ISSN 0178-8930

G 20 141

RDV

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

3/2016

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

FRANCK, Das System der Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO)

SÖBBING, Customer-Relationship-Management (CRM) – Rechtliche Möglichkeiten beim CRM

LÜDEMANN/ORTMANN/POKRANT, Datenschutz beim Smart Metering – Das geplante Messstellenbetriebsgesetz (MsbG) auf dem Prüfstand

Kurzbeiträge

GOLA, Aus den aktuellen Berichten der Aufsichtsbehörden (25): Unerwünschte Kunden/Mitarbeiter

WEISS, Nach dem Ende von Safe Harbor: Das EU-U.S.-Privacy Shield

Rechtsprechung

Aus dem Inhalt

BVERFG, Verfassungsbeschwerde gegen Ermittlungsbefugnisse des BKA zur Terrorismusbekämpfung teilweise erfolgreich (Ls)

BVERFG, Gegenüber dem mutmaßlich leiblichen Vater gebietet das Grundgesetz keinen Abstammungsklärungsanspruch (Ls)

BVERFG, Der Anordnung einer Betreuung muss eine persönliche Anhörung vorausgehen (Ls)

BGH, Zu den Prüfpflichten des Betreibers eines Ärztebewertungsportals

BGH, Zur Zulässigkeit von Altmeldungen in Onlinearchiven

BAG, Mitbestimmung bei betrieblichem Eingliederungsmanagement (Ls)

BAG, Zuständigkeit des Konzernbetriebsrats beim Einsatz von Überwachungseinrichtungen

32. Jahrgang
Juni 2016
Seiten 109–170

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

32. Jahrgang 2016
Heft 3
Seiten 109–170

RDV
Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 109

Veranstaltungen 110

Aufsätze

Dr. iur. Lorenz FRANCK
Das System der Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO) 111

Dr. Thomas SÖBBING, LLM (HHU)
Customer-Relationship-Management (CRM)
– Rechtliche Möglichkeiten beim CRM 120

Prof. Dr. Volker LÜDEMANN, Manuel Christian ORTMANN LL.M., Patrick POKRANT LL.M.
Datenschutz beim Smart Metering – Das geplante Messstellenbetriebsgesetz (MsbG) auf dem Prüfstand 125

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten der Aufsichtsbehörden (25): Unerwünschte Kunden/Mitarbeiter 133

Steffen WEISS, LL.M
Nach dem Ende von Safe Harbor:
Das EU-U.S.-Privacy Shield 135

Rechtsprechung

Verfassungsbeschwerde gegen Ermittlungsbefugnisse des BKA zur Terrorismusbekämpfung teilweise erfolgreich (Ls)
(BVerfG, Urteil vom 20.04.2016) 138

Gegenüber dem mutmaßlich leiblichen Vater gebietet das Grundgesetz keinen Abstammungsklärungsanspruch (Ls)
(BVerfG, Urteil vom 19.04.2016) 140

Der Anordnung einer Betreuung muss eine persönliche Anhörung vorausgehen (Ls)
(BVerfG, Beschluss vom 23.03.2016) 140

Zu den Prüfpflichten des Betreibers eines Ärztebewertungsportals
(BGH, Urteil vom 01.03.2016) 140

Zur Zulässigkeit von Altmeldungen in Onlinearchiven
(BGH, Urteil vom 16.02.2016) 144

Mitbestimmung bei betrieblichem Eingliederungsmanagement (Ls)
(BAG, Beschluss vom 22.03.2016) 149

Zuständigkeit des Konzernbetriebsrats beim Einsatz von Überwachungseinrichtungen
(BAG, Beschluss vom 26.01.2016) 149

Nutzung einer Domain-Adresse mit dem Namensbestandteil des Arbeitgebers durch einen Arbeitnehmer (Ls)
(BAG, Urteil vom 09.09.2015) 151

Zur Datenübermittlung nach § 28a BDSG
(OLG Frankfurt, Beschluss vom 02.02.2016) 152

Wettbewerbswidrigkeit des Facebook Like-Buttons auf einer Firmenwebsite
(LG Düsseldorf, Urteil vom 09.03.2016)
mit Anmerkung von Eva BEYVERS 152

Zur Umsetzungsfrist eines Werbewiderspruchs (Ls)
(LG Freiburg, Beschluss vom 14.01.2016) 161

Kein absolutes Beweiswertverbot von Dash-Cam-Aufnahmen im Schadensersatzprozess (Ls)
(LG Landshut, Hinweisbeschluss vom 01.12.2015) 161

Auskunftsanspruch des Betriebsrats zu Zielvereinbarungen (Ls)
(LAG Frankfurt/M., Beschluss vom 24.11.2015) 161

Verpflichtung des Arbeitgebers zur Auskunfterteilung gegenüber dem Betriebsrat bzgl. der Kriterien für die Leistung von Zulagen und Einmalzahlungen
(LAG Frankfurt/M., Beschluss vom 04.05.2015) 162

Berichte, Informationen, Sonstiges

37. Internationale Datenschutzkonferenz in Amsterdam (GÜRTLER) 163

91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6./7. April 2016 in Schwerin 164

Neuer Bitkom-Praxisleitfaden „Das Verfahrensverzeichnis“ 165

Patienten wollen Zugang zu ihren Gesundheitsdaten 165

GPS-Tracking erfordert DSB-Bestellung 166

Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge 166

Eine neue Rolle für Gewerkschaften in der digitalen Arbeitswelt 167

Literaturhinweise

Buchbesprechungen

Christina M. Berchtold, Der Wandel genetischer Information (REDAKTION) 168

Thorsten Hennrich, Cloud Computing
– Herausforderungen an den Rechtsrahmen für Datenschutz (REDAKTION) 168

Neuerscheinungen

Aufsätze 169

Nachgefasst 170

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 3/2016; DATAKONTEXT, Frechen

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 3
Seiten 109–170

RDV
Recht der Datenverarbeitung

32. Jahrgang · Juni 2016 · Seiten 109–170

Editorial

Nach dem BDSG ist vor dem BDSG

Mit rückschauend immer noch bemerkenswerter Zügigkeit wurde nach Beginn des Trilogs im Juni 2015 die die Zukunft des Europäischen Datenschutzes wohl über die kommenden Jahrzehnte bestimmende EU-Datenschutz-Grundverordnung verabschiedet und mit Wirkung vom 25.05.2016 in Kraft gesetzt. Geltung haben wird sie ab dem 25.05.2018 (Art. 99 DS-GVO). Der Titel Grundverordnung macht deutlich, dass auf europäischer und aber auch auf nationaler Ebene für ergänzende Regelungen Raum ist. Die je nach Zählweise für den nationalen Gesetzgeber ermittelten 50 – 60 sog. „Öffnungsklauseln" zeigen ihn auf. Der Handlungsspielraum ist jedoch insofern begrenzt, da das mit der Verordnung gewollte Prinzip der Vollharmonisierung als unabdingbare Vorgabe gilt. Demgemäß sollte statt des möglicherweise zu weitreichende Regelungsspielräume vermuten lassenden Begriffs der Öffnungsklausel eher von ergänzenden Regelungsbefugnissen gesprochen werden. Einige von ihnen geben den Mitgliedsstaaten einen Handlungsauftrag; Andere – und das ist die Mehrzahl – eröffnen eine in das Ermessen der Staaten gestellte Handlungsoption.

Der Bundesgesetzgeber hat damit zunächst den Auftrag, das am 24.05.2018 außer Kraft tretenden BDSG insoweit durch gesetzliche Regelungen zu ersetzen, wie sie ihm von der Verordnung zur Vorgabe gemacht werden. Daneben hat er, bezogen auf das BDSG und auch im weiten Feld der bereichsspezifischen Datenverarbeitungsregelungen, die Vereinbarkeit mit der Verordnung zu überprüfen. Diesem Auftrag will er in zwei Schritten nachkommen und zwar indem er zunächst dem zur Ablösung durch die GVO anstehenden BDSG ein neues „abgespecktes" BDSG unmittelbar nachfolgen lassen will, das zum einen den Regelungspflichten der Verordnung nachkommt und zum anderen aus dem BDSG „rettbare und rettwünschbare", d.h. politisch weiterhin gewollte Bestimmungen beibehält.

Das neue BDSG, dessen Entwurf noch vor der Sommerpause vorliegen soll, wird in 7 Kapitel gegliedert sein. Das als allgemeiner Teil konzipierte Kapitel I soll u.a. die Regelungen zur Bestellpflicht betrieblicher Datenschutzbeauftragter enthalten. Eine neue Zulässigkeitsnorm soll die Basis für in Art. 6 Abs. 1 lit. e DS-GVO zugelassene normenklare nationale Regelungen des öffentlichen Sektors bilden. Erhalten werden soll § 6a BDSG insoweit, als dass die automatisierte Einzelentscheidung über die Regelung in Art. 22 Abs. 2 lit. a DS-GVO hinaus auch bei einem sonstigen Rechtsverhältnis erlaubt sein soll. Auch §§ 28a, 28b und 29 Abs. 7 BDSG sollen, wobei über die Rechtsgrundlage hierfür noch diskutiert wird, fortbestehen. Fortgeschrieben werden soll ohne Änderungen auch § 32 BDSG, der damit den Beschäftigtendatenschutz nur partiell national regelt. Längerfristig wird es mit der Anpassung der außerhalb des BDSG angesiedelten Datenschutznormen dauern, wobei die Frist bis Mai 2018 hinsichtlich der anstehenden Mammutaufgabe durchaus kurz ist. An Diskussionsthemen zum Datenschutz wird es also nicht fehlen.

Prof. Peter Gola

Prof. Peter Gola
Mitherausgeber und federführender Schriftleiter der Fachzeitschrift RDV sowie Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn

Termin	Thema	Ort	Kontakt
27.06.2016	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert.)	Köln	GDD e.V. und DATAKONTEXT
29.06.2016	Die Datenschutz-Grundverordnung	Hannover	GDD e.V. und DATAKONTEXT
06.07.2016	Die Datenschutz-Grundverordnung	Düsseldorf	GDD e.V. und DATAKONTEXT
01.-03.08.2016	GDD-Sommer-Workshop	Timmendorfer Strand	GDD e.V. und DATAKONTEXT
25.08.2016	Die Datenschutz-Grundverordnung	Berlin	GDD e.V. und DATAKONTEXT
07.09.2016	Datenschutz-Schwachstellen und Bußgeldrisiken vermeiden – auch für den nebenamtlichen Datenschutzbeauftragten machbar	Köln	GDD e.V. und DATAKONTEXT
08.09.2016	Die Datenschutz-Grundverordnung	Köln	GDD e.V. und DATAKONTEXT
12.-16.09.2016	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
19.09.2016	Einsatz mobiler Endgeräte: Datenschutz und IR-Sicherheit	Frankfurt/M.	GDD e.V. und DATAKONTEXT
20.09.2016	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Frankfurt/M.	GDD e.V. und DATAKONTEXT
21.09.2016	Die Datenschutz-Grundverordnung	Bremen	GDD e.V. und DATAKONTEXT
27.-28.09.2016	Datenschutz Kompakt	Frankfurt/M.	GDD e.V. und DATAKONTEXT
28.09.2016	Social Media rechtskonform nutzen – Abmahnungen vermeiden	Stuttgart	GDD e.V. und DATAKONTEXT
05.10.2016	Beschäftigtendatenverarbeitung: Zulässigkeit und Kontrolle	Frankfurt/M.	GDD e.V. und DATAKONTEXT
06.10.2016	Die Datenschutz-Grundverordnung	Dortmund	GDD e.V. und DATAKONTEXT
11.10.2016	Datenschutz und Videoüberwachung – Was geht und was geht nicht?	Frankfurt/M.	GDD e.V. und DATAKONTEXT
10.-12.10.2016	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Berlin	GDD e.V. und DATAKONTEXT
12.10.2016	Datenschutz und Strafrecht – Beschäftigten- und Kundendaten in internen Ermittlungsverfahren und Strafverfolgungsmaßnahmen	Köln	GDD e.V. und DATAKONTEXT
13.10.2016	Grenzüberschreitender Datenverkehr – Anforderungen-Fallen-Lösungen	Stuttgart	GDD e.V. und DATAKONTEXT
17.10.2016	Datenschutz Aktuell	Stuttgart	GDD e.V. und DATAKONTEXT
24.10.2016	Prüfung von SAP-Systemen durch Datenschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
25.10.2016	Herausforderung Unternehmenskommunikation im Zeitalter 4.0	München	GDD e.V. und DATAKONTEXT
25.10.2016	Kundendatenschutz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
26.10.2016	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Frankfurt/M.	GDD e.V. und DATAKONTEXT
26.10.2016	Die Datenschutz-Grundverordnung	Frankfurt/M.	GDD e.V. und DATAKONTEXT

DATAKONTEXT, Verlagsgruppe Hüthig Jehle Rehm GmbH, Telefon: 02234/9894940

Aufsätze

Dr. iur. Lorenz Franck

Das System der Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO)

„Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen." So heißt es ausdrücklich in Erwägungsgrund (ErwGr) Nr. 11 der Europäischen Datenschutz-Grundverordnung. Der folgende Beitrag führt das in RDV 3/2015 entworfene System der Betroffenenrechte[1] fort und ordnet dabei unter anderem die neuformulierten Einzelansprüche auf Vergessenwerden, Datenübertragbarkeit und Vertretung ein.

I. Überblick

Die DS-GVO soll die in die Jahre gekommene Datenschutzrichtlinie 95/46/EG nicht nur ersetzen, sondern endlich für die lange angestrebte Vollharmonisierung sorgen.[2] Hierzu setzt sie unmittelbar für alle Mitgliedsstaaten anwendbares Recht. Am 14. April 2016 ist die von Kommission, Rat und Parlament erarbeitete Kompromissfassung[3] der bisherigen Entwurfstexte verabschiedet worden. Zu den wesentlichen Neuerungen gehören demnach umfassende Transparenzpflichten, das Recht auf Vergessenwerden, das Recht auf Datenportabilität, eine Niederlegung der Grundsätze von Datenschutz „by design" und „by default" sowie ein ausgesprochen drastisches Sanktionsregime.

Betroffenenrechte sind Ansprüche und Gestaltungsmöglichkeiten, die den Berechtigten aufgrund ihrer Betroffeneneigenschaft zukommen und einen hinreichend konkreten, idealerweise vollstreckungsfähigen Inhalt besitzen. Die beabsichtigte Stärkung der Betroffenenrechte erschöpft sich nicht allein in der Formulierung neu erdachter Einzelansprüche, sondern verleiht ihnen auch insgesamt mehr Gewicht. Die anhand des BDSG entwickelte und in der Lehre bewährte Systematisierung nach fünf Zielrichtungen gilt unterdessen fort: Permissionsrechte gestatten Datenverarbeitungen, die an sich ausgeschlossen wären; Interventionsrechte vermögen bestimmte Datenverarbeitungen zu verhindern; Informationsrechte vermitteln ein Bild darüber, was mit den Daten geschieht; Petitionsrechte verbriefen Beschwerdemöglichkeiten und Kompensationsrechte gewähren Schadensersatz bzw. Entschädigung.

1 Franck, RDV 2015, 137 ff.

2 Näher ErwGr Nr. 9 DS-GVO; vgl. aber Leucker, PinG 2015, 195 ff. ausdrücklich zum „Harmonisierungsmärchen" bzw. Buchner, DuD 2016, 155, 160.

3 Http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE.

Betroffenenrechte				
Permission	**Intervention**	**Information**	**Petition**	**Kompensation**
Einwilligung Einwilligung von Kindern Werbeeinwilligung Schweigepflicht-entbindung Erlass Löschwiderspruch	Widerruf der Einwilligung Widerspruch Unterlassungsanspruch Gegendarstellung Löschung Vergessenwerden Einschränkung Berichtigung	Tranzparenzpflichten bei Direkterhebung Transparenzpflichten außerhalb der Direkterhebung Datenpannen Auskunfts- und Einsichtsrechte Datenübertragbarkeit	Datenschutz-beauftragter Betriebsrat Datenschutzaufsicht Vertretung Staatsanwaltschaft Standesrechtliche Gremien	Art. 82 DSGVO §§ 280 ff. BGB §§ 823 ff. BGB

II. Betroffenenrechte nach Zielen

1. Permission

a) Allgemeine Einwilligung

Die datenschutzrechtliche Einwilligung bewahrt „auch im digitalisierten Lebensalltag eine Entscheidungsmacht des Einzelnen über das Ausmaß der Offenbarung personenbezogener Informationen."[4] Sie wird definiert in Art. 4 Nr. 11 DS-GVO als „jede freiwillig für den bestimmten Fall, in informierter Weise und 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."

Das hergebrachte Verbot mit Erlaubnisvorbehalt liegt auch der DS-GVO zugrunde und lebt in ErwGr Nr. 40 fort. Die Einwilligung wird deswegen bei Datenverarbeitungen nach Art. 6 Abs. 1 lit. a DS-GVO erforderlich, darüber hinaus müssen ggf. besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 2 lit. a DS-GVO für die Verarbeitung freigegeben werden. Es besteht kein grundsätzliches Schriftformerfordernis mehr, ErwGr Nr. 32 stellt insoweit fest, dass die Einwilligung schriftlich, elektronisch oder auch mündlich abgegeben werden kann. Die Erteilung der Einwilligung muss jedoch nach Art. 7 Abs. 1 DS-GVO nachweisbar sein. Ein stillschweigendes Einverständnis soll es nach ErwGr Nr. 32 nicht geben. Art. 7 Abs. 4 DS-GVO und ErwGr Nr. 42 widmen sich der Freiwilligkeit und geben Anhaltspunkte für deren Bewertung.

Nach bisheriger herrschender Meinung kann eine Einwilligung nach § 4a BDSG auch den Verzicht auf technisch-organisatorische Maßnahmen rechtfertigen, da sowohl das „Ob" als auch das „Wie" der Verarbeitung umfasst sind.[5] Eine Bank oder Versicherung kann daher per unverschlüsselter eMail mit dem Betroffenen kommunizieren, wenn dieser dem zugestimmt hat, obwohl anderweitige Kommunikationswege zur Verfügung stünden. Ob diese Möglichkeit allerdings nach Art. 6 Abs. 1 lit. a DS-GVO weiter bestehen wird, ist höchst fraglich.[6] Die Einwilligung wird künftig ausdrücklich an bestimmte Verarbeitungszwecke, also die inhaltliche Datenverarbeitung, geknüpft. Das Datensicherheitsniveau ist demgegenüber objektiv nach Art. 32 DS-GVO zu bestimmen,[7] zudem wird der Datensicherheit durch die neuformulierten Grundsätze des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen nach Art. 25 DS-GVO eine größere Aufmerksamkeit zuteil. Eine abweichende Vereinbarung mit Bordmitteln der DS-GVO erscheint daher auf den ersten Blick unzulässig.[8]

b) Einwilligung von Kindern

Bislang können auch Minderjährige je nach Verwendungszusammenhang in Ansehung ihrer persönlichen Einsichtsfähigkeit wirksam einwilligen[9]. Eine Neuerung bringt insoweit Art. 8 Abs. 1 DS-GVO, wonach eine Altersgrenze von mindestens 16 Jahren bei Angeboten für Dienste der Informationsgesellschaft[10] eingezogen wird.[11] Social Networks, Online-Spiele, Webshops oder die Verknüpfung eines Smartphones mit einem Appstore bzw. Cloud-Speicher werden hiervon erfasst.[12] In all diesen Fällen müssen die Eltern einwilligen, der Einwilligung des Kindes zuvor zustimmen oder diese nachträglich genehmigen.[13] Zugleich muss der für die Verarbeitung Verantwortliche gem. Art. 8 Abs. 2 DS-GVO technisch sicherstellen, dass die Erklärung der Eltern nachweisbar vorliegt.[14]

Die starre Altersgrenze[15] von 16 Jahren stößt auf erhebliche rechtliche Bedenken.[16] Zum einen erschließt sich die besondere Gefährdungslage von Diensten der Informationsgesellschaft gegenüber etwa einer Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO nicht. Der Parlamentsentwurf bezog sich insoweit noch auf sämtliche Angebote von Waren und Dienstleistungen. Jedenfalls aber ist nach Art. 8 Abs. 2 S. 1 GRCh die Einwilligung der betroffenen Person stets nach Treu und Glauben zu ermöglichen. Der Wegfall der Einwilligungsmöglichkeit eines eigentlich einsichtsfähigen Kindes stellt insofern einen ungerechtfertigten Eingriff in ein Betroffenenrecht dar.

c) Werbeeinwilligung

Die Einwilligung hinsichtlich konkreter Werbemaßnahmen per Telefon-, Fax-, eMail- und SMS-Werbung richtet sich nach § 7 UWG. Formvorschriften gelten hierbei nicht, im eigenen Interesse sollten Werbetreibende jedoch eine Nachweismöglichkeit schaffen[17]. Die Werbeeinwilligung fußt ihrerseits auf europarechtlichen Vorgaben und wird

4 Albrecht, CR 2016, 88, 91. Zur Bedeutung der Einwilligung nach der DS-GVO Buchner, DuD 2016, 155, 158 ff.

5 VG Berlin, Urt. v. 24.05.2011, Az.: I K 133.10 (https://dejure.org/2011,29976); Koch, DuD 2014, 691, 692; Franck, RDV 2015, 137; Lotz/Wendler, CR 2016, 31, 35.

6 Noch unentschieden Lotz/Wendler, CR 2016, 31, 36.

7 Nach § 9 S. 2 BDSG sind Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Art. 32 Abs. 1 DS-GVO fordert hingegen ein dem Risiko angemessenes Schutzniveau.

8 Zu entsprechenden Lösungsmöglichkeiten wie der grundrechtskonformen Auslegung von Art. 6 DS-GVO bzw. der unmittelbar aus Art. 8 GRCh abgeleiteten Einwilligung sui generis siehe Franck, in: CR 2016, 238 ff.

9 Simitis, in: Simitis, BDSG, 8. Aufl. 2014, § 4a Rn. 20 f.; Kühling, in: Wolff/Brink, Datenschutzrecht, 2013, § 4a Rn. 32; Gola/Schulz, ZD 2012, 475, 478.

10 Art. 4 Nr. 25 DS-GVO definiert Dienste der Informationsgesellschaft als solche im Sinne von Art. 1 Nr. 2 der Richtlinie 98/34/EG, also „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung".

11 Hierzu insb. Gola/Schulz, ZD 2012, 475 ff.

12 Oder bspw. die Anmeldung eines DeMail-Kontos, vgl. § 3 Abs. 3 S. 4 DeMailG.

13 Schwebende Unwirksamkeit, vgl. parallel § 108 Abs. 1 BGB.

14 Vgl. diesbezüglich Apple Family Sharing, https://support.apple.com/en-us/HT201084.

15 Nach nationalstaatlichem Recht kann ein anderes Alter zugrundegelegt werden, nicht jedoch unter 13 Jahren.

16 So auch Albrecht, CR 2016, 88, 97, der „vollkommen unrealistische Altersgrenzen" moniert.

17 OLG München, Urt. v. 27.09.2012, 29 U 1682/12 (openjur.de/u/566511.html).

insbesondere in Ansehung von Art. 95 DS-GVO unangetastet bleiben.

d) Schweigepflichtentbindung

Die Entbindung von der Schweigepflicht stellt eine Offenbarungsbefugnis im Sinne des § 203 StGB dar. Sie kann ebenfalls formfrei erfolgen. Verschwiegenheitspflichten der Berufsgeheimnisträger bleiben nach Art. 90 Abs. 1 DS-GVO unberührt.

e) Erlass

Der Erlass (§ 397 Abs. 1 BGB) datenschutzrechtlicher Pflichten ist bislang nur eingeschränkt möglich. § 6 Abs. 1 BDSG steht einer (dauerhaften) rechtsgeschäftlichen Abbedingung der Ansprüche auf Auskunft, Berichtigung, Löschung oder Sperrung entgegen. Der Betroffene ist diesbezüglich schlichtweg nicht dispositionsbefugt[18]. Die DS-GVO enthält demgegenüber keine dem § 6 Abs. 1 BDSG vergleichbare Vorschrift.

f) Löschwiderspruch

Durch den Löschwiderspruch sorgt der Betroffene dafür, dass Daten länger als nötig vorgehalten werden. § 35 Abs. 2 S. 2 Nr. 4 BDSG hat insoweit eher eine untergeordnete Rolle gespielt und wird ersatzlos entfallen. Stattdessen kann der Betroffene nach Art. 18 Abs. 1 lit. b DS-GVO bei unrechtmäßiger Verarbeitung eine sog. „Einschränkung der Verarbeitung" erwirken.

2. Intervention

a) Widerruf der Einwilligung

Die datenschutzrechtliche Einwilligung ist bereits heute grundsätzlich frei widerruflich. Durch den Widerruf werden weitere Datenverarbeitungen zukünftig gem. Art. 7 Abs. 3 S. 2 DS-GVO ex nunc gehindert, es sei denn, die verantwortliche Stelle kann sich auf einen anderen Erlaubnistatbestand stützen[19]. Der Rückgriff auf gesetzliche Erlaubnistatbestände kann jedoch ausgeschlossen sein, sofern in der Datenschutzerkärung zugesichert wird, ausschließlich auf Grundlage einer Einwilligung personenbezogene Daten verarbeiten zu wollen.

Der Widerruf der Einwilligung muss dem Betroffenen so einfach gemacht werden wie die Erteilung derselben. Ausnahmsweise ist der Widerruf der Einwilligung ausgeschlossen, wenn er in rechtsmissbräuchlicher Weise erfolgt (§§ 226, 242 BGB), hieran sind jedoch hohe Anforderungen zu stellen.

b) Widerspruch

Art. 21 DS-GVO enthält mehrere Widerspruchsrechte. Verarbeitungen auf Grundlage von Art. 6 Abs. 1 litt. e und f DS-GVO kann aus Gründen widersprochen werden, die sich aus der besonderen Situation der betroffenen Person ergeben. Der Widerspruch richtet sich ausschließlich gegen Verarbeitungen im öffentlichen Interesse oder im Rahmen einer Interessenabwägung bzw. ein auf diese Bestimmungen gestütztes Profiling. Wie sich aus ErwGr Nr. 69 ergibt, kommen hier Aspekte zum Tragen, die der verantwortlichen Stelle etwa zum Zeitpunkt der Interessenabwägung noch unbekannt waren. Der Betroffene hat insoweit eine Initiativverantwortung, entgegenstehende Gesichtspunkte der verantwortlichen Stelle zur Kenntnis zu bringen.[20] Da der Verantwortliche ggf. zwingende schutzwürdige Gründe für die Verarbeitung ins Feld führen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, besteht eine Begründungspflicht für den Widerspruch.[21]

Ähnlich verhält es sich mit dem Widerspruch gegen Datenverarbeitungen zu wissenschaftlichen, historischen Forschungs- oder statistischen Zwecken nach Art. 21 Abs. 6 DS-GVO.

Art. 21 Abs. 2 und 3 DS-GVO betrifft Datenverarbeitungen zum Zwecke des Direktmarketings inklusive des Profilings zu Werbezwecken. Etwaige Gegenrechte der verantwortlichen Stelle sind nicht vorgesehen, eine Begründungspflicht entfällt daher. ErwGr Nr. 70 stellt stattdessen klar, dass der Werbewiderspruch jederzeit und unentgeltlich gewährleistet sein muss. Der Widerspruch gegen konkrete Werbemaßnahmen nach § 7 UWG wird parallel geregelt bleiben.

c) Allgemeiner Unterlassungsanspruch

Ein allgemeiner Unterlassungs- und Beseitigungsanspruch ergibt sich aus den §§ 1004 Abs. 1 analog, 823 Abs. 1 und 2 BGB i.V.m. mit dem allgemeinen Persönlichkeitsrecht bzw. konkreten datenschutzrechtlichen Vorschriften. Er hat neben den spezialgesetzlichen Unterlassungsansprüchen auf Löschung, Einschränkung oder Berichtigung seine Bedeutung keineswegs verloren. So gewährt § 1004 Abs. 1 BGB bei Wiederholungs- oder Erstbegehungsgefahr einen Titel auf zukünftige Unterlassung, der in den spezielleren Anspruchsgrundlagen nicht ausdrücklich enthalten ist.

d) Unterlassung automatisierter Verarbeitung

Das Verbot der automatisierten Verarbeitung einschließlich Profiling in Art. 22 Abs. 1 DS-GVO ist als besonderer Unterlassungsanspruch ausgestaltet. Ausnahmen sind in Abs. 2 festgelegt. Funktional hätte es dieses Anspruches nicht bedurft, er entspricht wegen der enthaltenen Ausnahmeregelung eher einem Erlaubnistatbestand ähnlich Art. 6 DS-GVO. Die Öffnungsklausel zur Beschränkung von Betroffenenrechten in Art. 23 Abs. 1 DS-GVO schlägt hierdurch in eine Öffnungsklausel für bestimmte Datenverarbeitungen um.

18 Der Gesetzgeber beabsichtigte ausdrücklich eine Einschränkung der Privatautonomie im Interesse der Betroffenen, BT-Drs. 11/4306, S. 41.

19 Umkehrschluss aus Art. 17 Abs. 1 lit. b DS-GVO.

20 Nach derzeitiger Rechtslage können dies etwa Fälle sein, in der eine bereits von Datenschutzverstößen betroffene Person weiteren Beeinträchtigungen vorbeugen will, Brink, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 35 BDSG Rn. 76.

21 Dies jedoch ggf. erst auf weitere Nachfrage. Durch Art. 21 Abs. 5 DS-GVO wird immerhin auch die Verwendung automatisierter Verfahren zur Ausübung des Widerspruchsrechts ermöglicht (zur „Do-not-track"-Einstellung des Browsers Albrecht, CR 2016, 88, 93).

e) Gegendarstellung

Der datenschutzrechtliche Gegendarstellungsanspruch nach § 35 Abs. 6 S. 2 BDSG wird ersatzlos entfallen. Das medienrechtliche Pendant bleibt hingegen spezialgesetzlich in den Pressegesetzen der Länder (Zeitungen und Zeitschriften) sowie § 56 RStV (Fernsehen, Radio, Internetveröffentlichungen) erhalten. Das Anspruchsbegehren richtet sich gegen Tatsachenbehauptungen, wobei die Gegendarstellung in Platzierung und Umfang der ursprünglichen Äußerung entsprechen muss. Bei zulässiger Verdachtsberichterstattung besteht kein Anspruch auf Gegendarstellung, sondern lediglich auf die Mitteilung, dass der Verdacht ausgeräumt ist[22].

f) Löschung

Die Löschverpflichtung nach Art. 17 Abs. 1 DS-GVO greift bei

- Zweckerreichung (lit. a),
- Widerruf der Einwilligung (lit. b),
- Widerspruch (lit. c),
- unrechtmäßiger Verarbeitung (lit. d),
- rechtlicher Verpflichtung nach Unions- oder nationalstaatlichem Recht (lit. e) oder bei
- Erhebung der Daten für Dienste der Informationsgesellschaft nach Art. 8 Abs. 1 DS-GVO (lit. f).

Die letzte Tatbestandsvariante meint ausweislich ErwGr Nr. 65 vor allem Konstellationen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte. Jede Löschung hat ohne unangemessene Verzögerung zu erfolgen.

Ausnahmen finden sich in Art. 17 Abs. 3 DS-GVO, namentlich sind dies

- Gründe der Meinungs- und Informationsfreiheit (lit. a),
- die rechtliche Verpflichtung nach Unions- oder nationalstaatlichem Recht bzw. die Wahrnehmung öffentlicher Interessen (lit. b)[23],
- Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (lit. c),
- im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche, historische Forschungs- oder statistische Zwecke (lit. d) oder schließlich
- die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (lit. e)[24].

Da die Löschung nicht nur auf Verlangen der betroffenen Person, sondern gerade auch auf Initiative der verantwortlichen Stelle vonstattengehen soll, müssen zuvor taugliche Löschkonzepte erstellt werden.

g) Recht auf Vergessenwerden

Eine der konkreten Neuerungen findet sich in Art. 17 Abs. 2 DS-GVO mit dem sog. „Recht auf Vergessenwerden". Die Formulierung ist identisch mit derjenigen, die der sog. „Google-Spain"-Entscheidung des EuGH zugeschrieben wird.[25]

In der Sache ging es bei „Google-Spain" um eine Sperrverpflichtung von Suchmaschinenbetreibern, die über die Löschplichten der eigentlichen Webseitenbetreiber hinausgeht.[26] Das Recht auf Vergessenwerden in Art. 17 Abs. 2 DS-GVO zäumt nun das Pferd von hinten auf. Der für die Verarbeitung Verantwortliche, der personenbezogene Daten öffentlich gemacht hat und zur Löschung verpflichtet ist, hat Dritte darüber zu informieren, dass die betroffene Person die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten auch vom Dritten verlangt hat. Suchmaschinen, Linkaggregatoren oder News-Sites, die ihrerseits zur Löschung eines Links verpflichtet sind, müssen also den Erstveröffentlichenden vom Löschbegehren in Kenntnis setzen. Gleichzeitig ist der Erstveröffentlichende gehalten, auf jeden Dritten einzuwirken, der die Daten nun weiterverarbeitet.[27] Eine eigenständige Löschverpflichtung Dritter wird durch die Mitteilung nicht begründet, diese richtet sich originär nach Art. 17 Abs. 1 DS-GVO. Etwaige Ausnahmen vom Recht auf Vergessenwerden sind in Art. 17 Abs. 3 DS-GVO geregelt und decken sich mit denjenigen der Löschung.

Dieses Recht auf Vergessenwerden kann nur greifen, wenn der zur Löschung Verpflichtete die jeweiligen Dritten identifizieren kann. So fordert Art. 17 Abs. 2 DS-GVO angemessene Maßnahmen zur Gewährleistung dieses Rechts unter Berücksichtigung der verfügbaren Technologie und der jeweiligen Implementierungskosten.[28] Wie diese angemessenen Maßnahmen aussehen könnten, darüber schweigt sich der Entwurf aus.[29] Eine neue Vorratsdatenspeicherung zur Abbildung und späteren Verfolgung sämtlicher Informationsströme kann jedenfalls nicht gemeint sein. Disruptive DRM-Technologien würden in unzulässiger Weise in die Löschsouveränität der Dritten nach Art. 17 Abs. 3 DS-GVO eingreifen.

h) Einschränkung der Verarbeitung

Ein Recht auf Sperrung in Form der §§ 20 Abs. 3 und 4, 35 Abs. 3 und 4 BDSG wird es künftig nicht mehr geben. Als funktionales Äquivalent tritt die sog. „Einschränkung der Verarbeitung" nach Art. 18 DS-GVO an deren Stelle. Einschränkung bedeutet in diesem Zusammenhang, dass die

22 BGH, Urt. v. 18.11.2014 - Az. VI ZR 76/14 (http://dejure.org/2014,35148).

23 Etwa handels- und steuerrechtliche Aufbewahrungsfristen (§ 257 HGB; § 147 AO) oder anderweitige Archivierungspflichten (§ 10 Abs. 3 MBO-Ä; § 28 RöntgenVO, § 6 PBV).

24 Hierbei sind insbesondere Verjährungs- und Klageausschlussfristen zu beachten, vgl. etwa §§ 195 f. BGB; § 438 BGB; § 4 S. 1 KSchG; § 21 Abs. 5 AGG.

25 EuGH, Urt. v. 13.05.2014, Az. C-131/12 (https://dejure.org/2014,9457).

26 Kritisch hierzu Arning/Moos/Schefzig, CR 2014, 447, 450 ff.; Holznage/Hartmann, MMR 2016, 228, 231 f. Zur Herleitung ausführlich Boehme-Neßler, NVwZ 2014, 825, 827 ff.

27 So bereits jetzt BGH, Urt. v. 28.06.2015, Az. VI ZR 340/14 (https://dejure.org/2015,21630). Die Urteilsbegründung verweist sogar ausdrücklich auf Art. 17 des DS-GVO-Ratsentwurfs.

28 Siehe auch ErwGr Nr. 66.

29 Kritisch hierzu auch Kipker/Voskamp, DuD 2012, 737, 742; Orthwein/Rücker, DuD 2014, 613, 617.

Daten (abgesehen von ihrer Speicherung) nur noch unter besonders engen Voraussetzungen und besonderen Zweckbestimmungen verarbeitet werden dürfen.[30] Der Anspruch nach Art. 18 Abs. 1 DS-GVO besteht nur,

- wenn die Richtigkeit der Daten bestritten wird (lit. a),
- wenn die Verarbeitung unzulässig war, aber ein Löschwiderspruch eingegangen ist (lit. b),
- nach Zweckerreichnung sofern der Betroffene die Daten noch zur Geltendmachung von Rechtsansprüchen benötigt (lit. c) oder
- wenn ein Widerspruch nach Art. 21 Abs. 1 DS-GVO eingelegt wurde (lit. d).

ErwGr Nr. 67 präzisiert die Methoden zur Einschränkung dahingehend, dass etwa ausgewählte Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentlichte Daten vorübergehend von einer Website entfernt werden.

i) Berichtigung

Der Berichtigungsanspruch nach Art. 16 S. 1 DS-GVO gehört zu den prohibitiven Betroffenenrechten. Der Rechtskreis der datenverarbeitenden Stelle wird durch die Berichtigung nicht erweitert, vielmehr handelt es sich um einen speziellen Unterlassungsanspruch bezogen auf die Verarbeitung unzutreffender Daten. Im Gegensatz zum Wortlaut der §§ 20 Abs. 1, 35 Abs. 1 BDSG ist in Art. 16 S. 2 DS-GVO nunmehr auch die Vervollständigung unvollständiger Daten ausdrücklich enthalten. Die Berichtigung ist ohne unangemessene Verzögerung durchzuführen.

3. Information

a) Informationspflichten

Die Erhebung von Daten löst Informationspflichten aus. Art. 13 DS-GVO betrifft die Direkterhebung, Art. 14 DS-GVO regelt alle übrigen Fälle. Der Transparenzgrundsatz gehört zu den Kernanliegen der Reform und ergibt sich ausweislich ErwGr Nr. 39 aus Treu und Glauben. Die Grundsätze einer fairen und transparenten Verarbeitung machen es mindestens erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird.[31] Sämtliche Informationen sollen leicht zugänglich, verständlich sowie in klarer und einfacher Sprache abgefasst sein und können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (Art. 12 DS-GVO).

aa) Erhebung bei betroffener Person

Zum Zeitpunkt der Erhebung sind gem. Art. 13 Abs. 1 DS-GVO mitzuteilen:

- Kontaktinformationen der verantwortlichen Stelle nebst Vertreter und ggf. Datenschutzbeauftragtem (litt. a und b),
- Zwecke und Rechtsgrundlagen der Verarbeitung (lit. c),
- berechtigte Interessen im Sinne von Art. 6 Abs. 1 lit. f DS-GVO (lit. d),
- Empfänger oder Kategorien von Empfängern (lit. e) sowie
- ein etwaiger Drittlandsbezug nebst Angemessenheitsbeschlusses der Kommission (lit. f).

Nach Art. 13 Abs. 2 DS-GVO sind darüber hinaus zur Verfügung zu stellen:

- die Speicherdauer oder Kriterien zur Festlegung derselben (lit. a),
- Bestehen der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Datenübertragbarkeit (lit. b),
- Bestehen des Rechts auf Widerruf der Einwilligung für Fälle der Artt. 6 Abs. 1 S. 1 lit. a und 9 Abs. 2 lit. a DS-GVO (lit. c),
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (lit. d),
- gesetzliche oder vertragliche Erforderlichkeit und mögliche Folgen einer Nichtbereitstellung (lit. e),
- Durchführung automatisierter Entscheidungsfindung einschließlich Profiling nebst aussagekräftiger Informationen über die verwendete Logik (lit. f).

Die Unterscheidung von „mitteilen“ und „zur Verfügung stellen“ in den Abs. 1 und 2 hat keine Bedeutung, im englischen Entwurfstext wird gleichermaßen das Verb „to provide“ verwendet.

Pikant ist die Forderung nach aussagekräftigen Informationen über die verwendete Logik bei Profiling und automatisierter Einzelentscheidung. Der pauschale Verweis auf Betriebs- und Geschäftsgeheimnisse wie im Schufa-Urteil des BGH[32] wird in Zukunft vss. nicht mehr fruchten.

Art. 13 Abs. 3 DS-GVO statuiert eine erneute Mitteilungspflicht, sofern sich der Zweck der Datenverarbeitung ändert. Ausnahmen von der Mitteilungspflicht bestehen nach Art. 13 Abs. 4 DS-GVO nur, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

bb) Erhebung nicht bei betroffener Person

Der Katalog des Art. 14 Abs. 1 und 2 DS-GVO ist nahezu identisch mit demjenigen des Art. 13 DS-GVO. In Art. 14 Abs. 2 lit. f DS-GVO treten lediglich Angaben zur Datenquelle hinzu, insbesondere, ob es sich um öffentlich zugängliche Quellen handelt. Ein Äquivalent zu Art. 13 Abs. 2 lit. e DS-GVO erübrigt sich außerhalb der Direkterhebung. Für die nachträgliche Zweckänderung gilt Art. 14 Abs. 4 DS-GVO.

Art. 14 Abs. 3 DS-GVO enthält dafür Fristenregelungen. Grundsätzlich ist innerhalb einer angemessenen Frist nach Erlangung der Daten (spätestens nach einem Monat) zu benachrichtigen (lit. a). Sollen die Daten vor Ablauf der Monatsfrist zur Kommunikation mit der betroffenen Person verwendet werden, hat die Mitteilung spätestens zum Zeit-

30 Vgl. Art. 18 Abs. 2 DS-GVO: Einwilligung; Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen; Schutz der Rechte einer anderen natürlichen oder juristischen Person; wichtiges öffentliches Interesse.

31 ErwGr Nr. 60.

32 BGH, Urt. v. 28.01.2014, Az. VI ZR 156/13 (https://dejure.org/2014,492).

punkt der ersten Kontaktaufnahme zu erfolgen (lit. b). Sofern hingegen eine Weitergabe beabsichtigt ist, ist der Zeitpunkt der ersten Weitergabe maßgeblich (lit. c).

Auch der Katalog an Ausnahmetatbeständen ist außerhalb der Direkterhebung umfangreicher. Nach Art. 14 Abs. 5 DS-GVO wird von der Benachrichtigung abgesehen,

- wenn die betroffene Person bereits informiert ist (lit. a),
- wenn sich die Benachrichtigung als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde (lit. b),
- wenn die Erlangung bzw. Weitergabe durch Unions- oder mitgliedsstaatliches Recht ausdrücklich geregelt ist und geeignete Maßnahmen zum Schutz der Person vorgesehen sind (lit. c) oder
- wenn Daten einem Berufsgeheimnis bzw. einer satzungsmäßigen Geheimhaltungspflicht unterliegen (lit. d).

Die Vorschrift erreicht zwar nicht die Regelungsdichte des bisherigen § 33 Abs. 2 BDSG, die Öffnungsklauseln in Art. 14 Abs. 4 litt. c und d DS-GVO leisten jedoch einem gewissen Wildwuchs Vorschub.

cc) Form

Die Menge an bereitgestellten Informationen geht insgesamt weit über das hinaus, was derzeit in den §§ 4 Abs. 3 und 33 Abs. 1 BDSG gefordert wird. Insoweit stellt sich die Frage nach einer geeigneten Darreichungsform. Bei Vorgängen im Internet wird eine elektronische Wiedergabe genügen, wenn die dauerhafte Speichermöglichkeit besteht.[33] Die Frage ist allerdings, ob etwa bei Verwendung von Papierunterlagen oder auch einer Videoüberwachung eine körperliche Wiedergabe der Transparenzinformationen nötig ist.

Art. 12 Abs. 1 S. 2 DS-GVO stellt insofern klar, dass die Transparenzinformationen sowohl dem Einzelnen als auch der Öffentlichkeit in elektronischer Form bereitgestellt werden können. Art. 12 Abs. 7 DS-GVO betrifft darüber hinaus die Verwendung von standardisierten Bildsymbolen in elektronischer und maschinenlesbarer Form. Der leichte Zugang wird stets betont[34], insofern dürfte neben der Angabe essentieller Informationen z.B. ein Verweis auf eine Kurz-URL nebst QR-Code genügen.

dd) Folgen eines Transparenzverstoßes

Handelt es sich bei den Artt. 13 und 14 DS-GVO nun um bloße Ordnungsvorschriften oder um echte Rechtmäßigkeitsvoraussetzungen? Die Entwurfsfassung äußert sich hierzu nicht ausdrücklich. ErwGr Nr. 39 macht deutlich, dass jede Verarbeitung personenbezogener Daten rechtmäßig und nach Treu und Glauben erfolgen sollte und führt sodann in die Transparenzpflichten ein. Dies ist jedoch zu wenig, um aus einem Transparenzverstoß unmittelbar die Rechtswidrigkeit der gesamten Verarbeitung zu folgern und dementsprechend drastische Sanktionen zu verhängen. Etwaigen Transparenzverstößen sollte daher vielmehr durch Bußgeldtatbestände im Sinne von Art. 84 Abs. 1 DS-GVO begegnet werden.

b) Datenpannen

Die Meldepflicht bei Datenpannen nach den Artt. 33 und 34 DS-GVO soll physische, materielle oder immaterielle Schäden verhüten helfen[35] und wartet mit vielfältigen Neuerungen gegenüber der bisherigen Rechtslage auf. So wird die bisherige Unterscheidung in Risiko- und sonstige Daten aufgegeben.[36] Die Meldepflicht trifft öffentliche und private Stellen künftig gleichermaßen.[37] Vor allem aber beschränkt sich die tatbestandliche Definition der „Verletzung des Schutzes personenbezogener Daten" nicht mehr nur auf die unrechtmäßige Kenntnisnahme durch Dritte. Auch Verfügbarkeits- und Integritätsverletzungen sind nun umfasst.[38] Selbst die unbefugte interne Weitergabe kann als Schutzverletzung angesehen werden.[39] Die Meldepflicht des Auftragsverarbeiters gegenüber dem Auftraggeber ist in Art. 33 Abs. 2 DS-GVO gesetzlich niedergelegt.[40]

aa) Meldung an die Aufsichtsbehörde

Ohne unangemessene Verzögerung und möglichst binnen 72 Stunden ist gem. Art. 33 Abs. 1 und 3 DS-GVO eine Meldung an die Aufsichtsbehörde abzusetzen, die im Wesentlichen derjenigen nach § 42a S. 3 und 4 BDSG gleicht. Von der Meldung kann abgesehen werden, sofern der Vorfall voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen führt. Eine Regelung, die den Grundsatz der Selbstbelastungsfreiheit[41] nach Art. 14 Abs. 3 IPbpR bzw. Art. 6 Abs. 1 S. 1 EMRK berücksichtigen würde, fehlt komplett. Hier müsste ggf. auf Sanktionsebene im Rahmen von Art. 84 Abs. 1 DS-GVO nachgebessert werden.

bb) Meldung an die betroffene Person

Besteht ein wahrscheinlich hohes Risiko für die persönlichen Rechte und Freiheiten, ist daneben grds. den Betroffenen eine Meldung nach Art. 34 Abs. 1 und 2 DS-GVO zuzuleiten. Nach Art. 34 Abs. 3 DS-GVO kann die Benachrichtigung wiederum entfallen,

33 Ggf. in Anlehnung an die Form einer Widerrufsbelehrung, vgl. BGH, Urt. v. 15. Mai 2014, Az. III ZR 368/13 (https://dejure.org/2014,11644).

34 ErwGr Nrn. 39, 58; Art. 12 Abs. 1 S. 1, 12 Abs. 7 DS-GVO.

35 ErwGr Nr. 85 zählt mögliche Fallkonstellationen auf.

36 Vgl. § 42a S. 1 Nrn. 1-4 BDSG.

37 Kritisch zur Beschneidung des Adressatenkreises nach § 42a BDSG Franck, GDD-Ratgeber Datenpannen, 2. Aufl. 2015 (http://t1p.de/Datenpannen2015), S. 18 m.w.N.

38 Definition in Art. 4 Nr. 12 DS-GVO. Näher hierzu Marschall, DuD 2015, 183, 184; anschauliches Fallbeispiel bei der Art. 29-Gruppe, Opinion 3/2014 on Personal Data Breach Notification, 693/14/EN, (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/ 2014/wp213_en.pdf), S. 5.

39 Marschall, DuD 2015, 183, 184.

40 Vgl. stattdessen die vertragliche Ausgestaltung nach geltendem Recht, Franck, Datenpannen (Fn. 41), S. 41 f.

41 Vgl. insoweit § 42a S. 6 BDSG, näher hierzu Franck, Datenpannen (Fn. 41), S. 31 ff.

- wenn geeignete technische und organisatorische Sicherheitsvorkehrungen (insb. Verschlüsselung) eingesetzt wurden (lit. a)[42],
- das hohe Risiko durch nachfolgende Maßnahmen aller Wahrscheinlichkeit nach eingedämmt wurde (lit. b) oder
- die Meldung mit einem unverhältnismäßigen Aufwand verbunden wäre (lit. c).

In letzterem Fall tritt an die Stelle der Einzelbenachrichtigung eine öffentliche Bekanntmachung.

c) Allgemeine datenschutzrechtliche Auskunft

Das allgemeine Auskunftsrecht erfasst nicht nur die vorhandenen Daten, sondern nach Art. 15 Abs. 1 Hs. 1 DS-GVO auch ausdrücklich die Frage, ob überhaupt Daten vorhanden sind.[43]

aa) Inhalt

Der für die Verarbeitung Verantwortliche hat nach Art. 15 Abs. 1 Hs. 2 DS-GVO Auskunft zu erteilen über

- die Verarbeitungszwecke (lit. a),
- die Kategorien personenbezogener Daten (lit. b),
- Empfänger oder Kategorien von Empfängern (lit. c),
- die Speicherdauer oder Kriterien für die Festlegung derselben (lit. d),
- umfassende Betroffenenrechte (litt. e und f),
- die verfügbaren Informationen über die Herkunft der Daten außerhalb der Direkterhebung (lit. g) sowie
- das Bestehen einer automatisierten Entscheidungsfindung nebst aussagekräftiger Informationen über die verwendete Logik (lit. h)[44].

Nach Art. 15 Abs. 2 DS-GVO besteht zudem ein Unterrichtungsrecht hinsichtlich geeigneter Datenschutzgarantien bei unsicheren Drittländern.

Art. 19 S. 2 DS-GVO enthält an etwas versteckter Stelle noch einen weiteren Anspruch auf Information darüber, welchen Empfängern die Berichtigung, Löschung oder Einschränkung von Daten mitgeteilt wird. Diese Information muss allerdings durch den Betroffenen konkret angefragt werden.

Das Auskunftsrecht wird nach Art. 15 Abs. 4 DS-GVO nur durch Rechte und Freiheiten anderer Personen beschränkt.[45] Dies darf entsprechend ErwGr Nr. 63 jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.

bb) Form und Entgelt

Der für die Verarbeitung Verantwortliche stellt gem. Art. 15 Abs. 3 S. 1 DS-GVO eine Kopie der angefragten Daten zur Verfügung. Die erste Kopie ist kostenfrei, für jede weitere Kopie darf ein „angemessenes" Entgelt verlangt werden. Wird der Antrag in elektronischer Form gestellt, so soll die Auskunft nach Art. 15 Abs. 3 S. 3 DS-GVO ebenfalls auf gängigem elektronischem Wege erfolgen, sofern der Betroffene nichts anderes angibt. Dies stellt jedoch keinen Freibrief zum Unterlaufen technisch-organisatorischer Maßnahmen nach Art. 32 DS-GVO dar. Nach Vorstellung des Verordnungsgebers könnte der Verantwortliche z.B. den Fernzugang zu einem sicheren System bereitstellen, um den Betroffenen direkten Zugang zu ihren personenbezogenen Daten zu ermöglichen.[46] Nach ErwGr Nr. 64 sollten allerdings alle vertretbaren Mittel genutzt werden, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen.

d) Spezielle Einsichtsrechte

Die Einsicht in Personalakten nach § 83 BetrVG bzw. § 110 BBG oder Einsicht in Patientenakten nach § 630g BGB werden nach Inkrafttreten der DS-GVO voraussichtlich erhalten bleiben. Zu den uneigentlichen Betroffenenrechten[47] gehören ferner das vertragliche Informationsrecht nach den §§ 311, 242 BGB[48] und das Urkundeneinsichtsrecht nach § 810 BGB[49]. Für die Urkundeneinsicht bedarf es eines konkreten rechtlichen Interesses. Dieses fehlt, wenn der Anspruchsteller nur auf Grund vager Vermutungen Material für eine spätere Rechtsverfolgung sammeln möchte[50].

e) Recht auf Datenübertragbarkeit

Das Recht auf „data portability" in Art. 20 Abs. 1 DS-GVO ist ein Informationsanspruch mit gesetzlich festgelegter, besonderer Form. Es geht um die Herausgabe strukturierter und maschinenlesbarer Daten[51] zwecks Übertragung zu einem anderen Dienstleister. Die Daten werden dabei nicht nur über die Bande des heimischen Rechners gespielt, sondern nach Art. 20 Abs. 2 DS-GVO auf Wunsch auch direkt zwischen den konkurrierenden Anbietern transferiert, soweit dies technisch möglich ist.

Der Anspruch besteht nur, sofern die Datenverarbeitung auf Grundlage einer Einwilligung (Artt. 6 Abs. 1 S. 1 lit. a bzw. 9 Abs. 2 lit. a DS-GVO) oder einer vertraglichen Verpflichtung (Art. 6 Abs. 1 lit. b DS-GVO) erfolgt und bezieht sich ausschließlich auf Daten, die die betroffene Person selbst bereitgestellt hat.

42 Vgl. hierzu § 109a Abs. 1 S. 3 TKG, näher Franck, Datenpannen (Fn. 41), S. 44.

43 Entsprechend der bisherigen h.M. zu § 34 BDSG, vgl. Weichert, NVwZ 2007, 1004, 1005; Dix, in: Simitis, BDSG, 8. Aufl. 2014, § 34 Rn. 18; Schmidt-Wudy, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 34 Rn. 14; Franck, ZD-Aktuell 2015, 04740.

44 Zur Offenbarung von Algorithmen siehe oben, Abschn. II. 3. a) aa).

45 Der umfangreiche Ausnahmenkatalog des § 34 Abs. 7 BDSG scheint damit abgeschafft. Über die Öffnungsklausel in Art. 23 DS-GVO bleibt dem nationalen Gesetzgeber jedoch einiges an Spielraum.

46 ErwGr Nr. 63.

47 „Uneigentlich", siehe Franck, RDV 2015, 137, 141.

48 BGH, Urt. v. 23.11.1982, VI ZR 222/79 (dejure.org/1982,125); LG Bochum, Urt. v. 22.08.2008, I-5 S 72/08 (openjur.de/u/133343.html); AG München, Urt. v. 24.02.2009, 282 C 26259/08 (openjur.de/u/474499.html).

49 LG Kiel, Urt. v. 04.04.2008, 8 O 50/07 (openjur.de/u/167342.html).

50 BGH, Beschl. v. 20.06.2013, IX ZB 50/12 (openjur.de/u/643776.html).

51 Also Datenbankformate (XML, kommaseparierte Liste, SQlite etc.) oder Ordnerstrukturen. Eine bloße Wiedergabe in HTML wird nicht genügen, Kipker/Voskamp, DuD 2012, 737, 740. ErwGr Nr. 68 regt insoweit die Entwicklung interoperabler Formate an; näher zur Frage von Interoperabilität und Strukturierung auch Schätzle, PinG 2016, 71, 74.

Ursprünglich war der Anspruch für den Umzug von social-media-Profilen zu konkurrierenden Anbietern gedacht,[52] erfasst aber nunmehr alle automatisierten Verarbeitungen auf Grundlage von Einwilligung und Vertrag.[53] Wegen der Möglichkeit des Direkttransfers nach Art. 20 Abs. 2 DS-GVO ist der Anspruch vor allem für den Wechsel des Cloudspeicher-Anbieters bei großen Datenmengen interessant.

Das Recht auf Datenportabilität gilt nicht bei Verarbeitungen im öffentlichen Interesse (Art. 20 Abs. 3 S. 2 DS-GVO) oder, soweit Rechte und Freiheiten anderer Personen beeinträchtigt werden (Art. 20 Abs. 4 DS-GVO).

4. Petition

a) Datenschutzbeauftragter

Erste Anlaufstelle bei Beschwerden, gewissermaßen als „Anwalt der Betroffenen", ist der betriebliche oder behördliche Datenschutzbeauftragte.[54] Nach Art. 38 Abs. 4 DS-GVO kann der Datenschutzbeauftragte durch Betroffene in allen Fragen zu Rate gezogen werden, die mit der Verarbeitung von personenbezogenen Daten oder mit der Wahrnehmung von Betroffenenrechten in Zusammenhang stehen.

b) Betriebsrat

Über Fragen des Beschäftigtendatenschutzes wacht zudem gem. § 80 Abs. 1 Nr. 1 BetrVG der Betriebsrat, er kann gem. § 85 Abs. 1 BetrVG angerufen werden.[55] Die Vorschriften des Betriebsverfassungsgesetzes werden vss. Bestand haben.

c) Datenschutzaufsichtsbehörde

Jede betroffene Person kann sich nach Art. 77 Abs. 1 DS-GVO bei einer Aufsichtsbehörde beschweren, wenn sie der Ansicht ist, dass die Verarbeitung ihrer personenbezogenen Daten gegen Vorgaben der DS-GVO verstößt. Nach Art. 78 Abs. 2 DS-GVO muss die Behörde künftig den Betroffenen innerhalb von drei Monaten über den Stand oder das Ergebnis der Beschwerde unterrichten.[56]

Die jeweiligen Zuständigkeiten ergeben sich aus den Artt. 55 ff. DS-GVO und wurden aus Betroffenensicht stark vereinfacht.[57] Schlichtweg jede Aufsichtsbehörde ist nach Art. 56 Abs. 2 DS-GVO für die Entgegennahme von Beschwerden zuständig, alles Weitere regeln die Behörden untereinander. Zur weiteren Erleichterung wird in ErwGr Nr. 141 angeregt, Maßnahmen wie die Bereitstellung eines elektronischen Beschwerdeformulars zu ergreifen.

d) Vertretung

Das Verbandsklagerecht bei Datenschutzverstößen nach dem UKlaG ist noch druckfrisch.[58] Verbraucherschutzverbände können seit dem 24. Februar 2016 intervenieren, wenn die Erhebung personenbezogener Daten eines Verbrauchers durch einen Unternehmer in rechtswidriger Weise erfolgt oder wenn die Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden.[59] Die Verbände werden dieses Instrument nach Art. 80 Abs. 2 DS-GVO behalten.

Art. 80 Abs. 1 DS-GVO gewährt den Betroffenen darüber hinaus auch die Möglichkeit, Einrichtungen, Organisationen oder Vereinigungen konkret mit der Durchsetzung ihrer Betroffenenrechte zu beauftragten. Vertretungsberechtigt sind nur solche Institutionen, die keinen Erwerbszweck verfolgen, deren satzungsmäßige Ziele von öffentlichem Interesse sind und die bereits im Bereich des Datenschutzes tätig sind. Erfasst sind das Beschwerderecht bei der Aufsichtsbehörde (Art. 77 DS-GVO), die justiziellen Rechte (Artt. 78 f. DS-GVO) sowie die Inanspruchnahme wegen Schadensersatzes (Art. 82 DS-GVO). Es handelt sich hierbei nicht um ein gewillkürt-standschaftliches Verhältnis, sondern um ein reines Vertretungsrecht.[60]

e) Standesrechtliche Gremien

Berufs- und gewerbespezifische Strukturen bieten ebenfalls Ansprechpartner für Fragen des Datenschutzes. Verstöße gegen berufsrechtliche Verschwiegenheitspflichten können insofern weiterhin von den jeweiligen Kammern standesrechtlich geahndet werden. Auch andere standesrechtliche Gremien, wie z.B. der Rat der deutschen Markt- und Sozialforschung bieten eigenständige Beschwerdemöglichkeiten[61].

f) Staatsanwaltschaft

Strafrechtliche Datenschutzverstöße nach den §§ 201 ff. und 303a f. StGB, § 33 KUG[62] oder auch § 17 UWG können schließlich gem. § 158 Abs. 1 StPO bei Staatsanwaltschaft und Polizei zur Anzeige gebracht werden.

5. Kompensation

a) Art. 82 DS-GVO

Die allgemeine Schadensersatznorm findet sich in Art. 82 DS-GVO. Bei Verstoß gegen die Verordnung sind sowohl Ver-

52 Zum Sinn dessen Kipker/Voskamp, DuD 2012, 137, 140 f.

53 So z.B. auch das Arbeitsverhältnis. Zur Übertragung von Fahrverhaltensdaten von einem Fahrzeug-Leasinggeber zum nächsten Schätzle, PinG 2016, 71, 73, obschon sich die Frage stellt, ob diese Daten tatsächlich „bereitgestellt" wurden im Sinne von Art. 20 Abs. 1 DS-GVO.

54 Eingehend Jaspers/Reif, RDV 2016, 61 ff.

55 Näher Kort, NZA 2015, 1345 ff.; Franck/Reif, ZD 2015, 405, 408.

56 Anders bisher, da überhaupt keine Frist zur Äußerung angenommen wurde, vgl. VG Neustadt, Beschl. v. 22.12.2015, Az. 4 K 867/15.NW (https://dejure.org/2015,40610). Auch wenn weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde nötig wird, sollte hierüber informiert werden, ErwGr Nr. 141.

57 Zum sog. „one-stop-shop"-Prinzip Gierschmann, ZD 2016, 51, 51 f.

58 BGBl. 2016 I, S. 233 ff.

59 Im Einzelnen Gola, RDV 2016, 17 ff.; Spindler, ZD 2016, 114 ff.; Jaschinski/Piltz, WRP 2016, 420 ff.; Halfmeier, NJW 2016, 1126 ff.

60 Die englische Textfassung „lodge the complaint on his or her behalf" ließe auch eine Standschaft zu, die redaktionelle Überschrift "Vertretung"/"Representation" dürfte jedoch eindeutig sein.

61 Einzelheiten unter http://rat-marktforschung.de/beschwerde/.

62 Das KUG wird vss. erhalten bleiben.

antwortliche als auch Auftragsverarbeiter zum Ersatz des materiellen bzw. immateriellen Schadens verpflichtet. Der Begriff des Schadens soll ausweislich ErwGr Nr. 146 „im Lichte der Rechtsprechung des Europäischen Gerichtshofs" weit ausgelegt werden, und zwar auf eine Art und Weise, die den Zielen der DS-GVO in vollem Umfang entspricht.

Wie beim bisherigen § 7 BDSG handelt es sich um eine Haftung für vermutetes Verschulden (Art. 82 Abs. 3 DS-GVO). Auftragsverarbeiter können sich gem. Art. 82 Abs. 2 S. 2 DS-GVO exkulpieren, wenn sie ihren speziellen gesetzlich auferlegten Pflichten nachgekommen sind und unter Beachtung der rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt haben.

Sind mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter wegen derselben Verarbeitung ersatzpflichtig, greift eine gesamtschuldnerische Haftung nebst Innenausgleich nach Art. 82 Abs. 4 und 5 DS-GVO.

b) Sonstiges Schadensersatzrecht

Das Schicksal von spezialgesetzlichen Anspruchsgrundlagen wie § 44 TKG oder auch § 82 SGB X ist bislang noch ungewiss. Die §§ 280 ff. BGB für die vertragliche sowie die §§ 823 ff. BGB für die deliktische Haftung werden jedoch auch weiterhin Anwendung finden und durch Art. 77 DS-GVO nicht verdrängt. Bei einem Verstoß gegen die DS-GVO als solche besteht insoweit Anspruchsgrundlagenkonkurrenz.

III. Zusammenfassung und Ausblick

Die neuen Vorschriften haben unmittelbaren Einfluss auf die Datenschutzorganisation. Nach ErwGr Nr. 59 und dem darauf aufbauenden Art. 12 DS-GVO gilt es, Modalitäten festzulegen, die es einer betroffenen Person ermöglichen, die ihr zustehenden Rechte wahrzunehmen, darunter insbesondere auch Mechanismen, die dafür sorgen, dass sie unentgeltlich den Zugang zu Daten, deren Berichtigung bzw. Löschung beantragen oder von ihrem Widerspruchsrecht Gebrauch machen kann. Anträge sollen spätestens innerhalb eines Monats beantwortet werden, Ablehnungen sind zu begründen.

In RDV 3/2015 hieß es, eine Zergliederung der Betroffenenrechte nach ihren fünf Zielrichtungen werde „das Verständnis der neuen Regelungen erleichtern und das Selbstbewusstsein der Betroffenen stärken."[63] In der Tat hat das anhand geltenden Rechts erarbeitete Schema weiterhin Bestand. Die neuen Vorschriften fügen sich nahtlos in das System der Betroffenenrechte ein. Das Instrumentarium erscheint auch durchaus geeignet, die beabsichtigte Stärkung und Präzisierung herbeizuführen.[64] Freilich ergeben sich Detailabweichungen zur bisherigen Rechtslage, jedoch sind diese im Interesse eines gesamteuropäischen Regelwerkes hinzunehmen. Spannend bleibt unterdessen die Frage, welche Einschränkungen von Betroffenenrechten der nationale Gesetzgeber auf Grundlage von Art. 23 DS-GVO schaffen oder beibehalten wird.

Dr. iur. Lorenz Franck
ist Referent für Beschäftigten-, Sozial- und Gesundheitsdatenschutz bei der Gesellschaft für Datenschutz und Datensicherheit e.V. in Bonn sowie Lehrbeauftragter für Datenschutzrecht an der TH Köln.

63 Franck, RDV 2015, 137, 141.

64 Zustimmend Gierschmann, ZD 2016, 51,55; Albrecht, CR 2016, 88, 92.

Bitte vormerken

40. DAFTA

„Vom BDSG zur DS-GVO – Der Countdown läuft"

17 – 18.11.2016 in Köln

35. RDV-FORUM

16.11.2016 in Köln

Dr. Thomas Söbbing, LLM (HHU)

Customer-Relationship-Management (CRM) – Rechtliche Möglichkeiten beim CRM

Das Customer-Relationship-Management (Kurzform CRM) wird in der Praxis dazu genutzt, um Kunden-, Anbieter- und Partnerbeziehungen systematisch zu sammeln und zu pflegen. Diese so gesammelten Daten sind notwendig, um Vertragsbeziehungen erfüllen zu können. Denn manche Unternehmen sind so groß, dass eine Vertragserfüllung fast unmöglich ist, wenn man den richtigen Ansprechpartner nicht kennt. Dabei ist in der Praxis kaum bekannt, dass dem Sammeln von personenbezogenen Daten in einem CRM-System sehr enge rechtliche Schranken gesetzt sind. Diese orientieren sich vor allem an § 28 BDSG und dem Grundsatz der Datensparsamkeit und der Datenvermeidung. Der folgende Artikel zeigt die rechtlichen Grenzen des Datensammelns in einem CRM-System auf. Erschwerend kommt dabei hinzu, dass diese Grenzen nicht immer einheitlich sein müssen und je nach Art der Vertragserfüllung auch unterschiedlich gestaltet sein können.

I. Definition

Der Erfolg eines Unternehmens ist auch abhängig von der Bindung des Kunden/Partners an das Unternehmen.[1] Eine Bindung von Kunden/Partnern an ein Unternehmen ist immer dann erfolgsversprechend, wenn das Unternehmen in besonders guter Weise die Bedürfnisse und Interessen von Kunden/Partnern kennt und versteht. Um diese Bedürfnisse und Interessen besser zu verstehen, dient das sog. Customer-Relationship-Management, kurz CRM (dt. Kundenbeziehungsmanagement). Die Betriebswirtschaftslehre versteht unter einem CRM einen strategischen Ansatz, der zur „vollständigen Planung, Steuerung und Durchführung aller interaktiven Prozesse mit den Kunden genutzt wird."[2] Dabei bezeichnet das CRM auch die Dokumentation und Verwaltung von Kundenbeziehungen und ist ein wichtiger Baustein für das (Beziehungs-)Marketing der Unternehmen. Die Informationen aus den Beziehungen zu Kunden und Partnern sind in speziell dafür gestalteten Datenbanken („CRM-Systemen") gespeichert.[3] Bekannte Anbieter für CRM-Systeme sind Unternehmen wie Oracle (vormals Siebel) und Salesforce.com. Dabei bietet Salesforce.com eine innovative Software-as-Service-(SaaS)-Lösung an. Die CRM-Systeme dienen dazu, alle Beziehungen und Interaktionen eines Unternehmens mit bestehenden und potenziellen Kunden, Anbietern und Partnern zu sammeln und zu pflegen.[4] Durch die systematische Pflege der Kundenbeziehungen soll letztendlich eine Steigerung des Unternehmenserfolges erzielt werden.[5] Dabei ist es möglich, CRM-Systeme mit anderen IT-Systemen wie ERP, Marketing etc. zu koppeln, um eine höhere Durchdringung zu erreichen.

Bei der Speicherung und Verarbeitung von personenbezogenen Daten ist der Frage der datenschutzrechtlichen Zulässigkeit große Aufmerksamkeit zu schenken, da landläufig eine andere Meinung in der Praxis dazu besteht, was gespeichert werden darf und was nicht.

II. Rechtliche Fragen

Viele Unternehmen stellen sich die Frage, welche personenbezogenen Daten sie in einem CRM-System speichern dürfen. Der das Datenschutzrecht bestimmende Grundsatz des Verbotes mit Erlaubnisvorbehalt stellt die Einwilligung des Betroffenen in das Zentrum der datenschutzrechtlichen Zulässigkeitsprüfung. Liegt keine wirksame Einwilligung vor, stellt sich die Frage nach dem gesetzlichen Erlaubnistatbestand. Die Verwendung von CRM-Systemen unterliegt dann den Voraussetzungen des § 28 BDSG.[6]

1. Speicherung von Daten nach Vertragsabschluss

Gem. § 28 Abs. 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Insoweit enthält diese Norm einen gesetzlichen Erlaubnistatbestand, der eine sonst gesetzlich notwendige Einwilligung überflüssig macht.[7]

a) Erforderlichkeit

Der Wortlaut des Gesetzes stellt auf die Erforderlichkeit der Erhebung, Speicherung, Veränderung oder Übermittlung der Daten für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses ab.[8] Die Erforderlichkeit führt dazu, dass eine Einwilligung des Betroffenen nicht notwendig ist. Die Erforderlichkeit der Speicherung der Daten im CRM-System ist rechtlich nur zulässig, soweit diese in dem gesetzlich genannten Zusammenhang

1 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 1. Aufl. 2014, Teil VI, Rn. 1.

2 Gabler, Wirtschaftslexikon Online, Stichwort Customer-Relationship-Management, abgerufen am 16.02.2016.

3 Grützner/Jakob, Compliance von A-Z, 2. Aufl. 2015.

4 Hippner/Hubrich/Wilde, Grundlagen des CRM: Strategie, Geschäftsprozesse und IT-Unterstützung, 3. Aufl. 2011, S. 3.

5 Bergmann, Angewandtes Kundenbindungsmanagement, 1. Aufl. 1998, S. 38.

6 Nach § 27 Abs.1 Nr. 1 BDSG ist der § 28 BDSG auch auf nicht öffentliche Stellen, damit auch auf den unternehmerischen Verkehr, anwendbar.

7 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 1. Aufl. 2014, Teil VI, Rn. 35.

8 Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 14, 26.

zu einem Vertrag stehen.[9] Voraussetzung hierfür ist, dass diese Daten nur für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses „mit dem Betroffenen" erforderlich ist.[10]

Erforderlich sind sicherlich vertraglich festgehaltene Ansprechpartner. Solche Informationen sind regelmäßig notwendig, damit ein Lieferant seine Waren beim Kunden wirklich an den richtigen Ansprechpartner liefert. Es ist auch im Interesse des Kunden, dass die Waren des Lieferanten an die richtige Stelle beim Kunden gelangen, da sonst die Waren innerhalb des Betriebs transferiert werden müssen oder im schlimmsten Falle auch verloren gehen können. Dies gilt insbesondere dann, wenn ein Unternehmen sehr groß ist. In solchen Fällen ist eine Speicherung von CRM-Daten durchaus im Sinne des Betroffenen.

b) Berechtigtes Interesse

Soweit die Verwendung personenbezogener Daten für die Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist, gestattet § 28 Abs. 1 Nr. 2 BDSG dies, sofern im Rahmen der Güterabwägung kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt.[11]

Leider ist aus § 28 BDSG nicht zu entnehmen, was konkret unter einem „berechtigten Interesse" zu verstehen ist. Rechtsprechung[12] und Literatur[13] kommen hier zu unterschiedlichen Ergebnissen. Dabei kann als herrschende Meinung angesehen werden, was nach vernünftiger Erwägung durch die Sachlage gerechtfertigt erscheint.[14] Darunter kann auch ein wirtschaftliches Interesse wie eine Kundengewinnung gesehen werden.[15] Man zieht die Grenze hierbei dort, wo das Interesse auf die Abwerbung von Kunden gerichtet ist, die in einem Rechtsverhältnis zu einem Konkurrenten stehen.[16] Des Weiteren dürften rechtswidrig erlangte Daten[17] oder Daten, die für rechtswidrige Zwecke verwendet werden,[18] ebenfalls kein berechtigtes Interesse darstellen, welches eine Speicherung, Verarbeitung etc. nach § 28 BDSG rechtfertigt.

c) Eigene Geschäftszwecke

Der Begriff des „Geschäftszwecks" in § 28 Abs. 1 BDSG beruht auf einer bemerkenswerten redaktionellen Fehlleistung,[19] denn grundsätzlich ist eine Gewinnerzielung nicht erforderlich. Als „Geschäftszwecke" i.S.v. § 28 Abs. 1 BDSG werden alle Zwecke einer privaten Stelle verstanden, außer jenen, bei denen das BDSG gem. § 1 Abs. 2 Nr. 3 und § 27 nicht greift.[20] So kann sich das Einrichten einer eigenen Homepage durch eine Privatperson als die Verfolgung (eigener) Geschäftszwecke darstellen.[21]

Der Begriff der eigenen Geschäftszwecke in § 28 Abs. 1 BDSG ist nicht zu eng, sondern teleologisch auszulegen.[22] Danach liegen bereits einige Zwecke vor, wenn die Datenverarbeitung als Hilfsmittel zur Erfüllung von Zielstellungen außerhalb der reinen Datenverarbeitung eingesetzt wird.[23] Der verfolgte Zweck darf bei § 28 gerade nicht in der Datenverarbeitung selbst liegen.[24] Die Datenverarbeitung ist bloßes Hilfsmittel zur Erfüllung anderer Zwecke.[25] Liegt der verfolgte Zweck in der Datenverarbeitung selbst, so liegen wahrscheinlich die Voraussetzungen des § 29 BDSG vor.[26]

Die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, sind nach § 28 Abs. 1 S. 2 BDSG bei der Erhebung konkret festzulegen. Die Festlegung muss bei der Erhebung erfolgen. Sie muss daher vor Abschluss der Erhebung vorliegen, nicht unbedingt schon vor ihrem Beginn.[27] Der Text des § 28 Abs. 1 S. 2 bezieht sich nur auf die Erhebung von Daten. Erlangt die verantwortliche Stelle die Daten ohne Erhebung, ist in Analogie zu S. 2 zu verlangen, dass der Zweck spätestens im Augenblick der Speicherung vorliegen muss. Besitzt die verarbeitende Stelle die Daten schon und will sie sie nun zu einem neuen Zweck einsetzen, ist § 28 Abs. 1 S. 2 nicht anwendbar.[28]

Dass die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, bereits vor dem Ende ihrer Erhebung und vor der Verarbeitung festgelegt werden müssen, ermöglicht der verantwortlichen Stelle auch, die Zweckfestlegung zu überprüfen und festzustellen, ob eine Zweckentfremdung vorliegt, deren Zulässigkeit sich nach § 28 Abs. 2, Abs. 3 und Abs. 8 bemisst. Des Weiteren bildet die Festlegung die Grundlage für die Hinweispflicht nach § 4 Abs. 3 S. 1 Nr. 2 BDSG.[29] Nach dem Zweckbindungsgrundsatz dürfen die Daten nur zu dem Zweck verarbeitet werden, zu dem sie in rechtmäßiger Weise erhoben wurden.[30] Werden die Daten zu einem anderen Zweck verarbeitet, bedarf es einer speziellen Grundlage.[31]

Die Zweckbestimmung soll nach dem Text des nach § 28 Abs. 1 S. 2 BDSG konkret sein. Konkret bedeutet dies eine

9 Forgó/Helfrich/Schneider/Helfrich, Betrieblicher Datenschutz, 1. Aufl. 2014, Teil VI, Rn. 42.

10 Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 8 ff.

11 Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 24.

12 BGH, 22.05.1984 – VI ZR 105/82 = NJW 1984, 1886, VGH Baden-Württemberg, 24.10.1983 – 10 S 902/82 = NJW 1984, 1911.

13 Simitis, in: Simitis, BDSG, § 28 Rn. 177.

14 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 1. Aufl. 2014, Teil VI. Rn. 46

15 Bergmann/Möhrle/Herb, BDSG § 28 Rn. 231; Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 1. Aufl. 2014, Teil VI, Rn. 46.

16 OLG Köln, 14.08.2009 – 6 U 70/09 = NJW 2010, 90.

17 Bergmann/Möhrle/Herb, BDSG, § 28 Rn. 233

18 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 1. Aufl. 2014, Teil VI, Rn. 46.

19 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 10.

20 VGH, München, ZD 2015, 324.

21 Simitis, in: Simitis, BDSG, § 28 Rn. 31.

22 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 11.

23 Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 4.

24 Simitis, in: Simitis, BDSG, § 28 Rn. 31.

25 BGH, 04.06.2013 – 1 StR 32/13 = BGHSt 58, 268; NJW 2013, 2530; NStZ-RR 2014, 187; NZV 2014, 369; NJ 2013, 482; K&R 2013, 669.

26 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 10.

27 Andere Ansicht: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2016, Rn. 63.

28 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 15.

29 Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 35.

30 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 14.

31 Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 36.

so genaue Umschreibung der Aufgaben, für die die Daten benötigt werden, dass der mögliche Verwendungsraum erkennbar ist.[32] Nach einer engen Auslegung müsste sich die Festlegung des Zwecks der Erhebung und Verarbeitung auf die Zwecke der Datenverarbeitung beziehen und somit eine Begrenzung der Datenverarbeitung zum Ziel haben. Aber in der Festlegung des Schuldverhältnisses (i.S.v. Abs. 1 Nr. 1) oder der berechtigten Interessen (i.S.v. Abs. 1 Nr. 2) ist noch nicht die Festlegung des Zwecks der Datenverarbeitung enthalten. Somit ist nach der engen Auslegung eine Vereinbarung notwendig, die sich auf die Datenverarbeitung bezieht (schriftliche Vereinbarung).[33] Dieses Ergebnis erscheint aber eher praxisfern zu sein, da bei jeder Erfassung eines Kunden eine ausdrückliche, schriftliche Bestimmung erforderlich wäre, dass die Kundendatei der Pflege der Beziehung mit den Kunden diene. Es ist nicht davon auszugehen, dass der Gesetzgeber eine so strenge Auslegung wollte.[34]

Es wird daher in der Literatur vertreten, dass das Merkmal der konkreten Festlegung teleologisch restriktiv interpretiert werden muss: „Maßstab muss der Zweck dieses Merkmals sein".[35] Dies meint: Wenn die vertragliche Festlegung des Schuldverhältnisses hinreichend deutlich ergibt, dass beide Betroffenen mit einer Datenverarbeitung zur Erfüllung des Vertragszwecks einverstanden sind, liegt in dieser konkludenten Zweckbestimmung zugleich die konkrete Festlegung i.S.v. § 28 Abs. 1 S. 2 BDSG vor, dass die Verarbeitung der Daten ausdrücklich der Durchführung des Vertrags dienen soll.[36] Auch wenn die Festlegung weder fixiert noch ausdrücklich ist, ist dennoch der Zweck der Erhebung und Verarbeitung der personenbezogenen Daten ausreichend dokumentiert. Hierbei bedarf es aber der Vorsicht, dass tatsächlich aus dem Vertragszweck ein entsprechender Zweck der Verarbeitung ersichtlich ist. Sonst ist die Zweckbestimmung nach § 28 Abs. 1 S. 2 BDSG nicht ausreichend konkret.

2. Speicherung von Daten vor Vertragsabschluss

Fraglich ist, ob personenbezogene Daten des Kunden/Partners bereits vor dem Vertragsabschluss in einem CRM-System gesammelt und gespeichert werden dürfen. Der § 28 Abs. 1 Nr. 1 BDSG erteilt die Erlaubnis bereits für die Begründung eines rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen. Zulässig ist die Speicherung von personenbezogenen Daten dann, wenn sich die Parteien in Vertragsverhandlungen befinden oder wenn bereits ein bindendes Angebot der anderen Partei vorliegt.[37] Grundsätzlich muss die Verarbeitung einen unmittelbaren sachlichen Zusammenhang zwischen der beabsichtigten Verwendung und dem konkreten Zweck des rechtsgeschäftlichen Schuldverhältnisses, welches auch schon vor Vertragsabschluss liegen kann, bestehen.[38] Welchen Zweck die Beteiligten verfolgen, ergibt sich entweder aus den geführten Gesprächen oder aus dem gesamten Inhalt einer vorvertraglichen Vereinbarung, wie z.B. einer Geheimhaltungsvereinbarung (NDA) oder eines Letter of Intent.[39]

Wurde ein erstes Vertriebsgespräch geführt und der Kunde/Partner hat erkennbar Interesse daran gezeigt, ein Angebot zu erhalten bzw. mit dem Dienstleister einen Vertrag abzuschließen, dürften generell personenbezogene Daten bereits vor dem Vertragsabschluss im CRM-System gespeichert werden. Dies lässt sich auch durchaus mit § 311 Abs. 2 BGB begründen, wonach ein Schuldverhältnis mit Pflichten nach § 241 Abs. 2 BGB bereits entsteht, wenn Vertragsverhandlungen aufgenommen werden (Nr. 1), wenn die Anbahnung eines Vertrags, bei welcher der eine Teil im Hinblick auf eine etwaige rechtsgeschäftliche Beziehung dem anderen Teil die Möglichkeit zur Einwirkung auf seine Rechte, Rechtsgüter und Interessen gewährt oder ihm diese anvertraut (Nr. 2) oder ähnliche geschäftliche Kontakte (Nr. 3).

Ein reines Datensammeln auf Verdacht schließt sich aber grundsätzlich aus („Data-Mining"), da hierbei die Voraussetzung nach § 28 Abs. 1 BDSG nicht erfüllt sein dürften.

3. Speicherung von Daten nach Vertragsende

Die Rechtmäßigkeit der Speicherung von personenbezogenen Daten über den Vertragsabschluss hinaus ist insoweit nur gedeckt, wenn berechtigte Interessen der verantwortlichen Stelle vorliegen, vgl. § 28 Abs. 1 Nr. 2 BDSG. Dabei muss im Rahmen einer Güterabwägung kein Grund zur Annahme bestehen, dass das schutzwürdige Interesse des Betroffenen am Ausschluss gegenüber der Verarbeitung oder Nutzung überwiegt.[40] Denkbar sind vor allem die Fälle, in den ein Lieferant auch nach Vertragsende eine Sachmängelhaftung erbringen muss oder solche Fälle, in den aus steuerlichen Gründen weiterhin Daten über den Kunden gespeichert werden müssen, vgl. § 47 AO.

4. Umfang der Speicherung

Grundsätzlich muss eine Abwägung zwischen den personenbezogenen Daten bestehen, die im CRM-System gespeichert werden, und den Interessen der betroffenen Person.[41] Es muss eine angemessene Verhältnismäßigkeit bestehen, die im Einzelfall unterschiedlich ausfallen kann.

So kann es im Hotelgewerbe erlaubt sein, dass Schlafgewohnheiten des Kunden im CRM-System gespeichert werden (der Kunde mag kein Wasserbett oder ist Nichtraucher). Der Servicegedanke des Hotels rechtfertigt an dieser Stelle ein Kundenprofil mit den persönlichen Vorlieben des Kunden.[42] Die Speicherung der personenbezogenen Daten mit

32 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 14.

33 Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 35; Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2016, Rn. 64; OLG Köln, 19. 11. 2010 – 6 U 73/10 = CR 2011, 680.

34 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 16.

35 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 17.

36 Siehe auch in die gleiche Richtung: BGH, 08.02.2007 – III ZR 148/06 – NJW 2007, 1528; MDR 2007, 825; NZM 2007, 375; VersR 2007, 801; WM 2007, 1423.

37 Taeger/Gabel-Taeger, Kommentar zum BDSG, 1. Aufl. 2010, § 28 Rn. 43.

38 Bergmann/Möhrle/Herb, BDSG, § 28, Rn. 25; Duhr/Naujok/Danker/Seiffert, DuD 2003, 6.

39 Simitis, in: Simitis, BDSG, § 28 Rn. 22, 12.

40 Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 24 ff.

41 Bergmann/Möhrle/Herb, BDSG, § 28 Rn. 233.

42 Selk, RDV 2008, 187; Taeger/Gabel-Taeger, Kommentar zum BDSG, 1. Aufl. 2010, § 28 Rn. 53.

den Schlafgewohnheiten eines Kunden dürfte aber wiederum bei einer Bank nicht gerechtfertigt sein, da sie nicht zur Erfüllung von vertraglichen Verpflichtungen notwendig ist.[43]

Ferner ist ein Kreditinstitut nicht befugt, die Daten seiner Bankkunden nach dem Merkmal „Fahrzeughalter" und den Prämienzahlungen an die Versicherung des Fahrzeugs außerhalb des Vertrages in der Zweckbestimmung zu nutzen, um den Fahrzeughaltern in einem Werbeschreiben mitzuteilen, dass man mit dem Verbundpartner ein günstigeres Angebot als das des bisherigen Versicherers machen könne.[44] Ähnlich liegt auch der vom LDI NRW sanktionierte Fall der Weitergabe von Kontobewegungsdaten an Berater der Tochtergesellschaft der Bank, um der werblichen Ansprache ein präzises Kundenprofil zugrunde legen zu können.[45] Auch nicht mehr im Rahmen einer vertraglichen Betreuung liegt es, wenn Versicherungsvertreter oder Kundenbetreuer einer Bank, um eine gute Gesprächsatmosphäre mit dem Kunden herzustellen, Daten über Ess- und Trinkgewohnheiten, Hobbys etc. als sog. „Akquisedaten" speichern.[46]

Ist die Identität des Kunden für den Vertragsabschluss erforderlich, kann die Vorlage des Personalausweises verlangt werden.[47] Eine Anfertigung einer Kopie ist jedoch regelmäßig unzulässig,[48] und somit darf der Personalausweis auch nicht im CRM-System gespeichert werden. Zulässig ist aber die Speicherung der Unterschrift des Kunden zwecks Unterschriftenkontrolle durch die Bank[49] oder das Verlangen, vor Abschluss eines Verbraucherdarlehens zur Überprüfung der Kreditwürdigkeit Kontoauszüge vorzulegen, sofern sensible und nicht relevante Angaben zuvor geschwärzt werden.[50]

Grundsätzlich sind generelle Aussagen, was in einem CRM-System gespeichert werden darf, nur schwer zu treffen. Allgemein ist aber festzuhalten, dass der Umfang der gespeicherten und genutzten Daten der vom BDSG verlangten „Datensparsamkeit und Datenvermeidung" genügen muss, vgl. § 3a BDSG.[51] Durch das Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.8.2009[52] wurde der Geltungsbereich des § 3a BDSG über den bisherigen Systemdatenschutz hinaus auf jede Verwendung personenbezogener Daten erweitert. Damit gilt in Deutschland der Grundsatz, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten sind, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Somit ist eindeutig, dass sog. überschießende Daten, die der Zweckerfüllung dienen könnten, aber nicht erforderlich sind, nicht erhoben und verarbeitet werden dürfen.[53]

5. Allgemein zugängliche Daten

Ferner stellt sich die Frage, ob personenbezogene Daten gespeichert werden dürfen, wenn diese allgemein zugänglich sind. Gem. § 28 Abs. 1 Nr. 3 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Eine allgemein zugängliche Quelle liegt nach dem BVerfG[54] vor, wenn diese dazu bestimmt ist, nicht nur dem Einzelnen, sondern allgemein Informationen zu verschaffen. Sicherlich zählen traditionelle Quellen wie gedruckte Medien (Telefonbücher, Zeitschriften, Adressbücher, Flugblätter, Kataloge) dazu.[55] Im Zeitalter von Google, Facebook, Instagram etc. werden natürlich digitale Quellen bei der Informationsbeschaffung bevorzugt. Grundsätzlich können digitale Datenbanken auch als allgemein zugängliche Quelle betrachtet werden.[56] Hierbei ist aber der besondere Fall zu betrachten, dass der Zugang zu Datenbanken nur über eine spezielle Mitgliedschaft möglich ist (z.B. soziale Netzwerke wie Xing, LinkedIn etc.). Dabei ist es unerheblich, ob die Anzahl der Mitglieder in einem sozialen Netzwerk hoch oder niedrig ist. In beiden Fällen gilt das soziale Netzwerk als geschlossene Benutzergruppe.[57] Hierbei wird aber in der Literatur vertreten, dass solche Quellen ebenfalls als allgemein zugänglich angesehen werden können, wenn die Mitgliedschaft für jedermann einfach oder auch anonym möglich ist.[58] Dieser Gedanke wird auch durch die Tatsache unterstützt, dass viele Informationen in den sozialen Netzwerken auch öffentlich ohne einen entsprechenden Account im Internet zur Verfügung gestellt werden und leicht über eine Suchmaschine gefunden werden können.

43 Taeger/Gabel-Taeger, Kommentar zum BDSG, 1. Aufl. 2010, § 28 Rn. 53.

44 Datenschutzaufsicht NRW, Bericht für 1995/96 = RDV 1998, 271; vgl. auch 15. Bericht der hess. Landesregierung über die Datenschutzaufsicht im nicht öffentlichen Bereich, LT-Drs. 15/4659 vom 22.11.2002, S. 35; ferner zum Versicherungsgeheimnis und der Unzulässigkeit der Weitergabe von Daten von Interessenten an einer sog. „Riesterrente" an ein Schwesterunternehmen, das Krankenversicherungen betreibt, zwecks Vorlage eines zugeschnittenen Krankenversicherungsangebots: 16. Bericht der hess. Landesregierung über die Datenschutzaufsicht im nicht öffentl. Bereich, LT-Drs. 16/1680 vom 11.12.2003, S. 38.

45 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 10.

46 Vgl. BlnLDI, TB 2003, S. 100; Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 11.

47 LfDI Berlin bei Billigfliegern, TB 2002, 140.

48 IM Baden-Württemberg, 3. TB (2005), Ziff. 7.2; vgl. ferner Gola, RDV, 2012, 184.

49 15. Bericht der hess. Landesregierung über die Datenschutzaufsicht im nichtöffentlichen Bereich, LT-Drs. 15/4659 vom 22.11.2002, S. 32; Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 17.

50 BlnLDI, JB 2011, Ziff. 9.1.2; Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 17.

51 Taeger/Gabel-Taeger, Kommentar zum BDSG, 1. Aufl. 2010, § 28 Rn. 49.

52 BGBl. 2009, S. 2814

53 Taeger/Gabel-Taeger, Kommentar zum BDSG, 1. Aufl. 2010, § 28 Rn. 49.

54 BVerfG, 25. 4. 1972 – 1 BvL 13/67 = BVerfGE 33, 52; NJW 1972, 1934; DÖV 1972, 682.

55 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 1. Aufl. 2014, Teil VI, Rn. 42

56 Siehe Bergmann/Möhrle/Herb, BDSG, § 28 Rn. 262 mit Beispielen.

57 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz 1. Aufl. 2014, Teil VI. Rn. 55.

58 Bergmann/Möhrle/Herb, BDSG, § 28 Rn. 263; Forgo/Helfrich/Schneider/ Helfrich, Betrieblicher Datenschutz 1. Aufl. 2014, Teil VI. Rn. 55.

6. Einwilligung

Natürlich kann ein Unternehmen personenbezogene Daten in seinem CRM-System speichern, wenn der Betroffene hierzu seine Einwilligung gibt. Gem. § 4a S. 1 BDSG ist eine Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Dabei ist der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie – soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen – auf die Folgen der Verweigerung der Einwilligung hinzuweisen, vgl. § 4a S. 2 BDSG. Wichtig ist dabei, dass die Einwilligung vor der Erhebung und Verarbeitung erklärt wird, denn nachträglich ist die erforderliche Erklärung nicht mehr denkbar.[59] Des Weiteren muss die „Zustimmung", da es sich um eine Erklärung des Betroffenen handelt, vom Willen des Erklärenden getragen sein, und sie muss auf der freien Entscheidung des Betroffenen beruhen.[60]

Darüber hinaus bedarf die Einwilligung gem. § 4a S. 3 BDSG der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Dabei ist zu berücksichtigen: Wenn die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt wird, dann ist sie gem. § 4a S. 4 BDSG besonders hervorzuheben.

7. Auswertung

Die Auswertung der im Rahmen von Vertragsbeziehungen gespeicherten CRM-Kundendaten zwecks Ermittlung von Kundenprofilen sind enge Grenzen gesetzt.[61] Gem. § 28 Abs. 3 Satz 1 BDSG ist die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Abs. 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten gem. § 28 Abs. 3 S. 2 BDSG zulässig, wenn es sich um listenmäßig oder anderweitig zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist (Nr. 1). Eine Zulässigkeit besteht ebenfalls für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Abs. 1 S. 1 Nr. 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat (Nr. 2). Verwendet werden können die personenbezogenen Daten auch für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift.

Regelmäßig untersagt ist somit, dass personenbezogene Daten, welche anders als nach § 28 Abs. 3 S. 2 BDSG verwendet werden, für Werbung zu nutzen.[62] Bereits vor Big Data[63] war eindeutig, dass die mit der konkreten Zweckbestimmung der Vertragsabwicklung gespeicherten Daten der Kunden in einem CRM-System durch spezielle Abfragen (sog. „Data-Mining") und Kombinationen von Kundenprofilen und Verbraucherverhalten nicht zulässig ist,[64] da dies gem. § 28 Abs. 1 Satz Nr. 1 nicht mehr legitimiert ist und auch regelmäßig nicht unter Heranziehung der Alternative Nr. 2 gerechtfertigt werden kann.[65] Grundsätzlich bedarf ein Data-Mining, bei dem Benutzerprofile ausgewertet werden, einer Einwilligung.[66] Werden von einer Bank im Rahmen der nach dem Wertpapierhandelsgesetz (WpHG) bestehenden Beratungspflicht der Bank Daten über die persönliche finanzielle Situation des Kunden erhoben und gespeichert, so besteht insoweit eine strikte Zweckbindung.[67] Gleiches gilt für aufgrund des Geldwäschegesetzes erhobene Daten.[68]

III. Resümee

In einem CRM-System dürfen grundsätzlich viel weniger personenbezogene Daten gespeichert werden, als man landläufig glaubt. Grundsätzlich dürfen nur die Daten gespeichert werden, die für die Vertragserfüllung notwendig sind. Hierzu zählen sicherlich weder das Geburtsdatum der Ehefrau des Betroffenen noch die Freizeitaktivitäten der Kinder des Betroffenen. Anders verhält es sich, wenn der Betroffene sein Einverständnis zur Verarbeitung gibt bzw. wenn die zu verarbeitenden Daten öffentlich zugänglich sind. Aber auch dann gelten datenschutzrechtliche Anforderungen, die zu erfüllen sind. Wenngleich eine Verarbeitung zulässig ist, unterliegt der Umfang der gespeicherten und genutzten Daten den im BDSG verankerten Grundsätzen der „Datensparsamkeit und der Datenvermeidung".[69]

Dr. Thomas Söbbing, LLM (HHU)
ist als Chief Legal Specialist / Fachleiter Recht bei einem Finanzinstitut tätig und unterrichtet als Dozent an einer privaten Stiftungshochschule.

59 Simitis, in: Simitis, BDSG, § 4a Rn. 29.

60 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 1. Aufl. 2014, Teil VI, Rn. 23.

61 Wittig, RDV 2000, 59; Podlech/Pfeifer, RDV 1998, 139.

62 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 11.

63 Weichert, ZD 2013, 251; Bornemann, RDV 2013, 232; Ulmer, RDV 2013, 227.

64 Möncke, DuD 1998, 561; Weichert, DuD 2001, 264; Weichert, RDV 2003, 113.

65 Baeriswyl, RDV 2000, 7; LDSB Schleswig-Holstein, 21. TB (1998), 116 = RDV 1999, 236; BlnLDI, Jahresbericht 2000, Ziff. 1.1.1.

66 Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 11.

67 Aufsichtsbeh. Baden-Württemberg, Hinweis zum BDSG Nr. 34, Staatsanz. 1, 1996, S. 10; Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 11.

68 OLG Hamm, 11.04.2000 – 1 VAs 18/2000 = NJW 2000, 2599; Wolff, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink, 14. Edition, § 28 Rn. 11.

69 Taeger/Gabel-Taeger, Kommentar zum BDSG, 1. Aufl. 2010, § 28 Rn. 49.

Prof. Dr. Volker Lüdemann, Manuel Christian Ortmann LL.M., Patrick Pokrant LL.M.

Datenschutz beim Smart Metering – Das geplante Messstellenbetriebsgesetz (MsbG) auf dem Prüfstand

Die Digitalisierung der Energiewende nimmt Fahrt auf. Ihre Umsetzung soll die Elektrizitätsversorgung effizienter machen und auch die Verbraucherseite aktiv am Strommarkt beteiligen. Ein wichtiger Baustein auf diesem Weg ist nach dem Willen des Gesetzgebers die Einführung einer neuen Mess- und Kommunikationsinfrastruktur. Mit dem Messstellenbetriebsgesetz (MsbG) wird die rechtliche Grundlage für den verpflichtenden Einbau von intelligenten Messsystemen (sog. Smart Meter) gelegt. Das Gesetz soll noch in diesem Sommer in Kraft treten. Die Vorbehalte in der Bevölkerung sind jedoch groß. Grund hierfür sind vor allem Datenschutzbedenken. Der Beitrag zeigt die datenschutzrechtlichen Risiken auf und unterzieht den Gesetzentwurf auf dieser Grundlage einer ersten kritischen Würdigung.

I. Einleitung

Intelligente Messsysteme sind ein wichtiger Baustein für den Aufbau intelligenter Energieversorgungsnetze. Die bestehende Netzinfrastruktur ist auf den wachsenden Anteil erneuerbarer Energien nicht ausgelegt. Es fehlt vor allem an Flexibilität, um die wetterabhängige und dezentrale Einspeisung von Wind- und Sonnenenergie mit der Stromnachfrage in Einklang zu bringen. Intelligente Messsysteme bieten insoweit eine Lösung.[1] Mit ihrer Hilfe können vielfältige verbrauchsbezogene Messdaten generiert und über Kommunikationsschnittstellen für das Energieversorgungsnetz nutzbar gemacht werden.[2] Sie ermöglichen die kommunikative Vernetzung von Erzeugern, Verbrauchern und Speichern. Gleichzeitig bergen sie jedoch ein erhebliches Risikopotential für den Datenschutz. Dieses ergibt sich aus dem hohen Volumen an personenbezogenen Daten, das benötigt wird, um das Verhalten der Verbraucher und Energieerzeuger sinnvoll aufeinander abzustimmen. Zwischen einem möglichst umfassenden Datenschutz und der Generierung des vollen Nutzens aus dem Smart Metering bestehen insofern erhebliche Zielkonflikte.[3]

Heute erfolgt die Übermittlung der Messwerte in der Regel jährlich. Mit Einführung intelligenter Messsysteme steigt die Datenmenge und damit der Datenfluss aus dem Haushalt signifikant an. Die Daten geben nicht nur Auskunft über die Menge verbrauchter oder eingespeister Energie, sondern auch über den jeweiligen Zeitpunkt des Verbrauchs und der Einspeisung. Intelligente Messsysteme ermöglichen es damit in bisher unbekanntem Ausmaß, den Alltag der Verbraucher nachzuvollziehen, da ein Großteil der Alltagshandlungen mit Energieverbrauch verbunden ist.[4] Entsprechend groß ist die Skepsis in der Bevölkerung. Siebzig Prozent lehnt einen flächendeckenden Einsatz von Smart Metern ab, der Großteil hiervon wegen Datenschutzbedenken.[5] In den Niederlanden ist die Einführung von Smart Metern aufgrund ähnlicher Vorbehalte sogar zunächst gescheitert.[6] Der deutsche Gesetzgeber hat hieraus seine Schlüsse gezogen und den Aspekten des Datenschutzes und der Datensicherheit eine Schlüsselrolle im Messstellenbetriebsgesetz zugedacht. Die Akzeptanz der Bevölkerung für den angestrebten flächendeckenden Einbau intelligenter Messsysteme soll damit erhöht werden.[7]

Der Beitrag analysiert nach einem kurzen Überblick über den Stand der Gesetzgebungsarbeiten (II.) und die Funktionsweise intelligenter Messsysteme (III.) die Herausforderungen für den Datenschutz (IV.). Auf dieser Grundlage wird anschließend untersucht, inwieweit die bestehenden Gefahren mit den Datenschutzbestimmungen des Messstellenbetriebsgesetzes aufgefangen werden können (V.). Ein Fazit schließt den Beitrag ab (VI.).

II. Stand des Gesetzgebungsverfahrens

Die Einführung intelligenter Messsysteme geht auf die EU-Richtlinie 2009/72/EG[8] zurück. Als Teil des dritten Binnenmarktpaketes sieht sie die verpflichtende Ausstattung vor. Deutschland hat in Umsetzung der Richtlinie im Jahre 2011 gesetzliche Grundlagen für den Flächenausbau intelligenter Stromnetze und Stromzähler geschaffen.[9] Im Zuge der No-

1 BMWi, Pressemitteilung vom 17.01.2013: Smart Grids – Intelligenz entlastet Stromnetze; Roß, in: Servatius/Schneidewind/Rohlfing (Hrsg.), Smart Energy – Wandel zu einem nachhaltigen Energiesystem, S. 287 ff.; Seifert, ebd., S. 261; Pfändler, Smart Meter und Smart Grids, S. 4; Guckelberger, DÖV 2012, S. 613, 616.

2 Windoffer/Groß, VerwArch 2012, 491, 491 f.

3 BT-Drs. 18/5948, S. 97.

4 Art. 29-Datenschutzgruppe, Stellungnahme 4/2013, WP205, S. 5.

5 Die Befragung wurde im Oktober 2015 im Auftrag des Verbraucherzentrale Bundesverbands (vzbv) durch TNS Emnid durchgeführt. Die Ergebnisse können online abgerufen werden unter: http://www.vzbv.de/pressemitteilung/smart-meter-verbraucher-lehnen-zwangsdigitalisierung-ab.

6 Raabe/Lorenz/Pallas/Weis, in: Raabe/Pallas/Weis/Lorenz/Boesche (Hrsg.), Datenschutz in Smart Grids, 2011, S. 53; Raabe, DuD 2010, 379, 385.

7 So übereinstimmend BMWi, Strategie Intelligente Vernetzung, S. 24; Raabe, DuD 2010, 379, 379; Windoffer/Groß, VerwArch 2011, 491, 512.

8 Richtlinie 2009/72/EG des europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG (Elektrizitätsbinnenmarktrichtlinie).

9 Gesetz zur Neuregelung energiewirtschaftlicher Vorschriften, BGBl. I 2011, 1554.

vellierung des Energiewirtschaftsgesetzes[10] wurden neue Bestimmungen über den Messstellenbetrieb mitsamt einigen Bestimmungen zum Umgang mit personenbezogenen Daten eingefügt (§§ 21b-i EnWG). Der gesetzgeberische Ansatz sah sich von Anfang an der Kritik ausgesetzt, dass wesentliche Aspekte des Datenschutzes und der Datensicherheit nicht im EnWG selbst geregelt wurden.[11] Detaillierte Vorgaben waren einem Verordnungspaket vorbehalten.[12] Angesichts der geringen Regelungstiefe der EnWG-Normen stellte sich die Frage, ob sie hinreichend bestimmt und normenklar sind, um den verfassungsrechtlichen Anforderungen zu genügen. Da dem Recht auf informationelle Selbstbestimmung Grundrechtsstatus zukommt, vermag nur der Gesetzgeber, nicht der Verordnungsgeber, die Bedingungen einer möglichen Einschränkung festzulegen. Mit der Vorlage des Messstellenbetriebsgesetzes hat der Gesetzgeber auf die Kritik reagiert. Der bisherige Regelungsansatz über das EnWG in Verbindung mit einem Verordnungspaket wurde aufgegeben. Das federführende Ministerium für Wirtschaft und Energie hat sich im Hinblick auf die Grundrechtsrelevanz und zur Vermeidung einer weiteren Zersplitterung des Energierechts nunmehr dazu entschieden, die Regelungsmaterie in einem neuen Stammgesetz umfassend niederzulegen. Dies ist unter dem Gesichtspunkt der Rechtssicherheit uneingeschränkt zu begrüßen.

Der erste Entwurf für ein „Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG)“ wurde vom BMWi am 21. September 2015 vorgelegt.[13] Das Bundeskabinett nahm diesen im Anschluss an die öffentliche Anhörung mit geringfügigen Änderungen am 4. November 2015 an und leitete ihn dem Bundesrat zur Stellungnahme zu. Nachdem der Bundesrat am 18. Dezember 2015 umfangreich Stellung genommen hat,[14] liegt der Entwurf inzwischen in der Fassung vom 17. Februar 2016 vor, die nunmehr auch die Gegenäußerung der Bundesregierung enthält.[15] Nach derzeitigem Stand soll das Gesetzgebungsverfahren noch im Sommer 2016 abgeschlossen werden.

III. Begriff und Funktionsweise intelligenter Messsysteme

Ein intelligentes Messsystem besteht nach § 2 Nr. 7 MsbG-E aus einer modernen Messeinrichtung zur Erfassung des tatsächlichen Energieverbrauchs und der Nutzungszeit sowie einer Kommunikationseinheit (Smart-Meter-Gateway) zur sicheren Einbindung der Messeinrichtung in ein Kommunikationsnetz.[16] Ein verpflichtender Einbau intelligenter Messsysteme ist im MsbG-E lediglich für größere Letztverbraucher und Anlagenbetreiber vorgesehen.[17] So statuiert § 29 Abs. 1 MsbG-E eine Einbaupflicht bei Letztverbrauchern mit einem Jahresstromverbrauch[18] über 6.000 kWh und Anlagenbetreibern mit einer installierten Leistung über 7 kW. Diese Verpflichtung besteht allerdings nur unter der Voraussetzung technischer Möglichkeit[19] und wirtschaftlicher Vertretbarkeit. Wann ein Einbau wirtschaftlich vertretbar ist, wird in der zentralen Vorschrift des § 31 MsbG-E ausführlich für verschiedene Letztverbraucher- und Anlagenbetreibergruppen anhand von Preisobergrenzen festgelegt. Die Preisobergrenzen orientieren sich dabei an den Erkenntnissen und Annahmen einer Kosten-Nutzen-Analyse[20]. Können die Preisobergrenzen in der Praxis nicht eingehalten werden, besteht auch keine Einbaupflicht. Mit diesem Ansatz möchte der Gesetzgeber erreichen, dass nur diejenigen Letztverbraucher zum Einbau verpflichtet werden, die tatsächlich auch davon profitieren können.[21]

Für kleinere Letztverbraucher mit einem Jahresstromverbrauch bis einschließlich 6.000 kWh sieht § 29 Abs. 2 MsbG-E eine optionale Ausstattung vor. Die Optionalität bezieht sich hierbei aber nicht auf die freiwillige Entscheidung des Letztverbrauchers. Insofern ist der Gesetzeswortlaut hier missverständlich. Vielmehr obliegt es allein dem grundzuständigen Messstellenbetreiber, die Entscheidung über den Einbau zu treffen. Allerdings muss auch hier zunächst die wirtschaftliche Vertretbarkeit nach § 31 Abs. 3 MsbG-E gegeben sein. All diejenigen Letztverbraucher und Anlagenbetreiber, für die nach diesen Grundsätzen keine Pflicht zum Einbau eines intelligenten Messsystems besteht, sollen bis zum Jahr 2032 unter dem Stichwort der „nachhaltigen Komplettmodernisierung“[22] zumindest mit den nicht kommunikationsfähigen modernen Messeinrichtungen ausgestattet werden. Die wirtschaftliche Vertretbarkeit richtet sich hier nach § 32 MsbG-E und ist gegeben,

10 Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) vom 7. Juli 2005 (BGBl. I S. 1970, 3621).

11 Dazu näher Karg, DuD 2010, 365, 368; Wiesemann, MMR 2011, 355, 357.

12 Vgl. BMWi, Baustein für die Energiewende: 7 Eckpunkte für das „Verordnungspaket Intelligente Netze“; abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/E/eckpunkte-fuer-das-verordnungspaket-intelligente-netze,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

13 Als Art. 4 bildet es den Kern des Gesetzes zur Digitalisierung der Energiewende, BMWi, Entwurf eines Gesetzes zur Digitalisierung der Energiewende, Referentenentwurf vom 21.09.2015, Art. 4.

14 BR-Drs. 543/15.

15 BT-Drs. 18/7555.

16 Definitionen zum Smart-Meter-Gateway und zur modernen Messeinrichtung finden sich in § 2 Nr. 19 MsbG-E und in § 2 Nr. 15 MsbG-E.

17 Insoweit folgt der Gesetzentwurf den Empfehlungen der Kosten-Nutzen-Analyse und dem Grundsatz, dass es keinen Rollout „um jeden Preis“ geben solle, vgl. BT-Drs. 18/7555, S. 2, 63 und 91.

18 Für die Berechnung des Jahresstromverbrauchs ist gem. § 31 Abs. 4 MsbG-E der Durchschnittswert der letzten drei Jahre maßgeblich.

19 Technisch möglich ist die Ausstattung einer Messstelle nach § 30 MsbG-E, wenn mindestens drei voneinander unabhängige Unternehmen intelligente Messsysteme, die die Voraussetzungen des MsbG erfüllen, anbieten.

20 Die Elektrizitätsbinnenmarktrichtlinie eröffnet den Mitgliedstaaten die Möglichkeit, die Einführung von einer positiven gesamtwirtschaftlichen Bewertung abhängig zu machen. Das BMWi hat vor diesem Hintergrund eine Kosten-Nutzen-Analyse zur flächendeckenden Einführung intelligenter Messsysteme und Zähler in Deutschland in Auftrag gegeben. Der Endbericht wurde Ende Juli 2013 veröffentlicht, abrufbar unter: http://www.bmwi.de/DE/Mediathek/publikationen,did=586064.html. Die von der EU angestrebte Rolloutquote i.H.v. 80% bis zum Jahr 2020 wurde darin für einen Großteil der Kunden unter den derzeit geltenden Rahmenbedingungen als wirtschaftlich nicht zumutbar bewertet.

21 BT-Drs. 18/7555, S. 91 ff.

22 BT-Drs. 18/7555, S. 90.

wenn die jährlichen Kosten für den Messstellenbetrieb 20 Euro brutto nicht übersteigen.[23] Auch hier besteht für Letztverbraucher keine Möglichkeit, sich einem Einbau zu entziehen.

Verantwortlich für den Einbau und den Betrieb der neuen Messinfrastruktur sind als grundzuständige Messstellenbetreiber die örtlichen Verteilnetzbetreiber, die bereits heute den Messstellenbetrieb verantworten, sofern der Anschlussnutzer keinen Dritten damit beauftragt hat. Das Recht des Anschlussnutzers, einen anderen Betreiber zu wählen, ist auch künftig gegeben. Neu ist allerdings, dass auch der Anschlussnehmer ein Wahlrecht erhalten soll.[24] Dem Messstellenbetreiber wird durch § 3 Abs. 1 S. 2 MsbG-E auch die Funktion des sog. Smart-Meter-Gateway-Administrators übertragen.[25] Diese Rolle ist neu und wurde eigens dafür geschaffen, die Verantwortlichkeit für den technischen Betrieb, auch im Hinblick auf die Einhaltung der Vorgaben zur Datensicherheit, klarzustellen. Als „vertrauenswürdige Instanz"[26] kann nur der Gateway Administrator einen direkten Zugriff auf die Daten ermöglichen.[27] Der grundzuständige Messstellenbetreiber hat nach § 41 MsbG-E die Möglichkeit, die Grundzuständigkeit auf ein anderes Unternehmen zu übertragen.[28] Dies gilt allerdings nur für den Messstellenbetrieb von modernen Messeinrichtungen und intelligenten Messsystemen. Für alle weiteren Messstellen verbleibt die Zuständigkeit bei ihm.[29]

Beim Messstellenbetrieb fallen grundsätzlich drei wesentliche Arten von Daten an: Messwerte, Netzzustandsdaten und Stammdaten. Messwerte sind Angaben über entnommene, erzeugte oder eingespeiste Energiemengen.[30] Stammdaten umfassen Informationen über Art, technische Ausstattung, Ort, Spannungsebene und kommunikative Anbindung von etwaigen Erzeugungsanlagen oder steuerbaren Verbrauchseinrichtungen, die an das Smart-Meter-Gateway angeschlossen sind.[31] Netzzustandsdaten betreffen vor allem Spannungs- und Stromwerte, die zur Ermittlung des Netzzustands verwendet werden.[32] Die Übermittlung der Daten soll zukünftig sternförmig erfolgen.[33] Hierbei werden die Daten nach Erhebung und Aufbereitung direkt an die zum Datenempfang berechtigten Stellen übermittelt. Die Daten laufen somit nicht mehr über mehrere Stationen zum Empfänger.[34]

Die Kommunikationseinheit ist bidirektional ausgelegt, d.h. Daten können sowohl übermittelt als auch empfangen werden.[35] Bei den zu empfangenden Informationen handelt es sich in erster Linie um Tarifinformationen. In Verbindung mit der sog. Zählerstandsgangmessung[36] ermöglicht dies dynamische variable Tarife. Der Anschlussnutzer wird hierdurch in die Lage versetzt, seinen Strombezug an Preissignale zu knüpfen. Er kann mehr beziehen, wenn der Preis niedrig ist und den Bezug verringern, wenn der Preis hoch ist. Dieser richtet sich vor allem nach dem Angebot elektrischer Energie. Auch entsprechende Steuerungssignale für Verbrauchsgeräte und Erzeugungsanlagen sind auf diesem Wege möglich.[37]

IV. Herausforderungen für den Datenschutz

1. Personenbezug

Die datenschutzrechtliche Relevanz der intelligenten Messsysteme ergibt sich daraus, dass es sich bei den erhobenen Daten um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG handelt.[38] Für Messwerte liegt dies auf der Hand. Bei den Verbrauchs-, Erzeugungs- und Einspeisungsdaten handelt es sich um Daten aus dem häuslichen Bereich. Diese können in vielfältige tatsächliche Zusammenhänge zum Anschlussnutzer und den weiteren Bewohnern gesetzt werden. Sie geben Aufschluss über Umfang, Art und Zeitraum des Energieverbrauchs der im Haushalt lebenden Personen. Personenbezug weisen aber auch die beim Smart Meter anfallenden Stamm- und Netzzustandsdaten auf.[39] Hierbei handelt es sich zwar überwiegend um technische Daten. Der Begriff der personenbezogenen Daten ist im Bereich des Messwesens allerdings weit auszulegen.[40] Auch technische Daten, die in Bezug zu einer natürlichen Person gesetzt werden können, sind hiervon erfasst.

23 § 32 MsbG-E.

24 Vgl. für das Wahlrecht des Anschlussnutzers § 5 sowie für das Wahlrecht des Anschlussnehmers und dessen Folgen für das Recht des Nutzers § 6 MsbG-E.

25 § 3 Abs. 1 S. 2 MsbG-E.

26 BT-Drs. 18/7555, S. 73.

27 BT-Drs. 18/7555, S. 84; Zur Verteilung der Daten sieht der Gesetzentwurf insofern noch zwei optionale Modelle vor: Der Gateway Administrator kann hierbei entweder als automatisierte „Datendrehscheibe" dienen, oder es erfolgt eine direkte Verteilung durch das intelligente Messsystem. In beiden Fällen hat der Administrator selbst keinen Zugriff auf die unverschlüsselten Daten. Er kann den Zugriff lediglich ermöglichen, vgl. BT-Drs. 18/7555, S. 108.

28 Die Zuständigkeit für die Gateway Administration kann ebenfalls übertragen werden, § 2 Nr. 20 MsbG-E. Hierbei muss aber die Zertifizierung berücksichtigt werden.

29 § 43 Abs. 1 S. 2 MsbG-E.

30 Vgl. § 2 Nr. 14 MsbG-E.

31 Vgl. § 2 Nr. 22 MsbG-E sowie zum Anlagenbegriff BT-Drs. 18/7555, S. 75.

32 § 2 Nr. 16 MsbG-E.

33 Vgl. § 60 MsbG-E.

34 Besonders umstritten ist in diesem Zusammenhang die zukünftige Rolle der Verteilnetzbetreiber in diesem System. Einige Stimmen (so auch der Bundesrat, vgl. BT-Drs. 18/7555, S. 131 ff.) fordern, dass sie – abweichend vom Modell der sternförmigen Kommunikation – auch zukünftig als „Datendrehscheibe" fungieren sollen.

35 Karsten/Leonhardt, RDV 2016, 22, 23.

36 Die Zählerstandsgangmessung beinhaltet nach § 2 Nr. 27 MsbG-E die Messung einer Reihe viertelstündig ermittelter Zählerstände. Im Gegensatz zur jährlichen Ablesung des Zählerstandes bei der Abrechnung von Standardlastprofilkunden kann so eine zeitlich differenzierte Abrechnung erfolgen.

37 Dinter, ER 2015, 229, 229 f.

38 Wann personenbezogene Daten vorliegen, richtet sich auch im MsbG-E nach § 3 Abs. 1 BDSG, vgl. §§ 59 Nr. 1, 65 Nr. 2, 70 Nr. 2 MsbG-E sowie die Begründung zu § 49 MsbG-E, BT-Drs. 18/7555, S. 105.

39 Für Stammdaten vgl. auch Schmelzer (o. Fn. 7), S. 119 f.

40 Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Düsseldorfer Kreis, Orientierungshilfe datenschutzgerechtes Smart Metering, Juni 2012, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Orientierungshilfe_SmartMeter.pdf?__blob=publicationFile&v=1, S. 8, 9 sowie 18. Für eine weite Auslegung des Begriffs ebenso Eßer, in: Auernhammer, BDSG, 4. Aufl. 2014, § 3 Rdnr. 8; Schild, in: Wolff/Brink, BDSG, 2013, § 3 Rdnr. 1; kritisch dagegen Wiesemann, ZD 2012, 447, 448.

Die unterschiedliche Sensitivität von Messdaten kann sich nicht in der Qualifizierung als personenbezogenes Datum niederschlagen, sondern allenfalls in der Beurteilung des Datenschutzbedarfs.[41] Für die Beurteilung des Personenbezugs kommt es auch nicht darauf an, ob tatsächlich eine Verknüpfung mit einer natürlichen Person erfolgt. Ausreichend ist vielmehr die Bestimmbarkeit der Identität einer Person auf Basis der Daten.[42] Die Personenbeziehbarkeit ergibt sich daraus, dass es objektiv für andere möglich ist, direkt oder indirekt einen Personenbezug herzustellen.[43] Das Datenschutzrecht stellt dabei auf den Zeitpunkt der Erhebung ab.[44] Besteht zu diesem Zeitpunkt objektiv die Gefahr eines Personenbezugs, ist das jeweilige Datum als personenbezogen zu qualifizieren, auch wenn sich die Gefahr später nicht realisiert. Andernfalls käme es zu Schutzlücken.[45] Mit entsprechendem Zusatzwissen lassen sich die Daten ebenso in Mehrpersonenhaushalten konkreten Bewohnern zuweisen.[46] Ein Personenbezug scheitert schließlich auch nicht daran, dass sich eine Zuordnung als schwierig oder unmöglich erweist. Für die Qualifizierung als personenbezogenes Datum reicht es aus, wenn überhaupt die Zuordnung zu einer natürlichen Person erfolgt, selbst wenn die Zuordnung im Ergebnis unzutreffend ist.[47]

2. Gefahr detaillierter Personen- und Verhaltensprofile

Die anfallenden personenbezogenen Daten sind kritisch, weil sie detaillierte Rückschlüsse auf die Lebensgewohnheiten und persönlichen Verhältnisse der Stromverbraucher ermöglichen. Ein Großteil der Alltagshandlungen ist mit Energieverbrauch verbunden.[48] Auf Grundlage des Energieverbrauchs lässt sich etwa feststellen, wann der Nutzer aufsteht oder zu Bett geht, zu welchen Zeiten er duscht oder badet, ob er zur Zubereitung der Mahlzeiten die Mikrowelle, den Herd oder den Backofen einsetzt und wie häufig die Waschmaschine oder sonstige Elektrogeräte laufen.[49] Studien zufolge ist es sogar möglich, anhand des Lastprofils zu ermitteln, welches Fernsehprogramm der Energienutzer wählt.[50] Tiefe und Aussagekraft der möglichen Profile sind zudem aufgrund der Datendichte, Datenqualität und Erhebungsdauer sehr hoch. Bei einer viertelstündlichen Auslesung liefert ein Smart Meter rund 35.000 Datensätze pro Jahr. Bei der technisch möglichen, wenn auch im MsbG-E derzeit nicht vorgesehenen sekundengenauen Auslesung steigt das Datenvolumen auf 31,5 Millionen Datensätze pro Smart Meter.[51] Die Daten werden zudem über einen langen Zeitraum erfasst. Zufällige Schwankungen werden über die Zeitleiste ausgeglichen. Der stete Datenstrom erlaubt mithin hochdetaillierte Einblicke in das Verhalten, die Vorlieben und die Persönlichkeitsstruktur der Stromverbraucher. Noch detailliertere Nutzerprofile ergeben sich, wenn die Messsysteme zur verbesserten Steuerung und Lastverschiebung den Verbrauch einzelner Hausgeräte mit einbeziehen.[52] Das Risiko der Profilbildung und der Aussagegehalt erhöhen sich weiter, wenn die Messdaten mit Daten aus anderen Quellen verknüpft werden.[53] Mit der Möglichkeit einzelne Daten konkreten Personen zuzuordnen, lassen sich auch die Profile sehr genau individualisieren.

3. Unmerkliche Datenerhebung

Die datenschutzrechtliche Situation wird zudem dadurch verschärft, dass die Datenerhebung weitgehend unbemerkt vom Anschlussnutzer erfolgt. Intelligente Messsysteme erheben die Daten lautlos, unsichtbar und automatisch, das heißt, ohne aktive Beteiligung des Nutzers. Sie befinden sich außerhalb des Sichtbereichs des Nutzers, meist im Keller bzw. in einem Schaltschrank. Das Bewusstsein über die kontinuierliche Datenerhebung ist daher eher gering. Hinzu kommt, dass die Daten an Dritte übermittelt, dort weiter verarbeitet und genutzt werden, möglicherweise sogar zusätzlich durch zwischengeschaltete Dienstleister. Sie gelangen zudem in den Machtbereich verschiedener Empfänger. Der Weg der Daten ist intransparent.[54] Der Anschlussnutzer hat im Bereich der gesetzlich erlaubten Datenverwendungen praktisch keine Kenntnis darüber, wer wann welche Daten erhält und wofür diese Daten genau verwendet werden.[55]

4. Gefahr der Zweckentfremdung

Derart große Datenmengen unterliegen stets der Gefahr einer missbräuchlichen Verwendung. Wenn die Daten aus ihrem ursprünglichen Erhebungskontext herausgelöst werden, wird ein weiteres datenschutzrechtliches Prinzip verletzt: der Zweckbindungsgrundsatz. Personenbezogene Daten dürfen nur zu den Zwecken verwendet werden, zu denen sie erhoben worden sind.[56] Dieser Grundsatz ist mit den Möglichkeiten der Datenverwendung in und um intelligente Netze kaum in Einklang zu bringen. Durch technische Entwicklungen sowie die Kombination von Informationen im Sinne von „Big Data" werden künftig vielfältige, derzeit

41 Orientierungshilfe (o. Fn. 42), S. 9, 18.

42 Schild, in: Wolff/Brink (o. Fn. 42), § 3 Rdnr. 17 ff.

43 Kremer, RDV 2014, 240, 244; Pohle/Zoch, CR 2014, 409, 410.

44 Zur Problematik des Erhebungszeitpunktes bei Messeinrichtungen Lüdemann/Sengstacken/Vogelpohl, ZD 2015, 55, 59.

45 Vgl. Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, ZD-Aktuell, 04363.

46 Hornung/Fuchs, DUD 2012, 20, 22 unter Verweis auf Raabe, DuD 2010, 379, 381.

47 Taeger, in: Taeger/Gabel, BDSG, 2. Aufl. 2013, § 3 Rdnr. 5.

48 Güneysu/Vetter/Wieser, DVBl 2011, 870, 872.

49 Hornung/Fuchs, DuD 2012, 20, 22; Müller, DuD 2012, 359, 360 f.

50 Greveler/Justus/Löhr, Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz", abrufbar unter: http://1lab.de/pub/smartmeter_sep11_v06.pdf, S. 3.

51 Roßnagel/Jandt, Datenschutzfragen eines Energieinformationsnetzes, Alcatel-Lucent Stiftung für Kommunikationsforschung, SR 88, 2010, S. 8.

52 Wiesemann, ZD 2012, 447, 447.

53 BT-Drs. 18/5948, S. 94; Lüdemann, ZD 2015, 247, 250; Wiesemann, ZD 2012, 447, 447.

54 Hier entsteht ein Widerspruch zum Transparenzprinzip, vgl. Bizer, DuD 2007, 350, 353 f.

55 Karg, (o. Fn. 41), S. 4; Lüdemann/Jürgens/Sengstacken. ZNER 2013, 592, 593.

56 Zum Zweckbindungsgrundsatz: Bizer, DuD 2007, 350, 352.

nicht absehbare Verwendungszwecke möglich. Diese lassen sich im Vorhinein kaum mit der erforderlichen Genauigkeit eingrenzen.[57] Auf nationaler Ebene ist bereits geplant, die Smart-Meter-Daten mit Daten aus anderen Sparten, wie der Gas-, Wärme- und Wasserversorgung zu verknüpfen.[58] Auf europäischer Ebene gibt es Überlegungen, die Daten auch mit den Sektoren Verkehr und Telekommunikation zu verbinden.[59] Das Gefahrenpotenzial steigt zudem mit dem wirtschaftlichen Wert des häuslichen Datensatzes. Das Interesse hieran ist groß. Dies belegen nicht zuletzt Investitionen und Firmenübernahmen im Smart-Home-Bereich durch Konzerne mit originär datenbasierten Geschäftsmodellen, wie etwa Alphabet.[60] Die Einhaltung des Zweckbindungsgrundsatzes ist aber nicht nur durch die dynamische technische Entwicklung gefährdet. Verstöße gegen den Zweckbindungsgrundsatz drohen auch durch staatlichen Eingriff. Absehbar ist, dass Smart-Meter-Daten auch für Strafverfolgungs-[61] oder Finanzbehörden[62] interessant sind.

5. Datensicherheit

Die Einführung intelligenter Messsysteme stellt schließlich auch die Gewährleistung der Datensicherheit vor gewaltige Herausforderungen. Mit der umfassenden Vernetzung steigt die Vulnerabilität sowie die Gefahr, dass auch Kriminelle den Zugang suchen.[63] Die geplante Standardisierung der intelligenten Messsysteme erhöht die Verletzlichkeit zusätzlich.[64] Die Möglichkeit eines Stromdiebstahls, die Verfälschung von Daten oder die Infizierung von Messsystemen mit Schadsoftware wurden bereits nachgewiesen.[65] Bei manipulierten Verbrauchsdaten drohen dem Anschlussnutzer finanzielle Verluste.[66] Eine mutwillige Unterbrechung der Stromversorgung kann zum Ausfall lebenswichtiger Geräte führen.[67] Das Einbruchs- und Diebstahlrisiko wird erhöht, wenn unberechtigte Dritte die Abwesenheit der Bewohner aus der Ferne feststellen können.[68] Der aktuelle Fall der Schadsoftware Locky zeigt mit dem Erpressungspotential weitere Risiken.[69]

V. Datenschutzkonzept des MsbG

1. Bereichsspezifische Vorrangregelung

Mit Inkrafttreten des Messstellenbetriebsgesetzes werden die bisherigen datenschutzrechtlichen Regelungen über intelligente Messsysteme im EnWG abgelöst.[70] An deren Stelle treten die Bestimmungen des Messstellenbetriebsgesetzes zur Datenkommunikation in intelligenten Energienetzen. Diese sind in Teil 3 des Gesetzes enthalten (§§ 49–75 MsbG-E). Als bereichsspezifische Sonderregelungen gehen diese Vorschriften den allgemeinen Bestimmungen des BDSG vor.[71] Der Anwendungsvorrang ist im Gesetz ausdrücklich niedergelegt. Nach § 49 Abs. 1 S. 2 MsbG-E ist die „Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften unzulässig". Der Gesetzgeber hat damit das lange geforderte[72] spezifische Datenschutzrecht für die Digitalisierung im Energiebereich geschaffen. Zu Recht. Mit der verpflichtenden Einführung von intelligenten Messsystemen werden die Letztverbraucher den mit dieser Technologie verbundenen Gefahren zwingend ausgesetzt. Es ist daher konsequent, dem damit staatlich gesetzten Risiko einen korrespondierenden Sicherungsauftrag für die informationelle Selbstbestimmung zur Seite zu stellen.[73] Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten in Zusammenhang mit dem Messstellenbetrieb ist daher künftig nur noch zulässig, soweit dies im Messstellenbetriebsgesetz ausdrücklich vorgesehen ist oder der Anschlussnutzer eingewilligt hat (§ 50 Abs. 1 MsbG-E).

2. Berechtigte und Zweckbindung

Da das Gesetz umfassende Einbaupflichten vorsieht, widmet sich der Großteil der Regelungen dem zulässigen Umgang mit den an der Messstelle erhobenen Daten. Hier setzt folgerichtig auch das gesetzliche Datenschutzkonzept an. Einen wesentlichen Baustein dieses Konzeptes bildet zunächst die abschließende Aufzählung der Stellen, die von Gesetzes wegen zum Datenumgang berechtigt sein sollen: Messstellenbetreiber, Netzbetreiber, Bilanzkoordinatoren, Bilanzkreisverantwortliche, Direktvermarktungsunternehmer nach dem EEG und Energielieferanten (§ 49 Abs. 2 MsbG-E). Nur die hier genannten Stellen sind von den gesetzlichen Erlaubnistatbeständen erfasst. Alle anderen Datenempfänger bedürfen der vorherigen schriftlichen Einwilligung des

57 In diese Richtung auch Roßnagel, Datenschutz in einem informatisierten Alltag, 2007, S. 139 m.w.N.

58 BT-Drs. 18/7555, S. 76.

59 Vgl. nur Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Leitlinien für transeuropäische Telekommunikationsnetze und zur Aufhebung der Entscheidung Nr. 1336/97/EG, KOM(2011) 657 endg. vom 19.10.2011, Erwägung 5.

60 So hat im Jahr 2014 etwa Google (heute Alphabet) das Unternehmen Nest, einen Hersteller von Thermostaten und Rauchmeldern, für mehrere Milliarden US-Dollar übernommen, vgl. http://www.spiegel.de/netzwelt/gadgets/nest-uebernahme-google-will-in-ihr-schlafzimmer-a-943406.html.

61 Eine hohe gleichförmige Stromabnahme kann beispielsweise ein Indiz für die Existenz einer Beleuchtungsanlage zur Aufzucht von illegalen Hanfpflanzen darstellen, vgl. Raabe/Lorenz/Pallas/Weis (o. Fn. 7), S. 33.

62 Die Identifikation bestimmter strombetriebener Geräte oder Einrichtungen könnte auf den Betrieb eines nicht angemeldeten Gewerbes hinweisen.

63 BMWi, Strategie Intelligente Vernetzung, S. 24.

64 Lüdemann, ZD 2015, 247, 251.

65 BT-Drs. 18/5948, S. 94 m.w.N.

66 Art. 29-Datenschutzgruppe, Stellungnahme 4/2013, WP205, S. 8, 13.

67 Art. 29-Datenschutzgruppe, Stellungnahme 7/2013, WP209, S. 6.

68 Art. 29-Datenschutzgruppe, Stellungnahme 4/2013, WP205, S. 12; in diese Richtung ebenso Hornung/Fuchs, DuD 2012, 20, 21.

69 Vgl. http://www.faz.net/aktuell/technik-motor/computer-internet/erpresser-virus-locky-verbreitet-sich-rasant-in-deutschland-14080201.html.

70 Vgl. Art. 3 Gesetzesentwurfs zur Digitalisierung der Energiewende.

71 Karsten/Leonhardt, RDV 2016, 22, 23. Zu den Anforderungen an bereichsspezifische Sonderregelungen vgl. nur Schmidt, in: Taeger/Gabel (o. Fn. 49), § 1 Rn. 33; Dix, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 1 Rn. 158, 170.

72 Vgl. dazu Kap. II sowie Lüdemann/Jürgens/Sengstacken. ZNER 2013, 592, 597.

73 Raabe/Lorenz/Pallas/Weis (o. Fn. 7), S. 53, Raabe. DuD 2010, 379, 384 f.

Anschlussnutzers. Dies gilt insbesondere für die Anbieter der unter Datenschutzgesichtspunkten kritischen Mehrwertdienste.[74] Da Mehrwertdienste für die Erreichung der energiewirtschaftlichen Ziele nicht erforderlich sind, ist eine Privilegierung über die gesetzlichen Erlaubnistatbestände nicht angezeigt.[75] Der Kreis der gesetzlich Berechtigten ist gegenüber dem EnWG zwar erweitert.[76] Dies ist aber vor allem der neu eingeführten sternförmigen Kommunikation direkt an die beteiligten Akteure bzw. im Falle des Direktvermarktungsunternehmers der noch jungen Marktrolle geschuldet. Unbefriedigend ist allerdings, dass die Berechtigten ihre Pflichten weiterhin im Wege der Auftragsverarbeitung an externe Dienstleister auslagern können.[77] Der „numerus clausus" der Berechtigten wird hiermit in gewisser Weise wieder ausgehöhlt.[78]

Die gesetzlichen Erlaubnistatbestände zur Datenerhebung, -verarbeitung und -nutzung bauen auf den Kreis der berechtigten Stellen auf. So werden in den §§ 55 ff. in hoher Detailtiefe diejenigen Sachverhalte festgelegt, zu denen eine Erhebung, Übermittlung und Nutzung der Daten zulässig ist. Als Kriterien zur Differenzierung der Zulässigkeit dienen die Datenart, die Art der berechtigten Stelle und der Verwendungszweck. Hiernach bestimmt sich, wer wann welche Daten in welcher Taktung bzw. in welchem Detaillierungsgrad erhalten und weiter verwenden darf. Die gesetzlichen Vorgaben orientieren sich dabei an den energiewirtschaft-lichen Aufgaben der Akteure.[79] Das Gesetz soll damit der Gefahr der Zweckentfremdung vorbeugen.[80]

Dieser kleinteilige legislative Ansatz ist grundsätzlich geeignet, die von intelligenten Messsystemen ausgehenden Gefahren für den Datenschutz wirksam zu minimieren. Der Preis ist allerdings eine hohe Komplexität der Regelungen. Das Messstellenbetriebsgesetz steht insoweit in der Tradition moderner Spezialgesetzgebung.

3. Datensparsamkeit

Der zweite zentrale Ansatz des Gesetzgebers ist die Betonung und gesetzliche Ausformulierung der Datensparsamkeit. Im Kontext intelligenter Mess- und Energiesysteme ist eine vollständige Vermeidung personenbezogener Daten nicht möglich. Andernfalls könnte weder die Verbrauchsabrechnung noch eine verbrauchsbezogene Steuerung umgesetzt werden. Angesichts der Gefahren für die informationelle Selbstbestimmung ist es deshalb von entscheidender Bedeutung, die Prozesse so zu gestalten, dass möglichst wenig kritische Daten entstehen bzw. in Umlauf kommen.[81] Das Gesetz orientiert sich zu diesem Zweck an dem allgemeinen Gebot der Datenvermeidung und Datensparsamkeit aus § 3a BDSG. Dies zeigt sich vor allem durch die Verpflichtung zur Anonymisierung und Pseudonymisierung in § 52 Abs. 3 MsbG-E.

Die wichtigste diesbezügliche Vorgabe betrifft die Datenübermittlung bei Anschlussnutzern mit einem Jahresstromverbrauch bis einschließlich 10.000 kWh. Hier dürfen lediglich die Jahresarbeitswerte übertragen werden.[82] Bei einem Durchschnittsverbrauch von 3.500 kWh pro Jahr und Haushalt ist damit zunächst der Großteil der Privathaushalte von vornherein von einer Datenübermittlung ausgenommen.[83] Etwas anders gilt nur, wenn der Verbraucher sich freiwillig für einen variablen Tarif entscheidet. In diesem Fall ist nach § 35 Abs. 1 Nr. 2 MsbG-E die tägliche Bereitstellung der Zählerstandsgänge des Vortages auch bei einem Jahresstromverbrauch unter 10.000 kWh vorgesehen.[84] Auch für Anschlussnutzer mit einem Jahresverbrauch über 10.000 kWh enthält § 60 Abs. 3 MsbG-E den Datenumgang beschränkende Bestimmungen. Die Zählerstände dürfen nur viertelstündlich ausgelesen werden. Außerdem darf die Übermittlung erst am Folgetag erfolgen. Dies erschwert eine mögliche Profilbildung.

Im bisherigen Gesetzgebungsverfahren wurde teils gefordert, die gesetzlichen Regelungen noch weiter zu untersetzen und auszudifferenzieren.[85] Der Gesetzgeber hat gut daran getan, diesen Vorschlägen nicht zu folgen. Die Regelungen weisen aufgrund ihrer Verknüpfung mit den Datenarten und Nutzungszwecken bereits jetzt eine außergewöhnlich hohe Komplexität auf. Abstrakten Normen ist immanent, dass nicht jeder denkbare Einzelfall abgebildet werden kann. Dies ist auch nicht notwendig. Entscheidend ist, dass die zentralen Anwendungsfälle erfasst sind. Die Randbereiche lassen sich hinreichend scharf über die Anwendung der allgemeinen Grundsätze der Datenvermeidung und Datensparsamkeit regeln.

Eine andere Frage ist allerdings, ob es zur Erreichung der gesetzgeberischen Ziele überhaupt erforderlich ist, personenbezogene Verbrauchsdaten aus dem Haushalt im geplanten Umfang zu übermitteln. Smart Meter verfügen über die Möglichkeit, einen Großteil der Datenverarbeitung im System selbst vorzunehmen, ohne dass hierzu weitere Stellen einbezogen werden müssen.[86] Dies gilt insbesondere für die

74 Mehrwertdienste sind definiert als energieversorgungsfremde Dienstleistungen, die als Kommunikationsinfrastruktur das Smart-Meter-Gateway nutzen, § 2 Nr. 9 MsbG-E.

75 BT-Drs. 18/7555, S. 107.

76 Vgl. § 21g Abs. 2 S. 1 EnWG mit § 49 Abs. 2 MsbG-E, wonach nun auch Bilanzkoordinatoren, Bilanzkreisverantwortliche und EEG-Direktvermarktungsunternehmer zu den berechtigen Stellen zählen.

77 § 49 Abs. 3 MsbG-E.

78 Karsten/Leonhardt, RDV 2016, S. 22, 23.

79 Dinter, ER 2015, 229, 234.

80 So zuvor gefordert durch Europäischer Datenschutzbeauftragter, Stellungnahme zur Empfehlung der Kommission zu Vorbereitungen für die Einführung intelligenter Messsysteme, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_DE.pdf, Ziff. 43.

81 Vgl. § 3a S. 2 BDSG; Europäischer Datenschutzbeauftragter (o. Fn. 82), Ziff. 43.

82 § 60 Abs. 3 MsbG-E.

83 Etwas anderes würde nur gelten, wenn mit dem Netzbetreiber die Steuerung von unterbrechbaren Verbrauchseinrichtungen gem. § 14a EnWG vertraglich vereinbart worden ist; vgl. BT-Drs. 18/7555, S. 110.

84 Hier entsteht ein Widerspruch zur Regelung der abschließenden Standardkommunikation nach § 60 Abs. 3 MsbG-E, wonach lediglich eine jährliche Übermittlung zulässig ist. Bei der Wahl eines variablen Tarifes wäre für kleinteiligere Übermittlungen wohl eine Einwilligung gemäß § 65 Nr. 1 MsbG-E erforderlich.

85 Vgl. Stellungnahme des Bundesrates in: BT-Drs. 18/7555, S. 135.

86 Die Ermöglichung datensparsamer Tarife sowie eine Messwertverarbeitung im Smart-Meter-Gateway gehören zu den durch die Technischen Richtlinien verbindlich vorgegebenen Mindestanforderungen, vgl. Kapitel 4 der Technischen Richtlinie BSI TR-03109-1 (S. 79 ff.).

Realisierung und Abrechnung zeitvariabler Tarife und damit gerade in den Bereichen, denen der Gesetzgeber eine große Bedeutung für die Sicherstellung einer nachhaltigen Energieversorgung beimisst. Für die Umsetzung der variablen Tarife erscheint es nach heutigem Stand der Technik ausreichend, wenn die Tarifinformationen an das intelligente Messsystem gesendet werden. Das Gerät berechnet dann aus Tarif und Verbrauch die Abrechnungsbeträge und meldet diese aggregiert an den Lieferanten.[87] Es verbleibt eine einseitige Kommunikation in Richtung des Verbrauchers. Nur zum Zeitpunkt und zum Zweck der Abrechnung wird einmalig ein (einzelner) Wert zurückgeliefert. Auch für das Netzmanagement und die Bilanzierung sind nach heutigem Stand keine personenbezogenen Daten erforderlich. Aggregierte Daten reichen hierfür aus.[88] Der Gesetzgeber sollte vor diesem Hintergrund die zusätzliche Anordnung in den Entwurf aufnehmen, dass überall dort, wo nach technischem Stand kein Personenbezug erforderlich ist, die Daten zwingend aggregiert werden müssen.[89] Eine derartige Regelung wurde im Vorfeld auch durch das BMWi angekündigt.[90] In den Entwurf hat diese aber bisher keinen Eingang gefunden.[91] Der allgemeine Grundsatz der Anonymisierung und Pseudonymisierung in Art. 52 Abs. 3 MsbG vermag das Fehlen einer solchen Vorgabe angesichts der ausdrücklichen Zulässigkeit der nichtaggregierten Datenübermittlung in den gesetzlichen Erlaubnistatbeständen nicht zu kompensieren.

4. Anforderungen an die Einwilligung

Die Nutzer sollten auf Basis von Aufklärung und Partizipation selbstbestimmte, informierte Entscheidungen treffen können, die den Prinzipien der Freiwilligkeit und Souveränität entsprechen.[92] Um dies sicherzustellen sowie zur Gewährleistung eines ausreichenden Datenschutzes, werden bei der möglichen Einwilligung die hohen Anforderungen des § 4a BDSG übernommen. Bereits die geforderte Freiwilligkeit könnte fraglich sein, wenn etwa eine Inanspruchnahme von Mehrwertdiensten durch die Anschlussnutzer an die Preisgabe von Daten geknüpft wird, die zu diesem Zweck nicht erforderlich sind.[93] Notwendig ist darüber hinaus eine informierte Einwilligung. Der Betroffene muss wissen, worin er einwilligt, um die Tragweite seiner Entscheidung abzusehen.[94] Der Gesetzgeber flankiert dazu zwar bereits vertragliche Regelungen zur Datenkommunikation beim Smart Metering mit hohen Transparenzvorgaben durch ein standardisiertes Formblatt.[95] Ein Ansatz, der anzuerkennen ist. Allerdings stehen sich kurze, einfache Formblätter und die umfassenden Transparenzpflichten bei datenschutzrechtlichen Einwilligungserklärungen oftmals diametral gegenüber. Vor dem Hintergrund der möglichen Vielzahl von beteiligten Akteuren sowie Übermittlungs- und Verarbeitungsvorgängen innerhalb intelligenter Energienetze werden die zur Einwilligung erforderlichen Informationen sehr umfangreich sein. Insofern ist unter dem Stichwort des „information overload" Skepsis angezeigt. Es besteht die Gefahr, dass die Nutzer mit Informationen überfrachtet werden.[96] Wie dieses Spannungsfeld, welches für sämtliche modernen Technologieanwendungen typisch ist, im Rahmen der intelligenten Messsysteme aufgelöst werden soll, bleibt abzuwarten.

Schwer umsetzbar sind die Formerfordernisse an die datenschutzrechtliche Einwilligung im Sinne des BDSG. Die Einwilligung in den Datenumgang ist höchstpersönlicher Natur. Da sie einen Grundrechtseingriff rechtfertigt, kann nur der Grundrechtsinhaber selbst die Einwilligung erklären; die Abgabe durch einen Bevollmächtigten scheidet aus.[97] Nach dem Messstellenbetriebsgesetz soll die Einwilligung aber lediglich durch den Anschlussnutzer erfolgen. Dabei wird ausgeblendet, dass in Mehrpersonenhaushalten personenbezogene Daten von sämtlichen Bewohnern erfasst, zugeordnet und zu Profilen zusammengefasst werden können.[98] Folglich wären regelmäßig Erklärungen aller Bewohner einzuholen. Aufgrund dieses weiten Kreises an Betroffenen, lässt sich auch die Schriftform des § 4a Abs. 1 S. 3 BDSG in der Praxis kaum erfüllen. Die elektronische Form ist nur mittels qualifizierter elektronischer Signatur zulässig, welche allerdings eine zu geringe Verbreitung gefunden hat, um praktische Relevanz zu genießen.[99] Zudem ist eine Einwilligung für jede einzelne Datenverwendung geboten.[100] Dies scheint mit Blick auf die Schriftform sowie den Kreis der potenziell im Haushalt betroffenen Personen undurchführbar.

5. Organisatorische und technische Datensicherheit

Den datensicherheitsrechtlichen Gefahren begegnet der Entwurf schließlich durch die Aufstellung organisatorischer und technischer Mindestanforderungen für intelligente

87 In diese Richtung ebenso Schäfer-Stradowsky/Boldt, EnWZ 2015, 349, 351.

88 Raabe/Lorenz/Pallas/Weis (o. Fn. 7), S. 38; Orientierungshilfe (o. Fn. 42), S. 28; vzbv, Smart Meter Einbau: Zwangsdigitalisierung durch die Kellertür. Stellungnahme des Verbraucherzentrale Bundesverbandes zum Entwurf eines Gesetzes zur Digitalisierung der Energiewende, abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Stellungnahmen/Stellungnahmen-Gesetzentwurf-Digitalisierung-Energiewende/verbraucherzentrale-bundesverband,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, S. 5.

89 Schäfer-Stradowsky/Boldt, EnWZ 2015, 349, 351; Roßnagel, ZD 2013, 562, 563.

90 BMWi/BSI, Smart Metering – Datenschutz und Datensicherheit auf höchstem Niveau, abrufbar unter: www.bmwi.de/BMWi/Redaktion/PDF/S-T/smart-metering,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, S. 2.

91 Die einzige Ausnahme bildet § 67 II Nr. 1 und 2 MsbG, in denen die Übermittlung aggregierter Last- und Einspeisegänge vom Übertragungsnetzbetreiber an den Verteilernetzbetreiber und den Bilanzkreisverantwortlichen geregelt ist.

92 BMWi, Strategie Intelligente Vernetzung, S. 5, 24.

93 Dies gilt insbesondere dann, wenn dem Nutzer bei einer Ablehnung der Datenverwendung die Leistung verwehrt wird. Vgl. insoweit das Kopplungsverbot, Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5. Aufl. 2016, § 4a Rdnr. 24.

94 Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 4a Rdnr. 25.

95 Dort müssen Angaben zu Art, Umfang, Häufigkeit und Zweck von Datenübermittlungen übersichtlich und verständlich niedergelegt und dem Anschlussnutzer zur Verfügung gestellt werden, § 54 MsbG-E.

96 Buchner, DuD 2010, 39, 40; Katko/Babaei-Beigi, MMR 2014, 360, 362 f.

97 Simitis, in: Simitis (Hrsg.) (o. Fn. 73), § 4a Rdnr. 30 f. m.w.N.

98 Vgl. Kap. IV 1 und 2.

99 Kühling, in: Wolff/Brink (o. Fn. 42), § 4a Rdnr. 48.

100 Simitis, in: Simitis (Hrsg.) (o. Fn. 73), § 4a Rdnr. 33.

101 § 1 Nr. 4, §§ 19 ff. MsbG-E.

Messsysteme.[101] In organisatorischer Hinsicht betont der Entwurf die Rolle des Smart-Meter-Gateway-Administrators und weist ihm die zentrale Verantwortung für die Einhaltung der datensicherheitsrechtlichen Bestimmungen zu. Allein der Gateway Administrator kann den Zugriff auf die Daten aus dem intelligenten Messsystem ermöglichen.[102] Jegliche Kommunikation mit dem intelligenten Messsystem muss durch ihn autorisiert werden. Er wacht darüber, dass Dritte zum Datenempfang tatsächlich berechtigt sind und hat sich entsprechende Berechtigungsnachweise vorlegen zu lassen. Entsprechend dieser zentralen Stellung im Sicherheitskonzept, stellt der Entwurf hohe Anforderungen an die Integrität und Fachkunde des Gateway Administrators. Die Übernahme dieser Funktion ist erst nach einer entsprechenden Zertifizierung möglich.[103] Ebenso unterliegt auch das Smart-Meter-Gateway selbst einer Zertifizierungspflicht.[104]

Die Sicherstellung der technischen Datensicherheit überträgt der Entwurf weitestgehend dem Bundesamt für Sicherheit in der Informationstechnik (BSI), das über den Umweg der Vermutungsregelung des § 22 Abs. 2 MsbG-E im Rahmen von Schutzprofilen und Technischen Richtlinien faktisch alle technischen Vorgaben für den Einsatz der intelligenten Messsysteme macht. Daneben wird die Bundesnetzagentur ermächtigt, im Einvernehmen mit dem BSI die erforderlichen Festlegungen im Verordnungswege zu treffen.[105]

Insgesamt sind die Datensicherheitsvorgaben stimmig. Dies gilt auch für die im Entwurf gewählte Lösung, die Detaillierung der technischen Vorgaben auf das flexible Instrument der Ausgestaltung durch das BSI und die Bundesnetzagentur zu stützen. In einem sich rasch ändernden Umfeld sichert dies die notwendige Innovationsoffenheit und Flexibilität. Positiv hervorzuheben ist auch die klare Zuweisung der Verantwortung an eine Stelle, hier den Gateway Administrator. Dies erleichtert die Prüfung durch die Aufsichtsbehörden. Kritisch ist jedoch, dass die Datensicherheitsanforderungen nach dem Entwurf nur die Kommunikationswege vom Messsystem zu den berechtigten Stellen abdecken. Nicht erfasst sind nachgelagerte Datenverarbeitungen. Vor allem neue, unregulierte Dienstleistungsanbieter, die auf Grundlage einer Einwilligung des Anschlussnutzers tätig werden, können hier zur Sicherheitslücke werden.[106]

VI. Fazit

Die Zusammenführung der gesamten Regelungsmaterie zum Messstellenbetrieb in einem neuen Stammgesetz ist zu begrüßen. Auch die Vorgabe umfangreicher Mindeststandards in den Bereichen Datenschutz, Datensicherheit und Interoperabilität ist ein wichtiger Schritt. Das Datenschutzkonzept des MsbG-E stellt insgesamt eine deutliche Verbesserung gegenüber den bisher geltenden Regelungen dar. Der Entwurf vermag in seiner jetzigen Fassung dennoch nicht die Bedenken zu zerstreuen, dass die „Zwangsdigitalisierung durch die Kellertür"[107] erhebliche Risiken für das Recht auf informationelle Selbstbestimmung mit sich bringt. Kritisch sind vor allem drei Punkte:

- *Der Entwurf ermöglicht die Übermittlung personenbezogener Daten in einem Umfang, der weder technisch noch energiewirtschaftlich erforderlich ist. In vielen Fällen könnte die Verarbeitung der kritischen personenbezogenen Daten im intelligenten Messsystem selbst stattfinden. Übermittelt würden dann vorwiegend aggregierte Daten. Der das Haus verlassende Fluss sensibler Daten könnte so erheblich begrenzt werden. Zur Erreichung der energiewirtschaftlichen Ziele gibt es mithin weniger eingriffsintensive Alternativen. Es wäre daher – auch im Hinblick auf die Akzeptanz – zu wünschen, dass die Frage der Messwertverarbeitung im Smart-Meter-Gateway und weitere datensparsamere Alternativen im Gesetzgebungsverfahren nochmals vertieft behandelt werden.*
- *Problematisch ist zudem, dass der Entwurf bei Datenübermittlungen außerhalb der gesetzlichen Erlaubnistatbestände allein auf die Einwilligung des Anschlussnutzers abstellt, auch wenn die Daten mehrerer Haushaltsangehöriger erfasst werden. Für diesen Umstand bietet der Entwurf derzeit keine Lösung. Hier bedarf es auch angesichts der absehbaren Regelungen in der Datenschutz-Grundverordnung einer Klärung, um der Energiewirtschaft rechtssichere Lösungen anbieten zu können. Möglicherweise bietet eine Regelung wie im Telekommunikationsrecht zur Bekanntgabe des Einzelverbindungsnachweises einen Ausweg.[108] Für das Erfordernis der Schriftform zeichnet sich im Entwurf zur europäischen Datenschutz-Grundverordnung mit Art. 4 Nr. 11 in Verbindung mit Erwägungsgrund Nr. 32 eine Lockerung ab.[109]*
- *Kritisch ist zudem die zwangsweise Einführung von Smart Metern. Die Digitalisierung der eigenen vier Wände beruht bisher auf der freien Entscheidung der Wohnungsinhaber. Aus gutem Grund. Schließlich erlauben intelligente Messsysteme die Erhebung von Verbrauchsdaten in einem Umfang, durch den der Alltag der Menschen in der eigenen Wohnung in hoher*

102 BT-Drs. 18/7555, S. 84.

103 § 25 Abs. 5 MsbG-E.

104 § 24 MsbG-E

105 § 75 Nr. 1 MsbG-E.

106 Raabe/Lorenz/Pallas/Weis (o. Fn. 7), S. 49.

107 vzbv (o. Fn. 90), S. 5

108 Vgl. dazu auch Karsten/Leonhardt, RDV 2016, 22, 23 f.

109 Künftig soll eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung" ausreichend sein. Vgl. Standpunkt des Rates in erster Lesung im Hinblick auf den Erlass der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aushebung der Richtlinie 95/46/EG, 5419/16 vom 6. April 2016, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=DE.

Detailtiefe für Dritte nachvollziehbar ist.[110] *Dementsprechend hat der Bundesrat für eine Opt-Out-Option votiert.*[111] *Für eine solche Lösung spricht auch, dass der Nachbarstaat Österreich diesen Weg bereits gegangen ist.*[112] *Die Position der Bundesregierung, wonach über reine Marktmechanismen keine ausreichende Durchsetzung intelligenter Messsysteme erfolgen kann, vermag nur bedingt zu überzeugen. Dabei kann dahingestellt bleiben, ob die Energiewirtschaft eines weiteren Subventionstatbestandes bedarf, dessen Finanzierung auf die Verbraucher umgelegt wird. Die Grenzen der Marktbeeinflussung sind jedenfalls dort erreicht, wo diese erheblich zu Lasten grundrechtsrelevanter Positionen der Endverbraucher gehen.*

Es bleibt daher zu hoffen, dass der Gesetzgeber in diesen Punkten vor Inkraftsetzen des Messstellenbetriebsgesetzes nachsteuert.

110 Art. 29-Datenschutzgruppe, Stellungnahme 4/2013, WP205, S. 5.

111 Diese sollten sowohl in Bezug auf Ausstattung mit als auch auf die Verwendung von Daten aus intelligenten Messsystemen gelten, vgl. BT-Drs. 18/7555, S. 124 ff.

112 Vgl. § 83 Abs. 1 S. 4 ElWOG für den Strom- sowie § 128 Abs. 1 S. 4 GWG für den Gassektor.

Prof. Dr. Volker Lüdemann
ist Professor für Wirtschafts- und Wettbewerbsrecht an der Hochschule Osnabrück und wissenschaftlicher Leiter des Niedersächsischen Datenschutzzentrums (NDZ).

Manuel Christian Ortmann LL.M.
ist Doktorand im vom Land Niedersachsen sowie der VW-Stiftung geförderten Projekt „EOS-Energiespeicherlösungen in der Region Osnabrück-Steinfurt" und beschäftigt sich mit aktuellen Fragen des Energierechts.

Patrick Pokrant LL.M.
ist wissenschaftlicher Mitarbeiter im EOS-Projekt und beschäftigt sich mit aktuellen Fragen des Datenschutzrechts.

Kurzbeiträge

Aus den aktuellen Berichten der Aufsichtsbehörden (25): Unerwünschte Kunden/Mitarbeiter

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter*

Es gibt Personen mit denen möchte man nichts oder nichts mehr zu tun haben, weil man selbst oder andere schlechte Erfahrungen mit ihnen gemacht haben. Ggf. helfen dann interne oder externe Warndateien.

Unerwünschte Hotelgäste

In einem zu einer großen Hotelkette gehörenden Haus wurden potentielle Hotelgäste am Empfang abgewiesen, weil sie laut Empfangspersonal auf einer „Schwarzen Liste" standen. Die Nachforschungen der BlnBDI (Jahresbericht 2015, Ziff. 5.8.2) ergaben, dass in der Liste unerwünschte frühere Gäste mit dem Ablehnungsgrund „Raucher" bzw. „Schwarzschläfer" aufgeführt werden. Die BlnBDI hat gegen eine solche Liste keine grundsätzlichen Bedenken, sofern die datenschutzrechtlichen Belange der betroffenen Gäste gewahrt bleiben. Dazu verweist sie auf die dem Hotelier zustehende

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

Vertragsfreiheit und sein berechtigtes Interesse mit Gästen, die Regeln der Hotelnutzung nicht einhalten, indem sie in Nichtraucherzimmern geraucht oder nicht angemeldete Gäste als „Schwarzschläfer" aufgenommen haben, keine neuen Verträge abzuschließen.

Jedoch seien die Betroffenen von der Speicherung auf der Liste zu benachrichtigen, um ihre Datenschutzrechte geltend machen zu können. Eine Norm für die Benachrichtigung nennt die BlnBDI nicht. Offensichtlich wendet sie § 33 in der gebotenen extensiven Auslegung (vgl. Gola/Schomerus, BDSG § 33 Rn.) nicht nur auf Fälle der erstmaliger Speicherung der Daten des Kunden an, sondern auch, wenn eine neue Art von Daten gespeichert wird bzw. deren Weitergabe innerhalb der Hotelkette erfolgt.

Die Hotelkette führt die Hausverbotsliste nunmehr bei der Zentrale unter der Regie des betrieblichen DSB, worin die BlnBDI keine Probleme sieht.

Unerwünschte Versandhauskunden/ Unternehmensinterne Auskunftei

Der HambBfDI (25. TB (2014/2015), VIII, Ziff. 1.4) ermittelte, dass Mitarbeiter in Unternehmen eines Versandhandelskonzerns bei der Überprüfung von Neukunden auf insgesamt 33 Dateien zurückgreifen konnten. Dabei ging es um jeweils 3 eigene Dateien, nämlich eine allgemeine Kunden-, eine Inkasso- und eine Warndatei. Hinsichtlich der Dateien der Tochterunternehmen wurde die Mutter als Auftragsdatenverarbeiter tätig. Im Rahmen der sogenannten Neukundenkreditprüfung wurden die bonitätsrelevanten Kundendaten aus den drei Datenbanken abgefragt, wobei jedes der Unternehmen (eingeschränkten) Zugriff auf die Dateien der anderen Unternehmen hatte.

Der HambBfDI bewertete dieses Verfahren als den Betrieb einer Auskunftei, der besonderen BDSG-Regelungen unterliegt. U.a. dürften Meldungen über offene Forderungen nur unter den Voraussetzungen des § 28a BDSG erfolgen. Ferner seien besondere Pflichten zu beachten, wie Stichprobenverfahren, Benachrichtigungs- und Auskunftspflichten.

Letztendlich hat das Unternehmen den Betrieb einer Auskunftei zum Register des HambBfDI gemeldet und die insoweit bestehenden Pflichten anerkannt.

Unerwünschte Lastschriftzahler

Gegenüber Kunden, die ihre Rechnung im elektronischen Lastschriftverfahren (ELV), d.h. ohne sofortige Prüfung der Leistung der Bank, zahlen, sichern sich Händler dadurch ab, dass sie oder der Netzbetreiber Kunden mit zuvor z.B. wegen mangelnder Deckung oder Nichtbestehen des Kontos gescheiterten Lastschriftverfahren bei einer von einer Auskunftei geführten „Sperrdatei" einmelden. In der Datei geführte Kunden werden automatisiert von der Zahlung im ELV ausgeschlossen und auf das Girocardverfahren verwiesen.

Der HambBfDI (25 TB, 2014/2015, VIII, Ziff.1.5) bemängelte an einer derartigen Datei, dass dort auch berechtigte Rücklastschriften, d.h. d.h. Fälle, in denen berechtigt per Widerspruch bei der Bank die Zahlung verweigert wurde, gespeichert wurden. Hierüber wurden die Kunden auch in dem Belehrungstext, der ihnen zusammen mit der zu unterzeichnenden Einzugsermächtigung auf einem Kassenausdruck gezeigt wurde, nicht informiert. Dies wurde geändert, indem deutlich gemacht wird, dass, sofern bereits bei der Erklärung des Widerrufsrechts aus dem zugrundeliegenden Kaufvertrag Einwände, etwa ein Mangel der erworbenen Sache, geltend gemacht werden, von vorneherein keine Meldung mehr an die Auskunftei erfolgt.

Zur Unzuverlässigkeit finanzschwacher Bewerber

Sowohl die BremLfDI (38. TB, 2015, Ziff. 11.1) als auch die BlnBDI (Jahresbericht 2015, Ziff. 91) befassen mit der Zulässigkeit von Bonitätsanfragen über Bewerber, wobei es sich einmal um den Posten eines Autoverkäufers und zum anderen um eine Stelle im Bereich des Telefonmarketing handelte. Finanzielle Zuverlässigkeit sollte nach Ansicht der Arbeitgeber überprüft werden, weil der Verkäufer mit „viel Geld" in Berührung komme bzw. im Telefonmarketing die Gefahr der Bestechlichkeit bestehe.

Zutreffend ist zunächst, dass Bewerber wegen privater finanzieller Probleme nicht stigmatisiert und als kriminalitätsanfällig eingestuft werden dürfen. Dazu hält der BlnBDI für standardisierte Bonitätsauskünfte wie folgt fest: *„Standardisierte Bonitätsauskünfte enthalten auch Informationen, die Aufschluss über die privaten Lebensumstände und über Geld- und Warenkreditverträge der Betroffenen geben. Die Einholung einer solchen Auskunft ist in der Regel unzulässig, da diese über das für die Einstellungsentscheidung erforderliche Informationsinteresse hinausgeht und in das Persönlichkeitsrecht der Bewerberinnen und Bewerber eingreift."*

Gleiche bzw. zusätzliche Bedenken erhebt die BremLfDI, indem sie auch darauf verweist, dass die Auskünfte erheblich mehr Daten erhalten, als für die Entscheidung über den zu besetzenden Arbeitsplatz erforderlich seien, und dass Daten zur Kreditwürdigkeit häufig unzutreffend seien. Sie kommt zur uneingeschränkten Unzulässigkeit derartiger Auskunftseinholungen über Bewerber, da es ausreiche, im Wege der Direkterhebung bei den Betroffenen nach Verurteilungen wegen Straftaten im Zusammenhang mit Vermögensdelikten in den letzten fünf Jahren zu fragen. Dazu, ob eine Überprüfung dieser Angaben zulässig sei, äußert sie sich nicht.

Anders und zutreffend beurteilt jedoch die BlnBDI im Einzelfall das Informationsinteresse des Arbeitgebers. Einzelanfragen werden als zulässig angesehen, wenn der Bewerber eine Aufgabe übernehmen soll, in der Seriosität und Vertrauenswürdigkeit in finanziellen Fragen bedeutsam sind (z.B. Finanzberatung). Gleiches gelte aber auch für Beschäftigte, bei denen finanzielle Zuverlässigkeit gefordert sei (z.B. Kassierer).

Angemerkt sei jedoch, dass zunächst das Prinzip der Direkterhebung gilt und dass der Bewerber über den nachfolgenden sog. „Background-Check" zuvor informiert werden muss.

Unerwünschte „Terrorverdächtige“

Aufgrund der aktuellen Problematik (nach Pressemitteilungen sollen im Brüsseler Flughafen und im Atomkraftwerk der ISS-Nähe verdächtigte Personen beschäftigt gewesen sein) und der erneut aufgekommenen Diskussion in der Literatur (vgl. Behling, NZA 2015, 1359; Byers/Fetsch, NZA 2015, 1364) befasst sich der LfD-Baden-Württemberg (32. TB, 2014/2015, Ziff. 9.2) einmal mehr mit dem Abgleich von Beschäftigtendaten mit den Sanktionslisten der EU. Konkreter Anlass war, das in einem großen Konzern per Konzernbetriebsvereinbarung alle drei Monate die Daten von Mitarbeitern und Bewerbern an Hand von Vor- und Nachname, Geburtsdatum und Adresse mit den EU-Sanktionslisten mit Terrorverdächtigten “gescreent“ werden. Der Abgleich erfolgt, weil die Verordnungen verbieten, den aufgelisteten Personen Gelder zur Verfügung zu stellen und Verstöße nach dem Außenwirtschaftsgesetz mit Bußgeld geahndet werden können. Bei anderen Unternehmen erfolgt der Abgleich vor jeder Gehaltszahlung, bzw. sie verweisen auf den im Rahmen der unbaren Gehaltszahlung sowieso erfolgenden Abgleich bei den Banken. Dabei geht es den Unternehmen offensichtlich vorrangig auch um die die Prüfung voraussetzende Erteilung des sog. AEO-Status zwecks vereinfachter Zollabfertigung. Andere beschränken den Abgleich auf Mitarbeiter in sensiblen Bereichen, wobei hier deutlich wird, dass es vorrangig um den Eigenschutz des Unternehmens geht.

Nach Schilderung der unterschiedlichen Beurteilung der Rechtslage hinsichtlich der Pflicht zu bzw. der Zulässigkeit von Abgleichen zwischen den Aufsichtsbehörden und dem Wirtschaftsministerium bzw. der Bundeszollverwaltung, die zudem vom BFH bestätigt ist (RDV 2012, 303), sieht sich der LfDI jedenfalls derzeit zum Stillhalten als verpflichtet an, indem er festhält: *„Bei der Auslegung der Bußgeldtatbestände des Außenwirtschaftsgesetzes zieht die Bundeszollverwaltung nicht an einem Strang mit der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder. Anlasslose und systematische Abgleiche von Beschäftigtendaten mit den Sanktionslisten des EU-Rechts durch Arbeitgeber müssen daher bis auf weiteres hingenommen werden. Der Europäische Gesetzgeber ist aufgerufen, in dieser Frage für Klarheit zu sorgen.“*

Nach dem Ende von Safe Harbor: Das EU-U.S.-Privacy Shield

Steffen Weiß, LL.M, Hamburg*

I. Das Safe Harbor-Urteil und seine Folgen

Der EuGH hat mit seiner Entscheidung zu Safe Harbor am 6. Oktober 2015 hohe Wellen in die transatlantischen Datenströme geschlagen. Mit Verkündung des Urteils waren Datenexporte in die USA auf Basis der Angemessenheitsentscheidung der EU-Kommission zu Safe Harbor als rechtswidrig einzustufen, was an sich einen sofortigen Stopp diesbezüglicher Datenexporte bedeutet hätte. Schnell waren die europäischen Aufsichtsbehörden versucht, weitere Rückschlüsse aus den Entscheidungsgründen des EuGH zu ziehen, was sich in einer Vielzahl behördlicher Stellungnahmen manifestierte. Erst die Art. 29-Datenschutzgruppe auf europäischer Ebene sowie die Konferenz der Datenschutzbeauftragten von Bund und Ländern auf nationaler Ebene vermochten Datenverarbeitern eine erste konsolidierte und praktikable Meinung zu den Folgen des Safe Harbor Urteils zu vermitteln.

Sowohl das Positionspapier der Konferenz der Datenschutzbeauftragten von Bund und Ländern[1] als auch die Art. 29-Gruppe[2] forderten die Mitgliedstaaten und die europäischen Institutionen nachdrücklich dazu auf, offene Gespräche mit den US-amerikanischen Behörden zu führen, um *politische, rechtliche und technische Lösungen für einen angemessenen Schutz der Grundrechte der EU-Bürger* zu finden. Gleichzeitig würde weiter untersucht werden, wie sich das EuGH-Urteil auf *andere Werkzeuge* zur Herstellung eines angemessenen Datenschutzniveaus in einem Drittland wie die *EU-Standardvertragsklauseln* oder *Binding Corporate Rules (BCRs)* auswirkt. Letztgenannten Werkzeugen wurde eine Frist bis Ende Januar 2016 gesetzt, bevor konsolidierte Durchsetzungsmaßnahmen der Aufsichtsbehörden – je nach Ausgang der Prüfung – verpflichtend umzusetzen wären. Die von der Art. 29-Gruppe und der Konferenz der Datenschutzbeauftragten von Bund und Länder gesetzte Frist haben die Mitgliedstaaten und die europäischen Institutionen verstreichen lassen. Inzwischen drohen nationale Aufsichtsbehörden teilweise explizit Durchsetzungsmaßnahmen bezüg-

* Der Autor ist Repräsentant Internationales bei der GDD und aktives Mitglied des europäischen Datenschutz-Dachverbands CEDPO. Ferner ist er seit 2015 Lehrbeauftragter für Datenschutz an der Fachhochschule Wedel.

1 Https://www.datenschutz.rlp.de/de/grem_dsbkonferenz/sonstiges/20151021_Positionspapier_DSK_Safe_Harbor.pdf.

2 Http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

lich der Datenexporte an, die noch auf Basis von Safe Harbor von statten gehen.[3]

Erst kurz nach Ablauf der gesetzten Frist veröffentliche die EU-Kommission am 2. Februar eine Presseerklärung, in der eine Einigung zwischen der EU Kommission und den Vereinigten Staaten hinsichtlich einer Nachfolgeregelung von Safe Harbor, genannt *„EU-U.S. Privacy Shield"*, verkündet wurde und die bereits erste Eckpunkte vorgesehener Maßnahmen beinhaltete.[4]

II. EU-U.S. Privacy Shield

Zum Ende der durch die Art. 29-Gruppe festgesetzten Frist veröffentliche die EU-Kommission am 29. Februar verbindliche Inhalte des neuen *EU-U.S. Privacy Shield* als Nachfolgeinstrument zu Safe Harbor. Ziel soll es sein – wie bereits im Rahmen von Safe Harbor –, ein angemessenes Datenschutzniveau bei Datenempfängern in den USA zu gewährleisten, die sich nach den Vorgaben des EU-U.S. Privacy Shield *(„EU-U.S. Privacy Shield Framework Principles"*[5]*)* zertifiziert haben. Hierbei wurden auf Basis der bereits in 2013 durch die Kommission selbst vorgeschlagenen 13 Empfehlungen zur Verbesserung von Safe Harbor[6] sowie den Entscheidungsgründen des EuGH die Anforderungen an zertifizierte Datenverarbeiter in den USA erhöht. Hinsichtlich des Anwendungsbereichs der Angemessenheitsentscheidung der Kommission tritt beim Privacy Shield aber zunächst keine Neuerung ein: Nur zertifizierte Unternehmen in den USA sollen in den Genuss europäischer Daten kommen. Welche erweiterten Vorgaben das „Datenschutzschild" mit sich bringt, soll im Folgenden anhand ausgewählter Themen vorgestellt werden:

1. Transparenz

Eine Zertifizierung nach dem Privacy Shield erfolgt durch eine Erklärung gegenüber dem US-Handelsministerium und bedarf einer jährlichen Aktualisierung. Änderungen ergeben sich bei der Publizität von Zertifizierungen, die in der Vergangenheit nicht ausreichend gewährleistet war: Das US-Handelsministerium soll nunmehr ein Register führen, das neben bestehenden Zertifizierungen auch *unwirksame* bzw. *entzogene Zertifikate* sowie den diesbezüglichen *Grund* aufführt (Erwägungsgrund 24 und 39 der Angemessenheitsentscheidung im Entwurf)[7]. *Anhängige Verfahren* bei der Federal Trade Commission (FTC) als einem Organ der Aufsicht über das Privacy Shield, so beispielsweise aufgrund eines Verstoßes gegen dessen Vorgaben, sollen über das Register nun ebenfalls kommuniziert werden.

Dauerhafte Verstöße gegen die Vorgaben des Privacy Shields resultieren nicht nur in der Entfernung aus dem Register aktueller Zertifizierungen sondern münden in der Pflicht zur *Löschung aller unter dem Privacy Shield empfangenen Daten* (Erwägungsgrund 26). In anderen Fällen, die zu einem Entzug einer Zertifizierung führen, kann eine Stelle die empfangenen Daten zwar weiterhin verarbeiten. Das setzt aber voraus, dass sie gegenüber dem US-Handelsministerium erklärt, dass diese Daten weiterhin nach den Vorgaben der Privacy Shield Framework Principles oder mithilfe alternativer anerkannter Werkzeuge zur Herstellung eines angemessenen Datenschutzniveaus, so beispielsweise die EU-Standardvertragsklauseln, geschützt werden.

Die fälschliche Kommunikation einer gültigen Zertifizierung wird durch die Organe der Aufsicht verfolgt, wobei die Aufsicht im Wesentlichen der FTC, dem US-Handelsministerium bzw. dem US-Verkehrsministerium (Department of Transportation) obliegt. Um das Netz der Überwachung enger zu stricken, soll das Handelsministerium gar proaktiv kontrollieren, ob die Datenschutzerklärung des „ausgeschiedenen" Unternehmens keinerlei Bezüge zum Privacy Shield mehr enthält (Erwägungsgrund 28). Verstöße sollen wiederum den Aufsichtsorganen mit Durchsetzungskompetenzen zugeleitet werden. Ebenso stellt das Handelsministerium proaktiv sicher, so über das Versenden von *Fragebögen,* dass Unternehmen mit erloschener Privacy Shield Zertifizierung empfangene Daten gelöscht haben, bzw. freiwillig diese Daten nach den Vorgaben der Privacy Shield Principles oder alternativer anerkannter Angemessenheitswerkzeuge schützen (Erwägungsgrund 39).

2. Beschwerden und Abhilfemaßnahmen

Bereits unter Safe Harbor mussten US-Datenverarbeiter Beschwerdeverfahren zugunsten von Betroffenen einrichten und die eingerichtete Kontaktstelle zur Entgegennahme von Beschwerden über die Datenschutzerklärung kommunizieren. Um diese Verfahren zu beschleunigen, sind Beschwerden Betroffener nunmehr innerhalb einer Frist von *45 Tagen* durch den Datenverarbeiter zu beantworten. Auch die Streitschlichtung erfährt neue Blüte, indem eine unabhängige Stelle zu involvieren ist, die, neben kostenfreien Abhilfemaßnahmen zugunsten des Betroffenen, auch *einen jährlichen Bericht* hinsichtlich ihrer Aktivitäten mit Blick auf das Privacy Shield zu veröffentlichten hat, so unter anderem auch die Anzahl der Fälle, die Länge ihrer Bearbeitung sowie deren Ergebnis (Erwägungsgrund 31). Ebenso wird auf Seiten des Handelsministeriums sowie der FTC eine *Kontaktstelle für europäische Aufsichtsbehörden* eingerichtet, um Beschwerden Betroffener anzunehmen sowie beim US-Datenverarbeiter nachzuverfolgen. Die Kontaktstelle beim Handelsministerium hat innerhalb von höchstens *90 Tagen* über den Verlauf, bzw. Ausgang des Verfahrens zu informieren. Hierbei hat das Handelsministerium jährlich über eingegangene Beschwerden Bericht zu erstatten (Erwägungsgrund 36).

3 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Aktueller Sachstand zu Safe Harbor (Februar 2016), abrufbar unter https://www.datenschutz-hamburg.de/news/detail/article/safe-harbor-aktueller-sachstand-im-februar-2016.html; Der Landesbeauftragte für Datenschutz und Informationsfreiheit Rheinland-Pfalz, Pressemitteilung vom 10. Februar 2016, abrufbar unter https://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2016021001.

4 Http://europa.eu/rapid/press-release_IP-16-216_en.htm.

5 Zu den Privacy Shield Framework Principles ausführlich, Angemessenheitsentscheidung der Kommission, Er-wägungsgründe 16-23.

6 Http://europa.eu/rapid/press-release_MEMO-13-1059_de.htm.

7 Im Weiteren wird auf den Zusatz „Angemessenheitsentscheidung im Entwurf" verzichtet.

Im Zuge der Verbesserung von Safe Harbor wurde den europäischen Aufsichtsbehörden im EU-U.S. Privacy Shield bei den Beschwerde und Abhilfeverfahren eine besondere Rolle zugebilligt. Neben den erwähnten Kontaktstellen für aus Europa eingehende Beschwerden soll die Meinung der europäischen Aufsicht zu bestimmten Streitfällen über ein eigenes, jedoch *informelles Gremium* Gehör finden (s. Ergänzungsdokument zum EU-U.S. Privacy Shield „The Role of the Data Protection Authorities). Für die Beschleunigung des Verfahren sorgt wiederum eine Frist von *60 Tagen,* innerhalb derer die Aufsicht ihre Meinung gegenüber dem Handelsministerium bzw. der FTC kommuniziert haben muss. Sollte ein Unternehmen nicht innerhalb von *25 Tagen* den Rat der Aufsichtsbehörden umsetzen, werden wiederum die Aufsichtsorgane über das Privay Shield informiert, was in Durchsetzungsmaßnahmen münden kann.

Sollte der Beschwerde eines Betroffenen über keines der verfügbaren Verfahren Abhilfe verschafft werden können, soll das *Privacy Shield Panel* als letzte Instanz durch den Betroffenen angerufen werden können (Erwägungsgrund 46). Dieses aus 20 ständigen Mitgliedern bestehende und vom Handelsministerium ernannte Expertengremium wird sich mittels einer Unterarbeitsgruppe Beschwerden von Betroffenen anhand festgelegter Verfahrensregeln zuwenden. Betroffene können den Verhandlungen über eine Video- oder Telefonkonferenz beiwohnen. Auf Basis einer nachvollziehbaren Begründung des Betroffenen kann ebenfalls eine Übersetzung der Verhandlung kostenfrei zur Verfügung gestellt werden. An Vorbereitungsmaßnahmen des Betroffenen im Vorfeld der Verhandlung soll die zuständige nationale Aufsichtsbehörde unterstützend mitwirken. Sind Schlichtungs- oder Durchsetzungsmaßnahmen auch nach Einberufung des Privacy Shield Panels in den Augen eines Betroffenen immer noch nicht ausreichend erfolgt, um seiner Beschwerde Abhilfe zu verschaffen, besteht für den Betroffenen in letzter Instanz die Möglichkeit des Anrufens einer *Schiedsgerichtsbarkeit in den USA* nach dem *Federal Arbitration Act* (Erwägungsgrund 47).

3. Audits

Die Pflicht zur Überprüfung der Einhaltung der Privacy Shield Principles obliegt weiterhin jedem Datenverarbeiter selbst, indem er interne Audits durchführt oder Dritte mit der Überprüfung beauftragt. Daneben soll jedoch das Handelsministerium eine zusätzliche Kontrolle der Einhaltung durch die Versendung entsprechender *Fragebögen* durchführen. Dies kann anlassunabhängig erfolgen oder beispielsweise auf Basis der Eingabe eines Betroffenen, bzw. im Falle einer nicht erfolgten Streitschlichtung (Erwägungsgrund 35). Im Falle aufsichtsbehördlicher Ermittlungen sind Nachweise für die Implementierung der Privacy Shield Framework Principles vorzuhalten (Erwägungsgrund 30).

4. Onward Transfers

Die Verantwortlichkeit für die Weitergabe von Daten an weitere Stellen („Onward Transfers") wird erweitert. Im Unterschied zu Safe Harbor, das eine Weitergabe an ebenfalls zertifizierte Stellen ohne Einschränkungen zugelassen hatte, knüpft der Privacy Shield die Weitergabe an eine konkrete Zweckbindung und vertragliche bzw. vergleichbare Regelungen innerhalb von Unternehmensgruppen, die die Umsetzung der Vorgaben des Privacy Shields garantieren (vgl. Erwägungsgrund 22). Bei Datenschutzverstößen in einer Verarbeitungskette ist die für die Verarbeitung der Daten verantwortliche Stelle (Controller) uneingeschränkt haftbar, sofern sie sich nicht exkulpieren kann.

5. Verwendung von Daten des Privacy Shield für die nationale Sicherheit

Die Angemessenheitsentscheidung der Kommission enthält eine ausführliche Analyse bestehender Beschränkungen des US-Rechts hinsichtlich der Verwendung personenbezogener Daten des Privacy Shield durch Geheimdienste, bestehende Rechtschutzmöglichkeiten sowie der Überwachung solcher Dienste (vgl. Erwägungsgrund 52 ff.). Diese Rahmenbedingungen sind nach Auffassung der Kommission infolge der von ihr ausgesprochenen Empfehlungen von 2013 nochmals verschärft worden (vgl. Erwägungsgrund 55). Was zunächst als Klarstellung gegenüber verunsicherten EU-Bürgern bzw. Datenverarbeitern zu verstehen ist, wird jedoch auch mit Ergänzungen versehen, die im Zuge der Verhandlungen zwischen der Kommission und Vertretern der US-Regierung entstanden sind.[8] Hervorzuheben ist die Einrichtung eines unabhängigen Ombudsmanns für Datenschutz *(„Privacy Shield Umbudsperson")*. Diese Ombudsperson soll nicht nur auf Anfrage einer ausländischen Regierung hin Datenverarbeitungen der US-Geheimdienste auf ihre Zulässigkeit hin prüfen, sondern ebenfalls Beschwerden von Betroffenen zum Anlass für Prüfungen nehmen. Eine direkte Anlaufstelle für Betroffene stellt die Ombudsperson jedoch nicht dar. Vielmehr müssen sich Betroffene zunächst an die jeweilige nationale Aufsicht in der EU bezüglich vermuteter Geheimdienstaktivitäten wenden, bevor diese eine Beschwerde weiterleitet. Hierbei brauchen Betroffene jedoch nicht zu beweisen, dass ihre Daten tatsächlich durch Geheimdienste unzulässig verwendet wurden.

6. Stellungnahme der Art. 29-Gruppe

Die Art.-29-Gruppe hat im Sinne ihrer beratenden Funktion am 13. April 2016 eine Stellungnahme zu den Inhalten des EU-U.S. Privacy Shield abgegeben.[9] Darin begrüßt sie die erheblichen Verbesserungen durch das Privacy Shield im Vergleich zum vorherigen Safe-Harbor-Framework. Gleichwohl identifiziert sie im Rahmen der inhaltlichen Auseinandersetzung eine Reihe von Aspekten, bei denen sie Nachbesserungsbedarf sieht. Neben sprachlichen Ungereimtheiten bestünden u.a. Bedenken hinsichtlich einer fehlenden Regelung zur Datenlöschung, der weiterhin bestehenden Möglichkeit von massenhaften und willkürlichen Datensammlungen sowie einer unklaren Kompetenz und Stellung der Ombudsperson.

8 Ausführlich hierzu Erwägungsgründe 56 ff.

7. Angemessenes Datenschutzniveau

Unter den verbindlichen Dokumenten zum Privacy Shield findet sich auch ein Entwurf für eine Angemessenheitsentscheidung der Kommission zur Gewährleistung eines angemessenen Datenschutzniveaus hinsichtlich zertifizierter Stellen nach dem EU-U.S. Privacy Shield. Gem. Art. 25 Abs. 6 der EU-Datenschutzrichtlinie 95/46/EG kann die Kommission in einem Ausschussverfahren feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein *angemessenes Schutzniveau für personenbezogene Daten* gewährleistet. Ziel der Kommission ist es, allen Stellen in den USA, die sich den Vorgaben des Privacy Shield über eine Zertifizierung unterwerfen, ein angemessenes Datenschutzniveau zu attestieren. Eine Genehmigung der Aufsichtsbehörde für den einzelnen Datenexport an den nach dem Privacy Shield zertifizierten Empfänger wäre dann, wie schon im früheren Verfahren nach Safe Harbor, nicht mehr erforderlich.

In den Augen der Kommission bieten die USA durch die neuen Vorgaben des EU-U.S. Privacy Shield sowie die rechtlichen Rahmenbedingungen für die Verwendung personenbezogener Daten von EU-Bürgern durch US-Geheimdienste ein *angemessenes Datenschutzniveau* im Sinne der EU-Datenschutzrichtlinie. Um Veränderungen rechtlicher oder tatsächlicher Art Rechnung zu tragen, soll die Angemessenheitsentscheidung mit Blick auf die Wirksamkeit der darin vereinbartem Maßnahmen zum Privacy Shield eine *jährliche Überprüfung* zusammen mit dem Handelsministerium, der FTC sowie weiteren US-Behörden (falls erforderlich) durchlaufen (Erwägungsgrund 122). Sowohl die europäischen Aufsichtsbehörden als auch die Art. 29-Gruppe können dieser Überprüfung beiwohnen. Begründen Tatsachen die Annahme, dass die getroffenen Vereinbarungen rund um das EU-U.S. Privacy Shield nicht eingehalten werden oder die Rahmengesetzgebung der USA bezüglich Datenerhebungen und Verwendungen der Geheimdienste kein ausreichendes Schutzniveau mehr gewährleistet, soll die Angemessenheitsentscheidung *widerrufen* werden können (Erwägungsgrund 125 f.).

Da diese Angemessenheitsentscheidung auf Basis der Stellungnahme der Art. 29-Gruppe und einem Ausschußverfahren nach Art. 31 Abs. 2 der EU-Datenschutzrichtlinie erst noch verabschiedet werden muss, können Datenübermittlungen in die USA auf Basis des EU-U.S. Privacy Shield derzeit noch nicht erfolgen.

9 Abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

Rechtsprechung*

Verfassungsbeschwerde gegen Ermittlungsbefugnisse des BKA zur Terrorismusbekämpfung teilweise erfolgreich (Ls)

(**Bundesverfassungsgericht**, Urteil vom 20. April 2016 – 1 BvR 966/09 –)

1. a) Die Ermächtigung des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen (Wohnraumüberwachungen, Online-Durchsuchungen, Telekommunikationsüberwachungen, Telekommunikationsverkehrsdatenerhebungen und Überwachungen außerhalb von Wohnungen mit besonderen Mitteln der Datenerhebung) ist zur Abwehr von Gefahren des internationalen Terrorismus im Grundsatz mit den Grundrechten des Grundgesetzes vereinbar.

b) Die Ausgestaltung solcher Befugnisse muss dem Verhältnismäßigkeitsgrundsatz genügen. Befugnisse, die tief in das Privatleben hineinreichen, müssen auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein, setzen voraus, dass eine Gefährdung dieser Rechtsgüter hinreichend konkret absehbar ist, dürfen sich nur unter eingeschränkten Bedingungen auf nichtverantwortliche Dritte aus dem Umfeld der Zielperson erstrecken, verlangen überwiegend besondere Regelungen zum Schutz des Kernbe-

* Richtigstellung: Der im Heft 02/2016, Seite 98 wiedergegebene Leitsatz „Zum Gehaltsanspruch bei verweigertem Drogentest" gehört zu einer Entscheidung des Bundesarbeitsgerichts.

reichs privater Lebensgestaltung sowie einen Schutz von Berufsgeheimnisträgern, unterliegen Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle und müssen mit Löschungspflichten bezüglich der erhobenen Daten flankiert sein.

2. Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten richten sich nach den Grundsätzen der Zweckbindung und Zweckänderung.

   a) Die Reichweite der Zweckbindung richtet sich nach der jeweiligen Ermächtigung für die Datenerhebung; die Datenerhebung bezieht ihren Zweck zunächst aus dem jeweiligen Ermittlungsverfahren.

   b) Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus im Rahmen der ursprünglichen Zwecke dieser Daten erlauben (weitere Nutzung). Dies setzt voraus, dass es sich um eine Verwendung der Daten durch dieselbe Behörde zur Wahrnehmung derselben Aufgabe und zum Schutz derselben Rechtsgüter handelt. Für Daten aus Wohnraumüberwachungen oder einem Zugriff auf informationstechnische Systeme müssen zusätzlich für jede weitere Nutzung auch die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sein.

   c) Der Gesetzgeber kann darüber hinaus eine Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben (Zweckänderung).

   Die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung orientieren sich am Grundsatz der hypothetischen Datenneuerhebung. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Eine konkretisierte Gefahrenlage wie bei der Datenerhebung ist demgegenüber grundsätzlich nicht erneut zu verlangen; erforderlich, aber auch ausreichend ist in der Regel das Vorliegen eines konkreten Ermittlungsansatzes.

   Für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen darf die Verwendung zu einem geänderten Zweck allerdings nur erlaubt werden, wenn auch die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sind.

3. Die Übermittlung von Daten an staatliche Stellen im Ausland unterliegt den allgemeinen verfassungsrechtlichen Grundsätzen von Zweckänderung und Zweckbindung. Bei der Beurteilung der neuen Verwendung ist die Eigenständigkeit der anderen Rechtsordnung zu achten. Eine Übermittlung von Daten ins Ausland verlangt eine Vergewisserung darüber, dass ein hinreichend rechtsstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten ist.

Für 100%ige Datenschutzkonzepte

Bundesdatenschutzgesetz (BDSG)
Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften

Von **Dr. jur. Hans-Jürgen Schaffland** und **Dipl.-Kfm. Noeme Wiltfang**

Loseblattwerk, 2.180 Seiten, € (D) 112,–
ca. 6 Ergänzungslieferungen pro Jahr,
ISBN 978-3-503-01518-4

Die Grundlage für optimalen Datenschutz ist eine verlässliche, aktuelle Quelle: der „**Schaffland/Wiltfang**". Das Werk enthält in einem Band

- die **vollständige Kommentierung zum BDSG** unter Berücksichtigung des Entwurfs der EU-Datenschutz-Grundverordnung (**DS-GVO**),
- alle Landesdatenschutzgesetze und Auszüge aus wichtigen, vom BDSG tangierten Gesetzen.

Die Kommentierung befasst sich ausführlich mit der Entscheidung des BAG zur Einwilligung (und deren Widerruf) des Beschäftigten zur Veröffentlichung seines Bildnisses durch seinen Arbeitgeber.

www.BDSGdigital.de

ESV ERICH SCHMIDT VERLAG

Auf Wissen vertrauen

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

Gegenüber dem mutmaßlich leiblichen Vater gebietet das Grundgesetz keinen Abstammungsklärungsanspruch (Ls)

(**Bundesverfassungsgericht**, Urteil vom 19. April 2016 – 1 BvR 3309/13 –)

1. **Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) verpflichtet den Gesetzgeber nicht dazu, neben dem Vaterschaftsfeststellungsverfahren nach § 1600d BGB auch ein Verfahren zur isolierten, sogenannten rechtsfolgenlosen, Klärung der Abstammung von einem mutmaßlich leiblichen, aber nicht rechtlichen Vater bereitzustellen.**

2. **Der aus dem allgemeinen Persönlichkeitsrecht abgeleitete Schutz der Kenntnis der eigenen Abstammung ist nicht absolut, sondern muss mit widerstreitenden Grundrechten in Ausgleich gebracht werden. Hierfür verfügt der Gesetzgeber über einen Ausgestaltungsspielraum. Auch wenn eine andere gesetzliche Lösung verfassungsrechtlich denkbar wäre, so ist es vom Ausgestaltungsspielraum des Gesetzgebers – auch im Lichte der Europäischen Konvention für Menschenrechte – gedeckt, wenn die rechtsfolgenlose Klärung der Abstammung nur innerhalb der rechtlichen Familie, nicht aber gegenüber dem mutmaßlich leiblichen, aber nicht rechtlichen Vater besteht.**

(Leitsatz zu 2 nicht amtlich)

Der Anordnung einer Betreuung muss eine persönliche Anhörung vorausgehen (Ls)

(**Bundesverfassungsgericht**, Beschluss vom 23. März 2016 – 1 BvR 184/13 –)

1. **Angesichts der mit einer Betreuung verbundenen tiefen Eingriffe in das allgemeine Persönlichkeitsrecht ist eine persönliche Anhörung durch das Betreuungsgericht vor der Anordnung der Betreuung unverzichtbar (§ 278 Abs. 1 FamFG).**

2. **Die Anordnung einer Betreuung ohne diese Anhörung verletzt nicht nur das Recht auf rechtliches Gehör (Art. 103 Abs. 1 GG), sondern stellt auch eine Verletzung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG dar. Durch eine spätere Anhörung kommt daher eine Heilung nicht rückwirkend, sondern nur mit Blick auf die Zukunft in Betracht.**

3. **Die persönliche Anhörung darf nur im Eilfall bei Gefahr im Verzuge vorläufig unterbleiben, muss dann aber unverzüglich nachgeholt werden (§ 301 Abs. 1 Satz 1 und 2 FamFG).**

(Nicht amtliche Leitsätze)

Zu den Prüfpflichten des Betreibers eines Ärztebewertungsportals

(**Bundesgerichtshof**, Urteil vom 1. März 2016 – VI ZR 34/15 –)

a) **Ein Hostprovider ist zur Vermeidung einer Haftung als mittelbarer Störer grundsätzlich nicht verpflichtet, die von den Nutzern ins Netz gestellten Beiträge vor der Veröffentlichung auf eventuelle Rechtsverletzungen zu überprüfen. Er ist aber verantwortlich, sobald er Kenntnis von den Rechtsverletzungen erlangt.**

b) **Ist der Hostprovider mit der Behauptung eines Betroffenen konfrontiert, ein von einem Nutzer eingestellter Beitrag verletze ihn in seinem Persönlichkeitsrecht, und ist die Beanstandung so konkret gefasst, dass der Rechtsverstoß auf der Grundlage der Behauptung des Betroffenen unschwer bejaht werden kann, so ist eine Ermittlung und Bewertung des gesamten Sachverhalts unter Berücksichtigung einer etwaigen Stellungnahme des für den beanstandeten Beitrag Verantwortlichen erforderlich.**

c) **Zur Bestimmung, welcher Überprüfungsaufwand vom Hostprovider im Einzelfall zu verlangen ist, bedarf es einer umfassenden Interessenabwägung, bei der die betroffenen Grundrechte der Beteiligten zu berücksichtigen sind. Maßgebliche Bedeutung kommt dabei dem Gewicht der angezeigten Rechtsverletzung sowie den Erkenntnismöglichkeiten des Providers zu. Zu berücksichtigen sind aber auch Funktion und Aufgabenstellung des vom Provider betriebenen Dienstes sowie die Eigenverantwortung des für die persönlichkeitsbeeinträchtigende Aussage unmittelbar verantwortlichen – ggf. zulässigerweise anonym auftretenden – Nutzers.**

d) **Der vom Betreiber eines Arztbewertungsportals verlangte Prüfungsaufwand darf den Betrieb des Portals weder wirtschaftlich gefährden noch unverhältnismäßig erschweren, hat aber zu berücksichtigen, dass eine gewissenhafte Prüfung der Beanstandungen von betroffenen Ärzten durch den Portalbetreiber eine entscheidende Voraussetzung dafür ist, dass die Persönlichkeitsrechte der (anonym oder pseudonym) bewerteten Ärzte beim Portalbetrieb hinreichend geschützt sind.**

Sachverhalt:

Der Kläger nimmt die Beklagte darauf in Anspruch, die Verbreitung einer in einem Arztbewertungsportal von einem Dritten abgegebenen Bewertung zu unterlassen.

Der Kläger ist Zahnarzt und betreibt eine Zahnarztpraxis mit insgesamt zehn Ärzten und 60 nichtärztlichen Angestellten. Die Beklagte unterhält unter der Internetadresse www.jameda.de einen Internetdienst, in dem Interessierte bei Eingabe bestimmter Suchkategorien, wie etwa medizinischer Fachgebiete, Informationen über Ärzte aufrufen können. Registrierten Nutzern wird darüber hinaus die Möglichkeit geboten, die Tätigkeit von Ärzten zu bewerten. Bewertungen, die diese Nutzer in dem Bewertungsportal ohne Nennung ihres Klarnamens platzieren können, erfolgen durch die

Vergabe von Schulnoten für die vorformulierten Kategorien „Behandlung“, „Aufklärung“, „Vertrauensverhältnis“, „genommene Zeit“ und „Freundlichkeit“. Ferner hat der Bewertende die Möglichkeit, in einem Freitextfenster zusätzliche, den Arzt betreffende Kommentare in eigenen Worten niederzulegen.

Unter dem 10. August 2013 stellte ein anonymer Nutzer in der Rubrik „Bewertung für Dr. H. [Nachname des Klägers]“ eine den Kläger betreffende Bewertung in das Portal der Beklagten ein. Nach dem hervorgehobenen Hinweis

„Ich kann Dr. H. [Nachname des Klägers] nicht empfehlen“

bemerkte der Nutzer:

„Leider ist es einfach, eine positive Bewertung zu schreiben, eine negative dagegen ist – auch rechtlich – schwierig, weshalb ich für die Bewertung auf die Schulnotenvergabe verweise, welche ich mir sorgfältigst überlegt habe“.

Im folgenden Abschnitt „Notenbewertung dieses Patienten“ wurde die Gesamtnote 4,8 genannt, die sich aus den von dem genannten Nutzer in den vorbezeichneten fünf Kategorien vergebenen Einzelnoten, darunter jeweils die Note 6 für „Behandlung“, „Aufklärung“ und „Vertrauensverhältnis“, ergab.

Der Kläger wandte sich hierauf an die Beklagte und teilte ihr mit, er widerspreche „der […] unbegründeten und unsubstantiierten Bewertung“, die ihn verunglimpfe. Er kündigte an, „sowohl gegen Jameda als auch gegen den schmähenden (fraglichen) Patienten rechtlich […] vorzugehen, wenn die Schmähung nicht innerhalb von 48 Stunden entfernt“ werde. Die Beklagte entfernte den Beitrag zunächst, stellte ihn dann jedoch unverändert wieder in ihr Portal ein. Der Kläger wandte sich hierauf mit anwaltlichem Schreiben an die Beklagte. Er führte darin aus, bei der angegriffenen Bewertung gebe „sich erkennbar jemand Mühe, jegliche tatsächliche Aussage zu vermeiden“. Es liege nahe, dass dies seinen Grund darin habe, dass es eine solche Behandlung überhaupt nicht gegeben habe. Auf die anwaltliche Aufforderung des Klägers, den Beitrag zu löschen und ihm Auskunft darüber zu erteilen, auf welche Weise der „angebliche Patient“ die Behandlung belegt habe und welche Glaubhaftmachungen dazu vorgelegt worden seien, ferner über die „Klardaten“, die der Beklagten aufgrund des „angeblichen Kontakts“ mit dem Nutzer vorlägen, führte die Beklagte unter anderem aus:

„[…] Im Rahmen unserer Qualitätsprüfung haben wir den Bewerter angeschrieben und um Bestätigung der Bewertung sowie eine Erklärung gebeten. Der Bewerter hat die Bewertung sehr ausführlich bestätigt. Anschließend hatten wir keine Anhaltspunkte, die uns an der Authentizität der Bewertung zweifeln ließen.

Eine Überprüfung dieser Rückmeldung erfolgt immer manuell durch unsere Mitarbeiter auf Basis der Problem-Meldung Ihres Mandanten, wobei unser technisches System als Ergänzung fungiert. Dabei weisen uns vor allem Hintergrunddaten (bspw. E-Mail-Adresse), die bei der Abgabe einer Bewertung mitversandt werden, auf eine eventuelle Mehrfachbewertung hin.

Die Notenbewertung entspricht der freien Meinungsäußerung und ist durch das Gesetz geschützt. In seiner Rückmeldung erklärt der Nutzer, welche Vorkommnisse ihn dazu veranlasst haben, eine solche Notenbewertung abzugeben. Viele Patienten schildern ihre Erlebnisse und Erfahrungen in Kurzform und vermeiden eine Schilderung von Tatsachenbehauptungen (auch wenn sie der Wahrheit entsprechen), da diese für die Patienten oftmals nicht zu beweisen sind. […]

Bedauerlicherweise können wir Ihrem Wunsch auf Herausgabe der Nutzerdaten nicht nachkommen, da wir diese Daten schützen müssen (das Arzt-Patientenverhältnis ist äußerst sensibel). […]

Wir bitten um Ihr Verständnis, dass wir die Bewertung nicht löschen können.“

Eine Stellungnahme des Verfassers der angegriffenen Bewertung selbst hat die Beklagte dem Kläger nicht zur Verfügung gestellt.

Der Kläger hat die Beklagte – soweit im Revisionsverfahren noch von Interesse – darauf in Anspruch genommen, es zu unterlassen, die ihn betreffende Bewertung vom 10. August 2013 zu verbreiten und/oder verbreiten zu lassen, soweit diese die Bewertung „6,0“ in den Kategorien „Behandlung“, „Aufklärung“ und „Vertrauensverhältnis“ beinhalte. Er hat unter anderem behauptet, der abgegebenen Bewertung liege kein Behandlungskontakt zugrunde.

Das Landgericht hat der Klage insoweit stattgegeben. Auf die Berufung der Beklagten hat das Oberlandesgericht das landgerichtliche Urteil abgeändert und die Klage abgewiesen. Mit der vom Berufungsgericht zugelassenen Revision verfolgt der Kläger sein Unterlassungsbegehren weiter.

Aus den Gründen:

Das Berufungsgericht, dessen Urteil in ZD 2015, 430 veröffentlicht ist, ist der Auffassung, dem Kläger stehe gegen die Beklagte kein Anspruch auf Unterlassung der Veröffentlichung und/oder Verbreitung des streitgegenständlichen Beitrags zu. Zur Begründung hat es im Wesentlichen ausgeführt, die nur in ihrer Funktion als Hostprovider in Anspruch genommene Beklagte könne bezüglich des in ihre Website eingestellten Drittinhalts nur eine Haftung als mittelbare Störerin treffen. Die dafür nach der „Blog-Eintrag-Entscheidung“ des erkennenden Senats (Senatsurteil vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219) erforderlichen Voraussetzungen seien im Streitfall aber nicht erfüllt, weil die Beklagte der sie danach treffenden Prüfungspflicht mit den von ihr ergriffenen und gegenüber dem Kläger kommunizierten Maßnahmen genügt habe.

I. Das Berufungsurteil hält revisionsrechtlicher Überprüfung nicht stand. Mit den Erwägungen des Berufungsgerichts lässt sich die Störereigenschaft der Beklagten und damit der vom Kläger geltend gemachte Unterlassungsanspruch aus § 823 Abs. 1, § 1004 Abs. 1 Satz 2 BGB analog i.V.m. Art. 1 Abs. 1, Art. 2 Abs. 1 GG nicht verneinen.

1. Zutreffend geht das Berufungsgericht davon aus, dass es im Streitfall nicht um die Haftung der Beklagten als unmittelbare Störerin – in der Diktion des I. Zivilsenats „Täterin“ (zu den unterschiedlichen Begrifflichkeiten des erkennenden Senats einerseits und des I. Zivilsenats andererseits vgl. Senatsurteil vom 28. Juli 2015 – VI ZR 340/14, AfP 2015, 425 Rn. 34; v. Pentz, AfP 2014, 8, 16) – geht.

Indes lässt sich die Eigenschaft der Beklagten als mittelbare Störerin mit den Erwägungen des Berufungsgerichts nicht verneinen.

a) Grundsätzlich ist als mittelbarer Störer verpflichtet, wer, ohne unmittelbarer Störer zu sein, in irgendeiner Weise willentlich und adäquat kausal zur Beeinträchtigung des Rechtsguts beiträgt. Dabei kann als Beitrag auch die Unterstützung oder Ausnutzung der Handlung eines eigenverantwortlich handelnden Dritten genügen, sofern der in Anspruch Genommene die rechtliche und tatsächliche Möglichkeit zur Verhinderung dieser Handlung hatte (vgl. Senatsurteile vom 28. Juli 2015 – VI ZR 340/14, AfP 2015, 425 Rn. 34; vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 21 m.w.N. – Blog-Eintrag). Die Haftung als mittelbarer Störer darf nach ständiger höchstrichterlicher Rechtsprechung aber nicht über Gebühr auf Dritte erstreckt werden, welche die rechtswidrige Beeinträchtigung nicht selbst vorgenommen haben. Sie setzt deshalb die Verletzung von Verhaltenspflichten, insbesondere von Prüfpflichten, voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem als mittelbaren Störer in Anspruch Genommenen nach den Umständen des Einzelfalls eine Verhinderung der Verletzung zuzumuten ist (Senatsurteile vom 25. Oktober 2011 – VI ZR 93/10,

BGHZ 191, 219 Rn. 22 – Blog-Eintrag; vom 30. Juni 2009 – VI ZR 210/08, AfP 2009, 494 Rn. 18 – Domainverpächter; BGH, Urteile vom 17. August 2011 – I ZR 57/09, BGHZ 191, 19 Rn. 20 – Stiftparfüm; vom 17. Dezember 2010 – V ZR 44/10, AfP 2011, 156 Rn. 15; vom 1. April 2004 – I ZR 317/01, BGHZ 158, 343, 350 – Schöner Wetten; vom 11. März 2004 – I ZR 304/01, BGHZ 158, 236, 251 – Internetversteigerung I; vom 30. April 2008 – I ZR 73/05, NJW-RR 2008, 1136 Rn. 50 – Internetversteigerung III).

Danach ist ein Hostprovider zur Vermeidung einer Haftung als mittelbarer Störer grundsätzlich nicht verpflichtet, die von den Nutzern in das Netz gestellten Beiträge vor der Veröffentlichung auf eventuelle Rechtsverletzungen zu überprüfen. Er ist aber verantwortlich, sobald er Kenntnis von der Rechtsverletzung erlangt. Weist ein Betroffener den Hostprovider auf eine Verletzung seines Persönlichkeitsrechts durch den Nutzer seines Angebots hin, kann der Hostprovider verpflichtet sein, künftig derartige Störungen zu verhindern (Senatsurteil vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 24 – Blog-Eintrag; vgl. auch BGH, Urteile vom 17. August 2011 – I ZR 57/09, BGHZ 191, 19 Rn. 21 – Stiftparfüm; vom 12. Juli 2007 – I ZR 18/04, BGHZ 173, 188 Rn. 41 ff. – Jugendgefährdende Medien bei eBay; vom 11. März 2004 – I ZR 304/01, BGHZ 158, 236, 251 f. – Internet-Versteigerung I).

Wird eine Verletzung von Persönlichkeitsrechten behauptet, wird sich eine Rechtsverletzung allerdings nicht stets ohne Weiteres feststellen lassen. Denn sie erfordert eine Abwägung zwischen dem Recht des Betroffenen auf Schutz seiner Persönlichkeit aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG, Art. 8 Abs. 1 EMRK und dem durch Art. 5 Abs. 1 GG, Art. 10 EMRK geschützten Recht jedenfalls des Providers auf Meinungs- und Medienfreiheit. Ist der Provider mit der Beanstandung eines Betroffenen konfrontiert, die so konkret gefasst ist, dass der Rechtsverstoß auf der Grundlage der Behauptung des Betroffenen unschwer bejaht werden kann, ist eine Ermittlung und Bewertung des gesamten Sachverhalts unter Berücksichtigung einer etwaigen Stellungnahme des für den beanstandeten Beitrag Verantwortlichen erforderlich (Senatsurteil vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 25 f. – Blog-Eintrag). Entgegen der Auffassung der Revisionserwiderung gilt dies auch dann, wenn die beanstandete Äußerung – wie im Streitfall (vgl. nachfolgend unter b) – nicht als Tatsachenbehauptung, sondern als Werturteil zu qualifizieren ist, das Werturteil vom Betroffenen aber mit der schlüssigen Behauptung als rechtswidrig beanstandet wird, der tatsächliche Bestandteil der Äußerung, auf dem die Wertung aufbaue, sei unrichtig, dem Werturteil fehle damit jegliche Tatsachengrundlage.

b) Danach war die Beklagte entgegen der Auffassung der Revisionserwiderung im Streitfall gehalten, der Rüge des Klägers nachzugehen. Sie war hinreichend konkret gefasst und ließ den behaupteten Rechtsverstoß unschwer erkennen.

aa) Die Behauptung des Klägers, der angegriffenen Bewertung liege kein Behandlungskontakt zugrunde, war hinreichend konkret. Dem steht nicht entgegen, dass es sich letztlich um eine Mutmaßung des Klägers handelte, die er nicht weiter unterlegt hat. Denn zu konkreteren Darlegungen der Beklagten gegenüber war der Kläger angesichts der Tatsache, dass die Bewertung keinerlei tatsächliche, die konkrete Behandlung beschreibende Angaben enthielt, nicht in der Lage.

bb) Auf der Grundlage der Beanstandung des Klägers war der Rechtsverstoß unschwer zu bejahen. Denn trifft die Behauptung des Klägers zu, so verletzt die angegriffene Bewertung den Kläger offensichtlich – was auch die Beklagte nicht in Abrede stellt – in seinem allgemeinen Persönlichkeitsrecht.

(1) Die beanstandete Bewertung greift in den Schutzbereich des allgemeinen Persönlichkeitsrechts des Klägers ein. Betroffen sind die Ehre und soziale Anerkennung des Klägers. Denn die Bewertung seiner im Rahmen einer (behaupteten) Behandlung erbrachten Leistungen in den Kategorien „Behandlung", „Aufklärung" und „Vertrauensverhältnis" mit der Note 6 und damit als „ungenügend" bringt zum Ausdruck, dass der Kläger in zentralen Bereichen des Behandlungsgeschehens den an ihn gestellten Anforderungen aus Sicht des die Behandlung bewertenden Patienten nicht gerecht geworden ist. Die Kundgabe dieser Bewertung ist geeignet, sich abträglich auf das Bild des Klägers in der Öffentlichkeit auszuwirken.

(2) Liegt der angegriffenen Bewertung kein tatsächlicher Behandlungskontakt zugrunde, ist der Eingriff in das Persönlichkeitsrecht des Klägers auch rechtswidrig.

(a) Nach ständiger höchstrichterlicher Rechtsprechung (vgl. nur Senatsurteile vom 17. Dezember 2013 – VI ZR 211/12, BGHZ 199, 237 Rn. 22 – Sächsische Korruptionsaffäre; vom 15. September 2015 – VI ZR 175/14, VersR 2015, 1437 Rn. 20; vom 28. Juli 2015 – VI ZR 340/14, AfP 2015, 425 Rn. 29; vom 13. Januar 2015 – VI ZR 386/13, VersR 2015, 336 Rn. 13 – Filialleiter bei Promi-Friseur; vom 30. September 2014 – VI ZR 490/12, AfP 2014, 534, 536 – Innenminister unter Druck; vom 29. April 2014 – VI ZR 137/13, AfP 2014, 325 Rn. 8 – Adoptivtochter) liegt wegen der Eigenart des Persönlichkeitsrechts als Rahmenrecht seine Reichweite nicht absolut fest, sondern muss erst durch eine Abwägung der widerstreitenden grundrechtlich geschützten Belange bestimmt werden, bei der die besonderen Umstände des Einzelfalls sowie die betroffenen Grundrechte und Gewährleistungen der Europäischen Menschenrechtskonvention (EMRK) interpretationsleitend zu berücksichtigen sind. Der Eingriff in das Persönlichkeitsrecht ist nur dann rechtswidrig, wenn das Schutzinteresse des Betroffenen die schutzwürdigen Belange der anderen Seite überwiegt.

(b) Im Streitfall sind das durch Art. 1 Abs. 1, Art. 2 Abs. 1 GG (auch in Verbindung mit Art. 12 Abs. 1 GG) und Art. 8 Abs. 1 EMRK gewährleistete Interesse des Klägers am Schutz seiner sozialen Anerkennung und seiner (Berufs)Ehre mit der in Art. 5 Abs. 1 GG und Art. 10 EMRK verankerten Kommunikationsfreiheit der Beklagten und der Meinungsäußerungsfreiheit des Bewertenden abzuwägen. Trifft die Behauptung des Klägers, der angegriffenen Bewertung liege kein Behandlungskontakt zugrunde, zu, ergibt diese Abwägung, dass die geschützten Interessen des Klägers diejenigen der Beklagten und des Bewertenden überwiegen.

(aa) Dabei ist zunächst zu berücksichtigen, dass es sich bei dem angegriffenen Beitrag um eine Meinungsäußerung und nicht um eine Tatsachenbehauptung handelt.

Ob eine Äußerung als Tatsachenbehauptung oder als Werturteil einzustufen ist, ist eine Rechtsfrage, die der uneingeschränkten Beurteilung durch das Revisionsgericht unterliegt. Tatsachenbehauptungen sind durch die objektive Beziehung zwischen Äußerung und Wirklichkeit charakterisiert. Demgegenüber werden Werturteile und Meinungsäußerungen durch die subjektive Beziehung des sich Äußernden zum Inhalt seiner Aussage geprägt. Wesentlich für die Einstufung als Tatsachenbehauptung ist danach, ob die Aussage einer Überprüfung auf ihre Richtigkeit mit Mitteln des Beweises zugänglich ist. Das scheidet bei Werturteilen und Meinungsäußerungen aus, weil sie durch das Element der Stellungnahme und des Dafürhaltens gekennzeichnet sind und sich deshalb nicht als wahr und unwahr erweisen lassen. Sofern eine Äußerung, in der Tatsachen und Meinungen sich vermengen, durch die Elemente der Stel-

lungnahme, des Dafürhaltens oder Meinens geprägt ist, wird sie als Meinung von dem Grundrecht aus Art. 5 Abs. 1 Satz 1 GG geschützt. Das gilt insbesondere dann, wenn eine Trennung der wertenden und der tatsächlichen Gehalte den Sinn der Äußerung aufhöbe oder verfälschte (Senatsurteile vom 28. Juli 2015 – VI ZR 340/14, AfP 2015, 425 Rn. 24; vom 16. Dezember 2014 – VI ZR 39/14, AfP 2015, 41 Rn. 8 – Hochleistungsmagneten; jeweils m.w.N.).

Nach diesen Maßstäben ist die angegriffene Bewertung als Meinungsäußerung zu qualifizieren. Zwar enthält sie die tatsächliche Behauptung des Bewertenden, er habe sich beim Kläger in Behandlung befunden und bewerte die stattgefundene Behandlung. Kern der angegriffenen Äußerung ist aber die notenmäßige Bewertung selbst. Sie ist geprägt von Elementen der Stellungnahme, des Dafürhaltens und Meinens (vgl. Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 31 ff. – Spickmich.de).

Entgegen der Auffassung der Revision ist die Vergabe der Note 6 in den Bereichen „Behandlung", „Aufklärung" und „Vertrauensverhältnis" aus Sicht eines durchschnittlichen Nutzers der Plattform weder dahingehend zu verstehen, dass diese Leistungen überhaupt nicht erbracht worden oder dem Kläger ärztliche Kunstfehler unterlaufen seien, noch dahingehend, dass die vom Kläger erbrachten Leistungen den Anforderungen an eine professionelle Zahnbehandlung in keiner Weise entsprächen und selbst die hierfür erforderlichen Grundkenntnisse des Klägers so lückenhaft seien, dass er diese Mängel auch in Fortbildungskursen in absehbarer Zeit nicht beheben könne. Ein derartiger Aussagegehalt kommt der angegriffenen Bewertung – was der erkennende Senat selbst beurteilen kann (vgl. Senatsurteil vom 18. November 2014 – VI ZR 76/14, BGHZ 203, 239 Rn. 19 m.w.N. – Chefjustiziar) – nicht zu. Dass mit der Bewertung nicht der Vorwurf eines (objektiven) Behandlungsfehlers verbunden ist, ergibt sich bereits daraus, dass es sich beim Bewertenden – für den durchschnittlichen Leser erkennbar – typischerweise um einen medizinischen Laien handelt, der zur Feststellung eines Behandlungsfehlers regelmäßig überhaupt nicht in der Lage ist. Entsprechendes gilt für die Bewertung der Aufklärung mit der Note 6. Die Kategorie „Vertrauensverhältnis" betrifft schließlich schon im Ausgangspunkt keine für die Frage nach dem Vorliegen eines Behandlungs- bzw. Aufklärungsfehlers relevanten Umstände.

(bb) Liegt der angegriffenen Bewertung kein Behandlungskontakt zugrunde, überwiegt das von Art. 1 Abs. 1, Art. 2 Abs. 1 GG (auch in Verbindung mit Art. 12 Abs. 1 GG) und Art. 8 Abs. 1 EMRK gewährleistete Interesse des Klägers am Schutz seiner sozialen Anerkennung und seiner (Berufs)Ehre die von Art. 5 Abs. 1 GG und Art. 10 EMRK geschützten Interessen des Bewerten den an der Äußerung der dargestellten Meinung im Portal der Beklagten und der Beklagten an der Kommunikation dieser Meinung. Denn bei Äußerungen, in denen sich – wie im vorliegenden Fall – wertende und tatsächliche Elemente in der Weise vermengen, dass die Äußerung insgesamt als Werturteil anzusehen ist, fällt bei der Abwägung zwischen den widerstreitenden Interessen der Wahrheitsgehalt der tatsächlichen Bestandteile ins Gewicht (Senatsurteil vom 16. Dezember 2014 – VI ZR 39/14, AfP 2015, 41 Rn. 21 – Hochleistungsmagnet; BVerfG, NJW 2012, 1643 Rn. 34; BVerfGE 85, 1, 17 – kritische Bayer-Aktionäre; BVerfG, AfP 2003, 535, 536; vgl. ferner EGMR, NJW 2015, 759 Rn. 51 – Yazici/Türkei; AfP 2015, 30 Rn. 31 – Jalba/Rumänien; AfP 2014, 430 Rn. 39 – Lavric/Rumänien; NJW-RR 2013, 291, 292 – Floquet und Esménard/Frankreich; NJW 2006, 1645 Rn. 76 – Pedersen und Baadsgard/Dänemark; BeckOK InfoMedienR/Söder, § 823 BGB Rn. 173.1 [Stand: 01.11.2015]). Im Streitfall ist der tatsächliche Bestandteil der Äußerung, auf dem die Wertung aufbaut, unwahr, wenn der behauptete Behandlungskontakt nicht bestand. Ein berechtigtes Interesse des Bewertenden, eine tatsächlich nicht stattgefundene Behandlung zu bewerten, ist nicht ersichtlich; entsprechendes gilt für das Interesse der Beklagten, eine Bewertung über eine nicht stattgefundene Behandlung zu kommunizieren.

c) Ihrer durch den konkreten Hinweis auf eine unschwer zu bejahende Rechtsverletzung ausgelösten Prüfungspflicht hat die Beklagte auf der Grundlage der Feststellungen des Berufungsgerichts nicht genügt.

aa) Zur Bestimmung, welcher Überprüfungsaufwand vom Hostprovider im Einzelfall zu verlangen ist, bedarf es einer umfassenden Interessenabwägung, bei der die betroffenen Grundrechte der Beteiligten zu berücksichtigen sind (vgl. BGH, Urteile vom 26. November 2015 – I ZR 174/14, juris Rn. 32 m.w.N. – Störerhaftung des Access-Providers; vom 1. April 2004 – I ZR 317/01, BGHZ 158, 343, 352 ff. – Schöner Wetten). Zu welchen konkreten Überprüfungsmaßnahmen der Hostprovider verpflichtet ist, bestimmt sich damit nach den Umständen des Einzelfalls. Maßgebliche Bedeutung kommt dabei dem Gewicht der angezeigten Rechtsverletzung sowie den Erkenntnismöglichkeiten des Providers zu (vgl. Senatsurteil vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 26 – Blog-Eintrag). Zu berücksichtigen sind aber auch Funktion und Aufgabenstellung des vom Provider betriebenen Dienstes sowie die Eigenverantwortung des für die persönlichkeitsrechtsbeeinträchtigende Aussage unmittelbar verantwortlichen – ggf. zulässigerweise anonym auftretenden – Nutzers (vgl. Senatsurteil vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 22 – Hostprovider; BGH, Urteile vom 5. Februar 2015 – I ZR 240/12, GRUR 2015, 485 Rn. 50 – Kinderhochstühle im Internet III; vom 11. März 2004 – I ZR 304/01, BGHZ 158, 236, 251 f. – Internetversteigerung I; jeweils m.w.N.).

bb) Danach sind im Streitfall an die Prüfungspflicht der Beklagten strenge Anforderungen zu stellen.

Im Ausgangspunkt ist freilich festzuhalten, dass das von der Beklagten betriebene Ärztebewertungsportal eine von der Rechtsordnung gebilligte und gesellschaftlich erwünschte Funktion erfüllt (vgl. Senatsurteil vom 23. September 2014 – VI ZR 358/13, BGHZ 202, 242 Rn. 39 f. – Ärztebewertung II) und der Portalbetrieb zudem vom Schutzbereich des Art. 5 Abs. 1 GG und des Art. 12 Abs. 1 GG erfasst wird (vgl. Senatsurteil vom 23. September 2014 – VI ZR 358/13, BGHZ 202, 242 Rn. 28 f. – Ärztebewertung II). Der von der Beklagten als Providerin zu erbringende Prüfungsaufwand darf den Betrieb eines Ärztebewertungsportals deshalb weder wirtschaftlich gefährden noch unverhältnismäßig erschweren (vgl. BGH, Urteil vom 26. November 2015 – I ZR 174/14, juris Rn. 27 m.w.N. – Störerhaftung des Accessproviders). Ein solches Gewicht haben rein reaktive Prüfungspflichten, um die es im Streitfall allein geht, in der Regel aber nicht. Auf der anderen Seite kann bei der Bestimmung des der Beklagten zumutbaren Prüfungsaufwandes nicht außer Betracht bleiben, dass der Betrieb eines Ärztebewertungsportals im Vergleich zu anderen Portalen, insbesondere Nachrichtenportalen, schon von vornherein ein gesteigertes Risiko für Persönlichkeitsrechtsverletzungen mit sich bringt. Es birgt die Gefahr, dass es auch für nicht unerhebliche (vgl. Senatsurteil vom 23. September 2014 – VI ZR 358/13, BGHZ 202, 242 Rn. 32 – Ärztebewertung II) persönlichkeitsrechtsverletzende Äußerungen missbraucht wird. Der Portalbetreiber muss deshalb von Anfang an mit entsprechenden Beanstandungen

rechnen. Dabei werden die mit dem Portalbetrieb verbundenen Missbrauchsgefahren noch dadurch verstärkt, dass die Bewertungen – rechtlich zulässig (vgl. § 13 Abs. 6 TMG) – verdeckt abgegeben werden können (Senatsurteil vom 23. September 2014 – VI ZR 358/13, BGHZ 202, 242 Rn. 34 – Ärztebewertung II). Zudem erschwert die Möglichkeit, Bewertungen verdeckt abgeben zu können, es dem betroffenen Arzt regelmäßig erheblich, unmittelbar gegen den betreffenden Portalnutzer vorzugehen. Denn er kennt ihn nicht und kann sich die für seine Identifizierung erforderlichen Informationen selbst dann, wenn sie dem Portalbetreiber vorliegen sollten, mangels Auskunftsanspruchs gegen den Portalbetreiber (vgl. Senatsurteil vom 1. Juli 2014 – VI ZR 345/13, BGHZ 201, 380 Rn. 9 ff. – Ärztebewertung I) jedenfalls nicht auf diesem Weg beschaffen. Eine gewissenhafte Prüfung der Beanstandungen von betroffenen Ärzten durch den Portalbetreiber ist deshalb die entscheidende Voraussetzung dafür, dass die Persönlichkeitsrechte der (anonym oder pseudonym) bewerteten Ärzte beim Portalbetrieb hinreichend geschützt sind.

Im Streitfall kommt hinzu, dass die angegriffene Bewertung geeignet ist, die Chancen des Klägers im Wettbewerb mit anderen Ärzten nachhaltig zu beeinträchtigen. Die für jedermann abrufbare Bewertung einer Behandlungsleistung in drei zentralen Bereichen mit der Note „ungenügend" begründet nämlich die erhebliche Gefahr, dass (potentielle) Patienten an der ärztlichen Kompetenz des Klägers zweifeln und sich deshalb statt an den Kläger an einen anderen Zahnarzt wenden. Auch dies spricht dafür, dass an die von der Beklagten vorliegend zu ergreifenden Prüfungsmaßnahmen hohe Anforderungen zu stellen sind.

cc) Konkret muss die vom Portalbetreiber durchzuführende Überprüfung erkennbar zum Ziel haben, die Berechtigung der Beanstandung des betroffenen Arztes zu klären. Der Portalbetreiber muss ernsthaft versuchen, sich hierzu die notwendige Tatsachengrundlage zu verschaffen; er darf sich insbesondere nicht auf eine rein formale „Prüfung" zurückziehen.

Im Streitfall hätte die Beklagte die Beanstandung des betroffenen Arztes dem Bewertenden übersenden und diesen zur Stellungnahme anhalten müssen. Sie hätte ihn weiter auffordern müssen, ihr den angeblichen Behandlungskontakt möglichst genau zu beschreiben und ihr den Behandlungskontakt belegende Unterlagen, wie etwa vorhandene Rechnungen, Terminkarten und -zettel, Eintragungen in Bonushefte, Rezepte oder sonstige Indizien möglichst umfassend – soweit vom Bewertenden für nötig erachtet ggf. teilweise geschwärzt – zu übermitteln. Die bloße Bitte der Beklagten, „die Behandlung in mindestens zwei Sätzen [zu] umschreiben und den Behandlungszeitraum [zu] nennen", reicht hierfür nicht. In jedem Falle hätte die Beklagte dem Kläger diejenigen Informationen und Unterlagen über den behaupteten Behandlungskontakt weiterleiten müssen, zu deren Weiterleitung sie ohne Verstoß gegen § 12 Abs. 1 TMG in der Lage gewesen wäre. Auch dies hat sie nicht getan. So erschließt sich etwa nicht, warum die Beklagte dem Kläger den sich aus der Stellungnahme des Bewertenden ersichtlichen Behandlungszeitraum nicht mitgeteilt hat. Sollte dies deshalb nicht erfolgt sein, weil zu befürchten war, dass der Kläger den Bewertenden aufgrund des mitgeteilten Behandlungszeitraums identifizieren kann, hätte die Beklagte ein größeres Zeitfenster wählen können. Dass diese Information für den Kläger von vornherein in Bezug auf eine substantiierte „Replik" offensichtlich nicht hilfreich gewesen wäre, kann nicht angenommen werden. So kann etwa nicht von vornherein ausgeschlossen werden, dass der behauptete Behandlungszeitraum in die Zeit einer – beispielsweise – urlaubs- oder krankheitsbedingten Abwesenheit des Klägers fiel, der Kläger mit dieser Information den behaupteten Behandlungskontakt also hätte widerlegen können.

II. Nach § 563 Abs. 1 Satz 1 ZPO war das Berufungsurteil deshalb aufzuheben und der Rechtsstreit an das Berufungsgericht zurückzuverweisen. Die Parteien werden die Möglichkeit haben, zu den von der Beklagten ergriffenen Überprüfungsmaßnahmen ergänzend vorzutragen.

III. Für das weitere Verfahren wird auf Folgendes hingewiesen:

1. Eine Verletzung des Klägers in seinem allgemeinen Persönlichkeitsrecht kommt in Betracht, wenn der in der angegriffenen Äußerung enthaltene tatsächliche Bestandteil unrichtig war und dem Werturteil damit jegliche Tatsachengrundlage fehlte. Darlegungs- und beweisbelastet für das Fehlen eines Behandlungskontakts ist nach den allgemeinen Regeln insoweit der Kläger.

2. Allerdings trifft die Beklagte hinsichtlich des Behandlungskontakts eine sekundäre Darlegungslast, weil dem Kläger insoweit eine nähere Darlegung nicht möglich ist und er auch keine Möglichkeit zur weiteren Sachaufklärung hat. Die sekundäre Darlegungslast umfasst zunächst diejenigen für einen solchen Behandlungskontakt sprechenden Angaben, die der Beklagten, insbesondere ohne Verstoß gegen § 12 Abs. 1 TMG, möglich und zumutbar sind (vgl. zu den allgemeinen Voraussetzungen einer sekundären Darlegungslast nur BGH, Urteil vom 8. Januar 2014 – I ZR 169/12, BGHZ 200, 76 Rn. 17 m.w.N. – BearShare).

Die Beklagte hat im Streitfall jedoch eine darüber hinausgehende Recherchepflicht. Dem Bestreitenden obliegt es im Rahmen seiner sekundären Darlegungslast, Nachforschungen zu unternehmen, wenn ihm dies zumutbar ist (vgl. BGH, Urteil vom 8. Januar 2014 – I ZR 169/12, BGHZ 200, 76 Rn. 18 m.w.N. – BearShare). Im Streitfall folgt die Zumutbarkeit einer Recherche schon daraus, dass die Beklagte aufgrund ihrer materiellen Prüfpflicht ohnehin gehalten ist, vom Bewertenden zusätzliche Angaben und Belege zum angeblichen Behandlungskontakt zu fordern. Dem entspricht in prozessualer Hinsicht ihre Obliegenheit, im Rahmen ihrer sekundären Darlegungslast vom Bewertenden entsprechende Informationen zu fordern.

Kommt die Beklagte dieser Obliegenheit nicht nach, ist die Behauptung des Klägers, der von ihm angegriffenen Bewertung liege kein Behandlungskontakt zugrunde, nach den allgemeinen Regeln über die sekundäre Darlegungslast nach § 138 Abs. 3 ZPO als zugestanden zu bewerten (vgl. nur Senatsurteil vom 22. April 2008 – VI ZR 83/07, BGHZ 176, 175 Rn. 23).

Zur Zulässigkeit von Altmeldungen in Onlinearchiven

(**Bundesgerichtshof**, Urteil vom 16. Feburar 2016 – VI ZR 367/15 –)

1. **Die Frage, ob in dem Online-Archiv einer Tageszeitung nicht mehr aktuelle Beiträge (Altmeldungen) zum Abruf bereitgehalten werden dürfen, in denen über den Verdacht einer Straftat im Zusammenhang mit einem – später nach § 170 Abs. 2 StPO eingestellten – Ermittlungsverfahren berichtet und in denen der Be-**

schuldigte – durch Namen und/oder Bild – identifizierbar bezeichnet wird, ist aufgrund einer umfassenden Abwägung des Persönlichkeitsrechts des Beschuldigten mit dem Recht der Presse auf Meinungs- und Medienfreiheit zu entscheiden.

2. Für die Beurteilung der Rechtmäßigkeit einer solchen Berichterstattung ist im Rahmen der Abwägung von erheblicher Bedeutung, ob sie ursprünglich zulässig war. Ist dies nicht der Fall, ist das Bereithalten der Beiträge zum Abruf in einem Online-Archiv grundsätzlich unzulässig, soweit der Beschuldigte weiterhin identifizierbar bezeichnet bzw. dargestellt ist.

Sachverhalt:

Der Kläger, ein deutschlandweit bekannter Fußballprofi, nimmt die Beklagte in Anspruch, es zu unterlassen, fünf Beiträge in deren Online-Archiv zum Abruf bereitzuhalten, soweit in identifizierbarer Weise über ihn berichtet wird. Zudem verlangt er Erstattung seiner vorgerichtlichen Anwaltskosten.

Die Beiträge berichten über ein Ermittlungsverfahren, das Anfang des Jahres 2012 gegen den Kläger wegen des Verdachts des sexuellen Missbrauchs widerstandsunfähiger Personen eingeleitet worden war. Hintergrund war die Strafanzeige einer jungen Frau, die behauptete, nach einer Feier im Haus des Klägers von einem oder mehreren Männern mit sogenannten K.O.-Tropfen betäubt und anschließend missbraucht worden zu sein.

Im April 2012 stellte die Staatsanwaltschaft das Ermittlungsverfahren gegen den Kläger mangels hinreichenden Tatverdachts nach § 170 Abs. 2 StPO ein.

Im Zeitraum von Januar bis April 2012 berichtete die Beklagte – wie auch weitere Nachrichtenportale – auf ihrem Onlineportal mit insgesamt sechs Artikeln über das Ermittlungsverfahren unter namentlicher Nennung des Klägers. Fünf Artikel, von denen vier mit einem Lichtbild des Klägers versehen sind, sind derzeit – jeweils mit Datumsangabe gekennzeichnet – noch im Online-Archiv der Beklagten abrufbar und durch eine gezielte Suche zum Ermittlungsverfahren über Suchmaschinen auffindbar. Die Artikel vom 23. Januar 2012, 26. Januar 2012 und 11. Februar 2012 befassen sich mit der Einleitung bzw. dem Fortgang des Ermittlungsverfahrens, zwei Artikel vom 27. April 2012 mit dessen Einstellung.

Nach Einstellung des Ermittlungsverfahrens ergänzte die Beklagte die Artikel vom 23. Januar 2012, 26. Januar 2012 und 11. Februar 2012 um eine Fußzeile mit folgendem Inhalt:

„Anmerkung der Redaktion: Bei dem Artikel handelt es sich um eine Archivberichterstattung vom … Das Ermittlungsverfahren gegen [Name des Klägers] wurde im April 2012 eingestellt."

Auf eine außergerichtliche Aufforderung des Klägers, alle das Ermittlungsverfahren betreffenden Artikel aus dem Onlineportal zu löschen, teilte die Beklagte mit, die geforderte Löschung ohne Anerkennung einer Rechtspflicht vorzunehmen. Sie löschte jedoch lediglich einen Artikel vom 21. Januar 2012, in dem erstmalig über den Sachverhalt berichtet worden war. Auf eine erneute Aufforderung des Klägers unter konkreter Nennung aller weiteren Artikel verweigerte die Beklagte deren Löschung. Auf die Aufforderung zur Abgabe einer strafbewehrten Unterlassungserklärung reagierte die Beklagte nicht.

Das Landgericht hat es der Beklagten antragsgemäß verboten, die fünf verbliebenen Beiträge online zum Abruf bereitzuhalten, soweit in identifizierbarer Weise durch namentliche Nennung und/oder Bildnisveröffentlichung über den Kläger berichtet wird. Auf die Berufung der Beklagten hat das Oberlandesgericht das landgerichtliche Urteil abgeändert und die Klage abgewiesen

Aus den Gründen:

A. Das Berufungsgericht ist davon ausgegangen, dass dem Kläger gegen die Beklagte kein Unterlassungsanspruch aus § 823 Abs. 1, § 1004 BGB analog i.V.m. Art. 1, Art. 2 Abs. 1 GG zustehe, weil die weitere Bereithaltung der ihn identifizierenden Berichte im Online-Archiv nicht rechtswidrig in sein allgemeines Persönlichkeitsrecht eingreife.

Allerdings stelle das Bereithalten der Berichte im Internet einen Eingriff in das allgemeine Persönlichkeitsrecht des Klägers dar, weil hiermit sein angebliches Fehlverhalten öffentlich gemacht und seine Person in den Augen der Adressaten – auch bei einer bloßen Verdachtsberichterstattung – negativ qualifiziert werde.

Die notwendige Abwägung des Rechts des Klägers auf Schutz seiner Persönlichkeit und Achtung seines Privatlebens mit dem Recht der Beklagten auf Meinungs- und Medienfreiheit führe im Streitfall jedoch zu dem Ergebnis, dass der Kläger die weitere Vorhaltung der Berichterstattung im Online-Archiv der Beklagten zu dulden habe.

Bei der beanstandeten Berichterstattung der Beklagten handele es sich um wahre Tatsachenbehauptungen in Form der Verdachtsberichterstattung. Diese sei ursprünglich angesichts der Schwere des in Rede stehenden Delikts und der Prominenz des Klägers zulässig gewesen, da die Beklagte in allen fünf angegriffenen Beiträgen in ausgewogener Art und Weise über den Tatvorwurf und den Gang des Verfahrens berichtet habe. Bei der Abwägung der gegenseitigen Interessen könne nicht festgestellt werden, dass dem Kläger trotz der Einstellung des Ermittlungsverfahrens durch die fortwährende Bereithaltung der Berichterstattung eine besondere Stigmatisierung oder Ausgrenzung drohe. Alle fünf Beiträge entsprächen auch heute noch der Wahrheit und seien angesichts des Nachtrags über die Einstellung des Ermittlungsverfahrens weder unvollständig, noch spiegelten sie den Anschein einer nicht bestehenden Aktualität vor. Zwar habe der Kläger ein Interesse daran, mit dem Vorwurf einer Sexualstraftat, dem in der Öffentlichkeit ein besonders hohes Unwerturteil beigemessen werde, nicht mehr konfrontiert zu werden. Allerdings berichte die Beklagte in den angegriffenen Beiträgen nicht in einer Art und Weise, durch die der durchschnittliche Rezipient von einer Schuld oder Strafbarkeit des Klägers ausgehe, sondern stelle lediglich einen früher gegen diesen bestehenden Verdacht dar. Außerdem bestehe aufgrund der Art des Delikts, der Beteiligten sowie der Tatumstände ein hohes öffentliches Informationsinteresse. Zudem gehe von den Beiträgen der Beklagten auch keine erhebliche Breitenwirkung aus, da diese nur bei einer gezielten Suche zu finden seien. Um die durch eine Verdachtsberichterstattung hervorgerufene Störung abzustellen, sei ein Nachtrag geeignet, erforderlich, aber im Hinblick auf den Schutz der Pressefreiheit auch ausreichend.

B. Die Revision ist zulässig. Angegriffen ist entgegen der Ansicht der Revisionserwiderung nach wie vor allein das Bereithalten der den Kläger identifizierenden Altmeldungen in dem Online-Archiv der Beklagten.

C. Das angefochtene Urteil hält revisionsrechtlicher Nachprüfung nicht stand. Die Feststellungen des Berufungsgerichts tragen die Annahme, das weitere Bereithalten der den Kläger identifizierenden Wort- und Bildbeiträge sei rechtmäßig, nicht.

I. Wortberichterstattung:

1. Das Berufungsgericht hat zu Recht angenommen, dass das Bereithalten der angegriffenen Wortbeiträge zum Abruf im In-

ternet einen Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts des Klägers darstellt. Denn die Berichterstattung über ein Ermittlungsverfahren unter namentlicher Nennung des Beschuldigten beeinträchtigt zwangsläufig dessen Recht auf Schutz seiner Persönlichkeit und seines guten Rufes, weil sie sein mögliches Fehlverhalten öffentlich bekannt macht und seine Person in den Augen der Adressaten negativ qualifiziert (Senatsurteile vom 7. Dezember 1999 – VI ZR 51/99, BGHZ 143, 199, 202 f. m.w.N.; vom 18. November 2014 – VI ZR 76/14, BGHZ 203, 239 Rn. 31; vom 30. Oktober 2012 – VI ZR 4/12, AfP 2013, 50 Rn. 9 m.w.N.). Dies gilt nicht nur bei aktiver Informationsübermittlung durch die Medien, wie es im Rahmen der herkömmlichen Berichterstattung in Tagespresse, Rundfunk oder Fernsehen geschieht, sondern auch dann, wenn – wie im Streitfall – den Beschuldigten identifizierende Inhalte lediglich auf einer passiven Darstellungsplattform im Internet zum Abruf bereitgehalten werden. Diese Inhalte sind nämlich grundsätzlich jedem interessierten Internetnutzer zugänglich (Senatsurteile vom 15. Dezember 2009 – VI ZR 227/08, BGHZ 183, 353 Rn. 10 m.w.N.; vom 8. Mai 2012 – VI ZR 217/08, AfP 2012, 372 Rn. 34 m.w.N.; vom 30. Oktober 2012 – VI ZR 4/12, a.a.O.; vom 13. November 2012 – VI ZR 330/11, AfP 2013, 54 Rn. 8).

An dem Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts des Klägers vermag auch die Tatsache nichts zu ändern, dass mit den Beiträgen vom 27. April 2012 über die Einstellung des Ermittlungsverfahrens berichtet wurde und in der Fußzeile zu den Beiträgen vom 23. Januar 2012, 26. Januar 2012 und 11. Februar 2012 auf die Einstellung hingewiesen wurde. Denn alleine der Umstand, dass über vergangene Ermittlungen gegen den Kläger wegen des Verdachts des sexuellen Missbrauchs widerstandsunfähiger Personen berichtet wird, birgt die Gefahr, dass die Öffentlichkeit die bloße Einleitung eines Ermittlungsverfahrens mit dem Nachweis der Schuld gleichsetzt und trotz der späteren Einstellung des Ermittlungsverfahrens vom Schuldvorwurf „etwas hängenbleibt" (Senatsurteile vom 7. Dezember 1999 – VI ZR 51/99, a.a.O., 203; vom 30. Oktober 2012 – VI ZR 4/12, a.a.O. Rn. 14; jeweils m.w.N.).

Entgegen der Auffassung der Revision ist zwar nicht die absolut geschützte Intimsphäre des Klägers betroffen. Denn sexueller Missbrauch widerstandsunfähiger Personen, um den es in dem Ermittlungsverfahren ging, ist in § 179 StGB unter Strafe gestellt. Wäre eine Sexualstraftat begangen worden, fiele sie nicht in den unantastbaren Kernbereich höchstpersönlicher, privater Lebensgestaltung (vgl. Senatsurteile vom 17. Dezember 2013 – VI ZR 211/12, BGHZ 199, 237 Rn. 17; vom 19. März 2013 – VI ZR 93/12, AfP 2013, 250 Rn. 21 ff. m.w.N.; BVerfG, AfP 2009, 365 Rn. 26). Das Bereithalten von Berichten, die den Verdacht zum Gegenstand haben, der Kläger habe nach Einsatz von K.O.-Tropfen eine schwere Sexualstraftat begangen, stellt aber einen schwerwiegenden Eingriff in dessen persönliche Ehre dar (vgl. Senatsurteil vom 30. Januar 1996 – VI ZR 386/94, BGHZ 132, 13, 24).

2. Ebenfalls zutreffend hat es das Berufungsgericht für geboten erachtet, über den Unterlassungsantrag aufgrund einer Abwägung des Rechts des Klägers auf Schutz seiner Persönlichkeit und Achtung seines Privatlebens aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG, Art. 8 Abs. 1 EMRK mit dem in Art. 5 Abs. 1 GG, Art. 10 EMRK verankerten Recht der Beklagten auf Meinungs- und Medienfreiheit zu entscheiden. Wegen der Eigenart des Persönlichkeitsrechts als eines Rahmenrechts liegt seine Reichweite nicht absolut fest, sondern muss erst durch eine Abwägung der widerstreitenden grundrechtlich geschützten Belange bestimmt werden, bei der die besonderen Umstände des Einzelfalles sowie die betroffenen Grundrechte und Gewährleistungen der Europäischen Menschenrechtskonvention interpretationsleitend zu berücksichtigen sind. Der Eingriff in das Persönlichkeitsrecht ist nur dann rechtswidrig, wenn das Schutzinteresse des Betroffenen die schutzwürdigen Belange der anderen Seite überwiegt (st. Rspr.; vgl. etwa Senatsurteile vom 17. Dezember 2013 – VI ZR 211/12, a.a.O. Rn. 22; vom 30. Oktober 2012 – VI ZR 4/12, a.a.O. Rn. 10; vom 15. Dezember 2009 – VI ZR 227/08, a.a.O. Rn. 11; jeweils m.w.N.).

3. Ein solches Überwiegen hat das Berufungsgericht jedoch rechtsfehlerhaft verneint.

a) Im Rahmen der Abwägung ist von erheblicher Bedeutung, ob die Tatsachenbehauptungen in den angegriffenen Beiträgen im Zeitpunkt ihrer erstmaligen Veröffentlichung zulässig waren (vgl. Senatsurteil vom 15. Dezember 2009 – VI ZR 227/08, a.a.O. 2. Leitsatz u. Rn. 18). Da Gegenstand der Berichterstattung nicht nur das Ermittlungsverfahren, sondern auch der von der Beklagten als „Anfangsverdacht" bezeichnete Verdacht ist, der namentlich benannte Kläger habe eine 21jährige Frau anlässlich einer Feier in seinem Haus betäubt und sexuell missbraucht oder Beihilfe hierzu geleistet, müssen die Voraussetzungen einer zulässigen Verdachtsberichterstattung erfüllt sein (Senatsurteil vom 7. Dezember 1999 – VI ZR 51/99, a.a.O., 203). Die Revision rügt zu Recht, dass das Berufungsgericht dies angenommen hat.

Sie ist mit diesem Einwand nicht deshalb ausgeschlossen, weil der Kläger in den Vorinstanzen die Unzulässigkeit der ursprünglichen Verdachtsberichterstattung für nicht streiterheblich gehalten hat. Denn dabei handelt es sich um eine rechtliche Vorfrage, deren Beantwortung für die Beurteilung des streitgegenständlichen Unterlassungsanspruchs unabdingbar ist. Sie ist daher von den Gerichten auch dann zu prüfen, wenn die Parteien diese Frage für unerheblich halten; sollte hierzu weiterer Tatsachenvortrag der Parteien erforderlich sein, ist darauf gemäß § 139 Abs. 2 ZPO hinzuweisen. Dementsprechend haben sich die Vorinstanzen zu Recht – wenn auch nicht umfassend – mit der Frage befasst, ob die Berichterstattung im Zeitpunkt ihrer erstmaligen Veröffentlichung zulässig war.

aa) Nach der ständigen Rechtsprechung des Senats und des Bundesverfassungsgerichts darf eine Tatsachenbehauptung, deren Wahrheitsgehalt ungeklärt ist und die eine die Öffentlichkeit wesentlich berührende Angelegenheit betrifft, demjenigen, der sie aufstellt oder verbreitet, solange nicht untersagt werden, wie er sie zur Wahrnehmung berechtigter Interessen für erforderlich halten darf (Art. 5 GG, § 193 StGB). Eine Berufung hierauf setzt voraus, dass vor Aufstellung oder Verbreitung der Behauptung hinreichend sorgfältige Recherchen über den Wahrheitsgehalt angestellt werden. Die Pflichten zur sorgfältigen Recherche über den Wahrheitsgehalt richten sich dabei nach den Aufklärungsmöglichkeiten. Sie sind für die Medien grundsätzlich strenger als für Privatleute. An die Wahrheitspflicht dürfen im Interesse der Meinungsfreiheit keine Anforderungen gestellt werden, die die Bereitschaft zum Gebrauch des Grundrechts herabsetzen. Andererseits sind die Anforderungen umso höher, je schwerwiegender die Äußerung das Persönlichkeitsrecht beeinträchtigt (vgl. Senatsurteile vom 30. Januar 1996 – VI ZR 386/94, a.a.O., 23 f. m.w.N.; vom 7. Dezember 1999 – VI ZR 51/99, a.a.O., 203 f. m.w.N.; vom 22. April 2008 – VI ZR 83/07, BGHZ 176, 175 Rn. 35 m.w.N.; vom 17. Dezember 2013 – VI ZR 211/12, a.a.O. Rn. 26 m.w.N.; vom 18. November 2014 – VI ZR 76/14, a.a.O. Rn. 15).

Diese Grundsätze gelten auch für die Berichterstattung über Ermittlungsverfahren unter namentlicher Nennung des Beschuldigten. In diesem Verfahrensstadium steht lediglich fest, dass

ein Ermittlungsverfahren eingeleitet wurde, in der Regel ist aber nicht geklärt, ob der Beschuldigte die ihm zur Last gelegte Straftat begangen hat. Zwar gehört es zu den legitimen Aufgaben der Medien, Verfehlungen – auch konkreter Personen – aufzuzeigen (Senatsurteile vom 30. Oktober 2012 – VI ZR 4/12, a.a.O. Rn. 12; vom 13. November 2012 – VI ZR 330/11, a.a.O. Rn. 11; BVerfG, AfP 2012, 143 Rn. 39; jeweils m.w.N.). Dies gilt auch für die Berichterstattung über eine Straftat, da diese zum Zeitgeschehen gehört und die Verletzung der Rechtsordnung und die Beeinträchtigung von Rechtsgütern der betroffenen Bürger oder der Gemeinschaft ein anzuerkennendes Interesse der Öffentlichkeit an näherer Information über Tat und Täter begründen kann (vgl. Senatsurteile vom 7. Dezember 1999 – VI ZR 51/99, a.a.O., 204; vom 15. Dezember 2009 – VI ZR 227/08, a.a.O. Rn. 14; vom 7. Juni 2011 – VI ZR 108/10, BGHZ 190, 52 Rn. 19; vom 30. Oktober 2012 – VI ZR 4/12, a.a.O. Rn. 13; BVerfG, AfP 2009, 46 Rn. 11; AfP 2009, 365 Rn. 18; EGMR, EuGRZ 2012, 294 Rn. 96; jeweils m.w.N.). Besteht allerdings – wie im Ermittlungsverfahren – erst der Verdacht einer Straftat, so sind die Medien bei besonderer Schwere des Vorwurfs angesichts des damit verbundenen schwerwiegenden Eingriffs in die persönliche Ehre in besonderem Maße zu sorgfältigem Vorgehen verpflichtet (vgl. Senatsurteile vom 30. Januar 1996 – VI ZR 386/94, a.a.O., 24; vom 7. Dezember 1999 – VI ZR 51/99, a.a.O., 203; vom 17. Dezember 2013 – VI ZR 211/12, a.a.O. Rn. 28 m.w.N.). Dabei ist im Hinblick auf die aus dem Rechtsstaatsprinzip folgende und in Art. 6 Abs. 2 EMRK anerkannte Unschuldsvermutung die Gefahr in den Blick zu nehmen, dass die Öffentlichkeit die bloße Einleitung eines Ermittlungsverfahrens mit dem Nachweis der Schuld gleichsetzt und deshalb im Fall einer späteren Einstellung des Ermittlungsverfahrens oder eines Freispruchs vom Schuldvorwurf „etwas hängenbleibt" (Senatsurteile vom 7. Dezember 1999 – VI ZR 51/99, a.a.O., 203; vom 30. Oktober 2012 – VI ZR 4/12, a.a.O. Rn. 14; jeweils m.w.N.; vgl. auch BVerfG, AfP 2009, 46 Rn. 15).

Erforderlich ist jedenfalls ein Mindestbestand an Beweistatsachen, die für den Wahrheitsgehalt der Information sprechen und ihr damit erst „Öffentlichkeitswert" verleihen. Die Darstellung darf ferner keine Vorverurteilung des Betroffenen enthalten; sie darf also nicht durch eine präjudizierende Darstellung den unzutreffenden Eindruck erwecken, der Betroffene sei der ihm vorgeworfenen Handlung bereits überführt. Auch ist vor der Veröffentlichung regelmäßig eine Stellungnahme des Betroffenen einzuholen. Schließlich muss es sich um einen Vorgang von gravierendem Gewicht handeln, dessen Mitteilung durch ein Informationsbedürfnis der Allgemeinheit gerechtfertigt ist (vgl. Senatsurteile vom 7. Dezember 1999 – VI ZR 51/99, a.a.O., 203 f. m.w.N.; vom 17. Dezember 2013 – VI ZR 211/12, a.a.O. Rn. 26; vom 18. November 2014 – VI ZR 76/14, a.a.O. Rn. 16 m.w.N.; vgl. auch BVerfGK 9, 317, 322).

bb) Im Streitfall tragen die Feststellungen des Berufungsgerichts dessen Annahme, die Beklagte habe die Erfordernisse einer zulässigen Verdachtsberichterstattung eingehalten, nicht. Über den Umstand hinaus, dass gegen den Kläger aufgrund einer Anzeige ein Ermittlungsverfahren wegen des Verdachts des sexuellen Missbrauchs widerstandsunfähiger Personen eingeleitet worden war, hat das Berufungsgericht keine Feststellungen zum Vorliegen von Beweistatsachen getroffen, die für den Wahrheitsgehalt dieses Verdachts gesprochen haben.

(1) Die bloße Tatsache der Einleitung eines Ermittlungsverfahrens als solche genügt jedenfalls nicht für die Annahme des Vorliegens eines Mindestbestands an Beweistatsachen (Soehring, in: Soehring/Hoene, Presserecht, 5. Aufl., § 19 Rn. 36; Prinz/Peters, Medienrecht, Rn. 272; BeckOK InfoMedienR/ Söder, § 823 BGB Rn. 244 (Stand: 01.11.2015); HH-Ko/MedienR/Kröner, 2. Aufl., 33. Abschnitt Rn. 59; Lehr, NJW 2013, 728, 730; Schumacher, K&R 2014, 381, 382 Fn. 14). Die Staatsanwaltschaft hat schon beim Vorliegen eines Anfangsverdachts Ermittlungen aufzunehmen (vgl. § 152 Abs. 2, § 160 Abs. 1 StPO). Dafür ist bereits ausreichend, dass aufgrund zureichender tatsächlicher Anhaltspunkte nach kriminalistischer Erfahrung die bloße Möglichkeit einer verfolgbaren Straftat gegeben ist (BGH, Urteil vom 21. April 1988 – III ZR 255/86, NJW 1989, 96, 97; BVerfGK 3, 55, 61; jeweils m.w.N.). Die Schwelle für die Annahme eines Anfangsverdachts liegt damit niedrig (vgl. BVerfG, NJW 2002, 1411, 1412); es genügen schon entferntere Verdachtsgründe (BVerfG, NJW 1994, 783; NJW 1994, 783, 784), die eine geringe, wenngleich nicht nur theoretische Wahrscheinlichkeit des Vorliegens einer verfolgbaren Straftat begründen (Beulke, in: Löwe-Rosenberg, StPO, 26. Aufl., § 152 Rn. 23). So müssen die Ermittlungsbehörden auch auf völlig unbegründete, unter Umständen wider besseres Wissen in Schädigungsabsicht erstattete Strafanzeigen hin tätig werden (Soehring, a.a.O.).

(2) Aus den Feststellungen des Berufungsgerichts lässt sich nichts Weitergehendes herleiten. Ihnen ist insbesondere nicht zu entnehmen, dass – wie die Revisionserwiderung geltend gemacht hat – die angegriffenen Beiträge auf den Kläger identifizierenden amtlichen Verlautbarungen der Staatsanwaltschaft beruhen.

Zwar ist in der höchstrichterlichen Rechtsprechung anerkannt, dass den Verlautbarungen amtlicher Stellen ein gesteigertes Vertrauen entgegengebracht werden darf (Senatsurteile vom 17. Dezember 2013 – VI ZR 211/12, a.a.O. Rn. 30; vom 11. Dezember 2012 – VI ZR 314/10, AfP 2013, 57 Rn. 30; BVerfG, AfP 2010, 365 Rn. 35; jeweils m.w.N.). Dies beruht auf der Erwägung, dass Behörden in ihrer Informationspolitik unmittelbar an die Grundrechte gebunden sind und Amtsträger, wenn sie vor der Frage stehen, ob die Presse über amtliche Vorgänge informiert werden soll, die erforderliche Abwägung zwischen dem Informationsrecht der Presse und dem allgemeinen Persönlichkeitsrecht vorzunehmen haben (Senatsurteile vom 17. Dezember 2013 – VI ZR 211/12, a.a.O.; vom 11. Dezember 2012 – VI ZR 314/10, a.a.O.; BVerfG, AfP 2010, 365 Rn. 35; jeweils m.w.N.). Verletzen sie ihre Amtspflichten, kann ein Schadensersatzanspruch des Betroffenen wegen einer Verletzung seines allgemeinen Persönlichkeitsrechts gegen die zuständige Gebietskörperschaft als Träger der Behörde gegeben sein (Senatsurteil vom 17. Dezember 2013 – VI ZR 211/12, a.a.O. m.w.N.; vgl. auch BGH, Urteile vom 17. März 1994 – III ZR 15/93, NJW 1994, 1950, 1951 ff.; vom 23. Oktober 2003 – III ZR 9/03, NJW 2003, 3693, 3697). Daher ist regelmäßig die Annahme gerechtfertigt, dass eine unmittelbar an die Grundrechte gebundene, auf Objektivität verpflichtete Behörde wie die Staatsanwaltschaft die Öffentlichkeit erst dann unter Namensnennung über ein Ermittlungsverfahren unterrichten wird, wenn sich der zugrunde liegende Tatverdacht bereits einigermaßen erhärtet hat (BVerfG, AfP 2010, 365 Rn. 35). Auch das entlastet die Medien allerdings nicht von der Aufgabe der Abwägung und Prüfung, ob im Übrigen nach den Grundsätzen der Verdachtsberichterstattung eine Namensnennung des Betroffenen gerechtfertigt ist (Damm/Rehbock, Widerruf, Unterlassung und Schadensersatz, 3. Aufl., Rn. 64; Löffler/Steffen, Presserecht, 6. Aufl., § 6 LPG Rn. 208 f.; HH-Ko/MedienR/Kröner, 2. Aufl., 33. Abschnitt Rn. 60; HH-Ko/MedienR/Breutz/Weyhe, 2. Aufl., 39. Abschnitt Rn. 55).

Im Streitfall ist schon nicht festgestellt, ob und wann die Staatsanwaltschaft die Öffentlichkeit unter Namensnennung über das gegen den Kläger geführte Ermittlungsverfahren unter-

richtete. Dies ergibt sich entgegen der Ansicht der Revisionserwiderung nicht bereits hinreichend klar aus den angefochtenen Meldungen. So ist aus dem Bericht vom 23. Januar 2012 nicht erkennbar, von wem die Information stammte, dass die Staatsanwaltschaft nunmehr auch gegen den Kläger ermittelte. Soweit in den Meldungen vom 23. Januar 2012 und vom 11. Februar 2012 von Erklärungen der Staatsanwaltschaft die Rede ist, ist denkbar, dass sich diese auf das Ermittlungsverfahren gegen namentlich nicht genannte Teilnehmer der Feier bezogen.

b) Kann mangels Feststellungen des Berufungsgerichts zum Vorliegen eines Mindestbestandes an Beweistatsachen nicht von der Zulässigkeit der ursprünglichen Berichterstattung über den Verdacht, der Kläger habe eine schwere Sexualstraftat begangen, ausgegangen werden, so kann derzeit auch nicht beurteilt werden, ob das weitere Bereithalten der den Kläger identifizierenden Wortbeiträge zum Abruf aus dem Online-Archiv einen rechtswidrigen Eingriff in das Persönlichkeitsrecht darstellt.

aa) Für den Fall, dass – wie von der Revision geltend gemacht – die Wortberichte ursprünglich unzulässig gewesen sein sollten, ist grundsätzlich davon auszugehen, dass ihr Bereithalten in dem Online- Archiv der Beklagten unzulässig ist, soweit sie den Kläger weiterhin identifizieren.

(1) Eine abweichende Beurteilung wäre vorliegend nicht deshalb geboten, weil die Berichte vom 23. Januar 2012, 26. Januar 2012 und 11. Februar 2012 um den Zusatz in der Fußzeile ergänzt wurden, dass es sich um eine „Archivberichterstattung" handelt und das Ermittlungsverfahren gegen den Kläger im April 2012 eingestellt wurde. So, wie schon mit den Berichten über die Einstellung des Ermittlungsverfahrens vom 27. April 2012 zwangsläufig auch der dem Verfahren ursprünglich zugrunde liegende Verdacht transportiert und perpetuiert wurde, ist durch die nachträglich eingefügte Fußzeile bei den Berichten über die Einleitung und den Fortgang des Ermittlungsverfahrens dieser Verdacht nicht ausgeräumt worden. Denn beim Leser kann der Eindruck entstehen, dass der Kläger trotz der Verfahrenseinstellung „in Wahrheit" Täter der ihm vorgeworfenen Tat ist und lediglich die Strafverfolgung – zum Beispiel mangels ausreichender Beweise, wie in den Berichten vom 27. April 2012 erwähnt – nicht fortgeführt wurde (vgl. BVerfG, AfP 2009, 46 Rn. 15). Es ist aber gerade die Einstellung des Verfahrens nach § 170 Abs. 2 StPO, die nicht für, sondern gegen die Abrufbarkeit jedenfalls einer unzulässigen Berichterstattung in Online-Archiven spricht. Sollte es nämlich schon anfangs an einem Mindestbestand an Beweistatsachen als Voraussetzung für eine zulässige Berichterstattung gefehlt haben und ist das Ermittlungsverfahren sodann mangels ausreichender Beweisgrundlage eingestellt worden, so gäbe es keinen anerkennenswerten Grund für die fortdauernde Abrufbarkeit der Berichte im Internet. Eine Einstellung des Verfahrens nach § 170 Abs. 2 StPO dient – anders als eine Einstellung nach § 153a StPO (vgl. hierzu Senatsurteil vom 30. Oktober 2012 – VI ZR 4/12, a.a.O. Rn. 25 m.w.N.) – auch der Rehabilitation des Betroffenen (BGH, Beschluss vom 26. Juni 1990 – 5 AR (VS) 8/90, BGHSt 37, 79, 83); dieser Zweck wird durch die weitere Abrufbarkeit einer identifizierenden Verdachtsberichterstattung konterkariert. Ein anerkennenswertes Öffentlichkeitsinteresse, das bei Unzulässigkeit der ursprünglichen Berichterstattung schon von Anfang an als sehr gering eingeschätzt werden müsste, besteht demgegenüber im Hinblick auf die Einstellung des Verfahrens nach § 170 Abs. 2 StPO in noch geringerem Maße (vgl. Löffler/Steffen, Presserecht, 6. Aufl., § 6 LPG Rn. 211; Prinz/Peters, Medienrecht, Rn. 107, 272; HH-Ko/MedienR/Breutz/Weyhe, 2. Aufl., 39. Abschnitt Rn. 92; KG, NJW 1989, 397, 398; vgl. auch Wenzel/Burckhardt, Das Recht der Wort- und Bildberichterstattung, 5. Aufl., Kap. 10 Rn. 167; Soehring, in: Soehring/Hoene, Presserecht, 5. Aufl., § 19 Rn. 37). Im Übrigen geht aus dem von der Beklagten eingefügten Zusatz in der Fußzeile nicht hervor, dass das Verfahren mangels hinreichenden Tatverdachts eingestellt wurde.

(2) Die Entscheidung des Europäischen Gerichtshofs für Menschenrechte vom 16. Juli 2013 (abgedruckt in AfP 2014, 517) steht der Beurteilung, von Anfang an unzulässige Berichte dürften grundsätzlich auch nicht als Altmeldungen im Online-Archiv bereitgehalten werden, nicht entgegen. Der Gerichtshof hat es in dem dort zugrunde liegenden Fall für den Schutz des Einzelnen gemäß Art. 8 EMRK nicht für zwingend geboten gehalten, dass das nationale Gericht für rechtswidrige, in einem Online-Archiv zugreifbare Artikel die Löschung anordnet. Hierzu führt die Entscheidung aus, dass eine geltend gemachte Verletzung der von Art. 8 EMRK geschützten Rechte (Achtung des Privatlebens) durch geeignete Maßnahmen nach nationalem Recht behoben werden sollte (a.a.O. Rn. 66). Den Vertragsstaaten komme aber ein weiter Einschätzungsspielraum bei der Bestimmung der Maßnahmen zu, um die Einhaltung der Konvention unter Berücksichtigung der Bedürfnisse und Ressourcen der Gemeinschaft und des Einzelnen zu gewährleisten (a.a.O. Rn. 55). Wie sich aus dem von der Revisionserwiderung zitierten Urteil des Europäischen Gerichtshofs vom 10. März 2009 in dem Verfahren Times Newspapers Ltd. v. The United Kingdom Judgment (Bsw. 3003/03 und Bsw. 23676/03, Rn. 45) ergibt, ist der staatliche Ermessenspielraum bei der Abwägung zwischen den betroffenen Interessen noch größer, wenn es nicht um aktuelle Berichterstattung geht, sondern um Nachrichtenarchive über vergangene Ereignisse. Entscheidend ist, dass der Staat bzw. das nationale Gericht seine Verpflichtung erfüllt, den Umständen des jeweiligen Falles entsprechend einen Ausgleich zwischen den von Art. 10 EMRK gewährten Rechten einerseits und den von Art. 8 EMRK gewährten Rechten andererseits zu schaffen (EGMR, abgedruckt in AfP 2014, 517 Rn. 68). Dem trägt der oben genannte Grundsatz Rechnung. Hier kommt hinzu, dass der Kläger ohnehin nicht die vollständige Löschung der Beiträge aus dem Internet verlangt.

bb) Für den Fall, dass – wie von der Revisionserwiderung geltend gemacht – die Wortberichterstattung ursprünglich zulässig gewesen sein sollte, könnte für die auch dann gebotene umfassende Abwägung der Grundrechtspositionen unter anderem von Bedeutung sein, welches Gewicht den Tatsachen zukam, die anfangs für eine Beteiligung des Klägers an einer Straftat sprachen.

II. Bildberichterstattung:

Mit dem von dem Antrag des Klägers erfassten und im erstinstanzlichen Urteil ausgesprochenen Verbot, den Kläger identifizierend darstellende Bildnisse in den angegriffenen Beiträgen online zum Abruf bereitzuhalten, hat sich das Berufungsgericht bislang nicht gesondert befasst. Auch insoweit tragen die Feststellungen des Berufungsgerichts die Abweisung der Klage nicht.

1. Als Teil der Artikel vom 23. Januar, 26. Januar und 11. Februar 2012 und des zweiten Artikels vom 27. April 2012 dürfen die den Kläger zeigenden Bilder mangels dessen Einwilligung (§ 22 Satz 1 KUG) nur dann zum Abruf im Internet bereitgehalten werden, wenn es sich um Bildnisse aus dem Bereich der Zeitgeschichte handelt (§ 23 Abs. 1 Nr. 1 KUG) und durch

die Verbreitung berechtigte Interessen des Abgebildeten nicht verletzt werden (§ 23 Abs. 2 KUG). Anderenfalls steht dem Kläger ein Anspruch auf Unterlassung erneuter Verbreitung der in den Artikeln enthaltenen Bilder entsprechend §§ 1004 Abs. 1 Satz 2, 823 Abs. 1, Abs. 2 BGB i.V.m. §§ 22, 23 KUG, Art. 1 Abs. 1, Art. 2 Abs. 1 GG zu (vgl. Senatsurteil vom 9. Februar 2010 – VI ZR 243/08, AfP 2010, 162 Rn. 31 f. m.w.N.).

Die Beurteilung, ob ein Bildnis dem Bereich der Zeitgeschichte i.S. von § 23 Abs. 1 Nr. 1 KUG zuzuordnen ist, erfordert eine Abwägung zwischen den Rechten des Abgebildeten aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG, Art. 8 Abs. 1 EMRK einerseits und den Rechten der Presse aus Art. 5 Abs. 1 GG, Art. 10 Abs. 1 EMRK andererseits. Maßgebend ist hierbei das Interesse der Öffentlichkeit an vollständiger Information über das Zeitgeschehen, wobei dieser Begriff alle Fragen von allgemeinem gesellschaftlichem Interesse umfasst. Allerdings besteht das Informationsinteresse nicht schrankenlos. Vielmehr wird der Einbruch in die persönliche Sphäre des Abgebildeten durch den Grundsatz der Verhältnismäßigkeit begrenzt. Bei der Gewichtung der kollidierenden Interessen kommt dem Anlass und dem Gegenstand der Berichterstattung maßgebliche Bedeutung zu, wobei der Informationsgehalt der Bildberichterstattung unter Berücksichtigung der zugehörigen Textberichterstattung zu ermitteln ist. Entscheidend ist insbesondere, ob die Medien im konkreten Fall eine Angelegenheit von öffentlichem Interesse ernsthaft und sachbezogen erörtern, damit den Informationsanspruch des Publikums erfüllen und zur Bildung der öffentlichen Meinung beitragen oder ob sie – ohne Bezug zu einem zeitgeschichtlichen Ereignis – lediglich die Neugier der Leser befriedigen (Senatsurteile vom 9. Februar 2010 – VI ZR 243/08, a.a.O. Rn. 33 ff.; vom 7. Juni 2011 – VI ZR 108/10, BGHZ 190, 52 Rn. 17 ff.; vom 8. März 2012 – VI ZR 125/12, AfP 2013, 399 Rn. 12 f.; jeweils m.w.N.). Geht es um eine identifizierende Bildberichterstattung über den Verdacht einer Straftat, so ist darüber hinaus zu beachten, dass eine solche Berichterstattung in das Recht des Abgebildeten auf Schutz seiner Persönlichkeit eingreift, weil sie sein angebliches Fehlverhalten öffentlich bekannt macht und seine Person in den Augen der Adressaten von vornherein negativ qualifiziert (vgl. Senatsurteile vom 9. Februar 2010 – VI ZR 243/08, a.a.O. Rn. 34; vom 7. Juni 2011 – VI ZR 108/10, a.a.O. Rn. 19 ff.). Insbesondere ist auch in diesem Zusammenhang im Hinblick auf die Unschuldsvermutung die Gefahr in den Blick zu nehmen, dass die Öffentlichkeit die bloße Einleitung eines Ermittlungsverfahrens mit dem Nachweis der Schuld gleichsetzt und dass der Eindruck, der Abgebildete sei ein Straftäter, selbst bei einer späteren Einstellung des Ermittlungsverfahrens nicht beseitigt wird. Ob im Einzelfall dem Recht auf Schutz der Persönlichkeit oder dem Informationsinteresse Vorrang gebührt, hängt unter anderem von dem Verdachtsgrad ab, dem der Beschuldigte ausgesetzt war und gegebenenfalls noch ist (vgl. Senatsurteil vom 7. Juni 2011 – VI ZR 108/10, a.a.O. Rn. 25).

2. Ob nach diesen Grundsätzen das Bereithalten der Fotos des Klägers als Teil der Berichterstattung zum Abruf im Internet zu beanstanden ist, kann ohne weitere Feststellungen nicht abschließend beurteilt werden. Durch Anlass und Gegenstand der Berichterstattung werden die den Kläger in seinem Beruf als Fußballspieler zeigenden Bilder mit dem Verdacht, eine schwere Sexualstraftat begangen zu haben, in unmittelbare Verbindung gebracht. Ob dies berechtigte Interessen des Klägers verletzte bzw. verletzt, hängt unter anderem davon ab, ob und in welchem Umfang – jeweils zu dem Zeitpunkt, zu dem die Meldung erstmals „in das Netz" gestellt wurde, – Tatsachen vorlagen, die den Tatvorwurf stützten. Im Grundsatz kann auch bei der Bildberichterstattung davon ausgegangen werden, dass eine von Anfang an unzulässige Meldung auch nicht als Altmeldung im Online-Archiv zum Abruf bereitgehalten werden darf.

Danach ist das Berufungsurteil aufzuheben und die Sache zu neuer Verhandlung und Entscheidung an das Berufungsgericht zurückzuverweisen (§ 562 Abs. 1, § 563 Abs. 1 Satz 1 ZPO). Das Berufungsgericht wird – erforderlichenfalls nach ergänzendem Vortrag der Parteien – die notwendigen Feststellungen nachzuholen haben.

Mitbestimmung bei betrieblichem Eingliederungsmanagement (Ls)

(**Bundesarbeitsgericht,** Beschluss vom 22. März 2016 – 1 ABR 14/14 –)

1. **Das Mitbestimmungsrecht des Betriebsrats bei Maßnahmen des Gesundheitsschutzes nach § 87 Abs. 1 Nr. 7 BetrVG erfasst aufgrund der Rahmenvorschrift des § 84 Abs. 2 Satz 1 SGB IX nur die Aufstellung von Verfahrensgrundsätzen zur Klärung der Möglichkeiten, wie die Arbeitsunfähigkeit eines Arbeitnehmers überwunden und mit welchen Leistungen oder Hilfen einer erneuten Arbeitsunfähigkeit vorgebeugt werden kann.**

2. **Eine Einigungsstelle überschreitet ihre Zuständigkeit, wenn sie die Bildung eines Integrationsteams zur Begleitung der nur dem Arbeitgeber obliegenden Umsetzung der Maßnahmen vorgibt.**

(Nicht amtliche Leitsätze)

Zuständigkeit des Konzernbetriebsrats beim Einsatz von Überwachungseinrichtungen

(**Bundesarbeitsgericht,** Beschluss vom 26. Januar 2016 – 1 ABR 68/13 –)

1. **Die originäre Zuständigkeit des Konzernbetriebsrats erfordert, dass es sich zum einen um mehrere unternehmensbetreffende Angelegenheiten handelt und zum anderen objektiv ein zwingendes Erfordernis für eine unternehmensübergreifende Regelung besteht.**

2. **Eine unternehmensübergreifende Nutzungs- und Überwachungsmöglichkeit des Aufzeichnungssystems liegt nicht vor, wenn ein Arbeitgeber nur eigene Arbeitnehmer hierbei einsetzt und keine aufgezeichneten Daten oder hieraus bezogene Auswertungen an andere Konzernunternehmen weitergibt.**

3. Für die im Rahmen von Werk- oder Dienstverträgen eingesetzten Beschäftigten eines Fremdarbeitgebers, die den im Betrieb eingerichteten Überwachungseinrichtung unterliegen, sind – auch im Konzernverbund – der Vertragsarbeitgeber und dessen Betriebsrat zuständig. Gegenstand des Beteiligungsrechts des § 87 Abs. 1 Nr. 6 BetrVG ist, ob überhaupt sowie ggf. nach welchen Grundsätzen welche Arbeitnehmer für welche Dauer sich der bei dem Dritten installierten Überwachungseinrichtung unterziehen müssen.

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Beteiligten streiten über die Zuständigkeit des Konzernbetriebsrats beim Einsatz von Überwachungskameras.

Die antragstellende Arbeitgeberin ist die Konzernobergesellschaft eines Krankenhauskonzerns. Bei ihr ist der am Verfahren beteiligte Konzernbetriebsrat errichtet.

Die Arbeitgeberin betrieb bis zum 27. August 2013 das H Klinikum (Klinikum). Durch umwandlungsrechtliche Ausgliederung wurde das Klinikum auf die zu 8. beteiligte B-B GmbH (BB) übertragen. Bei dieser ist der zu 3. beteiligte Betriebsrat gebildet. Alleinige Gesellschafterin der BB ist die Arbeitgeberin.

Im Klinikum sind zu Überwachungszwecken verschiedene Kameras und Monitore installiert. Zwei Kameras dienen der Kontrolle des Zugangs zur Abteilung Neonatologie und der Flurüberwachung. Ihre Aufnahmen werden ohne Speicherung der Bilder auf drei Monitoren wiedergegeben. Auf dem Außengelände des Klinikums sind zwanzig Kameras eingesetzt, deren Bilder über Lichtwellenleiter an einen zentralen Schaltschrank übermittelt und durch dort installierte Geräte von Arbeitnehmern der BB weiterverarbeitet werden. Die Bilder dieser Kameras werden auf fünf Monitoren in unterschiedlicher Weise wiedergegeben.

Von den Kameras werden auch Arbeitnehmer von anderen Konzernunternehmen aufgenommen, die im Klinikum Werk- oder Dienstleistungen für ihren Vertragsarbeitgeber erbringen. Diese Arbeitgeber sowie die bei ihnen bestehenden Betriebsräte sind als Beteiligte zu 9. bis 18. sowie als Beteiligte zu 4., 5., 7. und 19. bis 23. in das Verfahren einbezogen.

Zwischen der Arbeitgeberin und dem Konzernbetriebsrat besteht eine Einigungsstelle mit dem Regelungsgegenstand „Konzernbetriebsvereinbarung zur Verwendung arbeitnehmerbezogener Daten durch die Nutzung von Informations- und Kommunikationstechnologien“. Diese bejahte durch Beschluss vom 17. August 2012 ihre Zuständigkeit für eine Regelung über den Einsatz der auf dem Klinikumsgelände installierten Kameras und Monitore.

Die Arbeitgeberin hat die Auffassung vertreten, der Konzernbetriebsrat sei für die Ausübung des Beteiligungsrechts in Bezug auf die Kameras und Monitore nicht zuständig. Ein zwingendes Erfordernis für eine unternehmensübergreifende Regelung folge insbesondere nicht aus der Aufzeichnung der Arbeitsleistung von Arbeitnehmern anderer Konzernunternehmen.

Der Konzernbetriebsrat hat die Abweisung des Antrags beantragt. Die weiteren Beteiligten haben keine Anträge gestellt.

Das Arbeitsgericht hat dem Antrag entsprochen. Das Landesarbeitsgericht hat ihn auf die Beschwerde des Konzernbetriebsrat abgewiesen. Mit der Rechtsbeschwerde begehrt die Arbeitgeberin die Wiederherstellung des erstinstanzlichen Beschlusses.

Aus den Gründen:

Der negative Feststellungsantrag der Arbeitgeberin ist begründet. Dem Konzernbetriebsrat steht das Beteiligungsrecht bei der Anwendung der im Klinikum installierten Kameras und Monitore nicht zu.

a) Die Ausgestaltung des von der BB betriebenen visuellen Aufzeichnungssystems unterliegt dem Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG.

Nach dieser Vorschrift hat der Betriebsrat ua. mitzubestimmen bei der Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Das Landesarbeitsgericht hat zutreffend erkannt, dass es sich bei den im Klinikum eingesetzten Kameras und Monitoren um eine solche technische Einrichtung handelt, die dazu bestimmt ist, das Verhalten und die Leistung der Arbeitnehmer zu überwachen (vgl. BAG 11. Dezember 2012 – 1 ABR 78/11 – Rn. 17, BAGE 144, 109). Hierüber besteht zwischen den Beteiligten auch kein Streit.

b) Der Konzernbetriebsrat ist nicht nach § 58 Abs. 1 Satz 1 Halbs. 1 BetrVG für die Ausübung des Mitbestimmungsrechts in Bezug auf die von der BB betriebenen Kameras und Monitore zuständig.

aa) Nach der Kompetenzzuweisung des Betriebsverfassungsgesetzes ist für die Wahrnehmung von Mitbestimmungsrechten in erster Linie der von den Arbeitnehmern unmittelbar durch Wahl legitimierte Betriebsrat zuständig. Er hat die Interessen der Belegschaften der einzelnen Betriebe gegenüber dem Unternehmer wahrzunehmen. Diese Aufgabe weisen § 50 Abs. 1 Satz 1 BetrVG dem Gesamtbetriebsrat und § 58 Abs. 1 Satz 1 BetrVG dem Konzernbetriebsrat nur für den Fall zu, dass die zu regelnde Angelegenheit nicht auf den einzelnen Betrieb oder das konzernangehörige Unternehmen beschränkt ist und deshalb die Interessen der Arbeitnehmer nicht mehr auf der betrieblichen Ebene bzw. der des Unternehmens gewahrt werden können. Nach § 58 Abs. 1 Satz 1 Halbs. 1 BetrVG ist der Konzernbetriebsrat für die Behandlung von Angelegenheiten zuständig, die den Konzern oder mehrere Konzernunternehmen betreffen und nicht durch die einzelnen Gesamtbetriebsräte innerhalb ihrer Unternehmen geregelt werden können. Diese originäre Zuständigkeit des Konzernbetriebsrats ist nach denselben Kriterien zu bestimmen wie die Zuständigkeit des Gesamtbetriebsrats. Erforderlich ist, dass es sich zum einen um eine mehrere Unternehmen betreffende Angelegenheit handelt und zum anderen objektiv ein zwingendes Erfordernis für eine unternehmensübergreifende Regelung besteht. Das Vorliegen eines zwingenden Erfordernisses bestimmt sich nach Inhalt und Zweck des Mitbestimmungstatbestands, der einer zu regelnden Angelegenheit zugrunde liegt (vgl. BAG 19. Juni 2012 – 1 ABR 19/11 – Rn. 21, BAGE 142, 87). Maßgeblich sind stets die konkreten Umstände im Konzern und in den einzelnen Unternehmen. Allein der Wunsch des Arbeitgebers oder der betroffenen Arbeitnehmervertretungen nach einer konzerneinheitlichen oder unternehmensübergreifenden Regelung, ein Kosten- oder Koordinierungsinteresse sowie reine Zweckmäßigkeitsgesichtspunkte genügen nicht, um in Angelegenheiten der zwingenden Mitbestimmung die Zuständigkeit des Konzernbetriebsrats zu begründen (BAG 25. September 2012 – 1 ABR 45/11 – Rn. 24).

bb) Bei der Mitbestimmung gegenüber der Ausgestaltung des im Klinikum und auf seinem Außengelände eingesetzten visuel-

len Aufzeichnungssystems handelt es sich nicht um eine mehrere Unternehmen betreffende Angelegenheit iSd. § 58 Abs. 1 Satz 1 Halbs. 1 BetrVG. Die der Mitbestimmung unterliegenden Gegenstände betreffen unterschiedliche betriebliche Vorgänge.

(1) Nach den nicht mit Verfahrensrügen angegriffenen und den Senat bindenden Feststellungen des Landesarbeitsgerichts liegt eine unternehmensübergreifende Nutzungs- und Überwachungsmöglichkeit des Aufzeichnungssystems nicht vor. An diesem werden von der BB nur deren Arbeitnehmer eingesetzt. Eine Weitergabe der erhobenen Daten oder darauf bezogener Auswertungen von der BB an andere Konzernunternehmen erfolgt nicht. Diese haben auch keine Zugriffsmöglichkeit auf die im Klinikum installierten Geräte und die aufgezeichneten Daten.

(2) Nach § 87 Abs. 1 Nr. 6 BetrVG muss die BB mit dem bei ihr errichteten Betriebsrat in Bezug auf die von diesem vertretenen Arbeitnehmer die Rahmenbedingungen für den Einsatz der installierten Kameras und Monitore regeln. Zu diesen Gegenständen gehören zB Abreden über die eingesetzte Hardware, den Gegenstand und die Dauer der visuellen Aufzeichnungen sowie ihre Verwertung und Archivierung. Für Arbeitnehmer von Drittunternehmen – unabhängig von deren Konzernzugehörigkeit – haben die BB und ihr Betriebsrat keine Regelungsbefugnis.

(3) Das nach § 87 Abs. 1 Nr. 6 BetrVG bestehende Beteiligungsrecht bei anderen Konzernunternehmen beschränkt sich auf Regelungen, ob und ggf. unter welchen Voraussetzungen die auf dem Betriebsgelände der BB eingesetzten Arbeitnehmer von dem dort bestehenden visuellen Aufzeichnungssystem erfasst werden.

(4) Für die im Rahmen von Werk- oder Dienstverträgen zu einem Fremdarbeitgeber entsandten Arbeitnehmer, die einer in dessen Betrieb eingerichteten Überwachungseinrichtung unterliegen, sind – auch im Konzernverbund – deren Vertragsarbeitgeber und dessen Betriebsrat zuständig.

(a) Der Betrieb iSd. § 87 Abs. 1 Nr. 6 BetrVG ist nicht räumlich auf die Betriebsstätte beschränkt, sondern funktional zu verstehen. Nach der Senatsrechtsprechung wird das Mitbestimmungsrecht des Betriebsrats nach der vorgenannten Vorschrift nicht dadurch ausgeschlossen, dass sich die Arbeitnehmer zur Verrichtung ihrer arbeitsvertraglichen Tätigkeit auf Anweisung des Arbeitgebers in den Betrieb eines anderen Arbeitgebers begeben, in dem ihre Leistung oder ihr Verhalten durch eine dort befindliche technische Überwachungseinrichtung aufgezeichnet wird. Dies folgt aus Sinn und Zweck des Mitbestimmungsrechts. Die Arbeitnehmer unterliegen bei der Arbeit in einem fremden Betrieb weiterhin den Weisungen ihres Vertragsarbeitgebers. Daher ist der von ihnen gewählte und sie repräsentierende Betriebsrat nach § 87 Abs. 1 Nr. 6 BetrVG auch dann zu beteiligen, wenn der entsendende Arbeitgeber im Einvernehmen mit einem Dritten seine Arbeitnehmer anweist, sich der Überwachung durch eine bei diesem bestehende technische Überwachungseinrichtung zu unterwerfen. Für das Mitbestimmungsrecht ist es ohne Bedeutung, ob die Überwachung in erster Linie oder gar ausschließlich im Interesse des Dritten erfolgt. Es wird durch die Entscheidung des jeweiligen Arbeitgebers ausgelöst, Informationen über das Verhalten der seiner Direktionsbefugnis unterliegenden Arbeitnehmer durch eine zur Überwachung bestimmte technische Einrichtung eines Dritten erfassen zu lassen. Gegenstand des Beteiligungsrechts aus § 87 Abs. 1 Nr. 6 BetrVG ist dann, ob überhaupt sowie ggf. nach welchen Grundsätzen welche Arbeitnehmer für welche Dauer sich der bei dem Dritten installierten Überwachungseinrichtung unterziehen müssen (vgl. BAG 27. Januar 2004 – 1 ABR 7/03 – zu B II 1 a bb und B II 1 c aa der Gründe, BAGE 109, 235). Für konzernverbundene Unternehmen gilt dies gleichermaßen.

(b) Danach können die Betriebsparteien der konzernangehörigen Unternehmen, deren Arbeitnehmer im Rahmen ihres gewöhnlichen Betriebsablaufs in dem von den Kameras überwachten Bereich des Klinikums eingesetzt sind, nicht die Bedingungen über den Einsatz und Betrieb der visuellen Aufzeichnungsanlage im Klinikum festlegen. Ihre Regelungsbefugnis ist auf Fragen des Zutritts der von ihnen vertretenen Arbeitnehmer in den von Kameras überwachten Bereich des Klinikums beschränkt. Entgegen der Auffassung des Beschwerdegerichts schließt eine etwaige Vorgreiflichkeit der bei der BB bestehenden Regelungen über die visuelle Aufzeichnungsanlage die Ausübung der Mitbestimmung in den anderen Konzernunternehmen nicht aus. Nach der Senatsrechtsprechung ist es Sache des entsendenden Arbeitsgebers dafür zu sorgen, dass der Betriebsrat sein Mitbestimmungsrecht auch bei einem Einsatz von Belegschaftsangehörigen in Betrieben von anderen Unternehmen wahrnehmen kann (BAG 27. Januar 2004 – 1 ABR 7/03 – zu B II 1 c bb der Gründe, BAGE 109, 235). Für die Zuständigkeit der zur Ausübung des Mitbestimmungsrechts aus § 87 Abs. 1 Nr. 6 BetrVG berufenen Arbeitnehmervertretung ist es auch ohne Belang, ob es sinnvoll wäre, das bei der zu 8. beteiligten Arbeitgeberin eingesetzte visuelle Aufzeichnungssystem durch eine Betriebsvereinbarung für alle betroffenen Arbeitnehmer in den konzernangehörigen Unternehmen einheitlich auszugestalten. Solche Zweckmäßigkeitserwägungen vermögen eine Verlagerung der Regelungsbefugnis von den originär zuständigen Betriebsräten für die von ihnen vertretenen Arbeitnehmer auf den Konzernbetriebsrat nicht zu begründen.

Nutzung einer Domain-Adresse mit dem Namensbestandteil des Arbeitgebers durch einen Arbeitnehmer (Ls)

(**Bundesarbeitsgericht,** Urteil vom 9. September 2015 – 7 AZR 668/13 –)

1. **Eine Verletzung des Namensrechts des Arbeitgebers in Form der Namensanmaßung liegt nicht vor, wenn ein Arbeitnehmer eine Domain-Adresse mit dem Namen des Arbeitgebers nebst dem Zusatz br verwendet und dadurch eine Namensverwechselung ausschließt.**
2. **Gleichermaßen wird nicht die sich aus § 241 Abs. 2 BGB ergebende Pflicht zur Rücksichtnahme auf die Rechte, Rechtsgüter und Interessen des Arbeitgebers verletzt.**
3. **Die Nutzung der Domain „xxx-br" als solche verstößt auch nicht gegen das Bundesdatenschutzgesetz. Die auf der Homepage ggf. verarbeiteten personenbezogenen Daten waren nicht Gegenstand des Verfahrens.**

(Nicht amtliche Leitsätze)

Zur Datenübermittlung nach § 28a BDSG

(**Oberlandesgericht Frankfurt,** Beschluss vom 2. Februar 2016 – 1 W 9/16 –)

§ 28 a Abs. 1 Nr. 5 BDSG erlaubt eine Übermittlung des Kündigungssachverhalts an eine Auskunftei, auch wenn der Schuldner die Zahlungsumstände bestreitet; es genügt, dass die Kündigungsvoraussetzungen bestehen und dem Schuldner die Übermittlung angekündigt wird.

Aus den Gründen:

Die sofortige Beschwerde des Klägers ist unbegründet. Das Landgericht hat mit Recht entschieden, dass die Kosten des Rechtsstreits – ohne die durch die Säumnis der Beklagten entstandenen Kosten – gegeneinander aufgehoben werden.

Diese Kostenverteilung entspricht billigem Ermessen, weil der Erfolg der Klage bei summarischer Betrachtung vom Ergebnis einer Beweisaufnahme abhing, die infolge der übereinstimmenden Erledigungserklärungen nicht mehr durchgeführt wurde. Dass die Beklagte die geforderte Unterlassungserklärung abgegeben hat, rechtfertigt es nicht, ihr die Kosten aufzuerlegen, weil die Abgabe der Erklärung angesichts des begleitenden Vortrags, dies erfolge ohne Anerkennung einer Rechtspflicht, nicht so verstanden werden kann, dass die Beklagte sich in die Rolle des Verlierers des Rechtsstreits begeben hat.

Dass der Kläger bestritten hat, Vertragspartner des Darlehensvertrages zu sein, und darüber hinaus in Abrede gestellt hat, dass Rückstände bestehen, reicht entgegen der Ansicht des Klägers noch nicht hin, um der Beklagten die Befugnis abzusprechen, der Schufa die Kündigung des Kreditvertrags aus wichtigem Grund wegen rückständiger Zahlungen zu melden. § 28a Abs. 1 Nr. 5 BDSG setzt nach überwiegender und zutreffender Ansicht nur voraus, dass die Kündigung objektiv mit Recht erfolgt; dass der Schuldner Zahlungsrückstände nicht bestreitet, ist dagegen, anders als in den Fällen des § 28a Abs. 1 Nr. 2-4 BDSG, keine formale Voraussetzung für die Übermittlung schuldner- und forderungsbezogener Daten an eine Auskunftei (Simitis-Ehmann, BDSG, 7. Aufl., § 28a Rn. 69 ff.; Däubler-Weichert, BDSG, 4. Aufl., § 28a Rn. 10; Gola/Schomerus, BDSG, 12. Aufl., § 28a Rn. 10; AG Frankfurt, U. v. 27.2.2013, Az. 31 C 1001/12). Das ergibt sich bereits daraus, dass § 28a Abs. 1 Nr. 5 BDSG praktisch keinen Anwendungsfall hätte, wenn es für seine Anwendung zusätzlich darauf ankäme, dass der Schuldner die zur Kündigung berechtigenden Zahlungsrückstände oder die Vertragsbeziehung nicht bestreitet. Die Regelung stärkt die Position von Gläubigern eines Dauerschuldverhältnisses, in dem regelmäßig wiederkehrende Zahlungen zu leisten sind. Dieser der Gesetzesformulierung zu entnehmende Zweck, der auch der amtlichen Begründung zu entnehmen ist (BT-DrS 16/10529, 14), kann nicht durch eine teleologische Reduktion oder individuelle Interessenabwägung (so aber Wolff/Brink/Kamp, Datenschutzrecht, 2013, § 28a BDSG Rn. 111 mit Hinweis auf LG Verden BeckRS 2011, 13582) aufgehoben werden. Auch in den Fällen des § 28 Abs. 1 Nr. 5 BDSG ergibt sich das berechtigte Interesse des Übermittelnden aus seiner Beteiligung an dem von der Auskunftei unterhaltenen Warnsystem. Die berechtigten Interessen des Schuldners werden hier dadurch gewahrt, dass der Gläubiger die bevorstehende Übermittlung ankündigen muss und der Schuldner dadurch Gelegenheit erhält, entweder die Rückstände noch auszugleichen oder gegen die beabsichtigte Übermittlung mittels einstweiligen Rechtsschutzes vorzugehen und dabei die Einwände gegen die aus Schuldnersicht nicht bestehenden Zahlungsrückstände geltend zu machen. Im Übrigen setzt sich der Gläubiger, der schuldhaft eine Übermittlung vornimmt, für die objektiv die Voraussetzungen des § 28a Abs. 1 Nr. 5 BDSG nicht vorliegen, Schadensersatzansprüchen aus.

Wettbewerbswidrigkeit des Facebook Like-Buttons auf einer Firmenwebsite*

(**Landgericht Düsseldorf,** Urteil vom 9. März 2016 – 12 O 51/15 –)

Es ist wettbewerbswidrig, wenn der Facebook Like-Button auf der Firmenwebsite integriert wird,

1. **ohne die Nutzer der Internetseite bis zu dem Zeitpunkt, in dem der Anbieter des Plugins beginnt, Zugriff auf die IP-Adresse und den Browserstring des Nutzers zu nehmen, ausdrücklich und unübersehbar über den Zweck der Erhebung und der Verwendung der so übermittelten Daten aufzuklären,**

und/oder

2. **ohne die Einwilligung der Nutzer der Internetseite zu dem Zugriff auf die IP-Adresse und den Browserstring durch den Plugin-Anbieter und zu der Datenverwendung einzuholen, jeweils bevor der Zugriff erfolgt,**

und/oder

3. **ohne die Nutzer, die ihre Einwilligung im Sinne des Klageantrags zu 2 erteilt haben, über deren jederzeitige Widerruflichkeit mit Wirkung für die Zukunft zu informieren.**

(Nicht amtliche Leitsätze)

Aus den Gründen:

Die Klage ist überwiegend begründet. Der Kläger kann als qualifizierte Einrichtung im Sinne von § 4 Abs. 1 Nr. 1 UKlaG gemäß § 8 Abs. 3 Nr. 3 UWG von der Beklagten Unterlassung der Einbindung des G1-Plugins „Gefällt mir" verlangen, sofern nicht die in den Klageanträgen zu 1.-3. genannten Voraussetzungen erfüllt werden.

I. Die Nutzung des G1-Plugins „Gefällt mir" auf der Webseite der Beklagten, ohne dass die Beklagte die Nutzer der Internetseite vor der Übermittlung deren IP-Adresse und Browserstring an G1 über diesen Umstand aufklärt, ist unlauter im Sinne des § 3a UWG i. V.m. § 13 TMG.

Nach § 13 Abs. 1 Satz 1 TMG hat der Betreiber eines Telemediendienstes den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs des EWR in allgemein verständlicher Form zu unterrichten. Dieser Pflicht ist

* Mit nachfolgender Urteilsanmerkung von Eva Beyvers

die Beklagte hinsichtlich ihrer Internetseite in dem Stand, der der gerichtlichen Beurteilung unterliegt, nicht nachgekommen.

1. Bereits mit dem Besuch der Webseite der Beklagten werden Nutzungsdaten, also Daten, die erforderlich sind, um eine Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (§ 15 Abs. 1 S. 1 TMG), erhoben. Zu solchen gehören nämlich auch Merkmale zur Identifikation des Nutzers, wie dessen IP-Adresse (vgl. Föhlisch/Pilou, a.a. O., S. 632).

Die Daten sind personenbezogen. Es handelt sich um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, § 3 Abs. 1 BDSG. Eine Einzelangabe im vorgenannten Sinn ist jede Information, die sich auf eine bestimmte, einzelne Person bezieht oder geeignet ist, einen Bezug zu ihr herzustellen.

Nutzer der Beklagtenseite, die bei deren Aufruf auf G1 eingeloggt sind, können mittels der IP-Adresse direkt ihrem G1-Konto zugeordnet werden, so dass für diese Gruppe ein Personenbezug gegeben ist. Auch bei G1-Nutzern, die sich zwar ausloggen, jedoch nicht ihre Cookies löschen, kann mittels gesetzter Cookies eine Zuordnung erfolgen. Das diesbezügliche Bestreiten der Beklagten mit Nichtwissen reicht im Hinblick auf den durch Vorlage einer gutachtlichen Bewertung (Anl. K2) substantiierten Vortrag des Klägers und die im juristischen Schrifttum insoweit eindeutig beschriebene Funktionsweise des Plugins unter Nutzung von Cookies (vgl. Föhlisch/Pilous, a.a. O., Schweda, ZD-Aktuell 2015, 04659; Hupperz/Ohrmann CR 2011, 449, 454; Ernst NJOZ 2010, 1917) nicht aus, um der Darlegung der beschriebenen Funktionsweise wirksam entgegenzutreten. G1 verfügt mit seinen Millionen aktiven Nutzern zudem über ein erhebliches Sonderwissen, das die Betreiber mit den gewonnenen Daten verknüpfen kann.

Die Kammer kann vor vorgenanntem Hintergrund offenlassen, ob gleiches auch für Besucher ohne G1-Konto und nicht eingeloggte Nutzer mit gelöschter Chronik gilt. In der Literatur wird diesbezüglich darauf hingewiesen, dass in diesem Fall über das Plugin Cookies gesetzt würden und dass, wenn ein Webseitenbesucher im Nachgang ein G1-Konto erstellt, ebenfalls ein Personenbezug hergestellt werden könne (vgl. Föhlisch/Pilous MMR 2015, 631 m.w. N.). Aber auch, soweit dies nicht festgestellt werden kann, ist ausweislich der Vorlage des Bundesgerichtshofs an den EuGH zu dieser Frage (BGH GRUR 2015, 192) zumindest naheliegend, dass der vor allem von Datenschutzbehörden vertretenen Theorie des absoluten Personenbezugs (vgl. Voigt/Alich NJW 2011, 3541) zu folgen ist und bereits die Übermittlung von IP-Adressen die Übermittlung personenbezogener Daten darstellt (so auch: KG Berlin BeckRS 2011, 10432).

2.Es handelt sich bei der Beklagten um die verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG.

Die datenschutzrechtliche Verantwortlichkeit nach dem TMG bestimmt sich allein nach § 3 Abs. 7 BDSG (Föhlisch/Pilous a.a. O.). Verantwortliche Stelle i. S.d. § 3 Abs. 7 BDSG ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Die Regelung geht auf Art. 2 d) der RL 95/46/EG (DS-RL) zurück, nach dem „für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle ist, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Begriff der Verantwortlichkeit ist weit zu verstehen (EuGH MMR 2014, 445). Er erfasst jede Stelle, die personenbezogene Daten über Dritte erhebt, verarbeitet oder verarbeiten lässt. Die Erhebung besteht in einem Beschaffen von Daten, § 3 Abs. 3 BDSG.

Während die Anbieterin des Plugins ohne Zweifel die Daten verarbeitet, beschafft die Beklagte diese im vorgenannten Sinne. Durch das Einbinden des Plugins ermöglicht sie die Datenerhebung und spätere Verwendung der Daten durch G1. Sie könnte durch ein Entfernen des Buttons den Zugriff von vorneherein verhindern bzw. durch eine vorgeschaltete Abfrage bei den Nutzern, ob die Funktionalität aktiviert werden soll, den Zugriff auf die Daten und hierdurch deren Verwendung einschränken. Bei der Beklagten handelt es sich nicht um eine Auftragnehmerin von G1, sondern sie wirkt durch die Einbindung des Plugins unmittelbar an der Erhebung durch G1 mit. Ihre Entscheidung und die technische Implementierung sorgen dafür, dass die Erhebung und die Verarbeitung stattfinden. Die Integration des Plugins ist nicht nur Vorbereitungshandlung für den Erhebungsprozess, sondern nimmt seinen Beginn damit, dass die Beklagte über ihren Server einen HTML-Code aussenden lässt, der den Browser des Nutzers zur Mitteilung seiner Daten an G1 veranlasst. Die Aussendung des HTML-Codes ist damit erster Teilakt des Abrufs des „Gefällt mir"-Buttons und der darin liegenden Funktionalität. Die Erhebung der Daten zu deren Verwendung findet damit im eigenen Tätigkeits-und Haftungsbereich der Beklagten statt.

Allein, dass die Beklagte keinen direkten Einfluss auf die Funktionsweise des Buttons und die Verarbeitung der Daten hat, ihr deren Umfang sogar unbekannt sein mag, und dass sich ihre aktive Tätigkeit auf die Einbindung des Plugins erschöpft, steht dem ebenso wenig entgegen, wie die Tatsache, dass nicht die Beklagte an sie übermittelte und in ihrem Besitz stehende Daten an G1 weiterleitet, sondern die Erfassung der IP-Adresse unmittelbar durch G1 erfolgt (so aber ohne nähere Begründung: Voigt/Alich NJW 2011, 3541; Piltz CR 2011, 657 mit dem Argument, es erscheine „nicht angebracht", den Webseitenbetreiber als verantwortliche Stelle einzusehen, da er keine Verfügungsgewalt über die Daten erlange). Denn der Vorgang wird durch den HTML-Befehl auf der Beklagtenseite initiiert. Die Eigenschaft als verantwortliche Stelle ist nicht streng an den Besitz der Daten und die physische Herrschaft über den Verarbeitungsprozess gebunden. Löst ein Webseitenbetreiber durch die Einbindung von Drittinhalten in das eigene Angebot einen Verarbeitungsprozess aus, ist er hierfür auch datenschutzrechtlich verantwortlich. Denn allein durch konkrete Gestaltung der Webseite wird die Datenweitergabe an G1 und damit die Datennutzung initiiert (so auch: KG Berlin BeckRS 2011,10432; Föhlisch/Pilou, a.a. O.; Ernst NJOZ 2010,1917).

3. Die Datenübermittlung ist nicht nach § 15 TMG gerechtfertigt, da sie für das Funktionieren und den Betrieb der Webseite der Beklagten nicht erforderlich ist.

Der Begriff der Erforderlichkeit impliziert ein enges Verständnis des Umfangs der Ausnahmeregel. Der „Gefällt mir"-Button ist für den Betrieb der Seite der Beklagten nicht unabdinglich. Vielmehr ist sie, wie jede Webseite, auch ohne Social Plugins zu betreiben und für die Nutzer aufzurufen. Eine große Verbreitung der Plugins oder Vorteile für die Beklagte auf Grund eines Marketing-Effekts führen nicht dazu, dass diese das Plugin in der beanstandeten Weise zwingend einzusetzen hätte.

Entgegen der Auffassung der Beklagten bedeutet ein solches Verständnis kein Verbot der Einbindung externer Dienste in eine Webseite, und dem Verbotstenor kommt keine zensurähnliche, grundrechtseinschränkende Wirkung zu. Denn die Einbin-

dung von Drittinhalten, wie sie im Web 2.0 häufig anzutreffen ist, wird durch diesen keineswegs unmöglich gemacht. Das vom Gericht ausgesprochene Verbot gilt vielmehr nur für den Einzelfall, der nach technischer Funktionsweise, dem Zweck der Datenerhebung und durch die bestimmte geschäftliche Natur der Beklagtenseite bestimmt ist. Will die Beklagte weiterhin die Vorteile einer Verknüpfung mit G1 nutzen, so muss sie lediglich die Rechte derer, die eine Drittweitergabe ihrer Daten weder erwarten, noch wünschen, angemessen beachten, etwa durch das von ihr nunmehr auch angewendete sog. „2 Klick-Verfahren", bei dem der Datenweiterleitung eine Einverständnisabfrage vorgeschaltet ist. Es wird der Beklagten hiernach nicht unmöglich gemacht, Drittinhalte einzubinden. Die Beklagte hat zu dem nicht einmal vorgetragen, in welcher Weise die Einbindung genau in der beanstandeten Form wirtschaftlich notwendig ist, um ihr Angebot im Internet vorzuhalten oder eine auf der Verkaufsseite geäußerte Meinung (stärker) zu verbreiten.

4. Die Datennutzung kann sich auch nicht auf eine Einwilligung aller Besucher der Seite der Beklagten stützen.

Personenbezogene Daten dürfen zur Bereitstellung von Telemedien nur erhoben und verwendet werden, sofern das TMG oder eine andere telemedienrechtliche Vorschrift dies erlauben oder der Nutzer eingewilligt hat. § 12 Abs. 1 TMG wiederholt damit das in § 4 Abs. 1 BDSG erhaltene Datenverarbeitungsverbot mit Erlaubnisvorbehalt für Telemedien. Eine elektronische Einwilligung ist zulässig, sofern sie die Voraussetzungen des § 13 Abs. 2 TMG erfüllt. Danach ist u.a. sicherzustellen, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat. Dies setzt eine aktive Handlung des Nutzers, wie etwa das Setzen des Häkchens in einer Checkbox, voraus (zum Ganzen: Föhlisch/Pilous a.a. O. m.w. N.). Eine Einwilligung ist zudem nur zulässig, wenn sie auf der freien Entscheidung des Betroffenen beruht. Weiter ist er auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie ggf. auf die Folgen der Verweigerung der Einwilligung hinzuweisen (§ 4a Abs. 1 BDSG). Dies bedeutet, dass eine Einwilligung freiwillig und informiert zu erfolgen hat. Die Einwilligung muss der Datenverarbeitung vorangehen und darf nicht erst nachträglich eingeholt werden. Die Einwilligung wiederum verlangt, dass der Nutzer über die Weitergabe seiner Daten vorher unterrichtet wird (vgl. OLG Düsseldorf K&R 2004, 591, 593).

Dass die Besucher der Beklagtenwebseite in diesem Sinne in die Datenübermittlung an G1 eingewilligt haben, behauptet die Beklagte nicht. Bevor das Plugin auf der Webseite der Beklagten erschien und die Datenweitergabe erfolgte, war durch die Besucher nichts diesbezügliches zu erklären oder anzuklicken. Auch hinsichtlich der Nutzer, die ein G1konto im Wissen um die Datenschutzrichtlinie von G1 angelegt haben, ergibt sich aus dem Beklagtenvortrag nicht, dass diese um die Nutzung auf der Seite der Beklagten konkret wussten oder sich einverstanden erklärten. Die Belehrung über Plugins an sich genügt hierfür nicht.

5. Eine Unterrichtung sah die Internetseite der Beklagten nicht vor, und zwar weder vor einer Weiterleitung von Daten an G1, noch während des Beginns des Nutzungsvorgangs. Der bloße Link zu einer Datenschutzerklärung in der Fußzeile der Webseite stellt keinen Hinweis zu Beginn bzw. vor Einleitung des Verarbeitungsvorgangs dar. Die von der Beklagten diesbezüglich aufgeführten Rechtsprechungsfundstellen befassen sich allein mit der jederzeitigen Abrufbarkeit der Belehrung, nicht aber mit dem Zeitpunkt in dem diese zu erfolgen hat.

6. Es handelt sich bei den §§ 12, 13 TMG, die Umstände des Einzelfalls berücksichtigend (vgl. Köhler/Bornkamm, UWG. 34. Aufl., § 3a, Rn. 1.74), nicht nur um Verbraucherschutzgesetze nach § 2 Nr. 11 UKlaG (in der Fassung vom 24.02.2016), sondern auch um Marktverhaltensregeln im Sinne des § 3 a UWG. Gesetze, die die Erhebung von Daten betreffen, schützen im Einzelfall nicht nur das Persönlichkeitsrecht und das informationelle Selbstbestimmungsrecht, sondern auch den Wettbewerb an sich (vgl. etwa die Entscheidungen des OLG Hamburg vom 27.06.2013, Az. 3 U 26/12, OLG Köln vom 19.11.2010, Az. 6 U 73/10; OLG Karlsruhe vom 09.05.2012, Az. 6 U 38/11 und des KG Berlin vom 24.01.2014, Az. 5 U 42/12; ferner: Huppertz/Ohrmann, CR 2011, 449), und es ist zu berücksichtigen, dass die zunehmende wirtschaftliche Bedeutung der Erhebung elektronischer Daten diese nicht nur als Wirtschaftsgut erscheinen lässt, sondern auch die Entwicklung des Verständnisses des Datenschutzrechts beeinflusst.

Das eingesetzte Plugin dient (auch) dem Absatz und der Werbung der Beklagten. Dem konkreten Verstoß kommt so auch wettbewerbliche Relevanz zu. Die Nutzer der Beklagtenwebseite sind nicht nur in ihrem Schutz vor unerwünschter Werbung betroffen (a. A. KG BeckRS 2011, 10432; LG Frankfurt BeckRS 2004, 22875), sondern die Einbindung des Plugins beeinflusst deren kommerzielles Verhalten bezogen auf das auf der Seite angebotene Warenangebot. Den Webseitenbesuchern wird vermittelt, wie vielen G1-Mitgliedern die Seite und damit mittelbar auch die angebotenen Waren der Beklagten gefallen; ihnen wird die Möglichkeit gegeben, zu dem Kreis dieser ihnen teilweise bekannten Personen zu gehören; beides kann die Kaufentscheidung eines Webseitenbesuchers beeinflussen. Auch nicht-angemeldete Nutzer von G1 erhalten die Zahl der „Likes" angezeigt und werden zumindest mittelbar durch das eingebettete Tool, das die Datenerhebung ermöglicht, in ihrem Marktverhalten beeinflusst (vgl. Duchrow, MMR aktuell 2001, 320091).

7. Hinsichtlich der Rechtsverletzung indiziert die Begehung durch die Beklagte die Wiederholungsgefahr. Soweit die Beklagte ihren Webauftritt nunmehr auf die sog. „2-Klick-Lösung" umgestellt hat, braucht die Kammer nicht zu bewerten, ob diese den gesetzlichen Anforderungen genügt. Denn der Unterlassungsanspruch gründet auf der vorherigen Art der Einbindung des Plugins und dem Umstand, dass die Beklagte diesbezüglich keine strafbewehrte Unterlassungserklärung abgegeben hat. Allein, dass bislang keine höchstrichterliche Rechtsprechung zu dem konkreten Plugin besteht und die Instanzrechtsprechung in der Bewertung uneinheitlich ist, lässt die Wiederholungsgefahr nicht entfallen. Ohnehin setzt der Unterlassungsanspruch kein Verschulden voraus, besteht also auch im Falle eines Rechtsirrtums.

Urteilsanmerkung zu Landgericht Düsseldorf vom 09.03.2016 – 12 O 51/15 –

Like-Button – gefällt dem LG Düsseldorf nicht?

Aktuelle Rechtsfragen des Datenschutzrechts und Wettbewerbsrechts rund um die Entscheidung zu sozialen Plugins

Mit dem Aufkommen sozialer Medien hat auch die Einbindung von Drittinhalten in Webseiten deutlich zugenommen. Insbesondere die Betreiber sozialer Online-Plattformen stellen HTML-Codes und entsprechende Anleitungen kostenlos zur

Verfügung, mit denen es möglich wird, sozial verknüpfte Inhalte dieser Anbieter in Webseiten zu integrieren. Bekannt sind diese externen Elemente unter dem Oberbegriff „soziale Plugins". Kontrovers diskutiert wird seither aber die datenschutzrechtliche und auch wettbewerbsrechtliche Beurteilung dieser Erscheinung. Dabei stellte sich insbesondere die Frage, ob Webseitenbetreiber eine datenschutzrechtliche (Mit-)Verantwortung für die mit dem Plugin in Zusammenhang stehenden Datenverarbeitungen haben. Das LG Düsseldorf hat nun in dieser Frage erstmals ausdrücklich entschieden: Ja, Seitenbetreiber sind für Datenverarbeitungen im Zusammenhang mit Social Plugins datenschutzrechtlich verantwortlich. Neben der Verantwortlichkeit berührt das Urteil jedoch noch weitere Grundsatzfragen des Datenschutz- und Wettbewerbsrechts. Der vorliegende Beitrag geht offenen Fragen nach und befasst sich näher mit der jeweiligen Argumentation des Gerichts.

I. Sachverhalt und Entscheidung im Überblick

Das LG Düsseldorf hatte auf Antrag der Verbraucherzentrale NRW zu entscheiden, ob der Betreiber eines Online-Shops (im Folgenden: Seitenbetreiber) es wegen Wettbewerbswidrigkeit zu unterlassen hatte, auf seiner Internetseite ein Plugin des sozialen Netzwerks Facebook[1] (im Folgenden: Facebook) einzubinden ohne die Nutzer ausreichend über im Zusammenhang mit dem Plugin stattfindende Datenverarbeitungen zu informieren bzw. ohne eine Einwilligung der Nutzer hinsichtlich dieser Datenverarbeitungen einzuholen und die Nutzer über die Widerruflichkeit dieser Einwilligung aufzuklären. Die Verbraucherzentrale hatte den Seitenbetreiber zuvor wegen eines Verstoßes gegen das Wettbewerbs- und Telemedienrecht abgemahnt und die Abgabe einer strafbewehrten Unterlassungserklärung verlangt.[2]

Das LG Düsseldorf[3] setzt sich zunächst detailliert mit den technischen Hintergründen auseinander und erörtert akkurat die technischen Spezifika der Einbindung des Plugins und die Datenübertragungsprozesse, die bei dessen Nutzung stattfinden. Auf der Grundlage dieser Erkenntnisse kommt das Gericht zu dem Schluss, dass die Verwendung des Plugins durch den Seitenbetreiber unlauter im Sinne des § 3a UWG i.V.m. §§ 12, 13 TMG[4] gewesen sei. Es handle sich bei dem Seitenbetreiber um eine verantwortliche Stelle im Sinne von § 3 Abs. 7 BDSG[5], weshalb er für die stattfindende Verarbeitung personenbezogener Daten rechtlich einstehen müsse. Die Verarbeitung sei nicht im Rahmen des von § 12 Abs. 1 TMG proklamierten Verbots mit Erlaubnisvorbehalt auf der Grundlage von § 15 TMG oder durch eine Einwilligung gemäß §§ 4a BDSG, 13 Abs. 2 TMG gerechtfertigt gewesen. Zudem habe der Seitenbetreiber die Nutzer nicht den Anforderungen von § 13 Abs. 1 TMG entsprechend zu Beginn des Nutzungsvorgangs über die von dem Plugin initiierten Datenverarbeitungsvorgänge unterrichtet. Die §§ 12 und 13 TMG stellten unter Berücksichtigung der Umstände des Einzelfalles Marktverhaltensregeln im Sinne von § 3a UWG[6] dar, da nicht nur das informationelle Selbstbestimmungsrecht und die Persönlichkeit des Betroffenen, sondern der Wettbewerb als solches durch die Bestimmungen geschützt würden. Die erforderliche konkrete wettbewerbsrechtliche Relevanz begründete das Gericht damit, dass das Plugin unter anderem den Werbe- und Absatzzwecken der Beklagten gedient habe. Die vom Seitenbetreiber gelieferte unvollständige Unterrichtung könne zwar sogar den falschen Eindruck erwecken, das bloße Ausloggen aus dem Netzwerk von Facebook könne eine Datenübertragung durch das streitige Plugin an Facebook gänzlich verhindern. Darin liegt aber nach Ansicht des LG Düsseldorf keine Täuschung oder Irreführung i.S.v. § 5 Abs. 1 Satz 2 Nr. 1 oder Nr. 7 UWG.

II. Datenschutzrechtliche Aspekte des Urteils

1. Personenbezug von im Zusammenhang mit dem Plugin verarbeiteten Daten

Das LG Düsseldorf folgt ganz eindeutig einem absoluten (auch: objektiven) Ansatz des Personenbezugs, d.h. es geht schon dann von einer Bestimmbarkeit des Betroffenen und damit vom Vorhandensein personenbezogener Daten aus, wenn theoretisch nicht vollkommen ausgeschlossen ist, dass der Verantwortliche oder ein Dritter den Bezug herstellen können.[7] Mit anderen Worten hält das Gericht es also nicht für erforderlich, dass die verantwortliche Stelle selbst Zusatzinformationen besitzt, die eine Zuordnung von Daten zu Betroffenen ermöglicht, sondern lässt es ausreichen, dass ein Dritter solche Informationen besitzt – unabhängig davon, ob tatsächlich die Möglichkeit oder das Risiko besteht, dass der Datenverarbeiter die Zusatzinformationen des Dritten zur Identifizierung Betroffener verwendet. Dazu bekennt es sich ausdrücklich im Rahmen der Erörterung eines Personenbezugs der von dem Plugin übermittelten Daten in Bezug auf nicht bei Facebook eingeloggte und nicht bei Facebook registrierte Nutzer des Online-Shops der Beklagten. Das Gericht hält für diese einen Personenbezug schon deshalb für herstellbar, weil IP-Adressen schon allein aufgrund der Identifizierbarkeit des Betroffenen durch den Zugangsanbieter personenbezogene Daten darstellen.[8]

Es verweist diesbezüglich auf das derzeit vor dem EuGH anhängige Vorlageverfahren,[9] das die Personenbezogenheit

1 Betreiber des sozialen Netzwerks in Europa ist die Facebook Ireland Ltd; das Netzwerk ist erreichbar unter: https://de-de.facebook.com (Stand: 01.04.2016).

2 Mitteilung der Verbraucherzentrale NRW zu den Abmahnungen abrufbar unter: http://www.verbraucherzentrale.nrw/likebutton (Stand: 04.04.2016). Vgl. auch näher zum Ablauf des Verfahrens: Meyer, MMR-Aktuell 2016, 376765.

3 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15. Die nachfolgenden Ausführungen dieses Absatzes beziehen sich sämtlich auf das genannte Urteil.

4 Telemediengesetz v. 26.02.2007 (BGBl. I, S. 179), zuletzt geändert durch Art. 4 des Gesetzes v. 17.07.2015 (BGBl. I, S. 1324).

5 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung v. 14.01.2003 (BGBl. I, S. 66), zuletzt geändert durch Art. 1 des Gesetzes v. 25.02.2015 (BGBl. I, S. 162).

6 Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung v. 03.03.2010 (BGBl. I, S. 254), zuletzt geändert durch Art. 4 des Gesetzes v. 17.02.2016 (BGBl. I S. 233).

7 Zur Definition des objektiven Ansatzes (im Ergebnis allerdings einer relativen, am tatsächlichen Risiko der Identifizierung orientierten Lösung zugeneigt): Dammann, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl. 2014, § 3 BDSG Rn. 23.

8 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

9 Rechtssache „Breyer", Az.: C-582/14.

von IP-Adressen klären soll.[10] Der EuGH hat allerdings in diesem Verfahren noch nicht entschieden, weshalb der Verweis als Nachweis für eine Klärung des bislang heftig geführten Meinungsstreits über die Voraussetzungen der Personenbeziehbarkeit, insbesondere im Zusammenhang mit dynamischen IP-Adressen,[11] nicht taugt. Ein früheres Urteil des EuGH, das im Ergebnis die Personenbezogenheit von IP-Adressen bejahte,[12] kann auf den vorliegenden Fall nicht vorbehaltlos übertragen werden, weil im dortigen Sachverhalt der Datenverarbeiter selbst Zugangsanbieter war und somit Zugriff auf eine Identifikation der Nutzer ermöglichende Zusatzinformationen hatte, die dem Seitenbetreiber im vorliegenden Fall nicht ohne weiteres zur Verfügung standen. Die EU-Kommission empfiehlt in einem in dem noch anhängigen Vorlageverfahren eingereichten Schriftsatz dennoch, dynamische IP-Adressen auch dann als personenbezogene Daten im Sinne von Art. 2 lit. a der RL 95/46/EG[13] zu behandeln, wenn eine tatsächliche Identifizierung für einen Diensteanbieter nur mithilfe von Zusatzinformationen möglich ist, die ein Dritter, in dem Fall der Zugangsanbieter, besitzt.[14]

a. Personenbezug und konkrete Gefährdung der Betroffenenrechte

Für diese weite Auslegung scheint auf den ersten Blick jedenfalls der Wortlaut von Art. 2 lit. a der RL 95/46/EG[15] zu sprechen, der für einen Personenbezug lediglich voraussetzt, dass eine Person „direkt oder indirekt identifiziert werden kann", nicht aber vorschreibt, ob diese Identifikation durch den Verantwortlichen selbst oder aber durch Dritte vorgenommen werden können muss. Erwägungsgrund 25 der RL 95/46/EG nennt stattdessen sowohl den Verantwortlichen als auch Dritte, will aber nur solche Mittel der Identifizierung bei der Beurteilung berücksichtigen, die „vernünftigerweise [...] eingesetzt werden könnten". Aus dieser letzten Formulierung geht hervor, dass eine völlig abstrakte, nur in der Theorie bestehende Gefährdung nicht ausreichen soll, um einen Personenbezug zu begründen.[16] Vielmehr kommt es darauf an, ob nach den Erwägungen der Vernunft damit zu rechnen ist, dass ein Personenbezug im konkreten Zusammenhang (gegebenenfalls unter der Mitwirkung Dritter) herstellbar ist, ob also eine einigermaßen konkrete Gefährdung der Persönlichkeitsrechte des Betroffenen im jeweiligen Zusammenhang unter Berücksichtigung der tatsächlichen äußeren Umstände besteht. Die Art. 29-Datenschutgruppe nennt als relevante „Kontextfaktoren" u.a. die Kosten der Identifizierung, den mit der Datenverarbeitung verfolgten Zweck, die Interessen der Beteiligten und die nach dem jeweiligen Stand der Technik zur Verfügung stehenden Möglichkeiten.[17]

b. Konkrete Gefährdung im Verhältnis zwischen Diensteanbietern und Facebook bei der Verwendung von Social Plugins

Diese Überlegungen scheinen auf den ersten Blick für das Ergebnis des LG nicht relevant zu sein, macht es doch die Ausführungen zur absoluten Theorie des Personenbezugs lediglich ergänzend, nachdem es einen Personenbezug jedenfalls für die zu eingeloggten Facebook-Nutzern gehörigen Daten festgestellt hat.[18] Bei genauerem Hinsehen offenbart sich dort aber eine Unregelmäßigkeit in der Argumentation, denn auch bei den eingeloggten Facebook-Nutzern ist es in aller Regel nicht der Seitenbetreiber, der den Personenbezug herstellen kann, sondern allein Facebook besitzt das entsprechend nötige Zusatzwissen. Damit stellt sich in dieser Konstellation im Grunde dieselbe Frage: Rechtfertigt das Verhältnis zwischen Facebook und dem Seitenbetreiber die Annahme, dass im Rahmen eines vernünftigen Einsatzes der zur Verfügung stehenden Mittel die im Zusammenhang mit dem sozialen Plugin verarbeiteten Daten mit einer natürlichen Person in Verbindung gebracht werden?

Anders als im Verhältnis zwischen Diensteanbietern und Zugangsprovidern muss die Antwort in diesem Fall aber eindeutig positiv ausfallen: Die Kooperation zwischen Seitenbetreibern und Facebook dient ja gerade dazu, sozial verknüpften, also individualisierten, auf den jeweiligen Nutzer zugeschnittenen Inhalt zur Verfügung zu stellen. Dem Seitenbetreiber wird es auf diese Weise möglich, seine Seite inhaltlich aufzuwerten, während Facebook die gewonnenen Daten zur kostenlosen Bereitstellung sozialer Netzwerkdienste und zur Finanzierung selbiger durch Werbemaßnahmen nutzt. Anders als der Zugangsprovider kooperiert Facebook also im Rahmen des Plugins mit dem Seitenbetreiber zu dem ausdrücklichen Zweck, einen Personenbezug für eingeloggte Mitglieder herzustellen, um diese Information zur Bereitstellung weiterer Dienste zu nutzen. Die Art. 29-Datenschutzgruppe formuliert schlüssig: „Das Argument, dass Personen nicht bestimmbar sind, wenn der eigentliche Zweck der Verarbeitung in der Identifizierung von Personen besteht, wäre ein Widerspruch in sich."[19] Wenn also der

10 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

11 Vgl. u.a.: Schmidt-Holtmann, Der Schutz der IP-Adresse im deutschen und europäischen Datenschutzrecht – Zur Auslegung des Begriffs des personenbezogenen Datums, 2014; Gerlach, CR 2013, 478-484; Meyerdierks, MMR 2013, 505-708; Meyerdierks, MMR 2009, 8-13; Specht/Müller-Riemenschneider, ZD 2014, 71.

12 EuGH, Urt. v. 24.11.2011 – C-70/10, Rn. 51.

13 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. EG 1995, L 281/31. Unmittelbar anwendbar war im Fall des LG Düsseldorf die deutsche Umsetzungsnorm, § 3 Abs. 1 BDSG. Dieser ist jedoch einer europarechtskonformen Auslegung zu unterziehen, weshalb der Wortlaut von Art. 2 lit. a RL 95/46/EG Berücksichtigung finden muss.

14 Schriftsatz im Verfahren C-582/14, eingereicht von der Europäischen Kommission am 31.03.2015, abrufbar unter: http://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2015-03-31_Kom_an_EuGH.pdf (Stand: 17.03.2016), S. 9.

15 Ähnlich bezüglich der deutschen Umsetzung dieser Vorschrift in § 3 Abs. 1 BDSG: Specht/Müller-Riemenschneider, ZD 2014, 71, 73.

16 Art. 29-Datenschutzgruppe, WP 136, S. 17. Ähnlich auch Dammann, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl. 2014, § 3 BDSG Rn. 24, 26.

17 Art. 29-Datenschutzgruppe, WP 136, S. 18.

18 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

19 Art. 29-Datenschutzgruppe, WP 136, S .19.

Zweck der Verarbeitung der Daten aus dem Plugin-Betrieb die Identifizierung zumindest eingeloggter Nutzer einschließt, so kann, folgt man der Argumentation der Art. 29-Datenschutzgruppe, davon ausgegangen werden, dass der Verantwortliche oder ein beteiligter Dritter über entsprechende Mittel zur Identifizierung verfügt und dass deren Einsatz im Sinne des Erwägungsgrundes 25 bei vernünftiger Erwägung der äußeren Umstände zumindest möglich erscheint.[20] Eine einigermaßen konkrete Gefährdung, wie sie Art. 2 lit. a der RL 95/46/EG vorsieht, ist damit aufgrund des speziellen Geschäftsmodells bei der Verarbeitung von Plugin-Daten gegeben, was die Annahme einer Personenbeziehbarkeit auch hinsichtlich der übermittelten IP-Adressen in diesem Fall rechtfertigt – eine generelle Aussage über die Personenbezogenheit von IP-Adressen ist damit aber nicht getroffen.

2. Seitenbetreiber als verantwortliche Stelle

Das LG Düsseldorf begründet im Wesentlichen die Verantwortlichkeit des Seitenbetreibers damit, dass dieser die Daten beschaffe, die von Facebook anschließend verarbeitet werden. Damit ermögliche er eine spätere Verwendung der Daten und wirke durch die technische Einbindung des Plugins, die nicht nur eine Vorbereitungshandlung darstelle, unmittelbar an den Datenerhebungen durch Facebook mit.[21] Diese Ausführungen zum „Mithandeln" des Seitenbetreibers wirken etwas gekünstelt, wenn man zur richtlinienkonformen Auslegung des § 3 Abs. 7 BDSG auf den insofern einschlägigen Wortlaut des Art. 2 lit. d RL 95/46/EG zurückgreift.[22] Demnach ist es nicht erforderlich, dass die verantwortliche Stelle zu irgendwelchen Datenverarbeitungen in Form von Teilnahmehandlungen Beiträge leistet, sondern es kommt ausschließlich auf ihre tatsächliche Entscheidungsgewalt hinsichtlich der Zwecke und Mittel der jeweiligen Datenverarbeitung an.

a. Datenübertragung an Facebook

Ein solcher Einfluss des Seitenbetreibers auf die Übertragung von IP-Adressen und zusätzlichen Informationen über eingeloggte Nutzer lässt sich beim Einsatz von sozialen Plugins auch einwandfrei begründen: Der Seitenbetreiber entscheidet selbst über die Einbindung des Plugins in seine Webseite, kennt den Programmcode und die dadurch ausgelösten Prozesse, und entscheidet somit im Sinne der Definition aus Art. 2 lit. d RL 95/46/EG über die Zwecke und Mittel der Datenübertragung an Facebook.

b. Weiterverarbeitung von Daten durch Facebook

Die Argumentation des Gerichts, die bis dahin lediglich die richtlinienkonforme Auslegung von § 3 Abs. 7 BDSG vernachlässigt hatte, führt aber im konkreten Zusammenhang auch zu einer Fehlannahme: Das LG kommt zu dem Schluss, die Beklagte habe nicht nur die Datenweitergabe an Facebook, sondern auch die von Facebook anschließend durchgeführte „Datennutzung initiiert".[23] Sofern das LG hier beim Wort genommen werden darf, impliziert es eine Verantwortlichkeit des Seitenbetreibers für die von Facebook nach der Übertragung der Daten durchgeführten Verarbeitungen, z.B. zur Auswahl der Profile von Kontakten oder anderen Facebook-Mitgliedern, die einem eingeloggten Nutzer konkret im Zusammenhang mit dem Like-Button angezeigt werden sollten oder zur zielgerichteten Platzierung von Werbung. Auf diese Vorgänge hat der Seitenbetreiber jedoch keinerlei unmittelbaren Einfluss; mit dem Einbinden oder Nichteinbinden des Plugins in einem bestimmten Zusammenhang und mit einem bestimmten Programmcode kann er lediglich die Übertragung bestimmter Nutzerdaten an die Server von Facebook zu dem gewünschten Zweck veranlassen oder unterbinden. Auf Algorithmen und sämtliche Software, die Facebook einsetzt, um Inhalte oder Werbung auf einzelne Nutzer zuzuschneiden und die entsprechenden Datenverarbeitungen, die Facebook zu diesem Zweck durchführt, hat der Seitenbetreiber durch den Programmcode des Plugins aber keinen Einfluss.

Unter der Definition des Art. 2 lit. d RL 95/46/EG, der sich eindeutig auf faktische (Mit-)Bestimmung („bestimmt"), nicht aber auf normative oder gar moralische Aspekte bezieht, bleibt für eine erweiternde Auslegung, für die sich mit dem Schutzzweck der Richtlinie und dem besonderen Gefährdungspotenzial profilbildender sozialer Webservices durchaus argumentieren ließe, wohl kein Raum. Auch der auf der Hand liegende Einwand, dass Facebook die Daten ohne die Mitwirkung des Seitenbetreibers gar nicht erhalten hätte und somit auch eine weitere Verarbeitung unmöglich gewesen wäre, überzeugt letztlich unter Berücksichtigung des eindeutigen Wortlauts von Art. 2 lit. d RL 95/46/EG nicht. Diesem Wortlaut zufolge kommt es auf die tatsächliche Bestimmungsgewalt bezüglich einer konkreten Verarbeitung an; dies schließt aber umgekehrt eine „Fernwirkung" oder „Fortwirkung" der Bestimmungsgewalt aus. Nur weil ein Seitenbetreiber über die Zwecke und Mittel der Übertragung von Daten durch das Plugin entscheiden konnte, wirkt diese Entscheidungsmöglichkeit nicht auf sämtliche unter Einbeziehung dieser Daten durchgeführten Verarbeitungsvorgänge fort, sondern eine Verantwortlichkeit beurteilt sich auch hier nach der tatsächlichen Verfügungsmöglichkeit über die Zwecke und Mittel des konkreten in Rede stehenden Datenverarbeitungsvorganges.

Eine Verantwortlichkeit des Seitenbetreibers ließe sich allenfalls für die Übermittlung und Anzeige der „fertigen" Ergebnisse der Auswertung im Rahmen des Plugins diskutieren. Denn z.B. können dem Nutzer die Profile bestimmter Kontakte, die das Plugin bereits betätigt haben, im Zusammenhang mit dem Plugin nur angezeigt werden, weil der Seiten-

20 Art. 20-Datenschutzgruppe, WP 136, S. 19.

21 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

22 Das LG Düsseldorf (Urt. v. 09.03.2016 – 12 O 151/15) erwähnt zwar Art. 2 lit. d RL 95/46/EG, verwendet die dortigen Begrifflichkeiten aber dennoch nicht zur weiteren Auslegung von § 3 Abs. 7 BDSG.

23 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

betreiber sich dazu entschieden hat, dieses Plugin in einer bestimmten Form und mit einer bestimmten Funktionsweise in seine Seite einzubetten. Hier bestimmt also (wenn auch möglicherweise nicht allein) der Seitenbetreiber selbst wieder über die Zwecke und Mittel der Verarbeitung.

3. Keine Erforderlichkeit von Datenverarbeitungen nach § 15 TMG

Das LG Düsseldorf hält Datenverarbeitungen im Zusammenhang mit dem sozialen Plugin nicht für gemäß § 15 Abs. 1 TMG gerechtfertigt. Nach § 15 Abs. 1 TMG sind Datenverarbeitungen im Rahmen des generellen Verbots mit Erlaubnisvorbehalt (§ 12 Abs. 1 TMG) gestattet, wenn sie erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Das Kriterium der Erforderlichkeit sei eng auszulegen, der ‚Gefällt mir'-Button sei aber für den Betrieb der eigentlichen Webseite nicht unverzichtbar.[24]

Angesichts der weiten Verbreitung eingebundener Drittinhalte im Web 2.0 könnte diese Annahme der Unverzichtbarkeit durchaus bestritten werden. Auch schreibt § 15 Abs. 1 TMG gerade nicht vor, wie das Telemedium gestaltet sein soll, sondern setzt lediglich voraus, dass die stattfindenden Datenverarbeitungen für das Angebot im jeweiligen Ist-Zustand erforderlich sein müssen – womit die Schaffung einer Situation der Erforderlichkeit im Wesentlichen der Gestaltungsfreiheit des Diensteanbieters unterliegt. Damit stellt auch das Plugin selbst im jeweils angebotenen Zustand ein Telemedium, d.h. einen elektronischen Informations- und Kommunikationsdienst nach der Definition des § 1 Abs. 1 TMG oder zumindest einen Teil eines solchen Dienstes dar. Für die Inanspruchnahme des Plugins selbst als Telemedium oder für die Nutzung der Webseite in ihrer konkreten Form mit dem eingebundenen Plugin sind dann aber gewisse Datenverarbeitungen durchaus erforderlich. Allerdings wird dem Nutzer das Plugin praktisch aufgedrängt, wenn er die Seite aufruft, auf der das Plugin eingebettet ist, da es direkt mit dem Seiteninhalt zusammen geladen wird, ohne dass der Nutzer es explizit aufgerufen hat. Dadurch wird der Zweck von § 15 Abs. 1 TMG, der die durch eine faktische (aber willentliche oder zumindest bewusste) Inanspruchnahme von Telemedien erforderliche Datenverarbeitung regeln soll, verzerrt. Die enge Auslegung des LG Düsseldorf hat an dieser Stelle also durchaus ihre Berechtigung, hätte aber entsprechend genauer begründet werden können.

4. Keine rechtzeitige Unterrichtung nach § 13 Abs. 1 TMG durch eine Verlinkung in der Fußzeile

Die Unterrichtung nach § 13 Abs. 1 TMG hat zeitlich spätestens zu Beginn des Nutzungsvorgangs zu erfolgen. Der Seitenanbieter hatte im vom LG Düsseldorf beurteilten Fall einen Link in der Fußzeile der Webseite bereitgehalten, über den ein entsprechender Informationstext abrufbar war. Um aber überhaupt als Unterrichtung zu gelten, muss diese Unterrichtung auf der Webseite „zuverlässig wahrnehmbar"[25] sein. Allgemein gilt diesbezüglich die Platzierung eines eindeutigen, hervorgehobenen Hinweises auf der Startseite in Verbindung mit einem Link zu einem Informationstext als ausreichend.[26] Das LG Düsseldorf präzisierte im vorliegenden Fall die Anforderungen dahingehend, dass ein Link, der lediglich in der Fußzeile der Homepage aufzufinden und nicht mit einem hervorgehobenen Hinweis versehen war, nicht in ausreichendem Maße zuverlässig wahrnehmbar war. Es folgerte mithin, eine Unterrichtung habe überhaupt nicht stattgefunden.[27]

Diese deutliche Unterscheidung zwischen der Anforderung einer rechtzeitigen, gut wahrnehmbaren erstmaligen Unterrichtung zu Beginn des Nutzungsvorgangs und der späteren jederzeitigen Abrufbarkeit des Informationstextes (darauf bezieht sich die vielfach diskutierte Zwei-Klick-Regelung)[28] ist nach dem Gesetzeswortlaut von § 13 Abs. 1 TMG zweifelsfrei gerechtfertigt, wird aber wohl bislang hinsichtlich allgemeiner Informationspflichten nach § 13 Abs. 1 TMG – auch deswegen, weil in ähnlicher Sache die Anforderungen der sogenannten Cookie-Richtlinie für viel Aufmerksamkeit sorgten[29] – häufig vernachlässigt.

III. Wettbewerbsrechtlicher Rahmen: Rechtsbruch nach § 3a UWG

Wettbewerbsrechtlich verfolgbar sind Datenschutzrechtsverstöße nur, wenn sie einem der Verbote des UWG unterfallen. Vor dem LG Düsseldorf ging es um die Frage, ob der zuvor festgestellte Verstoß gegen die §§ 12, 13 TMG durch das Einbinden eines sozialen Plugins einen Rechtsbruch im Sinne von § 3a UWG darstellt. Hierfür muss es sich bei den Regelungen des TMG, gegen die verstoßen wurde, (1.) um Vorschriften handeln, die auch dazu bestimmt sind, im Interesse der Marktteilnehmer das Marktverhalten zu regeln (sog. Marktverhaltensvorschrift), und (2.) der konkrete Verstoß muss dazu geeignet sein, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen.

1. §§ 12 Abs. 1, 13 Abs. 1 TMG als Marktverhaltensvorschriften im Interesse der Marktteilnehmer

Marktverhaltensvorschriften zielen zumindest auch auf die Regelung des Marktverhaltens im Interesse der Marktteilnehmer ab – dies muss aber nicht ihr einziger oder vorrangiger Zweck sein.[30] Unter Marktverhalten sind dabei solche Tätigkeiten auf einem Markt zu verstehen, die objektiv der Absatz- oder Bezugsförderung dienen und durch die ein Unternehmer auf andere Marktteilnehmer (z.B. Mitbewerber, Verbraucher) einwirkt, insbesondere also Angebot und

24 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

25 Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 13 TMG Rn. 8.

26 Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 13 TMG Rn. 8.

27 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

28 Dazu Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 13 TMG Rn. 8.

29 Vgl. für einen Überblick zur Problematik der sog. „Cookie-RL" 2009/136/EG: Rauer/Ettig, ZD 2015, 255-259.

30 Köhler, in: Köhler/Bornkamm, Gesetz gegen den Unlauteren Wettbewerb, 34. Aufl. 2016, § 3a UWG Rn. 1.61.

Nachfrage von Waren und Dienstleistungen, sowie Werbung.[31] Ein marktverhaltensregelnder Charakter ist für datenschutzrechtliche Vorschriften schon vielfach festgestellt worden, kann aber dennoch nicht pauschal vorausgesetzt werden.[32] Nachdem es sich zunächst ausführlich mit den datenschutzrechtlichen Aspekten des Sachverhalts auseinandergesetzt hat, scheint das LG Düsseldorf die Frage des marktverhaltensregelnden Charakters aber verhältnismäßig knapp abzuhandeln: Es begründet den marktverhaltensregelnden Charakter der §§ 12, 13 TMG pauschal damit, dass „Gesetze, die die Erhebung von Daten betreffen, [...] im Einzelfall nicht nur das Persönlichkeitsrecht und das informationelle Selbstbestimmungsrecht, sondern auch den Wettbewerb an sich" schützen; Außerdem sei die zunehmende Bedeutung elektronischer Daten als Wirtschaftsgut zu berücksichtigen.[33]

a. Regelung des Marktverhaltens im Interesse der Mitbewerber

Angesichts der teilweise stark divergierenden vertretenen Ansichten in Literatur und Rechtsprechung hätte es hier allerdings einer etwas ausführlicheren Begründung bedurft. So wurde gegenteilig vertreten, dass den deutschen Datenschutzvorschriften neben dem Schutz des Persönlichkeitsrechts Betroffener „ein weiterer – sei es auch nur sekundärer – Zweck, das Werbeverhalten von Unternehmen im Interesse der Marktteilnehmer zu regeln bzw. gleiche Voraussetzungen für werbende Unternehmen zu schaffen, nicht zu entnehmen" sei.[34] Gerade § 13 TMG sei eine „wertneutrale Vorschrift [...], die nicht im Interesse der Marktteilnehmer das Marktverhalten regelt, sondern den individuell Betroffenen schützen soll".[35] In dieser Hinsicht unterscheidet sich jedoch die ausdrücklich auf den Wettbewerb und Binnenmarkt bezugnehmende RL 95/46/EG wesentlich von der auch § 13 TMG betreffenden allgemeinen Zweckbestimmung in § 1 Abs. 1 BDSG. Eine richtlinienkonforme Auslegung des Regelungszwecks deutscher Datenschutzgesetze unter Hinzuziehung der Erwägungsgründe der Richtlinie ist deswegen unbedingt erforderlich. Völlig richtig argumentiert daher das OLG Hamburg, dass § 13 Abs. 1 TMG auf die Datenschutzrichtlinie 96/46/EG zurückzuführen sei, die, wie aus ihren Erwägungsgründen 6 bis 8 hervorgehe, den grenzüberschreitenden Verkehr personenbezogener Daten auch zu dem Zweck auf ein einheitliches Schutzniveau heben solle, um Hemmnisse für Wirtschaftstätigkeiten in der Gemeinschaft abzubauen und den Wettbewerb im Binnenmarkt zu stärken.[36] Daraus leitet es ab, dass § 13 Abs. 1 TMG gerade nicht ausschließlich auf überindividuelle Belange des freien Wettbewerbs abzielt, sondern zumindest auch die wettbewerbliche Entfaltung von Mitbewerbern durch die Herstellung gleicher Wettbewerbsbedingungen schützt.[37]

b. Regelung des Marktverhaltens im Interesse der Verbraucher

Ob die §§ 12 Abs. 1, 13 Abs. 1 TMG auch zusätzlich das Verhalten der betroffenen Verbraucher in ihrer Eigenschaft als Marktteilnehmer schützen, ist ebenfalls nicht völlig eindeutig. Immerhin hatte das LG Frankfurt/M. noch entschieden, dass „[d]ie fehlende Unterrichtung über die Erhebung und Verwendung personenbezogener Daten im Zusammenhang mit dem ‚Gefällt mir'-Button [...] sich nämlich – im Gegensatz zu geschäftsbezogenen Informationspflichten wie etwa der unrichtigen oder unvollständigen Belehrung der Verbraucher über ein etwaiges Widerrufs- oder Rückgaberecht – nicht auf das kommerzielle Verhalten des Besuchers der Website" auswirkt.[38] Die Informationspflicht nach § 13 Abs. 1 TMG bezwecke lediglich, den Nutzern von Telemediendiensten einen Überblick über die Verarbeitung ihrer personenbezogenen Daten zu verschaffen, schütze aber Verbraucher nicht vor der Beeinflussung geschäftlicher Entscheidungen.[39] Wo eine Datenverarbeitung zur Bereitstellung von Werbung geregelt wird, liegt eine Schutzfunktion zugunsten von Verbrauchern allerdings generell nahe.[40] Wenn also vorliegend die durch das Plugin durchgeführten Datenerhebungen unmittelbar die gezielte Platzierung von verhaltensbezogener Werbung ermöglichen, so liegt auch in dem von § 12 Abs. 1 TMG aufgestellten Verarbeitungsverbot mit Erlaubnisvorbehalt, gegen das vorliegend verstoßen wurde, eine marktverhaltensregelnde Vorschrift. Das OLG Hamburg geht sogar noch weiter und nimmt allgemein an, dass auch „Aufklärungspflichten [...] dem Schutz der Verbraucherinteressen bei der Marktteilnahme, also beim Abschluss von Austauschverträgen über Waren und Dienstleistungen, dienen, indem sie den Verbraucher über die Datenverwendung aufklären und dadurch seine Entscheidungs- und Verhaltensfreiheit beeinflussen".[41]

2. Spürbare Interessenbeeinträchtigung

Die wettbewerbliche Relevanz des konkreten Verstoßes rührt nach Ansicht des LG Düsseldorf daher, dass das Plugin auch

31 Köhler, in: Köhler/Bornkamm, Gesetz gegen den Unlauteren Wettbewerb, 34. Aufl. 2016, § 3a UWG Rn. 1.61 (mit Rechtsprechungsnachweisen).

32 Mit ausführlichen Rechtsprechungsnachweisen Köhler, in: Köhler/Bornkamm, Gesetz gegen den Unlauteren Wettbewerb, 34. Aufl. 2016, § 3a UWG Rn. 1.74.

33 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

34 OLG München, Urt. v. 12.01.2012 – 29 U 3926/11.

35 Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 13 TMG Rn. 2.

36 OLG Hamburg, Urt. v. 27.06.2013 – 3 U 26/12. Unter Bezugnahme auf die Richtlinie argumentiert ähnlich hinsichtlich des marktverhaltensregelnden Charakters der §§ 28 Abs. 3, 4a BDSG das KG Berlin, Urt. v. 24.01.2014 – 5 U 42/12 (wohl bestätigt durch BGH, Urt. v. 14.01.2016 – I ZR 65/14, Pressemitteilung abrufbar unter: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=73328&linked=pm, Stand: 30.03.2016).

37 OLG Hamburg, Urt. v. 27.06.2013 – 3 U 26/12; a.A. aber bezüglich des Aussagegehalts der ErwGr der RL 95/46/EG: Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 13 TMG Rn. 2.

38 LG Frankfurt/M., Teilurt. v. 16.10.2014 – 2-03 O 27/14 – ZD 2014, 136, 137.

39 LG Frankfurt/M., Teilurt. v. 16.10.2014 – 2-03 O 27/14 – ZD 2014, 136, 137.

40 Köhler, in: Köhler/Bornkamm, Gesetz gegen den Unlauteren Wettbewerb, 34. Aufl. 2016, § 3a UWG Rn. 1.74.

41 OLG Hamburg, Urt. v. 27.06.2013 – 3 U 26/12.

der Werbung und dem Absatz des Seitenbetreibers gedient habe; die Nutzer der Webseite seien deswegen unerwünschter Werbung ausgesetzt.[42] Ob der Zusammenhang zwischen der fehlenden Unterrichtung und gezielter Platzierung von Werbung so unmittelbar ist, dass dies eine spürbare Interessenbeeinträchtigung der Verbraucher oder Mitbewerber nach sich zieht, bleibt allerdings zweifelhaft. Ergänzend argumentiert das LG aber, die bei Facebook angemeldeten Besucher würden unmittelbar – nichtangemeldete Besucher dementsprechend mittelbar – durch das Plugin in ihrem Marktverhalten beeinflusst, weil der Inhalt des Plugins eine Aussage über die Beliebtheit der Seite und damit der dort angebotenen Waren mache und es dem Seitenbesucher selbst ermögliche, sich als zu der Gruppe derjenigen zugehörig zu kennzeichnen, denen die Seite bzw. die dort angebotenen Waren gefallen, wodurch auch die Kaufentscheidung beeinflusst werde.[43]

3. Keine Täuschung oder Irreführung durch falsche Informationen

Fast schon in einem Nebensatz äußerte das LG Düsseldorf außerdem, dass es in einer sachlich falschen Unterrichtung der Nutzer (der Seitenbetreiber hatte im Rahmen der an die Nutzer herausgegebenen Informationen fälschlich behauptet, es sei ausreichend, sich bei dem Netzwerk Facebook auszuloggen, um eine Datenverarbeitung durch das Plugin beim Besuch seiner eigenen Seite zu unterbinden) weder eine Täuschung über die Risiken der Dienstleistung noch eine Irreführung (§ 5 Abs. 1 Satz 2 Nr. 1 und Nr. 7 UWG) sieht.[44]

IV. Ergebnis und Ausblick

1. Komplexe Sachverhalte und offene Fragen

Wie so viele Entscheidungen im Bereich des Datenschutzrechts, die sich mit der Beurteilung vielschichtiger Geschäftsmodelle und komplexen Datenverarbeitungsprozessen auseinandersetzen, ist auch das vorliegende Urteil nicht in der Lage, alle offenen Fragen vollständig zu beantworten. Zwar überzeugt der Ansatz des LG Düsseldorf, die in Rede stehenden Datenverarbeitungsprozesse und die dahinter stehende Technik und Software detailliert zu analysieren und auf diese Analyse die datenschutzrechtliche Beurteilung zu gründen. Wie so häufig wird aber die unverzichtbare europarechtskonforme Auslegung der Vorschriften des deutschen Datenschutzrechts nicht konsequent genug betrieben, und es fehlt an einer Berücksichtigung der Besonderheiten des Geschäftsmodells sozialer Netzwerke und der daraus resultierenden spezifischen Gefährdungen für die Persönlichkeitsrechte Betroffener. Anders als andere Gerichte, die sich bereits mit den Funktionalitäten sozialer Netzwerke zu befassen hatten,[45] macht das LG Düsseldorf keinerlei Ausführungen zum räumlich anwendbaren Datenschutzrecht. Diese waren im vorliegenden Fall aber auch nicht erforderlich, da die als verantwortliche Stelle identifizierte Beklagte ihren Sitz unstreitig in Deutschland hatte, weshalb eine Anwendung des Rechts eines anderen EU-Mitgliedstaats auf der Grundlage des Niederlassungsprinzips (Art. 4 Abs. 1 lit. a RL 95/46/EG) ohnehin nicht in Frage kam. Dadurch blieb auch die von Literatur und Rechtsprechung teilweise divergierend beurteilte Frage des Verhältnisses der räumlichen Anwendbarkeitsvorschriften wettbewerbsrechtlicher und datenschutzrechtlicher Natur zueinander unberührt.[46] Angesichts der noch nicht ganz eindeutigen Rechtslage im Hinblick auf den marktverhaltensregelnden Charakter der §§ 12, 13 TMG wäre eine ausführliche argumentative Begründung unter Rückgriff auf die Erwägungsgründe der RL 95/46/EG hier aber durchaus berechtigt gewesen.

2. Alte Begriffe und die neue DS-GVO

Der bevorstehende Übergang der Datenschutzregelungen von der europäischen Richtlinie mit nationaler Umsetzung hin zu einer unmittelbar anwendbaren europäischen Datenschutzgrundverordnung (DS-GVO)[47] betont die besondere Wichtigkeit des Verständnisses und der Auslegung der grundlegenden Begriffe des europäischen Datenschutzrechts. Die Definitionen des für die Verarbeitung Verantwortlichen (Art. 4 Abs. 5 DS-GVO)[48] und die Voraussetzungen des Personenbezugs (Art. 4 Abs. 1 DS-GVO)[49] werden sich mit der neuen Regelung nicht grundlegend verändern,[50] und viele der aus der Richtlinie bekannten Begriffe werden auch durch die Datenschutzgrundverordnung wieder aufgegriffen. Diese werden künftig von deutschen Gerichten anzuwenden und auszulegen sein, was eine tiefergehende Beschäftigung mit diesen Begriffen im Rahmen der richt-

42 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

43 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

44 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

45 Vgl. für einen Überblick über die bisherige Rechtsprechung bezüglich der räumlichen Anwendbarkeit des Datenschutzrechts auf soziale Netzwerke: Beyvers/Herbrich, ZD 2014, 558-562.

46 Zum Verhältnis des insofern einschlägigen Art. 4 der RL 95/46/EG zu den räumlichen Anwendbarkeitsvoraussetzungen im internationalen Zivilrecht, öffentlichen Recht und Strafrecht vgl. Herbrich/Beyvers, RDV 2016, 3-10.

47 Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) v. 25.01.2012, KOM(2012) 11 endg. – 2012/0011 (COD), abrufbar unter: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf (Stand: 30.03.2016); Einigungsdokument v. 28.01.2016 nach den Trilogverhandlungen, Nr. ST 5455 2016 INIT, abrufbar unter: http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/de/pdf (deutsche Übersetzung, nicht konsolidiert, Stand: 30.03.2016).

48 Die Angabe bezieht sich auf das Einigungsdokument v. 28.01.2016 nach den Trilogverhandlungen, Nr. ST 5455 2016 INIT, abrufbar unter: http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/de/pdf (deutsche Übersetzung, nicht konsolidiert, Stand: 30.03.2016).

49 Die Angabe bezieht sich auf das Einigungsdokument v. 28.01.2016 nach den Trilogverhandlungen, Nr. ST 5455 2016 INIT, abrufbar unter: http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/de/pdf (deutsche Übersetzung, nicht konsolidiert, Stand: 30.03.2016).

50 Einige Präzisierungen gibt es aber durchaus – z.B. finden sich in den Erwägungsgründen zur DSGVO nun explizite Hinweise zum Personenbezug bei IP-Adressen: Laut ErwGr 24 DSGVO (die Angabe bezieht sich auf das Einigungsdokument v. 28.01.2016 nach den Trilogverhandlungen, Nr. ST 5455 2016 INIT, abrufbar unter: http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/de/pdf, deutsche Übersetzung, nicht konsolidiert, Stand: 30.03.2016) werden dem Nutzer „unter Umständen" Online-Kennungen wie IP-Adressen oder Cookies zugeordnet – im Rückschluss kann also zumindest nicht generell von einer Zuordenbarkeit ausgegangen werden.

linienkonformen Auslegung schon jetzt umso bedeutender erscheinen lässt.

3. Verantwortung für eingebundene Inhalte – das Ende des Web 2.0?

In dem Verfahren hatte der Seitenbetreiber vor dem LG Düsseldorf argumentiert, die Einbindung von Drittinhalten sei „integraler Bestandteil der Funktionsfähigkeit des Internet, speziell des Web 2.0 und der gängigen Standards HTML, HTTP".[51] Nutzer hätten mit der Einbindung von Drittinhalten und damit zusammenhängend auch mit der Übermittlung technischer Informationen an Drittanbieter regelmäßig zu rechnen.[52] In der Tat bedienen sich die meisten Webseiten mittlerweile umfangreich der Inhalte Dritter – bedeutet das Urteil also das Ende für das Web 2.0?

Es ist durchaus ein bedeutender Schritt, Seitenbetreibern für die Datenverarbeitungen Verantwortung zuzuweisen, die sie durch eine Einbindung von Drittinhalten auslösen. Wenn dabei jedoch – wie zuvor ausgeführt – konsequent zwischen der mit dem Plugin gesteuerten Übertragung der Daten, über die der Seitenbetreiber bei der Einbindung konkret mitbestimmen kann, und der weiteren Verarbeitung der Daten durch den Drittanbieter (zur Bereitstellung seines Angebots oder anderweitig) unterschieden wird, so führt die korrekte Anwendung der Datenschutzrichtlinie nicht zu einem völligen Ausufern der Verantwortlichkeit von Seitenbetreibern. Ob die von diesen Drittanbietern durchgeführten Datenverarbeitungen ihrerseits den Vorgaben des Datenschutzrechts entsprechen, ist davon getrennt zu betrachten.

Das LG Düsseldorf äußert sich ausdrücklich nicht zur Rechtskonformität der sogenannten „Zwei-Klick-Lösung", bei der das soziale Plugin inaktiv bleibt, bis der Nutzer es selbst auf der Seite aktiviert. Eine pauschale Beurteilung wird hier auch kaum möglich sein; vielmehr kommt es im Einzelfall darauf an, ob die bei der Aktivierung gelieferte Unterrichtung den gesetzlichen Anforderungen entspricht, und ob der Nutzer nötigenfalls eine wirksame Einwilligung in die Datenverarbeitung erteilt. Soweit das Plugin aber durch die Zwei-Klick-Lösung zunächst völlig inaktiv bleibt, löst es zumindest nicht bereits beim Laden der Seite, in die es eingebunden ist, eine wettbewerbsrechtlich relevante Unterrichtungspflicht nach § 13 Abs. 1 TMG aus.

(Eva Beyvers)

Zur Umsetzungsfrist eines Werbewiderspruchs (Ls)

(**Landgericht Freiburg,** Beschluss vom 14. Januar 2016 – 3 S 227/14 –)

1. **Eine Forderung nach Abgabe einer strafbewehrten Unterlassungserklärung ist berechtigt, wenn ein Unternehmen den Betroffenen 28 Tage nach ausdrücklich erklärtem Widerspruch gegen weitere Briefwerbung einen weiteren Werbebrief zusendet.**
2. **Ob und in welchem Umfang ein Zeitraum zur Umsetzung des Widerspruchs zu gewähren ist, kann offenbleiben, da der Zeitraum von nahezu einem Monat jedenfalls ausreicht.**

(Nicht amtliche Leitsätze)

Kein absolutes Beweiswertverbot von Dash-Cam-Aufnahmen im Schadensersatzprozess (Ls)

(**Landgericht Landshut,** Hinweisbeschluss vom 1. Dezember 2015 – 12 S 2603/15 –)

1. **Auch wenn Aufzeichnungen mit Dash-Cam-Kameras möglicherweise gegen das BDSG oder das allgemeine Persönlichkeitsrecht verstoßen sollten, führt dies nicht per se zu ihrem Verwertungsverbot im Schadensersatzprozess.**
2. **Im Rahmen der erforderlichen Abwägung des Beweisinteresses des Klägers mit dem Schutzinteresse des Beklagten ist vorliegend festzustellen, dass ein gravierender Grundrechtseingriff in der Aufzeichnung des rückwärtsfahrenden PKWs des Beklagten nicht zu erkennen ist, dass andererseits der Kläger ohne Verwertung der Aufzeichnungen mit einer ungerechtfertigten Klageabweisung rechnen müsste. Das Interesse, dass ein streitiger Verkehrsunfall nicht aufgeklärt werden soll, ist nicht schützenswert.**

(Nicht amtliche Leitsätze)

Auskunftsanspruch des Betriebsrats zu Zielvereinbarungen (Ls)

(**Landesarbeitsgericht Frankfurt/M.,** Beschluss vom 24. November 2015 – 16 TaBV 106/15 –)

1. **Die Zuständigkeit zur Überwachung der ordnungsgemäßen Durchführung einer Gesamtbetriebsvereinbarung durch den Arbeitgeber obliegt dem Betriebsrat.**
2. **Hierfür sind dem Betriebsrat die Namen der von der Zielvereinbarung betroffenen Mitarbeiter zu benennen, damit er die Erfüllung der dort aufgestellten Kriterien nachvollziehen kann.**
3. **Der Übermittlung der Namen stehen keine datenschutzrechtlichen Gründe entgegegen.**

51 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

52 LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15.

Verpflichtung des Arbeitgebers zur Auskunfterteilung gegenüber dem Betriebsrat bzgl. der Kriterien für die Leistung von Zulagen und Einmalzahlungen

(**Landesarbeitsgericht Frankfurt/M.,** Beschluss vom 4. Mai 2015 – 16 TaBV 175/14 –)

1. **Für den allgemeinen Unterrichtungsanspruch bedarf es keines konkreten Anlasses und auch keiner greifbaren Anhaltspunkte. Dies ergibt sich aus dem in § 80 Abs. 2 Satz 2 BetrVG generell auch für den Informationsanspruch geltenden Grundgedanken, dass der Betriebsrat die zur Erfüllung seiner Aufgaben notwendigen Informationen jederzeit zur Verfügung haben muss.**
2. **Der Beteiligten zu 2) wird aufgegeben, dem Antragsteller in Schriftform Auskunft darüber zu erteilen, an welche Arbeitnehmer mit Ausnahme leitender Angestellter der A in L in welcher Höhe, auf welcher Grundlage und nach welchen Kriterien Zulagen, Einmalzahlungen, Sonderzahlungen und Funktionsprämien ab dem 1. Januar 2013 gezahlt wurden.**

Aus den Gründen:

Der allgemeine Unterrichtungsanspruch des § 80 Abs. 2 S. 1 BetrVG wird nicht durch den Anspruch auf Einsicht in die Bruttoentgeltlisten (§ 80 Abs. 2 S. 2 Halbsatz 2 BetrVG) verdrängt (Bundesarbeitsgericht 10. Oktober 2006 – 1 ABR 68/05 – Rn. 20; 7. Februar 2012 – 1 ABR 46/10 – Rn. 15; GK-BetrVG, 10. Aufl., § 80 Rn. 54). Dies kann allenfalls dann der Fall sein, wenn die schriftliche Information inhaltlich einer Gehaltsliste gleichkommt. Letzteres scheidet hier aus, weil sich die Auskunft nur auf einen kleinen Teil der Vergütungsstruktur bezieht (so in dem ähnlich gelagerten Fall auch: LAG Hamburg 7. Februar 2012 – 2 TaBV 12/11 – Rn. 41 am Ende). Aus diesem Grund greifen auch die einschränkenden Voraussetzungen, unter denen der Arbeitgeber einem vom Betriebsrat gebildeten Ausschuss Einblick in die Bruttoentgeltlisten gewähren muss, für die Vorlage von Unterlagen nach § 80 Abs. 2 S. 2 Abs. 1 BetrVG nicht (Bundesarbeitsgericht der Februar 2012 – 1 ABR 46/10 – Rn. 15).

Entgegen der Meinung des Arbeitsgerichts und des Arbeitgebers bedarf es für den Auskunftsanspruch keines konkreten Anlasses und auch keiner greifbaren Anhaltspunkte. Da die Überwachungsaufgabe nach § 80 Abs. 1 Nr. 1 grundsätzlich besteht und nicht erst bei Vorliegen von Verdachtsmomenten für Verstöße des Arbeitgebers greift, muss der Betriebsrat auch keinen konkreten Anlass vortragen (GK-BetrVG, 10. Aufl., § 80 Rn. 61; Fitting, BetrVG, 26. Aufl., § 80 Rn. 68). Dies ergibt sich aus dem in § 80 Abs. 2 S. 2 BetrVG generell auch für den Informationsanspruch geltenden Grundgedanken, dass der Betriebsrat die zur Erfüllung seiner Aufgaben notwendigen Informationen jederzeit zur Verfügung haben muss. Hieraus folgt, dass der Betriebsrat die erforderlichen Auskünfte ohne besonderen Anlass verlangen kann (für § 80 Abs. 2 Satz 1 BetrVG: Bundesarbeitsgericht 19. Februar 2008 – 1 ABR 84/06 – Rn. 25; in Bezug auf § 80 Abs. 2 Satz 2 BetrVG: Bundesarbeitsgericht 14. Januar 2014 – 1 ABR 54/12 – Rn. 23).

Der Unterrichtungsanspruch des Betriebsrats gemäß § 80 Abs. 2 S. 1 BetrVG besteht nicht nur dann, wenn allgemeine Aufgaben oder Beteiligungsrechte feststehen. Die Unterrichtung soll es dem Betriebsrat auch ermöglichen, in eigener Verantwortung zu prüfen, ob sich Aufgaben im Sinne des Betriebsverfassungsgesetzes ergeben und er zu ihrer Wahrnehmung tätig werden muss. Dabei genügt eine gewisse Wahrscheinlichkeit für das Bestehen von Aufgaben. Die Grenzen des Auskunftsanspruchs liegen erst dort, wo ein Beteiligungsrecht oder eine sonstige betriebsverfassungsrechtliche Aufgabe offensichtlich nicht in Betracht kommt. Daraus folgt eine zweistufige Prüfung daraufhin, ob überhaupt eine Aufgabe des Betriebsrats gegeben und ob im Einzelfall die begehrte Information zur Aufgabenwahrnehmung erforderlich ist (Bundesarbeitsgericht 10. Oktober 2006 – 1 ABR 68/05 – Rn. 18; 7. Februar 2012 E1 ABR 46/10E Rn. 7). Als vom Betriebsrat wahrzunehmende Aufgabe kommt hier sowohl die Mitbestimmung nach § 87 Abs. 1 Nr. 10 BetrVG als auch die Überwachung des Gleichbehandlungsgrundsatzes nach § 80 Abs. 1 i.V.m. § 75 Abs. 1 BetrVG ernsthaft in Betracht (vgl. dazu näher: LAG Hamburg 7. Februar 2012 – TaBV 12/11 – Rn. 35ff; Bundesarbeitsgericht 10. Oktober 2006 – 1 ABR 68/05 – Rn. 27ff). Hierfür sind die vom Betriebsrat begehrten Informationen erforderlich. Der Betriebsrat benötigt die Information auch insoweit, wie sich die Einmalzahlungen seit Januar 2013 entwickelt haben, um die Entwicklung der Sonderzahlungen und die Einhaltung des Gleichbehandlungsgrundsatzes beurteilen zu können.

Die Erforderlichkeit entfällt auch nicht deshalb (teilweise), soweit der Betriebsrat durch Einblick in Tarifverträge oder Betriebsvereinbarungen nach Grund und Höhe Zulagen, Einmalzahlungen, Sonderzahlungen und Funktionsprämien erkennen und durch Einsicht in die Bruttoentgeltlisten überprüfen kann, ob diese auch gezahlt wurden. Dies ergibt sich daraus, dass der Betriebsrat grundsätzlich nicht gehalten ist, sich benötigte Informationen selbst zu beschaffen, auch wenn er dazu objektiv in der Lage wäre. Eine Ausnahme gilt nach § 2 BetrVG lediglich dann, wenn der Betriebsrat die begehrte Information aus den ihm bereits übermittelten Daten ohne weiteres auf rechnerisch einfachem Wege ableiten kann, was hier nicht der Fall ist (Bundesarbeitsgericht 10. Oktober 2006 – 1 ABR 68/05 – Rn. 40, 41).

Der Betriebsrat kann auch vom Arbeitgeber verlangen, dass dieser die Unterrichtung nach § 80 Abs. 2 S. 1 BetrVG schriftlich vornimmt, weil es sich um umfangreiche und komplexe Angaben handelt (vgl.: Bundesarbeitsgericht 30. September 2008 – 1 ABR 54/07 – Rn. 29; 7. Februar 2012 – 1 ABR 46/10 – Rn. 14).

Die Ansicht des Arbeitgebers, der Betriebsrat könne allenfalls eine anonyme Liste verlangen, trifft nicht zu. In Bezug auf den Einblick des Betriebsrats in die Bruttoentgeltlisten nach § 80 Abs. 2 S. 2 Halbsatz 2 BetrVG hat das Bundesarbeitsgericht entschieden, es sich hierbei um eine nach § 32 Abs. 1 Bundesdatenschutzgesetz zulässige Form der Datennutzung handelt. Dies folgt schon daraus, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten nach § 32 Abs. 3 Bundesdatenschutzgesetz durch die nach Abs. 1 dieser Bestimmung erlaubte Datennutzung nicht berührt werden. Zu den Interessenvertretungen der Beschäftigten in diesem Sinne zählt auch der Betriebsrat. Hinzu kommt, dass dieser selbst Teil der verantwortlichen Stelle im Sinne des § 3 Abs. 7 Bundesdatenschutzgesetz ist. Die Einsichtgewährung stellt daher keine Weitergabe von Daten an Dritte dar (Bundesarbeitsgericht 14. Januar 2014 – 1 ABR 54/12 – Rn. 28). Für den Unterrichtungsanspruch nach § 80 Abs. 2 S. 1 BetrVG gilt nichts anderes.

Berichte, Informationen, Sonstiges

37. Internationale Datenschutzkonferenz in Amsterdam

Vom 26.-29.10.2015 richtete die niederländische Datenschutzaufsicht die internationale Datenschutzkonferenz unter dem Motto „Privacy Bridges" aus. Der Kreis der beteiligten Aufsichtsbehörden und staatlichen Stellen wird immer größer. In Amsterdam waren 101 Mitglieder bei der ICDPPC (International Conference of Data Protection and Privacy Commissioners) akkreditiert, hinzu kommen 17 mit Beobachterstatus. Unter Leitung des neuseeländischen Datenschutzbeauftragten, John Edwards, der seit 2014 den Vorsitz der Konferenz führt, hat die Organisation einen neuen Auftritt bekommen. Die Webseite der Konferenz, https://icdppc.org/, dokumentiert gut die Arbeit der ICDPPC. Hier finden sich u.a. ein Archiv der bisherigen Konferenzen sowie ein Kalender mit künftigen Aktivitäten.

Zwei Themen prägten maßgeblich die Konferenz in Amsterdam – die von den Veranstaltern zentral geführte Diskussion um Datenschutzbrücken auf Basis eines von EU- und US-Datenschutzexperten erarbeiteten Positionspapiers sowie die Entscheidung des Europäischen Gerichtshofs zum fehlenden Schutzniveau von auf die Safe Harbor Regelung gestützten Datenverarbeitungen vom 6.10.2015 (C-362/14). Die mögliche Ausweitung dieser Entscheidung auf US-Datenverarbeitungen mit Standardvertragsklauseln beherrschte sämtliche Diskussionen und belegt, dass das eher akademisch anmutende Leitthema von hoher Praxisrelevanz ist.

Wie in den Vorjahren erfolgte der nichtöffentliche Teil der Konferenz bereits vor dem öffentlichen Teil, so dass die Erklärung von Amsterdam sowie vier Entschließungen vorgestellt werden konnten. Die vierseitige Erklärung von Amsterdam trägt den sperrigen, aber inhaltlich genauen Titel: Amsterdamer Deklaration zu Genetik- und Gesundheitsdaten, Herausforderungen von Morgen sowie Datenschutzaufsicht über Sicherheits- und Geheimdienste und die Rolle von Datenschutzaufsichtsbehörden in einer sich wandelnden Gesellschaft. Hervorzuheben sind die Ausarbeitungen zu den Datenschutzrisiken von genetischen Daten und potentielle Lösungsansätze durch Aufsichtsorgane in Institutionen (IRBs – Institutional Review Boards), Privacy Management Programme, Privacy Impact Assessments, Privacy by design und Zertifizierungen sowie ein notwendiger Dialog der Aufsichtsbehördenvertreter mit Wissenschaftlern. Zum Thema Geheimdienste werden u.a. die Berücksichtigung von Verhältnismäßigkeit und Rechtmäßigkeit der Aktivitäten der Dienste und Sicherheitsorgane, Verbesserung der Transparenz sowie spezielle aufsichtliche Datenschutzmaßnahmen gefordert. Die Themen der vier Entschließungen beschäftigen sich mit der strategischen Ausrichtung der Konferenz bis 2018, der Verankerung von Datenschutz im internationalen Recht auf UN-Ebene, der Weiterentwicklung des Datenschutzes bei humanitären Aktionen sowie der Schaffung von Datenschutzregeln in internationalen Organisationen. [1]

In der Vorkonferenz, die von der Privatwirtschaft und NGOs getragen wird, sind zwei Veranstaltungen hervorzuheben: Zum einen die von NYMITY und dem Center for Information Policy Leadership initiierte Diskussion zur Angleichung unterschiedlicher Datenschutzordnungen durch in Organisationen eingebettete Accountability. Das Thema wurde zu verschiedenen Schwerpunkten beleuchtet, wobei der Einsatz von betrieblichen Datenschutzbeauftragten als Teil der Accountability bemerkenswert ist. Zum anderen erfolgte eine von der niederländischen Organisation für Datenschutzbeauftragte NGFG in Zusammenarbeit mit der Confederation of European Data Protection Organisations (CEDPO) durchgeführte Diskussion zum Thema Brückenschlag zwischen internationalen Rechtsordnungen in einer von Daten getriebenen Welt, in der ebenfalls die unverzichtbare Rolle des betrieblichen Datenschutzbeauftragten herausgearbeitet wurde.

Der Hauptteil der Konferenz begann mit der Ansprache des ausscheidenden langjährigen Vorsitzenden der niederländischen Datenschutzaufsicht, Jakob Kohnstamm als Gastgeber. Hieran schloss sich nach einem Bericht von John Edwards über die Entscheidungen und Entschließungen der Internationalen Konferenz eine in vielen Kleingruppen geführte Diskussion über das *„Privacy Bridges Projekt"* an, was den Schwerpunkt des ersten Tages darstellte. Das in über einjähriger Arbeit erstellte fünfzigseitige Dokument „Privacy Bridges" wurde zu spät vor Konferenzbeginn veröffentlicht, was die Diskussion für viele Teilnehmer beeinträchtigte. Das Dokument, das keine überraschenden Erkenntnisse enthält, ist eine gute Grundlage, um die Fragestellung zu beantworten, wie sich unterschiedliche Datenschutzwelten am Beispiel der USA und Europa annähern und gemeinsam kooperieren können. Das Positionspapier stellt zehn Datenschutzbrücken zur Diskussion vor:

1. Formalisierung der Zusammenarbeit zwischen den betroffenen US/ EU-Aufsichtsbehörden, der Federal Trade Commission und der Art. 29 Arbeitsgruppe.
2. Verbesserung der Kontrollmöglichkeiten der Betroffenen über ihre Daten, z.B. durch Schaffung von entsprechenden Standards.
3. Neue Ansätze zur Schaffung von Transparenz, u.a. am Beispiel anderer Industriezweige hinsichtlich Kennzeichnungspflichten.
4. Klärung der Frage, wie Betroffene Schadensersatz erhalten, wenn die Verletzungen außerhalb ihres geographischen Lebensraums erfolgen.

1 Die Entschließungen sind unter https://icdppc.org/document-archive/adopted-resolutions/ abrufbar.

5. Zugriff von Regierungsstellen auf Daten des privaten Sektors.
6. Etablierung von Standards, wie der Personenbezug von Daten herausgenommen werden kann – sog. De-Identifikation.
7. Entwicklung weiterer Standards zur Information bei Datenpannen.
8. Accountability – hier verstanden als organisationale Verantwortlichkeit, d.h. die verbindliche Übernahme der Verantwortung für den Datenschutz und die Einhaltung und Umsetzung weiterer rechtlicher Verpflichtungen durch eine Organisation.
9. Größeres Engagement zwischen Regierungen, ihre regulatorischen Aktivitäten stärker miteinander zu koordinieren, was einen regelmäßigen intensiven Austausch auf Arbeitsebene voraussetzt.
10. Zusammenarbeit im Hinblick auf Forschungsprogramme zum Datenschutz.

Der zweite Konferenztag begann mit der Ansprache von Vera Jourová, EU-Kommissarin für Justiz, Verbraucherschutz und Gleichstellung, zum Stand der Verhandlungen der EU-Datenschutzgrundverordnung und zur Lösung der Safe Harbor Fragestellung nach dem Schrems-Urteil des Europäischen Gerichtshofs. Mit einer Datenschutztour um die Welt ging der offizielle Teil der Konferenz mit einer daran anschließenden Podiumsdiskussion zu Ende. Die *Datenschutztour du Monde* berichtet über Datenschutzereignisse der letzten 80 Monate vor der Konferenz. Sie ist als 57-seitiger Bericht verfügbar

Das auf der Konferenz inflationär genutzte Bild einer Datenschutzbrücke wird die weitere Entwicklung des internationalen Datenschutzes prägen, da sie ein gelungenes Synonym für den sperrigeren Begriff der Interoperabilität darstellt. Die Schrems-Entscheidung des Europäischen Gerichtshofs zur Unzulässigkeit der Safe-Harbor-Datenverarbeitungen unterstreicht die besondere Aktualität der praxisgerechten Suche nach sicheren Datenschutzbrücken.

Marokko wird die 38. Internationale Datenschutzkonferenz in Marrakesch ausrichten. Die Konferenz findet voraussichtlich vom 18. bis 22.10.2016 statt.

(Paul Gürtler, TARGOBANK, Düsseldorf)

Der Bericht gibt ausschließlich die persönliche Meinung des Referenten wieder.

91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6./7. April 2016 in Schwerin

Unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Reinhard Dankert, tagte am 6./7. April 2016 die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in Schwerin.

Unter anderem erörterte die Konferenz intensiv, welche Strukturen für die nationale und internationale Zusammenarbeit erforderlich sein werden und wie Deutschland die von der Europäischen Datenschutz-Grundverordnung (DSGVO) vorgesehenen Gremien besetzen soll. In einer Entschließung appelliert die Konferenz an Bundes- und Landesgesetzgeber, die Öffnungs- und Konkretisierungsklauseln der DSGVO konsequent und umfassend zu nutzen, um unverzichtbare Datenschutzstandards im Sinne des Grundrechts auf informationelle Selbstbestimmung auch weiterhin zu gewährleisten.

Hierzu zählt die Konferenz vor allem:

- Schaffung eines Beschäftigtendatenschutzgesetzes
- Stärkung der Befugnisse der Aufsichtsbehörden, insb. Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden
- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private
- Beibehaltung der Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten nach § 4 f Abs. 1 Bundesdatenschutzgesetz
- weitestgehende Erhaltung der Datenschutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Intervenierbarkeit und Transparenz

In einer weiteren Entschließung fordert die Konferenz den effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps. Die Datenschutzbeauftragten weisen darauf hin, dass zum notwendigen Schutz von Gesundheitsdaten die Grundsätze der Datenvermeidung, Datensparsamkeit und der Transparenz zu beachten sind. Hersteller von Wearables und Gesundheits-Apps fordert die Konferenz auf, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen und für eine am Nutzer orientierte Transparenz Sorge zu tragen.

Zudem fordert die Datenschutzkonferenz den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

Die Terroranschläge in Brüssel haben die Konferenz erneut veranlasst, sich zu Fragen des Datenschutzes bei der effektiven Bekämpfung des Terrorismus zu äußern. In ihrer Entschließung weist die Konferenz darauf hin, dass der Datenschutz nicht für etwaige Ermittlungs- oder Vollzugsdefizite der Sicherheitsbehörden verantwortlich gemacht werden kann. Das geltende Datenschutzrecht erlaubt es schon jetzt, ermittlungsrelevante und zur Strafverfolgung notwendige Daten zu speichern und Informationen zwischen den Sicherheitsbehörden wechselseitig auszutauschen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell, dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus daran zu messen sind, ob sie für dessen wirkungsvolle Bekämpfung tatsächlich geeignet, erforderlich und angemessen sind und somit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

Mit Blick auf die Empfehlung des IT-Planungsrates, so genannte Servicekonten für Bürgerinnen, Bürger und Unternehmen flächendeckend anzubie-

ten, hat die Konferenz in einer weiteren Entschließung Hinweise zur datenschutzkonformen Ausgestaltung dieser Konten formuliert. Die Datenschutzbeauftragten begrüßen darin die Bestrebungen, sichere Identifizierungsmöglichkeiten durch die Nutzung der eID-Funktion des Personalausweises zu unterstützen. Sie fordern jedoch, für den Umgang mit personenbezogenen Daten in Servicekonten eine tragende Rechtsgrundlage zu schaffen und beim Betrieb der Konten insbesondere die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz zu berücksichtigen.

Die Konferenz hat weiterhin eine Orientierungshilfe für Online-Lernplattformen im Schulunterricht verabschiedet. Immer mehr Bildungsinstitutionen setzen auf die webgestützte Wissensvermittlung und die elektronischen Kommunikationsmöglichkeiten zwischen Lehrenden und Lernenden. Die verabschiedete Orientierungshilfe richtet sich insbesondere an Schulen, die Online-Lernplattformen als Lernmittel einsetzen wollen. Sie sollen sich einen Überblick darüber verschaffen können, welche datenschutzrechtlichen Anforderungen Online-Lernplattformen erfüllen müssen. Diese Orientierungshilfe gibt auch den Anbietern von Online-Lernplattformen die Möglichkeit, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine Nutzung durch Schulen zulässig ist.

Neuer Bitkom-Praxisleitfaden „Das Verfahrensverzeichnis“

– Leitfaden liefert Anwendungsbeispiele und Musterformulare –

Der Digitalverband Bitkom hat eine Neuauflage des Praxisleitfadens „Das Verfahrensverzeichnis“ veröffentlicht.

Der aktualisierte Leitfaden gibt Datenschutzbeauftragten von Unternehmen und anderen Organisationen Hinweise, wie sie den gesetzlichen Anforderungen gerecht werden können. Neben Erläuterungen und Praxisbeispielen zu den gesetzlichen Vorgaben werden die einzelnen Schritte bei der Führung des Verfahrensverzeichnisses dargestellt. Die Autoren des Leifadens sind Datenschutzbeauftragte aus der IT-Branche mit langjähriger Praxiserfahrung. Die Bitkom-Experten geben Hinweise zur Aufsichtspraxis der Datenschutzbehörden und zur aktuellen Rechtsprechung. Sie empfehlen eine Dokumentation der Datenverarbeitung entlang der Unternehmensprozesse.

Da nach dem Abschluss der EU-Datenschutzreform weiterhin umfangreiche Dokumentationspflichten bestehen werden, stellt der Leitfaden auch mit Blick auf die kommenden Änderungen eine gute Grundlage für die Arbeit der betrieblichen Datenschutzbeauftragten dar.

(Bitkom-Pressemitteilung vom 25.03.2016)

Patienten wollen Zugang zu ihren Gesundheitsdaten

– E-Health-Gesetz verspricht bessere Versorgung dank digitaler Technologien –

Neun von zehn Bundesbürgern (87 Prozent) wollen direkten Zugang zu ihren persönlichen Gesundheitsdaten haben, die in Arztpraxen, Kliniken oder anderen Gesundheitseinrichtungen anfallen. Das hat eine repräsentative Umfrage unter 1.236 Personen ab 14 Jahren im Auftrag des Digitalverbands Bitkom ergeben. Gesundheitsdaten umfassen unter anderem Diagnosen von Ärzten, Laborergebnisse, OP-Berichte oder Röntgenbilder. Informationen aus einer Behandlungsakte können zum Beispiel bei einem Arztwechsel notwendig sein. So kann sich der jeweils behandelnde Mediziner anhand der Krankengeschichte sowie aktueller Befunde und Verordnungen ein besseres Bild über den Gesundheitszustand des Patienten machen. Die Behandelten haben laut Bundesdatenschutzgesetz und dem Bürgerlichen Gesetzbuch das Recht, jederzeit und „unverzüglich“ ihre Patientenakte einzusehen. Auf Wunsch müssen Kopien oder Ausdrucke angefertigt werden, die allerdings kostenpflichtig sind.

Der Bitkom setzt sich seit langem dafür ein, dass Gesundheitsdaten wie Befunde, Röntgenbilder oder Verordnungen von Medikamenten auf Wunsch des Patienten vom behandelnden Arzt

in einer elektronischen Akte gespeichert werden. Der Patient sollte dabei selbst entschieden können, welche Informationen gespeichert werden und wem er diese – zum Beispiel im Rahmen einer Behandlung – zugänglich machen will. Ein wichtiger Schritt in diese Richtung ist die Einführung der elektronischen Gesundheitskarte. Mit dem kürzlich verabschiedeten E-Health-Gesetz sollen nun weitere innovative Anwendungen eingeführt werden, die eine bessere Versorgung der Patienten gewährleisten sollen. Dazu zählen die Einführung eines digitalen Patientenfachs, eines elektronischen Medikationsplans sowie mehrerer telemedizinischer Anwendungen. Mit Hilfe des digitalen Patientenfachs können die Nutzer eigenverantwortlich Gesundheitsdaten verwalten, die sie zum Beispiel mit Fitness-Trackern oder Gesundheits-Apps gesammelt haben. Diese Daten können sie ihrem Arzt dann in strukturierter Form zur Verfügung stellen.

Eine weitere wichtige Anwendung ist in diesem Zusammenhang die Einführung eines elektronischen Medikationsplans. „Der Medikationsplan soll Ärzten einen Überblick über die verschriebenen Medikamente verschaffen und so unerwünschte Wechselwirkungen vermeiden helfen". Wichtig ist das vor allem bei Menschen, die bei mehreren Ärzten in Behandlung sind und mehrere verschreibungspflichtige Medikamente gleichzeitig einnehmen.

(Bitkom-Pressemitteilung vom 14.04.2016)

GPS-Tracking erfordert DSB-Bestellung

In ihrem Jahresbericht 2015 (Ziff. 9.4.) sah die BInBfDI einen Verstoß gegen das BDSG bei einem Handwerksunternehmen, das die Dienstfahrzeuge seiner Mitarbeiter mit einem GPS-Ortungssystem ausgestattet hatte, u.a. darin, dass kein betrieblicher DSB bestellt worden war. Die BInBfDI stellt fest: „Unabhängig von der Anzahl der mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschäftigten Personen besteht eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten, wenn eine Vorabkontrolle erforderlich ist. Diese ist bei einem geplanten Einsatz eines Ortungssystems vorzunehmen, da die Verarbeitung der Positionsdaten dazu bestimmt werden kann, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge

Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA)

Vorbemerkung

Bereits heute benötigt und produziert das moderne Kraftfahrzeug eine Vielzahl an Daten. Aufgrund der fortschreitenden informationstechnischen Ausstattung der Kraftfahrzeuge und deren Anbindung an das Internet sowie der Vernetzung der Verkehrsteilnehmer untereinander wird sich dieser Trend fortsetzen und in den kommenden Jahren zu weitreichenden Veränderungen im Straßenverkehr führen. Darüber hinaus entstehen zahlreiche neue Fahrzeugfunktionen und Verkehrstelematikanwendungen, z.B. in den Bereichen Service und Multimedia. Die Digitalisierung und insbesondere die Vernetzung bergen neben den unbestreitbaren Vorteilen für die Verkehrssicherheit und den Komfort zugleich auch Risiken für die Persönlichkeitsrechte der Fahrzeugnutzer. Vor diesem Hintergrund halten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder und der VDA nachfolgende datenschutzrechtliche Aspekte für besonders relevant[1].

1. *Personenbezogenheit:* Bei der Nutzung eines modernen Kraftfahrzeugs wird permanent eine Vielzahl von Informationen erzeugt und verarbeitet. Insbesondere bei Hinzuziehung weiterer Informationen können die anfallenden Daten auf den Halter oder auch auf den Fahrer und Mitfahrer zurückführbar sein und Informationen über persönliche oder sachliche Verhältnisse einer bestimmbaren Person enthalten. Die bei der Kfz-Nutzung anfallenden Daten sind jedenfalls dann personenbezogen im Sinne des Bundesdaten-schutzgesetzes (BDSG), wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt.
2. Entscheidend ist der *Zeitpunkt der Datenerhebung* durch eine verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes. Hier ist zu unterscheiden, ob es sich um Kraftfahrzeuge handelt, bei denen eine Datenspeicherung innerhalb des Fahrzeuges stattfindet („offline"), oder ob eine Übermittlung von Daten aus dem Fahrzeug heraus erfolgt („online"), wie etwa bei der Über-mittlung und Speicherung von Fahrzeugdaten auf Backend-Servern.

   Bei „Offline"-Autos ist von einer Datenspeicherung ohne vorherige Erhebung auszugehen. Eine Erhebung liegt mangels Erfüllung des Tatbestandes des § 3 Abs. 3 BDSG nicht vor; gleichwohl fallen anlässlich der Kfz-Nutzung Daten an, die im Fahrzeug abgelegt werden. Diese Daten müssen geschützt werden und machen – vergleichbar der Regelung in § 6c BDSG (Mobile personenbezogene Speicher- und Verarbeitungsmedien) – auch eine Sicherung des Rechts auf informationelle Selbstbestimmung erforderlich. Erst wenn die im Fahrzeug abgelegten Daten z.B. von einer Werkstatt für Reparaturzwecke ausgelesen werden, kommt es zu einer Erhebung durch eine verantwortliche Stelle nach § 3 Abs. 3 BDSG.

   Bei „Online"-Autos findet bereits im Zeitpunkt der Datenkommunikation aus dem Fahrzeug heraus eine Erhebung durch eine verantwortliche Stelle im Sinne des § 3 Abs. 3 BDSG statt.
3. *Verantwortliche Stelle:* Auch für die Identifikation der verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG ist zwischen „Offline"- und „Online"-Autos zu differenzieren.

1 Datenschutzrechtliche Fragestellungen, die sich bei der Besitzüberlassung eines Kfz z.B. im Rahmen eines Dienst- oder Arbeitsverhältnisses oder einer Vermietung ergeben, sind nicht Gegenstand des vorliegenden Papiers.

Bei „Offline"-Autos wird derjenige, der personenbezogene Fahrzeugdaten aus dem Fahrzeug ausliest (d.h. erhebt) und anschließend verarbeitet, zur verantwortlichen Stelle. Hierbei wird es sich in der Regel um Werkstätten handeln.

Auch wenn die Hersteller bei „Offline"-Autos regelmäßig mangels Erhebung nicht bereits beim „Entstehen" der Daten verantwortliche Stelle sind, trifft diese unter anderem nach dem Gedanken „Privacy by Design" dennoch eine Verantwortung im Hinblick auf den Datenschutz. Dies gilt insbesondere, weil der Hersteller im Rahmen seiner technischen Gestaltungsmöglichkeiten (Art und Umfang von Schnittstellen, Zugriffsmöglichkeiten, Verfolgung der in § 3a BDSG niedergelegten Grundsätze von Datenvermeidung und -sparsamkeit) Einfluss auf die zeitlich nach hinten verlagerte Erhebung und Verarbeitung hat (vergleichbar der Regelung in § 6c BDSG). Sofern es um die technischen Gestaltungsmöglichkeiten geht, sind die Hersteller auch bei dieser Fahrzeugkategorie als Ansprechpartner für die Datenschutzaufsichtsbehörden anzusehen.

Bei „Online"-Autos sind diejenigen als verantwortliche Stellen anzusehen, die personenbezogene Daten erhalten, d.h. in der Regel die Hersteller und gegebenenfalls dritte Dienste-Anbieter. Insbesondere wenn Hersteller Zusatzdienstleistungen für das Kfz anbieten und dabei in ihren Backend-Servern Daten speichern, sind sie verantwortliche Stelle für diese Datenverarbeitung.

4. Die *Zulässigkeit der Datenerhebung und -verarbeitung* kann sich insbesondere aus § 28 Abs. 1 S. 1 Nrn. 1 oder 2 BDSG, §§ 11 ff. Telemediengesetz oder aus einer Einwilligung ergeben, die den Voraussetzungen des § 4a BDSG genügt.

   Wie die Informationen über Datenerhebungs- und -verarbeitungsvorgänge aufbereitet sein müssen, um Teil des Vertrags oder Grundlage für eine ggf. relevante informierte Einwilligung sein zu können (ausführliche Informationen im Sinne eines Verfahrensverzeichnisses oder strukturierte, überblicksartige Informationen), bleibt Frage des Einzelfalls. Der Erstkäufer kann die notwendigen Informationen jedenfalls vom Verkäufer (Hersteller oder herstellergebundener Händler) erhalten.

   Grundsätzlich sind die wichtigsten Informationen zur Datenverarbeitung in allgemein verständlicher Form auch in der Borddokumentation nachlesbar vorzuhalten, die der Hersteller bereitstellt.

5. Gegenüber dem Hersteller besteht ein unentgeltliches *Auskunftsrecht* des Halters über seine durch den Hersteller erhobenen und gespeicherten personenbezogenen Daten nach § 34 BDSG. Darüber hinaus besteht aus § 34 BDSG kein datenschutzrechtliches Auskunftsrecht des Halters gegenüber dem Hersteller allein aufgrund dessen Gesamtverantwortung für die Gestaltung der datenspeichernden Systeme. Die Fahrzeughalter von „Offline"-Autos haben die Möglichkeit des Auslesens von Daten, ggf. mithilfe von Sachverständigen, was nicht zwingend unentgeltlich sein muss. Aufgrund des Transparenzgebots muss der Betroffene sich unentgeltlich und ohne sachverständige Hilfe über die Grundsätze der Datenverarbeitungsvorgänge einschließlich zumindest der Art der verarbeiteten personenbezogenen Daten beim Hersteller informieren können.

6. In Bezug auf die *Datenhoheit* sollen die Fahrzeugnutzer durch verschiedene Optionen über die Verarbeitung und Nutzung personenbezogener Daten selbst bestimmen können. Die Automobilhersteller streben an, durch standardisierte Symbole im Cockpit den aktuellen Vernetzungsstatus des Fahrzeugs erkennbar anzuzeigen und Möglichkeiten der jederzeitigen Aktivierung und Deaktivierung dieses Status' vorzusehen. Einschränkungen der Löschbarkeit bestehen bei rechtlichen Verpflichtungen oder dann, wenn entsprechende Daten im Zusammenhang mit Garantie- sowie Gewährleistungen oder der Produkthaftung von Bedeutung sind oder deren Verfügbarkeit für den sicheren Fahrzeugbetrieb erforderlich ist. Vom Nutzer eingegebene Informationen (z.B. Komfortdaten wie Sitzeinstellung, bevorzugte Radiosender, Navigationsdaten, E-Mail-/SMS-Kontaktdaten, etc.) muss der Nutzer jederzeit selbst ändern oder zurückstellen können.

Eine neue Rolle für Gewerkschaften in der digitalen Arbeitswelt

Arbeitszeitgesetz und Arbeitsstättenverordnung an die digitale Arbeitswelt anpassen

Durch die Digitalisierung verändert sich nicht nur die Arbeitswelt, auch die Gewerkschaften stehen vor einschneidenden Veränderungen. Dabei gehen acht von zehn Unternehmen in Deutschland (82 Prozent) davon aus, dass Gewerkschaften vor dem Hintergrund der Digitalisierung auch künftig eine Rolle spielen werden. Immerhin jedes sechste Unternehmen (16 Prozent) erwartet umgekehrt, dass Gewerkschaften künftig keine Rolle mehr spielen werden. Das ist das Ergebnis einer repräsentativen Befragung im Auftrag des Digitalverbandes Bitkom unter 504 Geschäftsführern und Personalverantwortlichen von Unternehmen ab 10 Mitarbeitern. Vor allem im Handel und in der Industrie (jeweils 19 Prozent) wird die Zukunft der Gewerkschaften skeptisch gesehen, bei Dienstleistern (10 Prozent) liegt der Anteil deutlich darunter. „Digitalisierung verändert die Geschäftsmodelle der Unternehmen und die Art, wie Menschen arbeiten. Das beruht auch auf neuen Arbeitsformen wie Crowdworking, aber auch auf hochspezialisierten Experten, die ihre Dienste freiberuflich auf Zeit zur Verfügung stellen".

Vor allem Dienstleistungsunternehmen (57 Prozent) und Industrie (52 Prozent) sehen Bedarf an einer breiteren Debatte zu Arbeitsbedingungen. „Arbeitszeitgesetz oder Arbeitsstättenverordnung orientieren sich immer noch zu stark an einem Bild von Arbeit, das aus dem vorigen Jahrhundert stammt. So geben 56 Prozent der Befragten an, die Arbeitsstättenverordnung, die etwa Vorgaben für Arbeit im Home Office macht, verhindere eine flexiblere Arbeitsorganisation in ihrem Unternehmen. Und jeder Dritte (33 Prozent) wünscht sich eine Flexibilisierung des Arbeitszeitgesetzes, etwa durch Öffnungsklauseln.

(Bitkom-Pressemitteilung vom 29.4.2016)

Literaturhinweise

Buchbesprechungen

Christina M. Berchtold, **Der Wandel genetischer Information**, Personalisierte Medizin zwischen Informations- und Verschwiegenheitsinteressen, Schriften zum Gesundheitsrecht, Band 40, Duncker & Humblot, Berlin 2016, 389 S., Print: 89,90 €, E-Book: 79,90 €, Print & E-Book: 107,90 €.

Gegenstand der Arbeit ist der Wandel genetischer Informationen, der sich gegenwärtig im Kontext der personalisierten Medizin vollzieht.

Die Besonderheit genetischer Information spiegelt dabei das Spezifikum diagnostischer und prädiktiver Gendiagnostik wider: Sowohl der Drittbezug der gendiagnostischen Ergebnisse als auch die auf Wahrscheinlichkeiten und Risikoabschätzungen beruhenden Diagnosen konfrontieren den Einzelnen mit multipolaren Interessenkonflikten, die nationale und auch europäische Normen zu adressieren suchen.

Die zentrale Herausforderung einer gesetzlichen Regulierung der Genmedizin ist insoweit eine angemessene diagnostische Wissensbalance, die den Konflikt zwischen Information und Verschwiegenheit von Betroffenen und Angehörigen im Einzelfall auflöst. In Zeiten der Postgenomics wird ein persönlich-kooperatives und informationsrechtlich umhegtes Miteinander einer freien, individuell geführten Abwägungsentscheidung über genetisches Wissen oder Nichtwissen zum rechtlichen Maßstab einer Neugestaltung des Arzt-Patienten-Verhältnisses.

(Redaktion)

Thorsten Hennrich, **Cloud Computing – Herausforderungen an den Rechtsrahmen für Datenschutz**, Internetrecht und Digitale Gesellschaft Band 4, Duncker & Humblot, Berlin 2016, 341 S., Print: 89,90 €, E-Book: 79,90 €, Print & E-Book: 107,90 €.

Cloud Computing steht für das flexible, dynamische, skalierbare und bedarfsorientierte Anbieten, Nutzen und Abrechnen von Infrastruktur- und Anwendungskomponenten über das Internet »als Dienst«. Die vielfältigen Chancen und Vorteile von Cloud Computing treffen jedoch auf einen Rechtsrahmen, der die Besonderheiten (global) verteilter, multimandantenfähiger und virtualisierter IT-Infrastrukturen konzeptionell noch gar nicht zu berücksichtigen hatte. Die zentralen Herausforderungen von Cloud Computing an den Rechtsrahmen für Datenschutz werden auf Grundlage des BDSG und der Entwicklungen im Zuge der EU-Datenschutzreform praxisnah und anhand typischer Spannungsfelder erörtert. Im Fokus stehen das anzuwendende Datenschutzrecht, der Personenbezug von Daten, die Daten- und Informationssicherheit sowie die Auftragsdatenverarbeitung. Da globale Datenströme das technische Rückgrat einer globalisierten Weltwirtschaft bilden, liegt ein Schwerpunkt auch auf internationalen Datentransfers – aus Gründen der Praxisrelevanz vor allem in die USA auf Basis der „Safe-Harbor-Vereinbarung".

(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.

Albrecht, Jan Philipp, **Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung,** CR 2016, 88 ff.

Der Autor gibt einen Überblick und schildert Hintergründe des finalen Textes der Datenschutz-Grundverordnung.

Alexander, Christian, **Digitaler Nachlass als Rechtsproblem?**, K&R 2016, 301 ff.

Digitale Daten überdauern den Tod eines Menschen. Der Beitrag untersucht, welche Rechtsprobleme mit dem digitalen Nachlass verbunden sind und welche Lösungsansätze in Betracht kommen.

Höller, Heinz-Peter, **Mining the Enterprise Social Graph,** CuA 5/2016, 8 ff.

Die Vernetzungs- und Kooperationsstrukturen im Unternehmen werden als der soziale Graph des Unternehmens bezeichnet, der zunehmend eine Analyse der Verhaltensweisen von einzelnen Beschäftigten ermöglicht.

Schaar, Katrin, **DS-GVO: Geänderte Vorgaben für die Wissenschaft,** ZD 2016, 224 ff.

Neben allgemein für die Wissenschaft relevanten Änderungen des Datenschutzrechts wird speziell eingegangen auf die Forschung mit sensiblen speziell genetischen Daten und Fragen von Open Data.

Schmitz, Barbara/Dall`Armi von, Jonas, **Standardvertragsklauseln – heute und morgen,** ZD 2016, 217 ff.

Der Beitrag erörtert Standardvertragsklauseln als Grundlage für den Drittlandtransfer nach derzeitigem Recht und nach der DS-GVO.

Schnabel, Christoph, **Rechtswidrige Praktiken als Betriebs- und Geschäftsgeheimnisse?**, CR 2016, 342 ff.

Betriebs- und Geschäftsgeheimnisse stellen einen wichtigen Vermögenswert für Unternehmen dar. Der Gesetzgeber schützt sie durch effektive strafrechtliche und wettbewerbsrechtliche Regelungen. Der Autor wendet sich dagegen, wenn auch rechtswidrige Praktiken dem Schutz unterstellt werden sollen, d.h. z. B. Vorgehensweisen wie die Manipulation von Abgasmessungen als rechtswidrige, aber verkaufs- und umsatzfördernde Maßnahme Schutz als Betriebs- und Geschäftsgeheimnis in Anspruch nehmen. Abschließend wird erläutert, ob und welche Veränderungen insoweit durch die Richtlinie über den Schutz von Geschäftsgeheimnissen zu erwarten sind.

Spindler, Gerald, **IT-Sicherheitsgesetz und zivilrechtliche Haftung,** CR 2016, 297 ff.

Nach einer knappen Einleitung präsentiert der Beitrag zunächst die Strukturen des IT-Sicherheitsgesetzes und sodann die wesentlichen Regelungen der NIS-Richtlinie der EU. Im Schwerpunkt werden zivilrechtliche Haftung und Haftungsrisiken erörtert, die aus beiden Regelungswerken resultieren.

Weichert, Thilo, **Die Zukunft des Datenschutzbeauftragten,** CuA 4/2016, 8 ff.

Nach Weichert wird das Amt des DSB durch die DS-GVO aufgewertet und gestärkt. Der nationale Gesetzgeber müsse aber jetzt seine Beziehung zur Arbeitnehmervertretung konkretisieren.

Wybitul, Tim, **Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte?,** ZD 2016, 203 ff.

Der Beitrag erhält einen Kurzüberblick über für die Praxis wesentlichen Rechtsänderungen im Beschäftigtendatenschutz und geht speziell auf die künftige Gestaltung durch Betriebsvereinbarungen ein.

Hilfssheriffs im Straßenverkehr

Dashcams sind Kameras für das Armaturenbrett im Auto. Sie sind für viele eine nützliche Sache. Sie filmen und speichern den Verkehr und natürlich auch Verkehrsverstöße. In Süddeutschland wurde ein Rotlichtsünder jetzt vor Gericht mit Hilfe einer solchen Aufnahme aus einem nachfolgenden Fahrzeug überführt und verurteilt.

Dass Datenschützer eine solche permanente gegenseitige Videoüberwachung für unzulässig halten, ist die eine Sache. Das Oberlandesgericht Stuttgart hat jetzt entschieden, dass auch datenschutzrechtlich verbotene Aufnahmen als Beweismittel benutzt werden dürfen. Das ist strafprozessrechtlich wenig überraschend, weil man hierzulande auch Früchte von verbotenen Bäumen pflücken darf. Es ist ein wenig so, wie bei den Informationen über Steuersünder aus „Steuer-CDs". Was der Staat daraus erfährt, darf auch dann verwendet werden, wenn die CDs selbst illegal beschafft wurden. Das ist zwar einerseits gerecht. Andererseits kann es aber dazu führen, dass wir uns alle irgendwann mit Kameras gegenseitig filmen, um uns anzuschwärzen.

Man hat zwar kein Recht darauf, dem Staat bei einem Verkehrsverstoß durch die Lappen zu gehen. Bislang konnte man aber davon ausgehen, dass man ungeschoren bleibt, wenn man nicht vom Staat – etwa per Blitze – überführt wird. Das ist jetzt vorbei, wenn ein höheres Gericht es nicht anders entscheidet.

Strafprozessrecht ist das eine, aber Datenschutzrecht ist das andere. Unabhängig von der Frage des Beweismittels kann also ordentlich Ärger mit der Datenschutzaufsicht drohen, wenn man künftig munter spitzelnd die Landschaft filmt. Verboten ist es auch, Aufnahmen von Unglücksfällen zu vermarkten. Wenn man es abgesehen davon darauf anlegt, anlasslos Beweismaterial für künftige Rechtsfälle zu sammeln, dann hat man mit dem neuen Urteil gute Argumente das zu tun. Ob man gut beraten ist, davon Gebrauch zu machen, hängt davon ab, ob wir uns als selbsternannte Hilfssheriffs sehen.