 = WRP 2015, 1341 – Schufa-Hinweis). Dafür ist Voraussetzung, dass die im Streitfall allein in Betracht kommende Belästigung die Entscheidungs- oder Verhaltensfreiheit des Verbrauchers oder sonstigen Marktteilnehmers im konkreten Fall unter Berücksichtigung aller Umstände tatsächlich oder voraussichtlich erheblich beeinträchtigt und dieser dadurch tatsächlich oder voraussichtlich veranlasst wird, eine geschäftliche Entscheidung zu treffen, die er anderenfalls nicht getroffen hätte (Art. 8 der Richtlinie 2005/29/E G). Für eine solche Beeinträchtigung der Entscheidungsfreiheit fehlen im Streitfall hinreichende Anhaltspunkte.

Nach den getroffenen Feststellungen hat sich die Beklagte in Kenntnis der Bedingungen des kostenpflichtigen Angebots der Klägerin ausdrücklich mit einem zweiten Telefonanruf einverstanden erklärt. Im Rahmen seiner Prüfung eines Irrtums im Sinne von § 119 Abs. 1 BGB hat das Berufungsgericht zudem festgestellt, dass die von ihm in Augenschein genommene Aufzeichnung des zweiten Telefongesprächs den Eindruck vermittele, die Beklagte habe – nicht zuletzt vor dem Hintergrund der wiederholten Nachfragen von Seiten der Klägerin – sehr wohl gewusst, was sie gesagt und erklärt hat.

C. Danach ist das angefochtene Urteil aufzuheben und die Sache zur neuen Verhandlung und Entscheidung, auch über die Kosten der Revision, an das Berufungsgericht zurückzuverweisen (§ 563 Abs. 1 ZPO). Der Senat vermag nicht in der Sache selbst zu entscheiden, weil sie nicht zur Endentscheidung reif ist. Das Berufungsgericht hat die Frage offengelassen, ob und für welchen Zeitraum sich die Beklagte bejahendenfalls auf die Einrede des nichterfüllten Vertrags gemäß § 320 Abs. 1 BGB berufen kann, weil die Klägerin den Werbeeintrag für die Beklagte nach deren Darstellung nicht vorgenommen hat.

Das Berufungsgericht hat deshalb – von seinem Rechtsstandpunkt aus folgerichtig – die insoweit notwendigen Feststellungen bislang nicht getroffen. So hat es insbesondere nicht geprüft, welche Partei vorleistungspflichtig ist. Ferner wird das Berufungsgericht festzustellen haben, ob die Klägerin den Werbeeintrag für die Beklagte auch nach Schluss der Berufungsverhandlung weiterhin nicht vorgenommen hat. In diesem Zusammenhang wird das Berufungsgericht auch zu prüfen haben, ob die Beklagte gemäß § 326 BGB von der Leistungspflicht ganz oder teilweise frei geworden ist, weil der Klägerin durch Zeitablauf – zwischen den Parteien war eine Leistung im Zeitraum vom 3. Mai 2013 bis 2. Mai 2016 vereinbart – die Erbringung der Leistung in dieser Zeit unmöglich geworden ist (§ 275 Abs. 1 BGB), oder ob die Klägerin die Leistung auch während eines späteren Zeitraums nachholen kann.

Entschädigung nach § 15 Abs. 2 AGG aufgrund einer Diskriminierung wegen Schwerbehinderung (Ls)

(**Bundesarbeitsgericht**, Urteil vom 11. August 2016 – 8 AZR 375/15 –)

Lädt eine Stadt einen gemäß vorgelegtem Lebenslauf schwerbehinderten Bewerber nicht gemäß § 82 SGB IX zu einem Vorstellungsgespräch ein, begründet dies die Vermutung, dass der Bewerber wegen seiner Schwerbehinderung aus den Auswahlverfahren vorzeitig ausgeschieden und dadurch benachteiligt wurde, es sei denn, dass sich auf der Grundlage der Angaben des Bewerbers davon ausgegangen werden kann, dass diesem die erforderliche fachliche Eignung offensichtlich fehlt.

(Nicht amtlicher Leitsatz)

Einsicht in Personalakten unter Hinzuziehung eines Rechtsanwalts (Ls)

(**Bundesarbeitsgericht**, Urteil vom 12. Juli 2016 – 9 AZR 791/14 –)

1. **§ 83 Abs. 1 BetrVG, nach dem der Arbeitnehmer das Recht hat, in die über ihn geführten Personalakten Einsicht zu nehmen, und dazu ein Mitglied des Betriebsrats hinzuzuziehen, begründet keinen Anspruch auf Einsichtnahme unter Hinzuziehung eines Rechtsanwalts.**
2. **Ein solcher Anspruch folgt weder aus der Rücknahmepflicht des Arbeitgebers (§ 241 Abs. 2 BGB) noch aus dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), wenn der Arbeitgeber dem Arbeitnehmer erlaubt, Kopien von den Schriftstücken der Personalakte zu fertigen. Vielmehr ist damit dem einem Beseitigungs- und Korrekturanspruch vorgelagerten Transparenzschutz genügt.**

(Nicht amtliche Leitsätze)

An- und Abmeldepflicht freigestellter Betriebsratsmitglieder (Ls)

(**Bundesarbeitsgericht**, Beschluss vom 24. Januar 2016 – 7 ABR 2014 –)

1. **Auch freigestellte Mitglieder des Betriebsrats sind verpflichtet, sich beim Arbeitgeber unter Angabe der voraussichtlichen Dauer der Betriebsratstätigkeit abzumelden, wenn sie außerhalb des Betriebes erforderlichen Betriebsratsaufgaben nachgehen, und sich bei der Rückkehr zurückzumelden.**
2. **Über den Ort und den Anlass der Tätigkeit sind keine Angaben zu machen.**

(Leitsatz 2 nicht amtlich)

Auskunft eines freigestellten Betriebsratsmitglieds über Gehälter vergleichbarer Arbeitnehmer

(**Bundesarbeitsgericht**, Urteil vom 4. November 2015 – 7 AZR 972/13 –)

1. **Nach § 37 Abs. 4 Satz 1 BetrVG darf das Arbeitsentgelt von Mitgliedern des Betriebsrats einschließlich eines Zeitraums von einem Jahr nach Beendigung der Amtszeit nicht geringer bemessen werden als das Arbeitsentgelt vergleichbarer Arbeitnehmer mit betriebsüblicher beruflicher Entwicklung.**
2. **Verlangt das Betriebsratsmitglied vom Arbeitgeber Auskünfte, um eine betriebsübliche Beförderungspraxis als Voraussetzung einer entsprechenden Gehaltssteigerung darlegen zu können, hat das Betriebsratsmitglied unter Berücksichtigung der ihm zugänglichen Tatsachen vorzutragen, mit welchen Arbeitnehmern es aus seiner Sicht vergleichbar ist und aus welchen Umständen zu schließen ist, dass die Mehrzahl der mit ihm vergeichbaren Arbeitnehmer die behauptete Beförderung erfahren hat. Verfügt das Betriebsratsmitglied etwa wegen der Größe des Betriebs und der Vielzahl vergleichbarer Arbeitnehmer nicht über ausreichende Erkenntnismöglichkeiten, kann es genügen, Referenzfälle darzulegen, aus denen sich mit hinreichender Wahrscheinlichkeit auf eine betriebsübliche Beförderungspraxis in dem Zeitraum seiner Zugehörigkeit zum Betriebsrat schließen lässt.**
3. **Kann das Betriebsratsmitglied das Bestehen eines Anspruchs auf Gehaltsanpassung nur prüfen, wenn es Auskunft über die Gehaltsentwicklung vergleichbarer Arbeitnehmer mit betriebsüblicher beruflicher Entwicklung erhält, kommt ein Anspruch auf Auskunft nach §§ 611, 242 BGB i.V.m. § 37 Abs. 4 BertrVG in Betracht. Dies gilt für die Gehaltshöhe vergleichbarer Arbeitnehmer, deren Kenntnis sich dem betroffenen Betriebsratsmitglied entzieht und über die der Arbeitgeber unschwer Auskunft geben kann.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien streiten darüber, ob dem Kläger als Betriebsratsmitglied unter Berücksichtigung der beruflichen Entwicklung vergleichbarer Arbeitnehmer oder seines fiktiven beruflichen Werdegangs eine höhere Vergütung zusteht und ob ihm in diesem Zusammenhang von der Beklagten Auskünfte zu erteilen sind.

Der Kläger hat behauptet, die Entwicklung vom Lead zum Acting Area Manager und anschließend zum Area Manager sei im Betrieb üblich. Es gebe bei der Beklagten eine strukturelle Beförderungspraxis. Deshalb stehe auch ihm als freigestelltem Betriebsratsmitglied nach § 37 Abs. 4 BetrVG ab 1. Januar 2013 die Vergütung eines Acting Area Managers zu. Ansonsten werde er wegen seines Betriebsratsamts benachteiligt und gegenüber anderen Arbeitnehmern sachwidrig ungleich behandelt. Da ihm die in der Sphäre der Beklagten liegenden anspruchsbegründenden Umstände nicht bekannt seien, sei die Beklagte verpflichtet, ihm die zur Begründung seines Anspruchs erforderlichen Auskünfte zu erteilen. Dazu gehöre auch die Angabe der vergleichbaren Arbeitnehmer. Aufgrund der Größe des Betriebs könne der Kläger nicht wissen und darlegen, welche Leads 2006 beschäftigt worden seien, welche fachlichen und persönlichen Qualifikationen sie gehabt hätten und wer von ihnen inzwischen zum Acting Area Manager befördert wurde.

Der Kläger hat zuletzt beantragt, die Beklagte zu verurteilen,

1. Auskunft über die einzelnen Gehaltssteigerungen anlässlich der in den Jahren 2011 und 2012 vom Lead zum Acting Area Manager beförderten Mitarbeiter zu erteilen;
2. ihm die aus der Auskunft gemäß Ziffer 1 sich ergebende durchschnittliche Gehaltssteigerung der zum Acting Area Manager beförderten Leads im Zeitraum vom 1. Januar 2011 bis 31. Dezember 2012 zu dem bisher ausgezahlten Gehalt ab dem 1. Januar 2013 nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz zu zahlen;

hilfsweise,

3. a) Auskünfte über die Arbeitnehmerinnen und Arbeitnehmer zu erteilen, die im Jahr 2006 als Lead bei der Beklagten beschäftigt waren und über einen Berufsabschluss eines Meisters oder den Abschluss eines Hochschulstudiums verfügen;

3. b) Auskunft über die Namen der Arbeitnehmerinnen und Arbeitnehmer zu erteilen, die zum 1. Januar 2013 von den unter a) Benannten zwischenzeitlich aa) ausgeschieden sind, bb) eine gewerbliche Tätigkeit im Betrieb ausüben unterhalb der Stufe des Leads oder cc) eine Tätigkeit im Gehaltsgefüge der Angestellten, also des „Level 3 Salary" oder darüber hinaus ausüben;

4. Auskunft darüber zu erteilen, welche Auswahlkriterien und welche Bewertungen in einem Assessment-Center angewendet werden, wenn eine Stelle mit der Tätigkeit Acting Area Manager mit einer Arbeitnehmerin oder einem Arbeitnehmer mit der Tätigkeit Lead besetzt werden soll;

5 Auskunft über die einzelnen Gehaltssteigerungen anlässlich der in den Jahren 2011 und 2012 vom Lead zum Acting Area Manager beförderten Mitarbeiter zu erteilen;

6. dem Kläger die aus der Auskunft gemäß Ziffer 5 sich ergebende durchschnittliche Gehaltssteigerung der zum Acting Area Manager beförderten Leads im Zeitraum vom 1. Januar 2011 bis 31. Dezember 2012 zu dem bisher ausgezahlten Gehalt ab dem 1. Januar 2013 nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz zu zahlen.

Aus den Gründen:

Das Landesarbeitsgericht hat die Klage zu Recht abgewiesen. Es bestehen weder die geltend gemachten Auskunftsansprüche, noch ist ein Zahlungsanspruch im Hinblick auf die berufliche Entwicklung vergleichbarer Arbeitnehmer oder des fiktiven beruflichen Werdegangs des Klägers begründet.

I. Der auf Auskunft gerichtete Antrag zu 1. hat keinen Erfolg.

1. Der Antrag zu 1. ist zulässig. Er ist nach gebotener Auslegung insbesondere hinreichend bestimmt i.S.v. § 253 Abs. 2 Nr. 2 ZPO. Der Kläger hat den Auskunftsantrag zu 1. in ein Stufenverhältnis zu dem unbezifferten Zahlungsantrag zu 2. gestellt.

a) Nach § 254 ZPO kann mit der Klage auf Rechnungslegung oder auf Vorlegung eines Vermögensverzeichnisses oder auf Abgabe einer eidesstattlichen Versicherung eine Klage auf Herausgabe desjenigen verbunden werden, was der Beklagte aus dem zugrunde liegenden Rechtsverhältnis schuldet. Bei der Stufenklage wird ein der Höhe oder dem Gegenstand nach noch unbekannter und daher entgegen § 253 Abs. 2 Nr. 2 ZPO noch nicht zu beziffernder Leistungsanspruch zugleich mit den zu seiner Konkretisierung erforderlichen Hilfsansprüchen (auf Auskunft und ggf. Richtigkeitsversicherung) erhoben. Entgegen dem Gesetzeswortlaut werden von § 254 ZPO Informationsansprüche jeglicher Art erfasst, sofern sie dazu dienen, den Leistungsantrag gemäß § 253 Abs. 2 Nr. 2 ZPO beziffern zu können (Zöller/Greger ZPO 30. Aufl. § 254 Rn. 6). Die Auskunft im Rahmen der Stufenklage ist lediglich ein Hilfsmittel, um die (noch) fehlende Bestimmtheit des Leistungsanspruchs herbeizuführen. Die der Stufenklage eigentümliche Verknüpfung von unbestimmtem Leistungsanspruch und vorbereitendem Auskunftsanspruch steht dagegen nicht zur Verfügung, wenn die Auskunft überhaupt nicht dem Zwecke einer Bestimmbarkeit des Leistungsanspruchs dienen, sondern dem Kläger sonstige mit der Bestimmbarkeit als solcher nicht in Zusammenhang stehende Informationen über seine Rechtsverfolgung verschaffen soll (BGH 2. März 2000 – III ZR 65/99 – zu 1 a der Gründe).

b) Auskünfte über die in den Jahren 2011 und 2012 beförderten Arbeitnehmer würden dem Kläger nach dem Wortlaut des Antrags Informationen verschaffen, die mit der Bestimmbarkeit des Zahlungsanspruchs in einem prozessual gebotenen Zusammenhang stehen. Der Kläger verlangt mit dem Antrag zu 1., dass die Beklagte ihm Auskunft über die einzelnen Gehaltssteigerungen anlässlich der in den Jahren 2011 und 2012 vom Lead zum Acting Area Manager beförderten Mitarbeiter erteilt. Das genügt für die Zulässigkeit des Auskunftsanspruchs im Rahmen einer Stufenklage.

Mit der Auskunft über die „einzelnen Gehaltssteigerungen" geht es dem Kläger darüber hinaus darum zu erfahren, welche Leads in den Jahren 2011 und 2012 zum Acting Area Manager aufgestiegen sind und eine entsprechende Vergütung erhalten, um danach vortragen zu können, dass es sich hierbei um eine betriebsübliche berufliche Entwicklung handelt. Der Kläger begehrt somit nicht nur Auskunft über die Höhe der Gehaltssteigerungen, die sich nach Gehaltsstufen des im Betrieb der Beklagten geltenden Vergütungssystems richten. Der Antrag ist vielmehr auch auf die namentliche Benennung der beförderten Leads gerichtet. Dies hat der Kläger in der mündlichen Verhandlung vor dem Landesarbeitsgericht am 1. Oktober 2013 ausweislich des Terminsprotokolls klargestellt.

Mit diesem Verständnis ist der Antrag hinreichend bestimmt i.S.v. § 253 Abs. 2 Nr. 2 ZPO.

2. Das mit dem Antrag zu 1. geforderte Auskunftsbegehren hat in der Sache keinen Erfolg.

a) Für den geltend gemachten Auskunftsanspruch besteht keine ausdrückliche gesetzliche Grundlage. Der Kläger stützt sein Klagebegehren auf § 37 Abs. 4 BetrVG und auf § 78 BetrVG. Eine Auskunftspflicht des Arbeitgebers ist dort nicht vorgesehen. Es gibt auch keine allgemeine Pflicht zur Auskunftserteilung im Arbeitsverhältnis. Auch die Zivilprozessordnung kennt keine – über die anerkannten Fälle der Pflicht zum substantiierten Bestreiten hinausgehende – Aufklärungspflicht der nicht darlegungs- und beweisbelasteten Partei. Weder die Aufgabe der Wahrheitsfindung noch das Rechtsstaatsprinzip hindern den Gesetzgeber daran, den Zivilprozess der Verhandlungsmaxime zu unterstellen und es in erster Linie den Parteien zu überlassen,

die notwendigen Tatsachenbehauptungen aufzustellen und die Beweismittel zu benennen. Darauf beruht die Regelung der Behauptungs- und Beweislast im Zivilprozess. Im Grundsatz gilt, dass keine Partei gehalten ist, dem Gegner das Material für dessen Obsiegen im Prozess zu verschaffen (BAG 1. Dezember 2004 – 5 AZR 664/03 – zu II 1 der Gründe, BAGE 113, 55; BGH 11. Juni 1990 – II ZR 159/89 – zu IV 2 der Gründe).

b) Es ist allerdings gewohnheitsrechtlich anerkannt, dass Auskunftsansprüche nach Treu und Glauben (§ 242 BGB) bestehen können, wenn die Rechtsbeziehungen zwischen den Parteien es mit sich bringen, dass der Berechtigte in entschuldbarer Weise über Bestehen und Umfang seines Rechts im Ungewissen ist und der Verpflichtete die zur Beseitigung der Ungewissheit erforderliche Auskunft unschwer geben kann. Der Ausgleich gestörter Vertragsparität gehört zu den Hauptaufgaben des Zivilrechts (BVerfG 19. Oktober 1993 – 1 BvR 567/89, 1 BvR 1044/89 – BVerfGE 89, 214, 231 ff.). Ein Ungleichgewicht kann auch aus einem erheblichen Informationsgefälle resultieren. Eine solche Situation kann es erfordern, Auskunftsansprüche zu statuieren, die eine Vertragspartei zur Wahrnehmung ihrer materiellen Rechte aus dem Vertrag benötigt. Im Regelfall setzt das einen dem Grunde nach feststehenden Leistungsanspruch voraus. Innerhalb vertraglicher Beziehungen, insbesondere bei Dauerschuldverhältnissen, kann der Auskunftsanspruch darüber hinaus die Funktion haben, dem Berechtigten Informationen auch schon über das Bestehen des Anspruchs dem Grunde nach zu verschaffen. Ein Rechtsgrund hierfür kann sich aus spezifischen Pflichten zur Rücksichtnahme im Arbeitsverhältnis ergeben (§ 241 Abs. 2 BGB), wenn ein billigenswertes Interesse an einer Auskunft besteht, soweit die Verpflichtung keine übermäßige Belastung des Vertragspartners darstellt und die gesetzliche Verteilung der Darlegungs- und Beweislast im Prozess berücksichtigt bleibt. Die Darlegungs- und Beweissituation darf nicht durch die Gewährung materiell-rechtlicher Auskunftsansprüche unzulässig verändert werden (BAG 14. November 2012 – 10 AZR 783/11 – Rn. 62, BAGE 143, 292; 1. Dezember 2004 – 5 AZR 664/03 – zu II 1 der Gründe, BAGE 113, 55). Außerdem muss der Berechtigte die Wahrscheinlichkeit seines Anspruchs dargelegt haben (vgl. etwa BAG 21. November 2000 – 9 AZR 665/99 – zu I 2 b der Gründe, BAGE 96, 274; ErfK/Preis 15. Aufl. § 611 BGB Rn. 633 m.w.N.). Mit dieser Maßgabe kann uU ein Auskunftsanspruch gemäß §§ 611, 242 BGB i.V.m. § 37 Abs. 4 BetrVG in Betracht kommen, wenn ein Mitglied des Betriebsrats eine betriebsübliche Steigerung der Vergütung mit derjenigen ihm vergleichbarer Arbeitnehmer geltend machen will, auch wenn der Anspruch dem Grunde nach noch nicht feststeht, aber eine gewisse Wahrscheinlichkeit für das Bestehen des Anspruchs nach § 37 Abs. 4 Satz 1 BetrVG gegeben ist.

c) Danach kann der Kläger die mit dem Antrag zu 1. begehrten Auskünfte nicht beanspruchen.

aa) Nach § 37 Abs. 4 Satz 1 BetrVG darf das Arbeitsentgelt von Mitgliedern des Betriebsrats einschließlich eines Zeitraums von einem Jahr nach Beendigung der Amtszeit nicht geringer bemessen werden als das Arbeitsentgelt vergleichbarer Arbeitnehmer mit betriebsüblicher beruflicher Entwicklung. Dies gilt nach § 37 Abs. 4 Satz 2 BetrVG auch für allgemeine Zuwendungen des Arbeitgebers.

(1) Nach der ständigen Rechtsprechung des Senats soll § 37 Abs. 4 Satz 1 BetrVG sicherstellen, dass Mitglieder des Betriebsrats weder in wirtschaftlicher noch in beruflicher Hinsicht gegenüber vergleichbaren Arbeitnehmern mit betriebsüblicher beruflicher Entwicklung Nachteile erleiden. Vergleichbar sind Arbeitnehmer, die im Zeitpunkt der Amtsübernahme ähnliche, im Wesentlichen gleich qualifizierte Tätigkeiten ausgeführt haben wie der Amtsträger und dafür in gleicher Weise wie dieser fachlich und persönlich qualifiziert waren. Üblich ist eine Entwicklung, die vergleichbare Arbeitnehmer bei Berücksichtigung der normalen betrieblichen und personellen Entwicklung in beruflicher Hinsicht genommen haben. Eine Üblichkeit entsteht aufgrund gleichförmigen Verhaltens des Arbeitgebers und einer von ihm aufgestellten Regel. Dabei muss der Geschehensablauf so typisch sein, dass aufgrund der Gegebenheiten und Gesetzmäßigkeiten zumindest in der überwiegenden Anzahl der vergleichbaren Fälle mit der jeweiligen Entwicklung gerechnet werden kann. Da § 37 Abs. 4 Satz 1 BetrVG das Benachteiligungsverbot des § 78 Satz 2 BetrVG konkretisiert, darf die Anwendung der Vorschrift auch nicht zu einer Begünstigung des Betriebsratsmitglieds gegenüber anderen Arbeitnehmern führen. Deshalb ist die Übertragung höherwertiger Tätigkeiten nur dann betriebsüblich, wenn diese dem Betriebsratsmitglied nach den betrieblichen Gepflogenheiten hätten übertragen werden müssen oder die Mehrzahl der vergleichbaren Arbeitnehmer einen solchen Aufstieg erreicht. Nicht ausreichend ist es deshalb, dass das Betriebsratsmitglied bei der Amtsübernahme in seiner bisherigen beruflichen Entwicklung einem vergleichbaren Arbeitnehmer vollkommen gleich gestanden hat oder die Besserstellung eines oder mehrerer vergleichbarer Arbeitnehmer auf individuellen, nur auf diese bzw. diesen Arbeitnehmer persönlich zugeschnittenen Gründen beruht (BAG 14. Juli 2010 – 7 AZR 359/09 – Rn. 30).

(2) Für das Betriebsratsmitglied als Anspruchsteller können nicht unerhebliche Schwierigkeiten bestehen, diese Anspruchsvoraussetzungen schlüssig darzulegen, weil es keinen vollständigen Überblick über die ihm vergleichbaren Arbeitnehmer und deren Gehaltsentwicklungen hat. Das Bestehen eines Anspruchs auf Gehaltsanpassung kann das Betriebsratsmitglied aber nur prüfen, wenn es Auskunft über die Gehaltsentwicklung vergleichbarer Arbeitnehmer mit betriebsüblicher beruflicher Entwicklung erhält. Im Gegensatz zu dem betroffenen Mitglied des Betriebsrats kann der Arbeitgeber unschwer Auskunft über die Gehaltshöhe seiner Arbeitnehmer geben (vgl. BAG 9. Januar 2005 – 7 AZR 208/04 – zu I 1 der Gründe). Dies hat der Senat entschieden für Fälle, in denen die vergleichbaren Arbeitnehmer, deren Gehaltsentwicklung nachgezeichnet werden sollte, namentlich bezeichnet waren.

(3) Geht es – wie hier – zunächst darum, eine betriebsübliche Beförderungspraxis als Voraussetzung einer entsprechenden Gehaltssteigerung darzulegen, hat das Mitglied des Betriebsrats unter Berücksichtigung der ihm zugänglichen Tatsachen vorzutragen, mit welchen Arbeitnehmern es aus seiner Sicht vergleichbar ist und aus welchen Umständen auf die hinreichende Wahrscheinlichkeit zu schließen ist, dass die Mehrzahl der mit ihm vergleichbaren Arbeitnehmer die behauptete Gehaltsentwicklung genommen hat. Verfügt das Betriebsratsmitglied etwa wegen der Größe des Betriebs und der Vielzahl vergleichbarer Arbeitnehmer nicht über ausreichende Erkenntnismöglichkeiten, kann es genügen, wenn das Betriebsratsmitglied Referenzfälle schlüssig darlegt, aus denen sich auf eine betriebsübliche Beförderungspraxis in dem Zeitraum seiner Zugehörigkeit zum Betriebsrat schließen lässt. Die abstrakte – gleichsam „ins Blaue“ zielende – Behauptung einer Beförderungspraxis ohne jeden konkreten Beispielfall genügt dazu jedoch nicht. Anderenfalls würde die Darlegungs- und Beweislast verkehrt.

bb) Danach hat das Landesarbeitsgericht im Ergebnis zu Recht entschieden, dass der Kläger eine Betriebsüblichkeit der Beförderung vom Lead zum Acting Area Manager nicht mit der dafür erforderlichen Wahrscheinlichkeit dargelegt hat, so dass die Beklagte nicht verpflichtet ist, ihm die begehrten Auskünfte zu erteilen.

(1) Eine allgemeine Beförderungspraxis vom Lead zum Acting Area Manager mit anschließendem Aufstieg zum Area Manager existiert bei der Beklagten nicht. Insbesondere ist kein entsprechender Zeit- oder Bewährungsaufstieg vorgesehen. Aus den vorgelegten Stellenbeschreibungen ergibt sich vielmehr, dass die Beförderung grundsätzlich nicht jedem Lead offensteht. Nach dem Anforderungsprofil müssen Acting Area Manager neben weiteren Fähigkeiten über eine formale Qualifikation verfügen, „wie z.B. BA-, FH- oder Uni-Abschlüsse verschiedener Disziplinen und/oder Berufserfahrung in vergleichbaren Branchen". Die Auswahl erfolgt aufgrund eines Assessment-Centers.

(2) Der Kläger hat auch nicht zumindest exemplarisch dargelegt, dass bei seiner Amtsübernahme im Jahr 2006 im Wesentlichen gleich qualifizierte Leads in der Folgezeit zu Acting Area Managern befördert wurden und dass daraus oder aus anderen Umständen mit hinreichender Wahrscheinlichkeit geschlossen werden kann, dass es sich um eine betriebsübliche berufliche Entwicklung handelte.

Soweit sich der Kläger auf die Mitarbeiter P und S bezogen hat, ergibt sich aus seinem Vortrag nicht, dass diese bereits im Zeitpunkt seiner Amtsübernahme im Jahr 2006 als Lead tätig waren. Soweit der Kläger den im Jahr 1999 als Versandmitarbeiter eingestellten Mitarbeiter F als vergleichbar betrachtet, lässt sich aus dessen Beförderung zum Acting Area Manager nicht auf die vom Kläger behauptete strukturelle Beförderungspraxis schließen. Vielmehr handelt es sich hierbei nach den Feststellungen des Landesarbeitsgerichts um einen untypischen Fall. Die Laufbahn vom Lead zum Acting Area Manager beruhte darauf, dass Herr F nach seinem Wechsel im August 2000 zur Abteilung „Training" als „Trainings-Lead" tätig und nach dem Erwerb der Ausbildereignung für die Auszubildenden zuständig war. Danach bewarb er sich Anfang 2009 erfolgreich auf die Stelle eines Acting Area Managers und im Juli 2009 um die Stelle eines Area Managers, auf der er seit dem 1. August 2009 eingesetzt ist. Der Kläger ist daher mit Herrn F, der über ein zusätzliches Eignungsmerkmal verfügte und vor seiner Beförderung zum Acting Area Manager eine Sonderaufgabe wahrnahm, nicht vergleichbar. Einen Arbeitnehmer, der mit ihm aufgrund seiner bei der Amtsübernahme ausgeübten Tätigkeit zu vergleichen ist und ohne zusätzliche Qualifikation aus der Funktion eines Leads mit den üblichen Abteilungsaufgaben heraus zum Acting Area Manager befördert wurde, hat der Kläger nicht benannt.

cc) Soweit der Kläger sein Auskunftsverlangen auf §§ 611, 242 BGB i.V.m. § 78 Satz 2 BetrVG gestützt und geltend gemacht hat, er habe sich wegen seines Betriebsratsamts nicht mit Erfolg auf eine ausgeschriebene Stelle als Acting Area Manager bewerben können, ist nicht ersichtlich, weshalb die mit dem Antrag zu 1. begehrten Auskünfte zur Geltendmachung eines Zahlungsanspruchs erforderlich sein könnten.

(1) Ein Anspruch des Betriebsratsmitglieds auf eine bestimmte Vergütung kann sich aus § 611 BGB i.V.m. § 78 Satz 2 BetrVG ergeben, wenn sich die Zahlung einer geringeren Vergütung als Benachteiligung des Betriebsratsmitglieds wegen seiner Betriebsratstätigkeit darstellt. Die Vorschrift enthält ein an den Arbeitgeber gerichtetes allgemeines Verbot, ein Betriebsratsmitglied wegen der Amtstätigkeit in seiner beruflichen Entwicklung zu benachteiligen. Der Arbeitgeber muss den Mitgliedern der in § 78 Satz 1 BetrVG genannten Arbeitnehmervertretungen eine berufliche Entwicklung gewährleisten, die derjenigen entspricht, die sie ohne ihre Amtstätigkeit durchlaufen hätten. Von dem Benachteiligungsverbot erfasst wird nicht nur die berufliche Tätigkeit, sondern auch das sich aus ihr ergebende Entgelt. Ein Betriebsratsmitglied, das nur infolge der Amtsübernahme nicht in eine Position mit höherer Vergütung aufgestiegen ist, kann daher den Arbeitgeber unmittelbar auf Zahlung der höheren Vergütung in Anspruch nehmen (BAG 17. August 2005 – 7 AZR 528/04 – zu 2 a der Gründe m.w.N.).

Will der Amtsträger geltend machen, dass er ohne Ausübung seines Amts oder ohne die Freistellung durch Beförderungen einen beruflichen Aufstieg genommen hätte, hat er hierzu mehrere Möglichkeiten (vgl. BAG 27. Juni 2001 – 7 AZR 496/99 – zu B II 1 b der Gründe, BAGE 98, 164). Er kann vortragen, dass seine Bewerbung auf eine bestimmte Stelle gerade wegen seiner Freistellung und/oder seiner Betriebsratstätigkeit erfolglos geblieben ist (vgl. BAG 27. Juni 2001 – 7 AZR 496/99 – zu B II 1 b aa der Gründe m.w.N, a.a.O.). Hat sich der Amtsträger auf eine bestimmte Stelle tatsächlich nicht beworben, kann und muss er zur Begründung des fiktiven Beförderungsanspruchs darlegen, dass er die Bewerbung gerade wegen seiner Freistellung unterlassen hat und eine Bewerbung ohne die Freistellung erfolgreich gewesen wäre. Aber auch wenn eine tatsächliche oder eine fiktive Bewerbung danach keinen Erfolg gehabt hätte oder hätte haben müssen, steht dies einem Anspruch nicht zwingend entgegen. Scheitert nämlich eine tatsächliche oder eine fiktive Bewerbung des freigestellten Betriebsratsmitglieds an fehlenden aktuellen Fachkenntnissen oder daran, dass der Arbeitgeber sich zur Beurteilung der fachlichen und beruflichen Qualifikation infolge der Freistellung außerstande gesehen hat, so ist zwar die Entscheidung des Arbeitgebers für den als qualifizierter erachteten Bewerber nicht zu beanstanden. Gleichwohl kann in einem solchen Fall ein fiktiver Beförderungsanspruch des Amtsinhabers bestehen, wenn das Fehlen von feststellbarem aktuellen Fachwissen gerade aufgrund der Freistellung eingetreten ist (vgl. BAG 14. Juli 2010 – 7 AZR 359/09 – Rn. 20 m.w.N).

(2) Diesen Vortrag könnte der Kläger halten, ohne auf weitere Auskünfte der Beklagten angewiesen zu sein. Allein der Kläger, nicht hingegen die Beklagte, kann darüber Auskunft geben, welche konkret ausgeschriebene Stelle sein Interesse geweckt hat oder hätte. Der Kläger hätte ohne weiteres darlegen können, dass er sich im Hinblick auf seine Betriebsratsaufgaben nicht beworben hat. Auch benötigte er die begehrten Informationen nicht, um vorzutragen, eine tatsächliche oder eine fiktive Bewerbung sei oder wäre an fehlenden aktuellen Fachkenntnissen oder daran gescheitert, dass er wegen seiner Tätigkeit als Betriebsratsmitglied nicht die erforderlichen fachlichen und beruflichen Qualifikationen habe erwerben können.

dd) Die Abweisung der auf den arbeitsrechtlichen Gleichbehandlungsgrundsatz gestützten Ansprüche hat der Kläger mit der Revision nicht angegriffen. Sie sind daher nicht Gegenstand der Revision.

II. Damit besteht kein Anspruch des Klägers auf Zahlung der durchschnittlichen Gehaltssteigerung der zum Acting Area Manager beförderten Leads. Dem Klageantrag zu 2. fehlt die materiell-rechtliche Grundlage, so dass die Stufenklage insgesamt durch Endurteil abgewiesen werden kann (vgl. BAG 14. November 2012 – 10 AZR 783/11 – Rn. 61, BAGE 143, 292; 28. Juni 2011 – 3 AZR 385/09 – Rn. 16, BAGE 138, 184).

III. Die Hilfsanträge zu 3.a) und 3.b) haben ebenfalls keinen Erfolg. Das Landesarbeitsgericht hat zutreffend erkannt, dass dem Kläger kein Anspruch nach §§ 611, 242 BGB i.V.m. § 37 Abs. 4 BetrVG und nach §§ 611, 242 BGB i.V.m. § 78 Satz 2 BetrVG auf die Benennung der Arbeitnehmer zusteht, die im Jahr 2006 als Lead bei der Beklagten beschäftigt waren und über einen Berufsabschluss eines Meisters oder den Abschluss eines Hochschulstudiums verfügen. Er kann auch nicht die mit dem Antrag zu 3.b) geltend gemachten Informationen zu diesem Personenkreis verlangen.

1. Die Hilfsanträge zu 3.a) und 3.b) sind nach gebotener Auslegung zulässig, sie sind insbesondere hinreichend bestimmt i.S.v. § 253 Abs. 2 Nr. 2 ZPO. Soweit sich der Hilfsantrag zu 3.a) auf Leads bezieht, die „über einen Berufsabschluss eines Meisters oder den Abschluss eines Hochschulstudiums verfügen", liegt es nach der Klagebegründung nahe, den Antrag über seinen Wortlaut hinaus dahin zu verstehen, dass sich der Kläger insoweit an die Stellenausschreibungen der Beklagten für Acting Area Manager und Area Manager anlehnen wollte. Danach erstreckt sich das Auskunftsbegehren nicht nur auf Leads, die über einen Meisterabschluss verfügen oder ein Hochschulstudium absolviert haben, sondern auch auf Leads mit Fachhochschulabschluss sowie mit dem Abschluss an einer Berufsakademie. Der Antrag zu 3.a), mit dem der Kläger Auskunft über die im Jahr 2006 als Lead beschäftigten Arbeitnehmer verlangt, ohne konkret anzugeben, welche Auskünfte die Beklagte erteilen soll, muss im Zusammenhang mit dem Antrag zu 3.b) gelesen werden. Dem Kläger geht es um die Mitteilung der Namen sämtlicher Leads der drei im Antrag bezeichneten Kategorien. Er möchte wissen, welche Leads im Jahr 2006 bei der Beklagten beschäftigt waren und zum 1. Januar 2013 ausgeschieden sind. Ferner begehrt er Auskunft darüber, welche Arbeitnehmer eine gewerbliche Tätigkeit im Betrieb ausüben unterhalb der Stufe des Leads und welche der Leads eine Tätigkeit im Gehaltsgefüge der Angestellten ausüben, also wenigstens in der Vergütungsstufe „Level 3 Salary". Mit diesem Inhalt genügen die Anträge zu 3.a) und 3.b) dem Bestimmtheitserfordernis.

2. Die so verstandenen Anträge zu 3.a) und 3.b) sind aus den unter I 2 dargelegten Gründen unbegründet.

IV. Der Antrag zu 4. ist wegen fehlenden Rechtsschutzbedürfnisses unzulässig. Der Kläger hat kein schutzwürdiges Interesse an dem begehrten Urteil. Er hat weder vorgetragen noch ist sonst ersichtlich, aus welchem Grund er Auskunft über angewandte Auswahlkriterien und Bewertungen in dem Assessment-Center bei Besetzung einer Acting-Area-Manager-Position mit einem Lead benötigt.

V. Die Anträge zu 5. und 6. sind identisch mit den Anträgen zu 1. und 2. Aus diesem Grund sind sie schon wegen doppelter Rechtshängigkeit unzulässig, § 261 Abs. 3 Nr. 1 ZPO.

Pflicht zur Vorlage der elektronischen Gesundheitskarte

(**Landessozialgericht Baden-Württemberg**, Urteil vom 21. Juni 2016 – L 11 KR 2510/15 –)

1. **Versicherte der GKV sind verpflichtet, dem behandelnden Vertrags(zahn)arzt vor Beginn der Behandlung zum Nachweis der Behandlungsberechtigung die elektronische Gesundheitskarte (eGK) auszuhändigen.**
2. **Der Umstand, dass die eGK geeignet sein muss, die in § 291a Abs. 3 SGB V aufgeführten Anwendungen zu unterstützen, führt nicht zu einem Verstoß gegen das Recht auf informationelle Selbstbestimmung der Versicherten, da das Erheben, Verarbeiten und Nutzen von Daten zu diesem Zweck nur mit der Einwilligung der Versicherten gestattet ist.**
3. **Die eGK darf ohne Einwilligung des Versicherten nur die in § 291a Abs. 1 SGB V genannten Daten enthalten. Unbestimmte Rechtsbegriffe wie zB der Begriff „Versichertenstatus" dürfen nicht durch (normsetzende) Vereinbarungen im Range unterhalb des Parlamentsgesetzes ausgefüllt und „datenmäßig erweitert" werden.**

Sachverhalt:

Die Beteiligten streiten über die Obliegenheit, die Berechtigung zur Inanspruchnahme von Leistungen mittels elektronischer Gesundheitskarte (eGK) nachzuweisen. Der Kläger wehrt sich grundsätzlich gegen die Einführung der elektronischen Gesundheitskarte (eGK) und die Nutzung derselben. Er hält §§ 291a und 291b Fünftes Buch Sozialgesetzbuch (SGB V) und die Rechtsprechung des Bundessozialgerichts (BSG) teilweise für verfassungswidrig.

Der Kläger beantragt, den Gerichtsbescheid des Sozialgerichts Karlsruhe vom 07.05.2015 und den Bescheid der Beklagten vom 04.04.2012 in der Gestalt des Widerspruchsbescheides vom 11.09.2012 aufzuheben und die Beklagten zu verurteilen, ihm eine nicht zur elektronischen Gesundheitskarte erweiterte Krankenversichertenkarte auszustellen und ihn mit Leistungen nach dem SGB V zu versorgen, ohne dass er die elektronische Gesundheitskarte (eGK) und die Telematik-Infrastruktur benutzen müsse, hilfsweise das Verfahren auszusetzen und eine Entscheidung des Bundesverfassungsgerichts einzuholen.

In der mündlichen Verhandlung vor dem Senat hat der Kläger mitgeteilt, er habe eine eGK ohne Lichtbild erhalten, um Leistungen in Anspruch nehmen zu können.

Aus den Gründen:

Klage und Berufung sind unbegründet. Die Beklagte lehnt es rechtmäßig ab, den Kläger mit einem anderen Berechtigungsnachweis als der eGK auszustatten. Die Regelungen der §§ 15, 291, 291a SGB V über die Obliegenheit der Versicherten, die elektronische Gesundheitskarte bei Inanspruchnahme vertragsärztlicher Leistungen vor Beginn der Behandlung zum Berechtigungsnachweis dem Vertrags(zahn)arzt auszuhändigen, sind mit Vorrang vor dem BDSG anwendbar (BSG 18.11.2014, B 1 KR 35/13 R a.a.O.). Ein Anspruch auf Befreiung von der Verwendung der elektronischen Gesundheitskarte besteht nicht. Jeder Versicherte ist grundsätzlich verpflichtet, die elektronische Gesundheitskarte zu nutzen. Das Recht auf informationelle Selbstbestimmung gewährt kein Recht auf Verhinderung der Digitalisierung und „Weiterleben in einer analogen Welt".

Die datenschutzrechtlichen Regelungen des SGB X verweisen u.a. auf die bereichsspezifischen Datenschutzregelungen des SGB V. Nach § 67a Abs. 1 S. 1 Zehntes Buch Sozialgesetzbuch (Sozialverwaltungsverfahren und Sozialdatenschutz – SGB X) ist das Erheben von Sozialdaten durch in § 35 SGB I genannte Stellen zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist. § 67b Abs. 1 S. 1 SGB X erlaubt die Verarbeitung und Nutzung

von Sozialdaten u.a. nur, soweit die datenschutzrechtlichen Vorschriften des SGB X oder eine andere Vorschrift des SGB es erlauben oder anordnen. Zu den anderen Vorschriften des SGB zählen auch die hier einschlägigen datenschutzrechtlichen Regelungen des SGB V, insbesondere die §§ 15, 291, 291a SGB V. Diese Vorschriften „kategorisieren nach dem Regelungskonzept des Gesetzgebers den für die eGK erforderlichen Datenschutz nach Pflichtangaben, Pflichtanwendungen sowie einwilligungsabhängigen freiwilligen Angaben und Anwendungen und gestalten ihn ebenfalls als „Verbotsnorm mit Erlaubnisvorbehalt" aus. Hierbei dürfen die KKn Sozialdaten für Zwecke der Krankenversicherung erheben und speichern, soweit diese für die Ausstellung der elektronischen Gesundheitskarte erforderlich sind (BSG 18.11.2014, B 1 KR 35/13 R, Rn. 15).

Das BSG, dem sich der Senat anschließt, hat mit Urteil vom 18.11.2014, B 1 KR 35/13 R a.a.O. entschieden, dass Versicherte kraft Gesetzes die Obliegenheit trifft, die eGK in ihrer gesetzlichen Ausgestaltung, erweitert um die Angaben des Geschlechts und Zuzahlungsstatus, bei Inanspruchnahme vertragsärztlicher Leistungen vor Beginn der Behandlung zum Nachweis seiner Berechtigung dem Vertrags(zahn)arzt auszuhändigen (vgl. § 15 Abs. 2 SGB V). Die Nachweisobliegenheit bezweckt neben der Missbrauchsabwehr die Abrechnung von Leistungen (§ 291 Abs. 1 S. 3 SGB V) und die Übermittlung ärztlicher Verordnungen (§ 291a Abs. 2 S. 1 Nr. 1 SGB V) zu ermöglichen. Versicherte haben nach der Gesetzeslage keinen Anspruch auf die vom Kläger gewünschten Ausnahmen. Die betroffenen Regelungen der §§ 15, 291, 291a SGB V stehen mit höherrangigem Recht in Einklang (vgl. zu alledem eingehend BSG 18.11.2014, B 1 KR 35/13 R a.a.O.).

Die bisher gültige Krankenversicherungskarte wird gemäß §§ 291, 291a SGB V zur eGK erweitert. Die Pflichtangaben für die eGK, die vom Kläger anzugeben sind, unterscheiden sich dabei nicht von den Angaben, die für die bisherige Krankenversicherungskarte erforderlich waren (vgl. BSG 18.11.2014, B 1 KR 35/13 R a.a.O.). Es handelt sich neben Unterschrift und Lichtbild des Versicherten um folgende Angaben: (1.) Bezeichnung der ausstellenden Krankenkasse einschließlich eines Kennzeichens für die Kassenärztliche Vereinigung, in deren Bezirk das Mitglied seinen Wohnsitz hat, (2.) Familienname und Vorname des Versicherten, (3.) Geburtsdatum, (4.) Geschlecht, (5.) Anschrift, (6.) Krankenversicherungsnummer, (7.) Versichertenstatus, (8.) Zuzahlungsstatus, (9.) Tag des Beginns des Versicherungsschutzes, (10.) bei befristeter Gültigkeit der Karte das Datum des Fristablaufs.

Soweit die eGK nach § 291a Abs. 2 Nr 1 SGB V geeignet sein muss, Angaben aufzunehmen für die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form, ist das „elektronische Rezept" noch nicht eingeführt, so dass derzeit eine Rechtsbeeinträchtigung weder ersichtlich ist noch in absehbarer Zeit drohen kann.

Soweit sich der Kläger gegen die in § 291a Abs. 3 Satz 1 SGB V vorgesehenen Anwendungsmöglichkeiten der eGK wendet, folgt der Senat seiner Auffassung nicht.

Nach § 291 Abs. 3 Satz 1 SGB V muss die eGK geeignet sein, folgende Anwendungen zu unterstützen, insbesondere das Erheben, Verarbeiten und Nutzen von (1.) medizinischen Daten, soweit sie für die Notfallversorgung erforderlich sind, (2.) Befunden, Diagnosen, Therapieempfehlungen sowie Behandlungsberichten in elektronischer und maschinell verwertbarer Form für eine einrichtungsübergreifende, fallbezogene Kooperation (elektronischer Arztbrief), (3.) Daten zur Prüfung der Arzneimitteltherapiesicherheit, (4.) Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten (elektronische Patientenakte), (5.) durch von Versicherten selbst oder für sie zur Verfügung gestellte Daten, (6.) Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für die Versicherten (§ 305 Abs. 2), (7.) Erklärungen der Versicherten zur Organ- und Gewebespende, (8.) Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen zur Organ- und Gewebespende sowie (9.) Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Vorsorgevollmachten oder Patientenverfügungen nach § 1901a des Bürgerlichen Gesetzbuchs.

Indes ist die Erhebung, Nutzung und Verarbeitung dieser Daten nur zulässig, wenn der Versicherte einwilligt (§ 291a Abs. 3 Satz 4 und Abs. 5 S 1 SGB V), wobei die Einwilligung jederzeit widerrufen werden kann (§ 291a Abs. 3 Satz 5 SGB V). Der Kläger kann damit schon durch die Verweigerung seiner Einwilligung verhindern, dass entsprechende Daten überhaupt erst erhoben werden. Damit ist auch im Hinblick auf das informationelle Selbstbestimmungsrecht des Antragstellers eine unmittelbare Beschwer nicht gegeben (vgl SG Düsseldorf 28.06.2012, S 9 KR 111/09, juris). Soweit der Kläger schließlich bereits aus der Möglichkeit, zukünftig an einer Krankheit zu erkranken, die ihn faktisch zwinge, über die Teilnahme an DMP-Programmen einer entsprechenden Datennutzung zuzustimmen, eine Rechtsverletzung ableitet, kann der Senat sich dem nicht anschließen. Der Kläger leidet aktuell an keiner Erkrankung, für die von der Beklagten DMP-Programme angeboten werden.

Die anzuwendenden Datenschutzregelungen des SGB (§ 35 SGB I; §§ 67 ff SGB X iVm §§ 15, 291, 291a SGB V) gehen den Regelungen des BDSG vor. Sie sind bereichsspezifisches Datenschutzrecht bezogen auf den Geltungsbereich des SGB iS von § 1 Abs. 3 S 1 BDSG (vgl BSG 18.11.2014, B 1 KR 35/13 R a.a.O.). Die Vorschriften des BDSG sind dagegen nur nachrangig und subsidiär heranzuziehen, soweit das SGB nicht hierauf verweist (vgl BSGE 107, 86 = SozR 4-1300 § 83 Nr 1, RdNr 22 m.w.N. zum Verhältnis von SGB I, SGB V, SGB X und BDSG; BSGE 102, 134 = SozR 4-2500 § 295 Nr 2, RdNr 18, 33 ff m.w.N.). Über § 291a Abs. 2 S 2 SGB V findet § 6c BDSG Anwendung, der sicherstellt, dass die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, den Betroffenen über ihre Identität und Anschrift, in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten, darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 BDSG ausüben kann, informieren muss. Damit sind i.V.m. mit den in § 15 Abs. 6 SGB V geregelten Maßnahmen zur Verhinderung missbräuchlicher Verwendung die mit der Einführung der egK verbundenen Ziele in Anbetracht der zukünftig zu bewältigenden Gesundheitskosten zur Legitimation der gesetzlichen Regelung in Anbetracht der getroffenen Vorkehrungen gegen Datenmissbrauch dem Grunde nach ausreichend (Luthe, in: Hauck/Noftz, SGB V, § 291a Rn. 8; Didong, in: jurisPK SGB V, 3. Aufl. 2016, § 291a Rn. 15).

Der Eingriff in das Recht auf informationelle Selbstbestimmungsrecht aus Art 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG, welcher in der Pflicht zur Angabe bzw zur Verfügungstellung von Lichtbild und Unterschriftsleistung sowie der zur Identifikation dienenden Angaben von Namen, Geburtsdatum, Geschlecht, Anschrift,

und Versichertennummer nach §§ 291 Abs. 2, 291a Abs. 2 S 1 SGB V zu sehen ist, ist gerechtfertigt (vgl BSG 18.11.2014 a.a.O.; LSG Berlin-Brandenburg 20.03.2015, L 1 KR 18/14; Hessisches LSG 26.09.2013, L 1 KR 50/13; vgl auch Senatsbeschluss vom 30.11.2012, L 11 KR 4746/12 ER-B). Der Kläger muss es nach der Gesetzeslage auch dulden, dass die Beklagte als Krankenkasse verpflichtet ist, Dienste anzubieten, mit denen die Leistungserbringer die Gültigkeit und die Aktualität der Versichertenstammdaten (Daten nach § 291 Abs. 1 und 2 SGB V) bei den Krankenkassen online überprüfen und auf der eGK aktualisieren können. Die an der vertragsärztlichen Versorgung teilnehmenden Ärzte, Einrichtungen und Zahnärzte prüfen bei der erstmaligen Inanspruchnahme ihrer Leistungen durch einen Versicherten im Quartal die Leistungspflicht der KK durch Nutzung der Dienste. Dazu ermöglichen sie den Online-Abgleich und die -Aktualisierung der auf der eGK gespeicherten Daten nach § 291 Abs. 1 und 2 SGB V mit den bei der Krankenkasse vorliegenden aktuellen Daten. Die Prüfungspflicht besteht ab dem Zeitpunkt, ab dem die Dienste nach § 291 Abs. 2b S 1 SGB V sowie die Anbindung an die Telematik-Infrastruktur zur Verfügung stehen und die Vereinbarungen nach § 291a Abs. 7a und 7b SGB V geschlossen sind. § 15 Abs. 5 SGB V ist entsprechend anzuwenden (Online-Versichertenstammdatendienst oder Versichertenstammdatenmanagement; vgl eingehend BSG 18.11.2014, B 1 KR 35/13 R, Rn. 21).

Dieses Grundrecht auf informationelle Selbstbestimmung gewährleistet die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (BVerfG 13.02.2006, 1 BvR 1184/14 unter Hinweis auf BVerfG 15.12.1983, 1 BvR 209/83 ua, BVerfGE 65, 1 ff; 29.09.2013, 2 BvR 939/13, juris Rn. 13). Diese Verbürgung darf nur im überwiegenden Interesse der Allgemeinheit und unter Beachtung des Grundsatzes der Verhältnismäßigkeit durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden; die Einschränkung darf nicht weiter gehen, als es zum Schutz des öffentlichen Interesses unerlässlich ist (vgl BVerfG 14.12.2000, 2 BvR 1741/99, BVerfGE 103, 21, 33).

Zwar wurzelt das informationelle Selbstbestimmungsrecht des Bürgers im allgemeinen Persönlichkeitsrecht und dem Grundrecht auf Menschenwürde und gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Der Einzelne hat jedoch kein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über „seine" Daten. Er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Informationen, auch soweit sie personenbezogen sind, stellen ein Abbild sozialer Realität dar, das nicht ausschließlich den Betroffenen allein zugeordnet werden kann. Das Recht auf informationelle Selbstbestimmung verlangt insoweit, dass die Einschränkung des Rechts von hinreichenden Gründen des Allgemeinwohls gerechtfertigt wird, das gewählte Mittel zur Erreichung des Zwecks geeignet und erforderlich ist und bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der rechtfertigenden Gründe die Grenze des Zumutbaren noch gewahrt ist (BVerfGE 65, 1, 41 f.; 56, 37, 41 ff.).

Vorliegend überwiegt das Allgemeininteresse an einer Funktionsfähigkeit des Sachleistungssystems der gesetzlichen Krankenversicherung im Verhältnis zur rechtlichen Betroffenheit des Klägers.

Die Identifikationsfunktion eines Lichtbilds auf der Karte wird benötigt, um eine missbräuchliche Verwendung möglichst einzuschränken. Dies kann im Rahmen der Massenverwaltung nur funktionieren, wenn die in § 15 Abs. 2 SGB V vorgesehene Verfahrensweise („Versicherte, die ärztliche oder zahnärztliche Behandlung in Anspruch nehmen, haben dem Arzt [Zahnarzt] vor Beginn der Behandlung ihre Krankenversichertenkarte zum Nachweis der Berechtigung zur Inanspruchnahme von Leistungen [...] auszuhändigen") auch von allen Versicherten der gesetzlichen Krankenversicherung befolgt wird. Entsprechendes gilt für den Onlineabgleich der Versichertenstammdaten (vgl BSG 18.11.2014, B 1 KR 35/13 R, Rn. 27). Da der Kläger von der Beklagten eine Karte ohne Lichtbild erhalten hat, fehlt es vorliegend ohnehin an einer Selbstbetroffenheit.

Soweit der Kläger sich schon heute durch die künftigen in § 291a Abs. 3 Satz 1 SGB V vorgesehenen Anwendungsmöglichkeiten der eGK in eigenen Rechten verletzt sieht und in Verbindung mit der Versichertennummer (§ 291 Abs. 2 Nr. 6 SGB V) den „gläsernen Patienten" befürchtet, teilt der Senat diese Auffassung nicht. Bei den Anwendungsmöglichkeiten nach § 291a Abs. 3 Satz 1 SGBV handelt es sich nicht um die Pflichtangaben der eGK, sondern um eine vom Gesetz vorgesehene Möglichkeit, auf freiwilliger Basis über die rein administrative Funktion der eGK Datenanwendungsmöglichkeiten zu nutzen. Bereits das Erheben als auch das Verarbeiten und Nutzen von Daten mittels der eGK ist in den Fällen des § 291a Abs. 3 Satz 1 SGB V nur mit dem Einverständnis der Versicherten zulässig (§ 291a Abs. 5 Satz 1 SGB V, vgl dazu Dochow, WzS 2015, 137, 144). Dafür, dass trotz Fehlens seines Einverständnisses mit seiner eGK fakultative Daten erhoben, verarbeitet oder genutzt werden, ist nichts ersichtlich. Eine Rechtsverletzung des Klägers ist diesbezüglich jedenfalls derzeit ausgeschlossen, eine verfassungsrechtliche Überprüfung erübrigt sich. Selbst wenn bei fehlender Einwilligung im Einzelfall medizinische Daten rechtswidrig gespeichert würden, könnten Ärzte oder Dritte hiervon weitgehend keinen Gebrauch machen (BSG 18.11.2014, B 1 KR 35/13 R Rn. 22).

Soweit der Kläger die Datensicherheit bezweifelt, begründet auch dies schließlich keine Grundrechtsverletzung (BSG 18.11.2014, B 1 KR 35/13 R). Die Rechtsordnung schützt bereits die betroffenen Daten vor unbefugtem Zugriff Dritter und vor missbräuchlicher Nutzung. So regelt § 291a Abs. 6 SGB V neben der Löschung das Gebot technischer Vorkehrungen für Zwecke der Datenschutzkontrolle. Er gebietet, die Protokolldaten durch geeignete Vorkehrungen gegen zweckfremde Verwendung und sonstigen Missbrauch zu schützen (vgl § 291a Abs. 6 Satz 5 SGB V).

Die Revision war nicht zuzulassen, weil die Voraussetzungen des § 160 Abs. 2 SGG nicht erfüllt sind.

Anforderungen an Einwilligungen bei Smart TV (Ls)

(**Landgericht Frankfurt a.M.**, Urteil vom 10. Juni 2016 – 2-03 0 364/15 –)

1. Datenschutzbestimmungen, die auf 56 Bildschirmseiten eines Smart-TV im Fließtext insbesondere ohne hervorgehobene Überschriften dargestellt werden, sind wegen ihrer Länge und Unübersichtlichkeit intransparent und keine geeignete Grundlage für eine Einwilligung in die Datenerhebung und -verwendung. Darüber hinaus ist über die Gefahr aufzuklären, dass bei Anschluss an das Internet personenbezogene Daten erhoben und verwendet werden.

Berichte, Informationen, Sonstiges

Tagungsbericht „Vertrauen und Vergessen(werden) in der digitalen Gesellschaft“ am 31.05. und 01.06. im Fraunhofer-Forum Berlin

Am 31. Mai und 01. Juni 2016 fand in Berlin die Fachtagung „Vertrauen und Vergessen(werden) in der digitalen Gesellschaft“ statt. Die gemeinsame Veranstaltung des Wissenschaftlichen Beirats der Gesellschaft für Datenschutz und Datensicherheit (GDD) und des Fraunhofer Forums Privatheit war mit insgesamt 120 angemeldeten Teilnehmerinnen und Teilnehmern aus Wissenschaft und Praxis erfreulich gut besucht. Am ersten Tag wurden in zwei interdisziplinär besetzten und vom Vorsitzenden des Wissenschaftlichen Beirats der GDD, Prof. Dr. Tobias Keber, moderierten Expertenrunden die Themen „Vertrauen und Sicherheitskultur in der digitalen Gesellschaft“ (Panel I) sowie das „Recht auf Vergessen(werden)“ (Panel II) diskutiert.

In der ersten Runde diskutierten Dr. Ulf Buermeyer, Matthias Kammer, Prof. Dr. Norbert Pohlmann, Prof. Dr. Rolf Schwartmann und Martin Wundram.

Matthias Kammer, Direktor des Deutschen Instituts für Vertrauen und Sicherheit (DIVSI) sowie Vorstandsvorsitzender bei ISPRAT e.V. (Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie) fasste die Ergebnisse der DIVSI Milieu-Studien zu Vertrauen und Sicherheit im Internet zusammen. Ziel dieser Studien war es, die Lebenswirklichkeit und die Erwartungen der Menschen in der digitalen Gesellschaft abzubilden. Bemerkenswert sei dabei, dass unabhängig vom Grad der Internetaffinität der Nutzer diese in neueren Umfragen dem Selbstschutz und der Eigenverantwortung für ihre Sicherheit im Netz eine deutlich größere Rolle beimessen. Nach wie vor würden auch Staat und Wirtschaft in der Verantwortung gesehen, wobei die Nutzer aber zunehmend skeptisch seien, dass diese Akteure dem Erwartungshorizont gerecht werden. Insgesamt sei der Internetoptimismus der befragten Nutzer aber gestiegen, so Kammer weiter.

Professor Dr. Rolf Schwartmann, Vorstandsvorsitzender der GDD sowie Mitglied der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft des Innenministeriums, informierte über Aufgaben und erste Arbeitsergebnisse dieser Plattform, die Bestandteil der Digitalen Agenda der Bundesregierung ist. Thematisiert wurde in dem Gremium seinen Ausführungen zufolge u.a. eine stärkere Verzahnung von Datenschutz und Datensicherheit, auch durch Zertifizierung für sichere Produkte, beispielsweise Car-Sharing-Apps. In der Sache gehe es darum, Datenschutz und Datensicherheit bereits auf Ebene der Produktkonzeption, also „by design“, zu implementieren und auch politisch entsprechende Anreize zu schaffen, so Schwartmann weiter.

Den Bereich Datenschutz und Datensicherheit vor dem Hintergrund staatlicher Ermittlungsbefugnisse, namentlich der so genannten Online-Durchsuchung und der hierzu 2008 ergangene Entscheidung des Bundesverfassungsgerichts adressierte Dr. Ulf Buermeyer, Richter am Landgericht Berlin und Mitglied im Centre for Internet and Human Rights, dem Chaos Computer Club und der Digitalen Gesellschaft e.V. Die Online-Durchsuchung, also die mittels durch den Staat heimlich in das informationstechnische System einer Zielperson eingebrachter Software, stelle bildlich gesprochen den größten anzunehmenden Unfall für das Vertrauen der Bürger in die Informationstechnik dar. Von zentraler Bedeutung sei daher, dass der Staat im Rahmen seiner Grundrechtsbindung handle und die Maßnahme nur in engen Grenzen und nur außerhalb des Kernbereichs privater Lebensführung eingesetzt werde.

Das vom Bundesverfassungsgericht 2008 vor diesem Hintergrund entwickelte Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme griff Prof. Dr. Rafael Capurro auf. Capurro, Gründer und Vorsitzender des International Center for Information Ethics (ICIE) sowie ehemaliges Mitglied der European Group on Ethics in Science and New Technologies (EGE) der EU-Kommission (2000-2010) hinterfragte die hinter den Begrifflichkeiten Vertrauen, Vertraulichkeit und Verlässlichkeit liegenden Konzepte und wies darauf hin, dass Vertrauen als Mittel zur Kompensation sozialer Unschärfe seiner Ansicht nach ausschließlich Menschen adressieren könne, man informationstechnischen Systemen, also Maschinen, per definitionem nicht vertrauen könne.

Prof. Dr. Norbert Pohlmann, Direktor am Institut für Sicherheit an der Westfälischen Hochschule if(is), Mitglied des Wissenschaftlichen Beirats der Gesellschaft für Datenschutz und Datensicherheit sowie Vorstandsmitglied beim Verband der Internetwirtschaft e.V. (eco-Verband) unterstrich, dass Sicherheit im IT-Bereich ein relatives Konzept sei, das sich letztlich nur nach Maßgabe des Einsatzes von Zeit und finanzieller, bzw. personeller Mittel der potentiellen Angreifer entfalten könne. Als zentrales Problem arbeitete er heraus, dass bei IT-Systemen eine klare Zuweisung der Gesamtverantwortung fehle, wie es beispielsweise bei Automobilherstellern der Fall sei. Der Nutzer müsse die Sicherheit selbst in die Hand nehmen, was er aufgrund fehlenden IT-Sachverstands nur sehr bedingt leisten könne. Auf Seiten der Unternehmen, namentlich der weitgehend konkurrenzlosen US-amerikanischen Hard- und Softwarehersteller, beklagte er fehlende Umsetzungsbereitschaft hinsichtlich der Konzepte security by design, privacy by design und compliance by design.

Martin Wundram (Digitrace), Diplom Wirtschaftsinformatiker und Sachverständiger für IT-Sicherheit und IT-Forensik schließlich berichtete aus seiner beruflichen Praxis und zeigte sich

hinsichtlich der IT-Sicherheitslage in deutschen Unternehmen sehr besorgt. Den zum Teil desaströsen Verhältnissen sei nur durch Awareness, sachadäquate Regulierung und praktisch handhabbare Sicherheitsmaßnahmen (Usability) zu begegnen.

Insgesamt waren sich die Diskutanten des ersten Panels dahingehend einig, dass die Herausforderungen der Digitalisierung sowie Vertrauen und Sicherheitskultur in der digitalen Gesellschaft nur als gesamtgesellschaftliche Aufgabe adressiert werden könnten und dem Thema seitens der Politik deutlich höhere Priorität eingeräumt werden müsse.

In der zweiten Runde diskutierten Bundesjustizministerin a.D. Sabine Leutheusser-Schnarrenberger, Rechtsanwalt Dr. Carlo Piltz, Dr. Thoralf Schwanitz und Prof. Dr. Rolf Schwartmann die Implikationen der EuGH-Entscheidung vom 13.5.2014 (C-131/12) in Sachen Google Spain.

Zu Beginn berichtete Frau Leutheusser-Schnarrenberger über ihre Arbeit im „Advisory Council to Google on the Right to be Forgotten“ (so genannter Lösch-Beirat), vor allem über die innerhalb des achtköpfigen interdisziplinär besetzten Gremiums umstrittenen Punkte. Aufgabe des Lösch-Beirats war die Erarbeitung unverbindlicher Empfehlungen für die im Einzelfall schwierige Abwägung unter besonderer Berücksichtigung der unterschiedlichen Verantwortungsbereiche der beteiligten Akteure (Inhalteanbieter, Suchmaschinenbetreiber und die von der Berichterstattung Betroffenen) sowie des Faktors Zeit. Frau Leutheusser-Schnarrenberger berichtete, dass vor allem die Fragen umstritten waren, ob Inhalteanbieter hinsichtlich der Löschung aus dem Index des Suchmaschinenbetreibers in Kenntnis zu setzen sind, ob statt der Entscheidung durch den Suchmaschinenbetreibers diejenige eines Streitschlichtungsgremiums vorzugswürdig wäre und ob im Falle eines erfolgreichen Löschersuchens dieses national, europaweit oder global umzusetzen ist.

Auf die enorme Zahl von Löschersuchen, die sein Unternehmen zu bewältigen habe, wies Thoralf Schwanitz, Public Policy & Government Relations Counsel bei Google Deutschland, hin. Allein aus Deutschland habe man derzeit 75.000 Löschersuchen abzuarbeiten, die insgesamt 270.000 URLs betreffen. Er unterstrich, dass die Entscheidung des Europäischen Gerichtshofs keine Ausführungen dazu enthalte, ob eine einem Löschersuchen stattgebende Entscheidung national, europaweit oder mit weltweiter Wirkung umzusetzen ist.

Carlo Piltz, Rechtsanwalt und Verantwortlicher des Blogs zum Datenschutzrecht „delegedata.de“ zeigte sich angesichts territorial begrenzter staatlicher Befugnisse äußerst skeptisch hinsichtlich der globalen Durchsetzung von Löschentscheidungen. Auch Rolf Schwartmann adressierte das insoweit betroffene völkerrechtliche Nichteinmischungsgebot, gelangte aber zu dem Ergebnis, dass ein Bußgeldverfahren unter Ägide der künftig einschlägigen Bestimmungen der Datenschutz-Grundverordnung möglich sei.

Zum Abschluss des ersten Tages präsentierte IT-Forensiker Martin Wundram noch eindrucksvoll verbreitete Sicherheitslücken. Unter Federführung des Forums Privatheit präsentierten am 2. Tag der Fachtagung insgesamt 16 vom Bundesministerium für Bildung und Forschung geförderte Projekte ihre Forschungs- und Lösungsansätze rund um das Thema Selbstdatenschutz.

(Prof. Dr. Tobias Keber)

Zwei von drei Internetnutzern sind in sozialen Netzwerken aktiv

- Von den 14- bis 49-Jährigen nutzen sogar 79 Prozent die Netzwerke
- Facebook wird am häufigsten eingesetzt, gefolgt von Youtube und Xing

Zwei Drittel (67 Prozent) der Internetnutzer in Deutschland sind aktive Mitglieder in sozialen Netzwerken. Am stärksten werden derzeit soziale Netzwerke in der jüngeren und mittleren Altersgruppe verwendet. Sowohl unter den 14- bis 29-Jährigen als auch unter den 30- bis 49-Jährigen liegt der Anteil der aktiven Nutzer bei 79 Prozent. Unter den 50- bis 64-jährigen Internetnutzern sind es 52 Prozent und in der Generation 65 Plus 38 Prozent. Das ist das Ergebnis einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom.

Das mit Abstand beliebteste soziale Netzwerk ist laut Umfrage weiterhin Facebook. 55 Prozent der deutschen Internetnutzer haben in den vergangenen vier Wochen die weltweit größte Social Community genutzt. Während Facebook als eine Art Multifunktionsnetzwerk gilt, haben sich andere soziale Netzwerke auf bestimmte Zielgruppen oder Medienarten spezialisiert. So liegt die Video-Plattform Youtube mit 44 Prozent auf dem zweiten Platz. Fast jeder fünfte Internetnutzer (19 Prozent) verwendet den Foto-Dienst Instagram. Auch die Dienste Pinterest (6 Prozent) und Flickr (3 Prozent) eignen sich vor allem für den Austausch von Fotos und Infografiken. Das primär für berufliche Zwecke verwendete Netzwerk Xing nutzen 26 Prozent der Befragten. Der Wettbewerber LinkedIn kommt auf 15 Prozent. Ein Fünftel (20 Prozent) der Befragten ist bei dem Nachrichtenkanal Twitter aktiv.

(Bitkom-Pressemitteilung vom 18.08.2016)

Bundesinnenminister will Vorratsdatenspeicherung auf Messenger-Dienste erweitern

Mit dem am 11.8.2016 vorgestellten Sicherheitskonzept will Bundesinnenminister Thomas de Maizière unter anderem die Vorratsdatenspeicherung auf Messenger wie Skype oder WhatsApp sowie E-Mails ausweiten. Bisher sind diese nicht von der Vorratsdatenspeicherung betroffen.

Ein schwerwiegender Punkt in de Maizières Forderungskatalog ist die Aufhebung der Trennung von „Telekommunikationsdiensten“ und „Telemediendiensten“.

Telekommunikationsdienste wie Telefon- oder Internetanschluss fallen

unter das Telekommunikationsgesetz (TKG) und damit unter die Vorratsdatenspeicherung (VDS) und die Telekommunikationsüberwachungs-Verordnung (TKÜV).

Zu den Telemediendiesnten gehören fast alle Angebote im Internet: Webshops, Messenger-Dienste, Suchmaschinen, Informationsdiesnte, Podcasts, Chatrooms, Dating-Communitys, Webportale, private Websites und Blogs. Sie alle fallen unter das Telemediengesetz (TMG).

In der Pressekonferenz sagte der Innenminister, dass beide Bereiche denselben Verpflichtungen unterliegen sollten, wenn sie denn zur Kommunikation genutzt würden.

Unter dem Schlagwort „intelligente Videotechnik" will der Innenminister den Datenschutz beim Einsatz von Überwachungskameras schwächen.

Videoüberwachung mit Gesichtserkennung und Kfz-Kennzeichenerfassung soll erlaubt werden.

Datenschützer wurden von De Maizière dafür kritisiert, durch das Verbot von Videoüberwachung die Ermittlungen im Fall einer Bombendrohung in Dortmund behindert zu haben. Sicherheitsinteressen sollten wichtiger sein als Datenschutzbelange, wenn es darum ginge, Videokameras etwa in Einkaufszentren zu genehmigen.

Bei der Videoüberwachung soll auch Gesichtserkennung erlaubt sein, die direkt mit Fahndungsdatenbanken abgeglichen wird.

Deutschland müsse auch die von der EU beschlossene schärfere Überwachung von Fluggästen in nationales Recht zügig umsetzen.

Große Mehrheit der Fluggäste will Ganzkörperscanner am Airport

Wer in den Urlaub oder auf Geschäftsreise fliegt, möchte sich am Flughafen so sicher wie möglich fühlen – und dazu sollten nach Ansicht der meisten Flugreisenden innovative digitale Technologien zum Einsatz kommen. Das zeigt eine repräsentative Befragung von 994 Flugreisenden im Auftrag des Digitalverbands Bitkom. Demnach befürworten fast alle Befragten (94 Prozent) die allgemeine Kameraüberwachung am Flughafen. Ein Großteil (85 Prozent) ist zudem für den Einsatz von Spezialkameras zur Erkennung von unbeaufsichtigtem Gepäck. Rund drei Viertel der Flugreisenden (72 Prozent) plädieren außerdem für Ganzkörperscanner. Hohe Zustimmungswerte gibt es ebenfalls für den Einsatz von Software zur Gesichtserkennung (64 Prozent), Fingerabdruck-Scanner (56 Prozent) sowie Iris-Scanner (51 Prozent).

Zwar gehört die Kameraüberwachung schon heute zum Standard an deutschen Flughäfen, andere digitale Sicherheits-Technologien werden dagegen noch nicht flächendeckend genutzt. Körperscanner beispielsweise können anders als Metalldetektoren auch gefährliche Flüssigkeiten erkennen und sind daher absolut sinnvoll.

Laut der Studie ist die Sicherheit am Flughafen neben der Sicherheit der Airline, dem Preis-Leistungs-Verhältnis und der Flugverbindung für Passagiere das wichtigste Kriterium bei einer Flugreise: Alle Befragten (100 Prozent) bezeichnen diese Punkte als „sehr wichtig" oder „eher wichtig". Es folgen Ticketpreis (98 Prozent), Verpflegung an Bord (86 Prozent), Beinfreiheit an Bord (83 Prozent), Service am Boden (83 Prozent) und das Prestige der Airline (75 Prozent). Ebenfalls wichtige Kriterien sind für die Befragten das Unterhaltungsangebot an Bord (71 Prozent), die Gepäckregeln der Airline (70 Prozent) sowie Kundenbindungsprogramme der Airline (49 Prozent). Fast die Hälfte (45 Prozent) sagt außerdem, dass Internet an Bord, das bisher erst von einigen Fluggesellschaften angeboten wird, „sehr wichtig" oder „eher wichtig" ist.

(Bitkom-Pressemitteilung vom 08.08.2016)

Literaturhinweise

Buchbesprechungen

Tamina Preuß, **Die Kontrolle von E-Mails und sonstigen elektronischen Dokumenten im Rahmen unternehmensinterner Ermittlungen** – Eine straf- und datenschutzrechtliche Untersuchung unter Berücksichtigung von Auslandsbezügen (Schriften zum Strafrecht, Band 292), Duncker und Humblot, Berlin, 2016, 653 S. Print: 119,90 €, Print & E-Book: 143,90 €.

Das Phänomen der unternehmensinternen Ermittlungen zur Aufklärung von Wirtschaftsstraftaten ist spätestens seit der »Siemens-Affäre« in den Fokus der Öffentlichkeit gerückt. Da elektronische Medien in hohem Maße Einzug in den Geschäftsverkehr der Unternehmen gehalten haben, haben die Sichtung, Auswertung und Weitergabe von E-Mails und sonstigen elektronischen Dokumenten hierbei einen herausragenden Stellenwert. Damit die positiven Effekte unternehmensinterner Ermittlungen – wie etwa die Vermeidung und Milderung unternehmensbezogener Sanktionen und die Aufrechterhaltung der Unternehmensreputation – erreicht werden, müssen diese sich innerhalb der Grenzen des materiellen Rechts bewegen. Neben den aus dem Kernstrafrecht zu beachtenden Straftatbeständen – insbesondere der Verletzung des Fernmeldegeheimnisses (§ 206 StGB) und des Ausspähens von Daten (§ 202a StGB) – sind auch die einschlägigen Vorschriften des Nebenstraf- und Ordnungswidrigkeitenrechts in die Überlegungen miteinzubeziehen. Die Autorin hat es sich zur Aufgabe gemacht, praktisch handhabbare Lösungsansätze für eine gesetzeskonforme Kontrolle zu finden.

Die Kapitel des Buches widmen sich neben thematischen Grundlagen der Kontrolle der Vermeidung von Verstößen gegen Strafnormen des StGB sowie gegen Gesetze aus dem Nebenstrafrecht und Ordnungswidrigkeitenrecht (Verstoß gegen Straf- und Bußgeldnormen des TKG – Verstoß gegen Bußgeldnormen des TMG – Verstoß gegen Straf- und Bußgeldnormen des BDSG – Verstoß gegen Straf- und Bußgeldnormen der Landesdatenschutzgesetze – Verstoß gegen Straf- und Bußgeldnormen des BetrVG). Es folgen Besonderheiten bei Sachverhalten mit Auslandsbezug und eine Darstellung von Reformbemühungen. Abgeschlossen wird das Buch mit einem Literatur- und Stichwortverzeichnis.

(Redaktion)

Neuerscheinungen

Aufsätze

Die RDV weist regelmäßig auch auf in anderen Zeitschriften erschienene Beiträge zum Recht der Datenverarbeitung hin, um Recherchen zu relevanten Themen zu erleichtern. Einreichungen von Beiträgen zur Aufnahme eines Hinweises werden gerne entgegengenommen.

Piltz, Carlo, **Die Datenschutz-Grundverordnung,** K&R 2016, 629 ff.

Im Anschluss an den ersten Teil der Beitragsreihe (Heft 9/2016) zur Datenschutz-Grundverordnung (DS-GVO) wird in diesem Teil 2 der Schwerpunkt der Untersuchung auf die Rechte der Betroffenen und die damit korrespondierenden Pflichten des Verantwortlichen gelegt.

Boehme-Neßler, Volker, **Das Rating von Menschen,** K&R 2016, S. 637 ff.

Menschen haben schon immer andere Menschen eingeschätzt und bewertet. Fremde Menschen, die einem begegnen, richtig einzuschätzen, war lange ein wichtiger Überlebensmechanismus. Genauso normal ist es, dass Menschen sich über andere Menschen austauschen. Fraglich ist jedoch, wann diese Meinungsbildung durch vom Menschen nicht vollziehbare Computeranalysen erfolgt.

Kort, Michael, **Arbeitnehmerdatenschutz gemäß der EU-DS-GVO,** DB 2016, 711 ff.

Europäische Vorschriften werden das bisherige deutsche Datenschutzrecht modifizieren. Nach der Erläuterung der wesentlichen Kerninhalte der Verordnung wird sich intensiv mit den Auswirkungen auf den Arbeitnehmerdatenschutz auseinandergesetzt.

Kugelmann, Dieter, **Datenfinanzierte Internetangebote** DuD 2016, S. 566 ff.

Das Internet generiert auch eigenständige Geschäftsmodelle. Diese nutzen in vielen Fällen die Ursprungsidee des Netzes als Medium weltweiter und kostenloser Freiheitsausübung, formen sie aber ökonomisch um. Das Grundprinzip lautet: Daten gegen Leistung. Kritisch hinterfragt wird, ob die Datenschutz-Grundverordnung für diese Geschäftsmodelle angemessene Regelungen bietet.

Laue, Philip, **Öffnungsklauseln in der DS-GVO - Öffnung wohin?**, ZD 2016, S. 463 ff.

Der Beitrag befasst sich mit dem Geltungsbereich einzelstaatlicher Sonderregelungen. Von Interesse ist dieser speziell auch für den Beschäftigtendatenschutz.

Lorenz, Bernd, **Einwilligungserklärungen im Fotorecht,** K&R 2016, S. 450 ff.

Das Anfertigen und Veröffentlichen von Fotos wirft u.a. die Frage auf, welche Personen in das Anfertigen und Veröffentlichen von Fotos einwilligen müssen und was im Rahmen der Einwilligungserklärung zu beachten ist. Bei dem Ausblick auf die DS-GVO bleibt die Frage der Fortgeltung des zuvor angesprochenen KUG offen.

Roßnagel, Alexander, **Wie zukunftsfähig ist die Datenschutz-Grundverordnung?** DuD 2016, S. 561 ff.

Die Datenschutz-Grundverordnung erhebt den Anspruch, den Datenschutz modernisiert und für das 21. Jahrhundert fit gemacht zu haben. Der Beitrag untersucht, inwieweit dies für zwei sehr wesentliche künftige Herausforderungen des Datenschutzes zutrifft: für die explosionsartige Vermehrung personenbezogener Daten durch datengetriebene Geschäftsmodelle und Ubiquitous Computing sowie für die Auswertung dieser enormen Datenfülle durch Big Data. Er kommt zu dem Ergebnis, dass die Datenschutz-Grundverordnung gegenüber diesen Herausforderungen versagt, weil ihre Vorschriften nicht risikoorientiert sind.

Schwichtenberg, Simon, **Die „kleine Schwester" der DS-GVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz,** DuD 2016, S. 605 ff.

Parallel mit der Datenschutz-Grundverordnung (DS-GVO) wurde die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates" veröffentlicht. Die Richtlinie hat bislang deutlich weniger Aufmerksamkeit als die DS-GVO erfahren, ist jedoch aufgrund ihrer sensiblen Regelungsmaterie nicht weniger bedeutsam, insbesonders für die deutsche Strafprozessordnung.

Ziegenhorn, Gero/Gaub, Daniela, **Die EU-Datenschutz-Grundverordnung – Eine erste Analyse für den Bereich der Inkassodienstleistungen,** PinG 2016, S. 89 ff.

Der Beitrag beleuchtet die Weitergabe von Daten an Inkassodienstleister u.a. unter dem Aspekt der Zweckänderung gemäß Art. 6 Abs. 4 DS-GVO. Insgesamt geht er davon aus, dass die DS-GVO die Übermittlung personenbezogener Daten an Inkassodienstleiter weiterhin ermöglicht.

Kein Kredit wegen Twitter

Wer sich für seinen Wohlstand nicht schämt, der erzählt seinen Freunden gerne davon. Heute macht man das effizient über Facebook. Man kann zum Beispiel Bilder von seinen Weihnachtsgeschenken posten und von dem Essen in den Nobelrestaurants, in denen man sich die Festtage versüßt. Solange man öffentlich zeigt, dass es einem gut geht, mag das für Ansehen oder Neid bei der Facebook-Öffentlichkeit sorgen und auch manchen Einbrecher neugierig machen.

Wer ein wenig mehr auf Informationen im Netz wert legt, der twittert. Twitter ist eine Art Nachrichtendienst für jedermann. Man kann dort Informationen loswerden, anderen folgen und sich gezielt informieren lassen. Die vielen Informationen bei Twitter sind aber auch für Zwecke aufschlussreich, die man nicht vermutet. Wer kommt schon auf die Idee, dass Twittern kreditschädigend sein kann. Wissenschaftler haben jetzt über einen längeren Zeitraum Posts bei Twitter von Unternehmen ausgewertet, aus denen sich deren Insolvenz vorhersagen ließ. Dazu wurde insbesondere ein Stimmungsindikator ausgewertet, der deutlich und sehr präzise auf eine Insolvenz und deren Zeitpunkt hinwies.

Datenschutzrechtlich ist dagegen nicht einmal etwas einzuwenden, denn schließlich sind alle ausgewerteten Informationen öffentlich und freiwillig ins Netz gelangt. Man darf aus ihnen genauso Rückschlüsse auf die Kreditwürdigkeit ziehen, wie aus einem dicken Auto, teurem Schmuck, häufigen Reisen und einem großen Haus.

Wer nicht will, dass Dritte sich positiv oder negativ über seine persönlichen Verhältnisse informieren, der sollte in sozialen Netzwerken diesbezüglich diskret auftreten. Eigentlich wissen wir ja, dass alles was wir im Netz öffentlich posten auch für jedermann verfügbar ist. Dennoch wundern wir uns über die Möglichkeiten der Auswertungstechnik. Von der Stimmung im Unternehmen auf dessen Kreditfähigkeit zu schließen, liegt auf den ersten Blick nicht nahe. Auf den zweiten Blick liegt es aber näher, als man es sich wünscht. Wer weiß, was uns noch erwartet? Die Kreativität und Präzision moderner Datenauswertungsmethoden erweitern jedenfalls die Grenzen des normalen Vorstellungsvermögens.