

Zeitschrift für
Datenschutz-,
Informations- und
Kommunikationsrecht

RDV

5/2017

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

EICKELPASCH, Die zweite Stufe der Anpassung des Datenschutzrechts des Bundes an die EU-Datenschutz-Grundverordnung

KROHM, Die wirtschaftliche Einheit als Bußgeldadressat unter der Datenschutz-Grundverordnung?

JACQUEMAIN, Haftung privater Stellen bei Datenschutzverstößen

ROLF/SIEWERT, Überlegungen zu den Rechtsgrundlagen des künftigen Beschäftigtendatenschutzes

Kurzbeiträge

GOLA, Aus den aktuellen Berichten der Aufsichtsbehörden (32): Beschäftigtendatenschutz und Datenschutzkontrolle

LEPPERHOFF, Gehaltsdaten für Benchmarks übermitteln – zulässig?

Rechtsprechung

Aus dem Inhalt

BGH, Zur Zulässigkeit einer allgemeinen Schweigepflichts-entbindung gegenüber einem Versicherer

BGH, Dynamische IP-Adresse als personenbezogenes Datum

OLG KARLSRUHE, Anforderungen an eine Einwilligung

VGH BADEN-WÜRTTEMBERG, Presserechtlicher Auskunftsanspruch gegenüber Staatsanwaltschaft (Ls)

ARBG BERLIN, Keine Taxifahrerüberwachung im Minutentakt (Ls)

ARBG HEILBRONN, Mitbestimmung bei Einrichtung und Betrieb einer Smartphone-App mit Kundenfeedbackfunktion

33. Jahrgang
Oktober 2017
Seiten 217–XXX



Gesellschaft für Datenschutz
und Datensicherheit e.V.



www.rdv-online.de

Die B·A·D Gruppe betreut mit mehr als 3.700 Experten europaweit 270.000 Betriebe mit 4 Millionen Beschäftigten in den verschiedenen Bereichen der Gesundheitsvorsorge und der Arbeitssicherheit. Allein in Deutschland betreiben wir 200 Gesundheitszentren. Damit gehören wir mit unseren Tochtergesellschaften zu den größten europäischen Anbietern von Präventionsdienstleistungen.

Syndikusanwalt (m/w)

für den Fachbereich Datenschutz und Vertragsrecht

Zentrale in Bonn – Voll- oder Teilzeit

Kennziffer IT-S/RDV

Unser Angebot:

- Zukunftssichere Beschäftigung in einem modernen Dienstleistungsunternehmen
- Leistungsbezogene Vergütung
- Betriebliche Altersvorsorge
- Strukturierte Einarbeitung sowie umfassende Möglichkeit zur Fortbildung
- Innerbetriebliches Gesundheitsmanagement
- Kooperation mit der AWO Lifebalance
- Car-Rent-Sharing-Modell

Ihre Aufgaben:

- Beratung der Geschäftsführung, des Datenschutzbeauftragten und verschiedener Fachabteilungen zum Datenschutz und zu vertragsrechtlichen Fragen
- Unterstützung bei der Implementierung von Datenschutz-Anforderungen in Geschäftsprozesse
- Rechtliche Beratung bei Projekten im Hinblick auf mögliche Datenschutz-Risiken
- Durchführung von Schulungen zum Datenschutz und/oder Vertragsrecht
- Zusammenarbeit und Verhandlungen mit externen Anwälten

Ihr Profil:

- Überdurchschnittlich erfolgreich abgeschlossene Examina
- Idealerweise einschlägige Berufserfahrung im Bereich Datenschutz und Vertragsrecht
- Affinität zu IT-, Informations- und Datensicherheit
- Hohes analytisches Denkvermögen sowie eine strukturierte und selbstständige Arbeitsweise
- Hohes Durchsetzungsvermögen und souveränes Auftreten
- Sehr gute MS Office-Kenntnisse
- Sehr gute Deutsch- und Englischkenntnisse

Unsere Mitarbeiter sind unser wertvollstes Kapital!

Gehören Sie bald auch zu uns?

Wir freuen uns auf Ihre Bewerbung unter Angabe der o. g. Kennziffer per E-Mail an

bewerbungen@bad-gmbh.de oder an:

B·A·D GmbH
Personalentwicklung und Recruiting
Frau König, Tel. 0228/40072-720
Herbert-Rabius-Straße 1, 53225 Bonn

»Personalentwicklung wird bei der B·A·D GmbH groß geschrieben. Ich werde gefordert und gefördert. Dank eines umfangreichen internen Seminarprogramms und externen Schulungen kann ich meine Kompetenzen erweitern und mich beruflich weiterentwickeln.«

Danica Greis, Managerin
Online-Marketing,
B·A·D-Zentrale



B·A·D
GESUNDHEITSVORSORGE UND
SICHERHEITSTECHNIK GMBH

Inhaltsverzeichnis

Editorial

- 217 Anforderungen an eine Einwilligung
(OLG Karlsruhe, Beschluss vom 28.06.2017) 253

Veranstaltungen

- 218 Presserechtlicher Auskunftsanspruch gegenüber
Staatsanwaltschaft (Ls)
(VGH Baden-Württemberg, Beschluss vom 04.08.2017) 254

Aufsätze

- Jörg EICKELPASCH
Die zweite Stufe der Anpassung des Datenschutz-
rechts des Bundes an die EU-Datenschutz-
Grundverordnung 219

- Dr. Niclas KROHM
Die wirtschaftliche Einheit als Bußgeldadressat
unter der Datenschutz-Grundverordnung? 221

- Dr. Tobias JACQUEMAIN
Haftung privater Stellen bei Datenschutzverstößen 227

- RA Dr. Christian ROLF/Katharina SIEWERT
Überlegungen zu den Rechtsgrundlagen des
künftigen Beschäftigtendatenschutzes 236

Kurzbeiträge

- Prof. Peter GOLA
Aus den aktuellen Berichten der Aufsichtsbehörden
(32): Beschäftigtendatenschutz und Datenschutz-
kontrolle 240

- Dr. Niels LEPPERHOFF
Gehaltsdaten für Benchmarks übermitteln
– zulässig? 242

Rechtsprechung

- Zur Zulässigkeit einer allgemeinen Schweigepflichts-
entbindung gegenüber einem Versicherer
(BGH, Urteil vom 05.07.2017) 245

- Dynamische IP-Adresse als personen-
bezogenes Datum
(BGH, Urteil vom 16.05.2017) 249

- 253 Anforderungen an eine Einwilligung
(OLG Karlsruhe, Beschluss vom 28.06.2017)

- 254 Presserechtlicher Auskunftsanspruch gegenüber
Staatsanwaltschaft (Ls)
(VGH Baden-Württemberg, Beschluss vom 04.08.2017)

- 254 Keine Taxifahrerüberwachung im Minutentakt (Ls)
(ArbG Berlin, Urteil vom 10.08.2017)

- 254 Mitbestimmung bei Einrichtung und Betrieb einer
Smartphone-App mit Kundenfeedbackfunktion
(ArbG Heilbronn, Beschluss vom 08.06.2017)

- 258 Zulässigkeit von On-Board-Kameras
(VerwG Göttingen, Urteil vom 31.05.2017)

Berichte, Informationen, Sonstiges

- 263 Internationale Arbeitsgruppe für Datenschutz in
der Telekommunikation: Arbeitspapier zum Thema
E-Learning-Plattformen

Literaturhinweise

Buchbesprechungen

- 268 *Schaffland/Wiltfang*, Datenschutz-Grundverordnung
(DS-GVO)/ Bundesdatenschutzgesetz (BDSG),
(SCHRIFTLEITUNG)

- 268 *Eßer/Kramer/von Lewinski* (Hrsg.) DS-GVO/BDSG –
Datenschutz-Grundverordnung, Bundesdatenschutz-
gesetz und Nebengesetze,
(PROF. PETER GOLA)

- 268 *Lutz Orgelmann*, Die rechtlichen Grenzen der
Nutzung von E-Books
(SCHRIFTLEITUNG)

Neuerscheinungen

- 269 Aufsätze

- 270 **Nachgefasst**

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

Prof. Dr. Rolf SCHWARTMANN, Leiter der Kölner Forschungsstelle für Medienrecht,
Technische Hochschule 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 LINNENKOHLE, 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 Bundesarbeits-
gericht a.D.

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

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

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

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 5/2017; 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

Willmuthstraße 30, 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

Telefax: (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
33. Jahrgang 2017 Heft 5
Seiten 217–270

RDV

Recht der Datenverarbeitung

33. Jahrgang · Oktober 2017 · Seiten 217–270

Editorial

Herausforderungen des Datenschutzrechts 2018

Das „alte“ Bundesdatenschutzgesetz ist noch einige Monate als geltendes Recht anzuwenden und dennoch betrachten wir Datenschützer es faktisch schon jetzt als Geschichte. Uns befasst die ab 25. Mai 2018 anwendbare Datenschutz-Grundverordnung und sie wirft drängende Fragen auf. Wie gehen wir in der Praxis mit Löschpflichten und den Möglichkeiten der Pseudonymisierung um? Bleibt im Beschäftigtendatenschutz wirklich alles beim Alten und was ändert sich für den betrieblichen Datenschutzbeauftragten? Bevor Datenschutz-Grundverordnung und neues BDSG anwendbar sind, wird deren Recht durch den Entwurf der ePrivacy-Verordnung schon in einen neuen Kontext gestellt. Für den Datenschutz bei Onlinediensten ist die DS-GVO schließlich überhaupt nicht einschlägig und die Datenschutzvorschriften des Telemediengesetzes werden mit Anwendbarkeit der DS-GVO in weiten Teilen ihre Geltung verlieren. Bevor wir die Herausforderungen des neuen Datenschutzrechts vollständig fokussiert haben, muss sich die Onlinewirtschaft auf weiteres, neues Datenschutzrecht einstellen. Schließlich soll die ePrivacy-Verordnung die DS-GVO schon ab dem 25.05.2018 ergänzen.

Natürlich interessieren uns neben der „zweiten Runde“ der gesetzlichen Umsetzung der DS-GVO in Deutschland (dazu der Beitrag von Eickelpasch in diesem Heft) in erster Linie die Positi-

onen der Aufsicht. Das gilt für die „Workingpapers“ der Art. 29-Gruppe zu Auslegungsfragen zum neuen Recht wie etwa zum Datenschutzbeauftragten, zur Datenportabilität oder zur Datenschutzfolgenabschätzung. Daneben stehen die Kurzpapiere der Datenschutzkonferenz (DSK) als konsolidierten Stimme der Aufsicht in Deutschland. Noch sind diese Papiere unverbindlich. Sobald aber die Art. 29-Gruppe zum Datenschutzausschuss wird, erlangen deren Position Verbindlichkeit. Schaut man etwa auf die „Leitlinien zum Recht auf Datenübertragbarkeit“ (WP 242), dann bekommt man einen Eindruck davon, wie weit das Recht auf Übertragung eingebrachter Daten reichen soll, indem es etwa die von Gesundheitstrackern aufgezeichnete Herzfrequenz erfasst.

Die Wirtschaft stellt diese neuen „faktischen“ Rechtsquellen vor Herausforderungen und sie werfen auch Widersprüche auf. Das Kurzpapier Nr. 10 der DSK zu Informationspflichten bei Dritt- und Direkterhebung vom 30.08.2017 erklärt den Medienbruch bei gestufter Informationerteilung nach Art. 13 und 14 DS-GVO in der Regel für unzulässig. Nach ErwG 58 der DS-GVO können solche Informationen aber auch über Webseiten zur Verfügung gestellt werden. Insofern ist zu hoffen, dass die Aufsicht ihre Position revidiert. In welche Richtung es für die Praxis beim Medienbruch gehen

kann, schlägt die GDD-Praxishilfe „DS-GVO VII zu Transparenzpflichten bei der Datenverarbeitung“ vor.

Es ist für die Wirtschaft höchste Zeit, die Herausforderungen des Datenschutzrechts 2018 anzunehmen, während weitere Stufen der Reform des deutschen Datenschutzrechts in den Ministerien des Bundes und zunehmend auch der Länder in Angriff genommen werden und sich auch die Aufsicht auf ihre neuen Aufgaben vorbereitet. Arbeiten wir alle an Lösungen für einen Datenschutz mit Augenmaß.

Professor Dr. Rolf Schwartmann



Prof. Dr. Rolf Schwartmann

Leiter der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln, Mitherausgeber von *Recht der Datenverarbeitung (RDV)* sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

Termin	Thema	Ort	Kontakt
15.11.2017	36. RDV-Forum	Köln	GDD e.V. und DATAKONTEXT
16.-17.11.2017	41. DAFTA „Perspektiven des Datenschutzrechts 2018 – Anforderung und Praxis“	Köln	GDD e.V. und DATAKONTEXT
21.11.2017	Datenlöschung und andere SAP-Funktionen für den Datenschutz	Köln	GDD e.V. und DATAKONTEXT
22.11.2017	Die Wahrnehmung der Überwachungsaufgaben des DSB gemäß DS-GVO	Köln	GDD e.V. und DATAKONTEXT
27.11.2017	Repetitorium GDDcert.	Köln	GDD e.V. und DATAKONTEXT
27.11.2017	Verfahrensverzeichnis, Verarbeitungsübersicht, Vorabkontrolle	Stuttgart	GDD e.V. und DATAKONTEXT
30.11.2017	Strafverfolgung, Whistleblowing, Internal Investigations – Datenschutz und Strafrecht	Köln	GDD e.V. und DATAKONTEXT
27.11.-01.12.2017	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
05.12.2017	Datenschutzkonforme Unternehmenskommunikation	Köln	GDD e.V. und DATAKONTEXT
04.-06.12.2017	SAP ERP für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
14.12.2017	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert.)	Köln	GDD e.V. und DATAKONTEXT
23.01.2018	Tätigkeitsbericht des betrieblichen Datenschutzbeauftragten	Köln	GDD e.V. und DATAKONTEXT
29.-30.01.2018	GDD-Winter-Workshop	Garmisch-Partenkirchen	GDD e.V. und DATAKONTEXT
06.-07.02.2018	Update-Workshop zur DS-GVO	Köln	GDD e.V. und DATAKONTEXT
20.02.2018	ISO 27001 und Datenschutz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
21.02.2018	Ausgewählte Themen zur Implementierung der DS-GVO in die Unternehmensorganisation	Düsseldorf	GDD e.V. und DATAKONTEXT
27.02.2018	Videüberwachung nach neuem BDSG und DS-GVO	Köln	GDD e.V. und DATAKONTEXT
26.02.-02.03.2018	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
05.03.2018	Basiswissen IT-Sicherheit	Frankfurt/M.	GDD e.V. und DATAKONTEXT
06.03.2018	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Frankfurt/M.	GDD e.V. und DATAKONTEXT
12.03.2018	Verfahrensverzeichnis, Verarbeitungsübersicht, Vorabkontrolle	Berlin	GDD e.V. und DATAKONTEXT
13.03.2018	DS-GVO-konforme Prüfung personenbezogener Daten mit SAP-Systemen	Berlin	GDD e.V. und DATAKONTEXT
14.03.2018	Dokumentation, Meldepflichten und IT-Sicherheitsmanagement nach DS-GVO	Köln	GDD e.V. und DATAKONTEXT
15.03.2018	Auftragsverarbeitung nach DS-GVO – Grundlagen für den Übergang vom BDSG zur DS-GVO	Köln	GDD e.V. und DATAKONTEXT
20.03.2018	Beschäftigtendatenverarbeitung: Zulässigkeit und Organisation	Stuttgart	GDD e.V. und DATAKONTEXT

Aufsätze

Jörg Eickelpasch*

Die zweite Stufe der Anpassung des Datenschutzrechts des Bundes an die EU-Datenschutz-Grundverordnung

Mit der am 5. Juli 2017 erfolgten Verkündung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU - DSAnpUG-EU) im Bundesgesetzblatt konnte die 1. Stufe der Anpassungen des Bundesrechts an die EU-Datenschutzreform erfolgreich abgeschlossen werden. Die Schwierigkeit bestand dabei darin, ein möglichst kohärentes, für den Anwender praktikables System zu schaffen. Zentraler Kern des DSAnpUG-EU ist ein grundlegend neu konzipiertes BDSG (BDSG 2018).

Mit dem Abschluss der 1. Stufe der Anpassungsarbeiten steht den Verantwortlichen in Deutschland Zeit zur Verfügung, ihre Datenverarbeitung auf das allgemeine Datenschutzrecht, bestehend aus der Verordnung (EU) 2016/679 (DS-GVO), der Richtlinie (EU) 2016/680 (DS-RL) und dem BDSG 2018 umzustellen. Zudem hat der Bundesgesetzgeber das erforderliche Fundament gelegt, um nunmehr in einer zweiten Reformstufe das ausdifferenzierte bereichsspezifische Datenschutzrecht, das sich in ca. 200 Normen des Bundesrechts findet, an das künftige allgemeine Datenschutzrecht anzupassen.

I. Zentrale Aspekte der Anpassung des bereichsspezifischen Bundesrechts an die DS-GVO

Folgende Aspekte sind im Rahmen der Anpassungsgesetzgebung des Fachrechts von zentraler Bedeutung:

1. Rechtsgrundlagen für die Datenverarbeitung

Es finden sich aktuell in den Fachgesetzen unterschiedliche Ausgestaltungen der Rechtsgrundlagen für die Datenverarbeitung.

a) Allgemeine Aufgabenzuweisungsnorm

Teils wird im Fachrecht einer bestimmten Behörde eine konkrete Aufgabe zur Erledigung zugewiesen („Aufgabenzuweisungsnorm“), ohne dass das Fachgesetz eine Rechtsgrundlage für die Datenverarbeitung liefert. Dieser Ansatz kann im Einklang mit der DS-GVO fortgeführt werden. Dies ergibt sich aus Artikel 6 Absatz 3 Satz 1 DS-GVO, wonach die nationalen Gesetzgeber weiterhin die Rechtsgrundlagen für Verarbeitungen nach Artikel 6 Absatz 1 Buchstaben c und e DS-GVO setzen dürfen. Auch wenn dies in der aktuellen Diskussion um Spielräume der DS-GVO teilweise anders gesehen wird, ist der Verordnungstext nicht zuletzt in der englischen Textfassung eindeutig („The basis for the processing referred to in point c and e of paragraph 1 shall be laid down by...or Member state law“..). Die Rechtsgrundlage der Datenverarbeitung findet sich in diesen Fällen anknüpfend an die fachgesetzliche Aufgabenzuweisungsnorm künftig in dem allgemeinen Auffangtatbestand des § 3 BDSG 2018.

Diese Konstruktion kann aber nur in einfacher gelagerten Fällen tragen. Je grundrechtsintensiver eine Datenverarbeitung ist, desto präziser muss der Gesetzgeber weiterhin die Einzelheiten der Verarbeitung („welche Daten zu welchem Zweck verarbeitet werden“) gesetzlich normieren.

b) Konkrete Rechtsgrundlage für die Datenverarbeitung

Regelmäßig enthält das Fachrecht selbst eine konkrete Rechtsgrundlage für die Datenverarbeitung durch eine zuständige Behörde. Im Fachgesetz erlaubt der Gesetzgeber einer öffentlichen Stelle, bestimmte Daten zu einem konkreten Zweck verarbeiten zu dürfen. Diesen Ansatz kann der nationale Gesetzgeber ebenfalls beibehalten und sich dabei sowohl auf Artikel 6 Absatz 2 als auch auf Artikel 6 Absatz 3 Sätze 2 f. DS-GVO stützen. Die präzisen Regelungen im bereichsspezifischen Fachrecht sind im Übrigen mit Blick auf den strengen Gesetzesvorbehalt, den das BVerfG 1983 mit dem Volkszählungsurteil aufgestellt hat, verfassungsrechtlich weiterhin geboten.

c) Einwilligung als Rechtsgrundlage der Datenverarbeitung

In manchen bereichsspezifischen Gesetzen des Bundes wird als Rechtsgrundlage für die Datenverarbeitung durch öffentliche Stellen auch die Einwilligung aufgeführt. Dies er-

* Der Beitrag gibt ausschließlich die persönliche Auffassung des Autors wieder.

scheint europarechtlich ab Mai 2018 problematisch. Schließlich gilt auch für den sogenannten öffentlichen Bereich die Rechtsgrundlage „Einwilligung“ gemäß Artikel 6 Absatz 1 Buchstabe a DS-GVO unmittelbar.

2. Verweise

Die Ressorts prüfen derzeit die Verweise im Fachrecht auf das bis zum 24. Mai 2018 geltende BDSG. Teils können die Verweise ersetzt werden durch solche auf das BDSG 2018. Sollte sich der Inhalt der Norm des jetzigen BDSG ab dem 25. Mai 2018 aus der DS-GVO ergeben, wie z.B. für Definitionen, Auftragsverarbeitung, technisch-organisatorische Maßnahmen oder auch den Drittstaatentransfer, hat der Gesetzgeber zwei Möglichkeiten. Er kann den Verweis ersatzlos streichen, schließlich gilt die DS-GVO unmittelbar. Alternativ kann er, aus Gründen der Rechtsklarheit, auf die DS-GVO verweisen. Beide Varianten sind europarechtlich zulässig und sind im Übrigen auch im BDSG 2018 zu finden.

3. Begriffsbestimmungen

Die bisherigen nationalen Begriffsverwendungen sind an Artikel 4 DS-GVO anzupassen. Das klingt trivial. Ist es auch, soweit lediglich z.B. „Betroffener“ durch „betroffene Person“, „verantwortliche Stelle“ durch „Verantwortlicher“ oder der „Auftragsdatenverarbeiter“ durch „Auftragsverarbeiter“ zu ersetzen ist.

Anspruchsvoller gestaltet sich diese Prüfung aber im Zusammenhang mit dem Begriff der „Verarbeitung“.

Im EU-Recht umfasst die Definition der „Verarbeitung“ schon seit der Richtlinie 95/46/EG sämtliche Teilschritte der Verarbeitung. Die DS-GVO hat diesen weiten Verarbeitungsbegriff in Artikel 4 Ziffer 2 DS-GVO fortgeführt, indem unter „Verarbeitung“ eine nicht abschließende Liste der Teilschritte aufgeführt ist.

Hingegen unterscheidet der deutsche Gesetzgeber in § 3 Absätze 3 bis 5 des bis zum 24. Mai 2018 geltenden BDSG nach der Trias des „Erheben, Verarbeiten und Nutzen“ und zudem in § 3 Absatz 4 Ziffern 1 bis 5 BDSG nach den fünf Teilschritten „Speichern, Verändern, Übermitteln, Sperren und Löschen“ der Verarbeitung.

Bei der Prüfung des Fachrechts ist nun im Einzelfall zu entscheiden, ob man den Begriff des „Verarbeitens“ unverändert fortführt. Tut man dies, so gilt hier ab dem 25. Mai 2018 die weite Begriffsbestimmung des Artikels 4 Ziffer 2 DS-GVO. Konsequenz wäre, dass der Verantwortliche sehr viel mehr darf als heute nach der engen Definition des „Verarbeitens“ gemäß § 3 Absatz 4 BDSG. So hätte er nunmehr z.B. auch eine Rechtsgrundlage zum Erheben der Daten. Will man dies vermeiden, muss man konkret die Teilschritte der Verarbeitung benennen, zu denen der Verantwortliche berechtigt sein soll. Dabei kann man auf gewohnte Begriffe wie „Erheben“, „Speichern“, „Verändern“, „Übermitteln“ etc. aber zurückgreifen, wobei es keine nationale Begriffsbestimmung dieser Teilaspekte der Verarbeitung mehr geben wird. Die DS-GVO enthält keine entsprechenden Definitionen, und der nationale Gesetzgeber hat keinen Spielraum mehr, die Begriffe zu definieren.

4. Rechte der betroffenen Personen

Unmittelbar regelt ab dem 25. Mai 2018 die DS-GVO im Kapitel III die Rechte der betroffenen Personen. Ausnahmen von den einzelnen Rechten in den Artikeln 12 bis 22 DS-GVO enthalten die DS-GVO selbst sowie punktuell und ergänzend das BDSG 2018. Ausnahmen im nationalen Recht müssen sich dabei an den Maßstäben in Artikel 23 DS-GVO messen lassen.

Im bereichsspezifischen Fachrecht des Bundes finden sich hinsichtlich der Rechte der betroffenen Personen aktuell unterschiedliche Ansätze: Teilweise hat der Gesetzgeber sowohl die Rechte der betroffenen Personen als auch die Ausnahmen spezifisch geregelt. Teils wird fachgesetzlich derzeit auf die Rechte aus dem BDSG verwiesen, um dann einzelne Ausnahmen neben den allgemeinen Ausnahmen nach dem BDSG vorzusehen. Nicht immer ergibt sich dabei rechtsklar aus den Normen des Bundesrechts, wie sich das Fachrecht und das BDSG zueinander verhalten.

In beiden genannten Fällen muss das Fachrecht an das neue allgemeine Datenschutzrecht aus DS-GVO und BDSG 2018 angepasst werden. Dabei ist zu berücksichtigen:

Geschaffen werden die Rechte der betroffenen Personen unmittelbar durch Kapitel III DS-GVO. Insofern enthält das BDSG 2018 hierzu auch keine Regelungen. Etwaige Verweise im Fachrecht auf Betroffenenrechte im jetzigen BDSG gehen damit ab dem 25. Mai 2018 ins Leere; schließlich wird das BDSG durch das BDSG 2018 ersetzt. Verweise auf die Rechte nach Kapitel III DS-GVO sind überflüssig. Die Rechte gelten unmittelbar.

Etwaige Ausnahmen von einzelnen Rechten sollten insbesondere mit Blick auf die an den spezifischen Verarbeitungskontext anknüpfenden Vorgaben des Artikels 23 Absatz 2 DS-GVO vorzugsweise bereichsspezifisch geregelt und konkret begründet werden.

5. Schadensersatz- und Bußgeldtatbestände

Die DS-GVO enthält in Artikel 82 bzw. Artikel 83 abschließende Regelungen zum Schadensersatz und zu Bußgeldtatbeständen. Bereichsspezifische Regelungen sind daher zu streichen. Lediglich in den Fällen, in denen nationale Bußgeldtatbestände nicht nur Datenschutzverstöße zum Gegenstand haben, könnten sie mit dem nichtdatenschutzrechtlichen Inhalt fortgeführt werden. Im Übrigen besteht bei Bußgeldtatbeständen Spielraum für den nationalen Gesetzgeber gemäß Artikel 83 Absatz 7 DS-GVO hinsichtlich der Frage, ob und in welcher Höhe Bußgelder gegen Behörden verhängt werden können. Das Verfahrensrecht steuert das BDSG 2018 bei.

II. Fazit und Ausblick

Die EU-Datenschutzreform hat für den deutschen Gesetzgeber umfangreichen Anpassungs- und, für den Anwendungsbereich der DS-RL, Umsetzungsbedarf zur Folge. Der hierfür zur Verfügung stehende Zeitraum von nur zwei Jahren ist ambitioniert.

Nach dem zügigen Abschluss der Arbeiten am DSAnPUG-EU im Juli 2017 ist in einer 2. Stufe das gesamte Fachrecht des

Bundes an DS-GVO anzupassen. Im Vordergrund stehen in erster Linie rechtstechnische „Reparaturarbeiten“, die durch die DS-GVO und das BDSG 2018 erforderlich werden. Es handelt sich, wie aufgezeigt, jedoch nicht um eine rein schematische Bereinigung. An den Grundstrukturen des Fachrechts wird sich indes vergleichsweise wenig ändern. Dies zeigt das bereits abgeschlossene Gesetzgebungsverfahren zur Anpassung einzelner Vorschriften (insbesondere des Sozialgesetzbuches X und der Abgabenordnung). Die umfangreiche 2. Stufe erfolgt unter massivem Zeitdruck und sollte idealerweise bis zum 25. Mai 2018 abgeschlossen sein, um ein reibungsloses Zusammenspiel von DS-GVO, BDSG 2018 und dem bereichsspezifischen Fachrecht sicherzustellen.

Über die 2. Stufe hinaus kann nicht ausgeschlossen werden, dass im Lichte der noch ausstehenden Anpassungsgesetze der anderen EU-Mitgliedstaaten die Frage aufkommen wird, ob der deutsche Gesetzgeber das BDSG 2018 punktuell überarbeiten sollte. Motiv könnte hierbei sein, auf nationaler Ebene der Spielräume der DS-GVO möglichst einheitlich zu nutzen, um die angestrebte Harmonisierung des Rechts insbesondere im privaten Bereich zu verwirklichen. Dies gilt z.B.

hinsichtlich der Altersgrenze bei Einwilligungen von Minderjährigen gemäß Artikel 8 Abs. 1 DS-GVO oder auch für den Anwendungsbereich der nationalen Regelungen.

Ferner wird sich zu einem noch nicht absehbaren Zeitpunkt weiterer Anpassungsbedarf aus der e-Privacy-Verordnung ergeben, die EU-Parlament und Rat derzeit beraten. Insbesondere betroffen sind hier das Telekommunikationsgesetz und das Telemediengesetz.



Jörg Eickelpasch

ist seit 2003 beschäftigt beim BMI. Zunächst eingesetzt als Referent in der Abteilung Öffentliche Sicherheit, dann als Personalreferent. Von September 2010 bis August 2015 Tätigkeit bei der Ständigen Vertretung der Bundesrepublik Deutschland bei der Europäischen Union in Brüssel (insbesondere ab Frühjahr 2012 Begleitung der Verhandlung über die EU-Datenschutzreform). Seit 2015 Einsatz im Referat „Datenschutzrecht, Reform des Datenschutzes in Deutschland und Europa“ des BMI, seit 2016 in der Funktion des Referatsleiters.

Dr. Niclas Krohm*

Die wirtschaftliche Einheit als Bußgeldadressat unter der Datenschutz-Grundverordnung?

Die Relevanz von Bußgeldern wird unter der Datenschutz-Grundverordnung voraussichtlich erheblich zunehmen. Infolgedessen wird die Rechtsfrage aufgeworfen, inwiefern und unter welchen Voraussetzungen Unternehmen und Konzerne Adressaten eines Bußgeldes sein können. Der Ausdehnung der Bußgeldhaftung entsprechend des Kartellrechts auf die wirtschaft-

liche Einheit sollte in diesem Zusammenhang aus Gründen der Bestimmtheit der derzeitigen Bußgeldregelungen der Datenschutz-Grundverordnung eine Absage erteilt werden. Die Systematik des Datenschutzrechts und der Grundsatz der Verhältnismäßigkeit sprechen ebenfalls gegen eine derartige Ausdehnung der Bußgeldhaftung.

I. Einleitung

Die Datenschutz-Grundverordnung wirft ihre Schatten voraus. Angesichts des nahenden Anwendungsbeginns der neuen Datenschutzregelungen am 25. Mai 2018 befinden sich viele Unternehmen derzeit in der Anpassungsphase ihrer Prozesse. Solche Anpassungen sind teilweise auch dringend erforderlich, damit auch zukünftig personenbezogene Daten rechtmäßig verarbeitet werden. Andernfalls sieht die Datenschutz-Grundverordnung einen empfindlichen Bußgeldkatalog vor.

In Berichten über die Datenschutz-Grundverordnung werden die neuen Bußgelder regelmäßig eher plakativ herausgestellt, und diese sind sicherlich ein Aspekt, warum der Datenschutz eine immer wichtigere Rolle in den Compliance-Strukturen von

Unternehmen einnimmt. Neu ist insbesondere der Bußgeldrahmen, der gemäß Art. 83 Abs. 4 DS-GVO bis zu 10 Mio. EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes bzw. in qualifizierten Verstößen gemäß Art. 83 Abs. 5 DS-GVO bis zu 20 Mio. EUR bzw. bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes eines Unternehmens betragen kann. Diese Zahlen verdeutlichen, dass ein Datenschutzbewusstsein im Unternehmen unbedingt erforderlich ist. Gleichzeitig sind die Zahlen jedoch lediglich Höchstgrenzen von Bußgeldern, und ein Grund für Panik besteht nicht.

Neben der Erhöhung des Bußgeldrahmens wurden auch die Bußgeldtatbestände im Vergleich zur bisherigen Rechts-

* Der Beitrag gibt ausschließlich die persönliche Meinung des Autors wieder.

lage erheblich erweitert, vgl. Art. 83 Abs. 4-6 DS-GVO. Vor dem Hintergrund des aus dem Kartellrecht entlehnen funktionalen Unternehmensbegriffs werden zudem Stimmen laut, die auch die Verantwortlichkeit für Datenschutzverstöße ausweiten wollen. Infolgedessen sollen auch Muttergesellschaften in einem Konzern gesamtschuldnerisch für das Fehlverhalten ihrer Tochtergesellschaften haften.¹ Hierfür müsse eine unmittelbare Beteiligung der Muttergesellschaft an dem Datenschutzverstoß der Tochter nicht bewiesen sein.²

Dabei stützen sich die Befürworter der Ausdehnung der Haftung auf die wirtschaftliche Einheit auf den EWG 150 S. 3 DS-GVO, der wiederum besagt, dass bei Geldbußen für Unternehmen der Begriff „Unternehmen“ im Sinne der Art. 101 und 102 AEUV verstanden werden soll. Daraus wird eine Parallele zum Kartellrecht gezogen: Sowohl bei der Bemessung eines Bußgeldes als auch bei der Bestimmung des Bußgeldadressaten nach Art. 83 Abs. 4-6 DS-GVO sei ein Unternehmen i.S.v. Art. 101 f. AEUV und damit die wirtschaftliche Einheit maßgeblich.

Ob die Datenschutz-Grundverordnung tatsächlich mit EWG 150 DS-GVO diesen weiten Ansatz verfolgt, der auf den ersten Blick im Widerspruch zum Unternehmensbegriff des Art. 4 Nr. 18 DS-GVO steht, und ob dieser überhaupt in die Systematik des Datenschutzrechts passt, soll im Folgenden untersucht werden.

II. Unternehmensbegriff

Zunächst ist aufzuzeigen, was überhaupt mit dem Verweis in EWG 150 S. 3 DS-GVO auf den Unternehmensbegriff nach AEUV gemeint ist und welche Folgen für das europäische Kartellrecht daraus resultieren. Im Anschluss ist zu erörtern, ob und ggf. welche Auswirkungen sich entsprechend für das Datenschutzrecht ergeben könnten.

1. Funktionaler Unternehmensbegriff im Kartellrecht

a) Art. 101 f. AEUV

Art. 101 und 102 AEUV definieren nicht unmittelbar den Begriff des Unternehmens. Für das Kartellrecht war daher die Rechtsprechung gefordert, nähere Konturen für den Unternehmensbegriff zu schaffen. Allgemein anerkannt ist, dass der Unternehmensbegriff unionsrechtlich definiert werden muss, und aufgrund der EuGH-Rechtsprechung hat sich ein funktionales Verständnis herausgebildet.³ Nach Ansicht des EuGH „umfasst der Begriff des Unternehmens jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung.“⁴

Eine wirtschaftliche Einheit kann aus mehreren juristischen Personen bestehen, die zusammen ein Unternehmen i.S.v. Art. 101 und 102 AEUV bilden. Ob die einzelnen juristischen Personen eine wirtschaftliche Einheit bilden, bemisst sich daran, inwiefern einzelne Gesellschaften ihr Marktverhalten autonom bestimmen können oder den Weisungen der beherrschenden Gesellschaft unterliegen. Sofern sie weisungsgebunden sind, liegt eine wirtschaftliche Einheit vor.⁵ Davon ist auszugehen, wenn die Muttergesellschaft zu (fast) 100 % an der Tochtergesellschaft beteiligt ist. In solchen Fällen bedarf es auch nicht

des Nachweises einer konkreten Weisungsabhängigkeit, und es greift eine widerlegliche Vermutung der Abhängigkeit.⁶ Die Vermutung ist widerlegt, wenn nachgewiesen werden kann, dass die Tochtergesellschaft sich autonom auf dem Markt verhält.

Bei geringeren Beteiligungen bedarf es für die Annahme einer wirtschaftlichen Einheit, dass die Muttergesellschaft die Kontrolle über die Tochtergesellschaft hat und insbesondere ein Weisungsrecht ausüben kann.⁷ Dabei ist wieder das Marktverhalten zu beurteilen, wobei dieses nur ein Anknüpfungspunkt von vielen für die Annahme einer wirtschaftlichen Einheit ist.⁸ Weitere können beispielsweise personelle Verflechtungen oder eine einheitliche Leitung sein.⁹

Diese weite Betrachtung des Unternehmensbegriffs wird vorgenommen, um dem Schutzzweck des Kartellrechts gerecht zu werden. Es soll ein freier, wirksamer und unverfälschter Wettbewerb gewährleistet¹⁰ und damit ein funktionierender Binnenmarkt nach Art. 26 Abs. 1 AEUV geschaffen werden.¹¹ Vor diesem Hintergrund sei es zweckmäßig, an das Marktverhalten der wirtschaftlichen Einheit als Ganzes anzuknüpfen.¹²

b) Gesamtschuldnerische Haftung der wirtschaftlichen Einheit

Der weite Unternehmensbegriff im Kartellrecht bewirkt sodann, dass Muttergesellschaften gesamtschuldnerisch für Kartellrechtsverstöße einer Tochtergesellschaft eintreten müssen.¹³ Dies lässt sich mit der Sicherung der zuvor genannten Schutzrichtung des Kartellrechts begründen, sodass bei der Verhängung von Bußgeldern nicht auf den einzelnen Rechtsträger abgestellt wird, sondern auf die wirtschaftliche Einheit als eine Art Unternehmensvereinigung im umgangssprachlichen Sinn.¹⁴

Dieser Zurechnung von Rechtsverstößen steht jedoch das Konzernprivileg gegenüber, wodurch Absprachen innerhalb einer wirtschaftlichen Einheit zulässig sind. Infolgedessen bestehen innerhalb der wirtschaftlichen Einheit aufgrund

1 Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht 2016, S. 33 f.; Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 8 D. Rn. 35; Hohmann, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, § 3 Rn. 321; Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 10 ff.; Rost, RDV 2017, 13 (17); Schönefeld/Thomé, PinG 2017, 126 (127 f.). Vorsichtiger in diese Richtung kommentieren Bergt, in: Kühling/Buchner, die DS-GVO, 2017, Art. 83 Rn. 28; ders., DuD 2017, 555 (556); Feiler/Forög, EU-DS-GVO, 2017, Art. 83 Rn. 12.

2 Schönefeld/Thomé, PinG 2017, 126 (128).

3 Weiß, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, Art. 101 AEUV Rn. 25.

4 EuGH, Urteil vom 23. 4. 1991 – C-41/90, Rn. 21.

5 Weiß, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, Art. 101 AEUV Rn. 34 mit Verweis auf die Rechtsprechung des EuGH.

6 EuGH, Urte. v. 25.10.1983 – 107/82, Rn. 50; EuGH, Urte. v. 10.09.2009 – C-97/08 P, Rn. 60; EuGH, Urte. v. 29.09.2011 – C-521/09 P, Rn. 56; EuGH, Urte. v. 18.07.2013 – C-501/11 P, Rn. 103 ff.

7 Weiß, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, Art. 101 AEUV Rn. 35.

8 EuGH, Urte. v. 10.09.2009 – C-97/08 P, Rn. 73.

9 Weiß, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, Art. 101 AEUV Rn. 74 m.w.N.

10 EuGH, Urte. V. 5. 6. 2014 – C-557/12.

11 Faust/Spittka/Wybitul, ZD 2016, 120 (121).

12 Faust/Spittka/Wybitul, ZD 2016, 120 (121).

eines fehlenden Wettbewerbs auch keine konzerninternen Wettbewerbsbeschränkungen, und Art. 101 AEUV ist auf die einzelnen Gesellschaften der wirtschaftlichen Einheit/Unternehmen nicht anwendbar.¹⁶ Die weite Haftung ist also eine Art Ausgleich für das Konzernprivileg.

2. Vorgaben der DS-GVO zum Unternehmensbegriff

Der Datenschutz-Grundverordnung ist stellenweise anzumerken, dass sie unter großem Zeitdruck verhandelt wurde. Dieser Umstand hinterließ selbstverständlich Spuren, und die Festlegung des Unternehmensbegriffs in der Datenschutz-Grundverordnung verursacht in gewisser Weise ein „legislatives Chaos“¹⁷: In Art. 4 Nr. 18 DS-GVO definiert der europäische Verordnungsgeber, was datenschutzrechtlich unter einem Unternehmen zu verstehen ist. Danach ist ein Unternehmen eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen. Zusätzlich definiert er in Art. 4 Nr. 19 DS-GVO auch, was unter einer Unternehmensgruppe zu verstehen ist, nämlich eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht. Mit der Definition des Unternehmens knüpft der Verordnungsgeber damit offenkundig nicht an den funktionalen Unternehmensbegriff aus dem Kartellrecht an, während er bei der Unternehmensgruppe eher eine funktionale Sichtweise offenbart.

Für den in Art. 83 Abs. 5 DS-GVO genannten Begriff des Unternehmens soll nun jedoch nicht der des Art. 4 Nr. 18 DS-GVO gelten. EWG 150 DS-GVO verlangt vielmehr, dass auf den aus dem Kartellrecht bekannten funktionalen Unternehmensbegriff nach Art. 101 f. AEUV zurückgegriffen wird. Ein Umstand, der erst im Trilog Einzug in die Datenschutz-Grundverordnung fand. Damit scheinen EWG 150 und Art. 4 Nr. 18 DS-GVO im Widerspruch zu stehen. Erwägungsgründe dürfen jedoch nur präzisieren, sollen aber keine Abweichung von Regelungen des verfügbaren Teils eines Rechtsaktes bewirken.¹⁸ Ein Erwägungsgrund einer Verordnung kann also eine Regelung im normativen Teil nicht überlagern.¹⁹ Die deutsche Fassung vermittelt infolgedessen den Eindruck, dass dem Verordnungsgeber ein Versehen unterlaufen ist und im Endeffekt dürfte EWG 150 DS-GVO aufgrund der bindenden Definition des Unternehmensbegriffs in Art. 4 Nr. 18 DS-GVO nicht maßgebend im Hinblick auf Art. 83 Abs. 4-6 DS-GVO sein.

Die vorangestellte Wertung kann jedoch so einfach nicht getroffen werden. Während in der deutschen Fassung jeweils in Art. 4 Nr. 18 und Art. 83 DS-GVO der Begriff „Unternehmen“ verwendet wird,²⁰ trifft dies nicht auf alle Sprachfassungen der Verordnung zu. In den beiden Normen werden teilweise unterschiedliche Begrifflichkeiten genutzt, so dass nicht zwangsläufig im Rahmen von Art. 83 DS-GVO auf den Unternehmensbegriff aus Art. 4 Nr. 18 DS-GVO abgestellt werden muss. In der englischen Sprachfassung wird beispielsweise in Art. 4 Nr. 18 DS-GVO der Begriff „enterprise“ und in Art. 83 Abs. 4-6 sowie EWG 150 DS-GVO „undertaking“ verwendet.²¹

Aufzulösen ist der Widerspruch zwischen den verschiedenen Sprachfassungen anhand der unionsrechtlichen Grund-

sätze. Diese kennen keinen Vorrang einer Landessprache der Europäischen Union.²² Nach dem Gebot des „effet utile“ ist vielmehr der Sprachfassung den Vorzug zu geben bzw. eine Norm so auszulegen, dass das Vertragsziel am besten erreicht werden kann.²³ Es könnte insofern argumentiert werden, dass bereits Art. 16 Abs. 1 AEUV im Einklang mit Art. 8 Abs. 1 GRCh zusichert, dass jede Person das Recht auf den Schutz personenbezogener Daten hat. Trägt die englische Sprachfassung der Datenschutz-Grundverordnung jedoch mehr zum Ziel des Schutzes personenbezogener Daten bei? Dann müsste man davon ausgehen, dass der ohnehin hohe Bußgeldrahmen des Art. 83 Abs. 4 und 5 DS-GVO mittels der Ausweitung des Unternehmensbegriffs auf eine wirtschaftliche Einheit eine noch abschreckendere Wirkung entfaltet. Verantwortliche und Auftragsverarbeiter müssten aufgrund dessen noch eher Bußgelder befürchten, so dass sie erhebliche Anstrengungen für den Datenschutz unternehmen. Letztendlich lässt sich dies wohl kaum belegen und darf zumindest angezweifelt werden.

Viel gewichtiger sind jedoch Zweifel an der Bestimmtheit der Norm des Art. 83 DS-GVO, wenn unklar ist, welcher Unternehmensbegriff in dessen Kontext gilt.²⁴ Das Bestimmtheitsgebot als Teil des Gesetzlichkeitsprinzips ist gemäß Art. 49 GRCh fest im Unionsrecht verankert und gilt auch für Normen mit verwaltungsrechtlichen Sanktionen²⁵ wie Bußgeldtatbestände.²⁶ Diese dürfen nach dem Bestimmtheitsgebot nur aufgrund einer Norm bzw. Rechtsgrundlage verhängt werden, die klar und unzweideutig formuliert sowie die Rechtsfolge vorhersehbar festlegt.²⁷ Dieser Umstand ist äußerst fraglich, wenn noch nicht einmal klar ist, wer als „Unternehmen“ i.S.d. Art. 83 DS-GVO Adressat eines Bußgeldes ist.

In diesem Zusammenhang ist auch Art. 4 Nr. 19 DS-GVO und damit der Begriff der Unternehmensgruppe zu berücksichtigen. Diese dem funktionalen Unternehmensbegriff nahestehende Definition sorgt für weitere Verwirrung, wenn die Abstufung vom Unternehmen nach Art. 4 Nr. 18 DS-GVO zur Unternehmensgruppe gerade nicht im Rahmen des

13 Diese weite Haftung ist mit der kürzlich in Kraft getretenen 9. GWB-Novelle auch in das deutsche Kartellbußgeldrecht übernommen worden.

14 Vgl. auch Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 9.

15 EuGH, Urt. v. 31.10.1974 – 15/74; Cornelius, NZWiSt 2016, 421 (423).

16 EuGH, Urt. v. 12.07.1984 – 170/83; Cornelius, NZWiSt 2016, 421 (423).

17 Cornelius, NZWiSt 2016, 421 (423).

18 Golla, in: Eßer/Kramer/von Lewinski, DS-GVO BDSG, 2017, Art. 83 Rn. 26 mit Verweis auf EuGH, Urt. v. 14.07.1972 – 48/6; a. A. Nemitz, in: Ehmann / Selmayr, Datenschutz-Grundverordnung, 2017, Art. 83 Rn. 42, nach dessen Auffassung sich EWG 150 DS-GVO als spezielle Regelungen bzw. aus Auslegungsdirektive gegenüber den Regelungen in Art. 4 Nr. 18 und 19 DS-GVO durchsetzt.

19 Faust/Spittka/Wybitul, ZD 2016, 120 (124); Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016, § 11 Rn. 28.

20 Denselben Begriff wie die deutsche Sprachfassung verwenden auch die spanische, niederländische, rumänische, italienische und estnische Version des Art. 4 Nr. 18, Art. 83 und EWG 150 DS-GVO, siehe Bergt, in: Kühling/Buchner, die DS-GVO, 2017, Art. 83 Rn. 43; ders., DuD 2017, 555 (559).

21 Weitere Beispiele bei Golla, in: Eßer/Kramer/von Lewinski, DS-GVO BDSG, 2017, Art. 83 Rn. 26.

22 Cornelius, NZWiSt 2016, 421 (424) mit Verweis auf EuGH, Urt. v. 27.03.1990 – C-372/88, Rn. 19.

23 Cornelius, NZWiSt 2016, 421 (424).

Art. 83 DS-GVO maßgebend sein soll. Andernfalls würde ein (funktionaler) Unternehmensbegriff bei Art. 83 DS-GVO gelten, der zwar weitgehend der Definition der Unternehmensgruppe entspricht, aber im Wortlaut nicht auf diese Weise bezeichnet wird. Legislativ ist dies ein Zustand, der für die Bußgeldpraxis kaum hinnehmbar ist. Letztendlich werden gleichwohl die Gerichte diese Problematik klären müssen, wobei der Ausgang eines solchen Verfahrens nur schwer abzuschätzen ist.

III. Auswirkungen auf die zukünftige Bußgeldpraxis

Da sich bislang insbesondere einzelne Vertreter der Datenschutzbehörden trotz der Bedenken hinsichtlich der Bestimmtheit und des Vorrangs des Verordnungstexts gegenüber den Erwägungsgründen positioniert haben, dass im Rahmen von Art. 83 DS-GVO gemäß EWG 150 DS-GVO der funktionale Unternehmensbegriff Anwendung finden soll,²⁸ stellt sich hier die Frage, welche Auswirkungen damit für die Haftung nach der Datenschutz-Grundverordnung verbunden und ob diese überhaupt mit der Systematik des Datenschutzrechts zu vereinbaren sind.

1. Ausdehnung der Haftung auf Muttergesellschaften

Für die zukünftige Bußgeldpraxis der Datenschutzbehörden wird es von großer Bedeutung sein, ob entsprechend einer Parallele zum Kartellrecht und der Anwendung des funktionalen Unternehmensbegriffs die Muttergesellschaft gesamtschuldnerisch für einen Verstoß einer Tochtergesellschaft einstehen muss.

a) Argumente für die gesamtschuldnerische Haftung der wirtschaftlichen Einheit auch im Datenschutzrecht

Eine Ausdehnung der Haftung nach Art. 83 DS-GVO auf die wirtschaftliche Einheit entsprechend EWG 150 DS-GVO wird befürwortet, um dem Betroffenenenschutz zu genügen und gleiche Bedingungen auf dem wettbewerbsträchtigen Markt herzustellen.²⁹ Es sei zu befürchten, dass das Bußgeldsystem andernfalls nicht wirksam und keinen ausreichenden abschreckenden Charakter habe, insbesondere wenn sich Muttergesellschaften trotz der Beherrschung des Verhaltens der Tochtergesellschaft aus der Verantwortung stehlen könnten.³⁰ Eine Umgehung der Haftung durch Umstrukturierungen im Konzern könnte zudem verhindert werden, wenn hierdurch die Haftung bei der Muttergesellschaft verbleibt.³¹

Hervorgehoben wird ferner, dass Muttergesellschaften bei Datenschutzverstößen einer Tochtergesellschaft nicht bebußt werden, sondern hierfür nur haften.³² Dies entspreche auch der Systematik des europäischen Sanktionsrechtes, das keine Trennung von Tatbestand und Rechtsfolge vornehme.³³ Bei der Bemessung des Bußgeldes werde insofern auf die Unternehmensgruppe bzw. wirtschaftliche Einheit abgestellt, wohingegen der Datenschutzverstoß allein von einem dieser Einheit zugehörigen Verantwortlichen oder Auftragsverarbeiter begangen sein muss.³⁴ Es sei daher unerheblich, dass das Unternehmen oder die Unternehmensgruppe nicht Normadressaten

im Datenschutzrecht sind.³⁵ Insofern sei es auch konsequent, in Art. 83 DS-GVO den Verantwortlichen und Auftragsverarbeiter als Normadressaten zu nennen. Dem liegt auch die Annahme zugrunde, dass nach europäischem Verständnis keine Trennung zwischen Verstoß und Haftungsadressat vorausgesetzt werde. Andernfalls könne ein Szenario entstehen, wonach einzelne Mitgliedsstaaten im Wege nationaler Regelungen bei der Ausgestaltung der rechtlichen Organisation des datenschutzrechtlichen Verantwortlichen die Wirksamkeit des europäischen Sanktionsrechts erheblich beeinträchtigen.³⁶

Zu guter Letzt wird darauf hingewiesen, dass Muttergesellschaften in der Systematik der gesamtschuldnerischen Haftung der wirtschaftlichen Einheit nicht vollkommen schutzlos gestellt seien. Schutz vor der Haftung werde der wirtschaftlichen Einheit nämlich bei nicht zurechenbaren Zuwiderhandlungen gewährt.³⁷

b) Argumente gegen die gesamtschuldnerische Haftung der wirtschaftlichen Einheit nach der DS-GVO

Die Argumente für eine Ausweitung der Haftung auf die wirtschaftliche Einheit sind erkennbar davon geprägt, ein möglichst wirksames und abschreckendes Bußgeldsystem im Datenschutzrecht zu implementieren. Diese Haftungssystematik müsste gleichwohl auch so in der Datenschutz-Grundverordnung abgebildet sein, was derzeit zumindest nicht unmittelbar erkennbar ist. Rechtspolitisch mag der Export des unternehmensbezogenen Bußgeldrechtes aus dem Kartellrecht noch verständlich sein, in „nicht-unternehmensbezogenen“ Rechtsbereichen wie dem Datenschutzrecht wären damit hingegen erhebliche Probleme verbunden.³⁸

Wenig nachvollziehbar ist bereits, dass der Verordnungsgeber eine so wichtige Entscheidung wie eine Ausdehnung der Haftung lediglich über die Erwägungsgründe der Daten-

24 Vgl. Bergt, in: Kühling/Buchner, die DS-GVO, 2017, Art. 83 Rn. 43; ders., DuD 2017, 555 (559); Faust/Spittka/Wybitul, ZD 2016, 120 (124); Gola, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 83 Rn. 14.

25 Bergt, in: Kühling/Buchner, die DS-GVO, 2017, Art. 83 Rn. 44.

26 Golla, in: Eßer/Kramer/von Lewinski, DS-GVO BDSG, 2017, Art. 83 Rn. 15.

27 Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 5.

28 Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht 2016, S. 33 f.; BayLDA, EU-Datenschutz- und Verordnung (DS-GVO) – Das BayLDA auf dem Weg zur Umsetzung der Verordnung, Papier Nr. VII, Sanktionen nach der DS-GVO; Rost, RDV 2017, 13 (17); Schönefeld/Thomé, PinG 2017, 126 (127 f.).

29 Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 14.

30 Nemitz, in: Ehmann / Selmayr, Datenschutz-Grundverordnung, 2017, Art. 83 Rn. 43.

31 Vgl. Gola, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 83 Rn. 13; Gola, K&R 2017, 144 (146).

32 Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 12.1.

33 Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 11 und 13.2.

34 Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 13.2.

35 Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 14.1.

36 Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 14.1.

schutz-Grundverordnung vorgenommen haben soll.³⁹ Dies könnte jedoch noch der Hektik der Trilog-Verhandlungen geschuldet sein. Neben den bereits aufgezeigten Zweifeln an der Bestimmtheit des Art. 83 Abs. 4-6 DS-GVO im Zusammenhang mit Art. 4 Nr. 18 und EWG 150 DS-GVO spricht allerdings vor allen Dingen die Systematik der Datenschutz-Grundverordnung gegen eine Ausweitung der Haftung auf eine wirtschaftliche Einheit im Datenschutzrecht.

Das Datenschutzrecht ist nach dem Prinzip der Verantwortung ausgestaltet. Verbotsnormen der Datenschutz-Grundverordnung richten sich daher auch nicht per se an Unternehmen, sondern an den für die Datenverarbeitung Verantwortlichen, vgl. Art. 5 Abs. 2 DS-GVO. Dieser ist für die Einhaltung der Datenschutzprinzipien nach Art. 5 Abs. 1 DS-GVO verantwortlich. Unter einem Verantwortlichen ist wiederum gemäß Art. 4 Nr. 7 DS-GVO u. a. jede natürliche oder juristische Person zu verstehen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

Die Datenschutz-Grundverordnung enthält ferner bereits ein ausdifferenziertes Adressatenmodell für Bußgelder. Gemäß Art. 58 Abs. 2 lit. i) DS-GVO können Bußgelder zusätzlich oder anstelle der weiteren in diesem Absatz genannten Maßnahmen verhängt werden. Die weiteren Maßnahmen richten sich an den Verantwortlichen oder Auftragsverarbeiter, so dass grundsätzlich diese und keine weiteren Protagonisten Adressaten von Bußgeldern sein können. Die Verordnung stellt also neben dem Auftragsverarbeiter explizit auf die Rolle des Verantwortlichen ab. Dementsprechend knüpft auch Art. 83 Abs. 4-6 DS-GVO an diese Systematik an und benennt Verantwortliche und Auftragsverarbeiter (sowie ggf. Zertifizierungsstellen) als Normadressaten.⁴⁰ Letztendlich ist es insofern konsequent, wenn derjenige, der über das „Ob“ und „Wie“ der Datenverarbeitung entscheidet, für Bußgelder haften soll. Dementsprechend kommt es bei der Bestimmung des Bußgeldadressaten nicht auf eine Unternehmensstellung, sondern vielmehr auf die Frage an, wer die Verantwortung trägt.⁴¹

Datenschutzrechtlich werden Konzerne und Unternehmensgruppen auch nicht ohne weiteres als Einheit betrachtet.⁴² Die Unternehmensgruppe ist in Art. 4 Nr. 19 DS-GVO legaldefiniert und gewinnt lediglich in Art. 37 Abs. 2, Art. 47 und Art. 88 Abs. 2 DS-GVO an Bedeutung. Darüber hinaus ist der Datenschutz-Grundverordnung ein derartiges einheitliches Konzernbild eher fremd. Infolgedessen wird eine entscheidende Abweichung zum Kartellrecht deutlich, die ebenfalls gegen eine Übernahme der Haftung für eine wirtschaftliche Einheit in das Datenschutzrecht spricht: Während das Kartellrecht ein Konzernprivileg kennt, existiert ein solches im Datenschutzrecht auch unter der Datenschutz-Grundverordnung nicht.⁴³ Diese Privilegierung der Unternehmensgruppe im Kartellrecht, welche eine Ausdehnung der Haftung begründet, kann somit mangels Entsprechung nicht zu einem ausgedehnten Bußgeldsystem im Datenschutzrecht führen.

Die rechtspolitischen Erwägungen zur Optimierung eines wirksamen und abschreckenden Bußgeldsystems wurden im Übrigen vom Ordnungsgeber der Datenschutz-Grundverordnung durchaus berücksichtigt. Dafür ist es auch nicht erfor-

derlich, eine Haftung der Muttergesellschaft für Datenschutzverstöße der Tochtergesellschaft über eine wirtschaftliche oder datenschutzrechtliche⁴⁴ Einheit zu entwickeln. Entsprechend des Verantwortungsprinzips kann eine Muttergesellschaft bei einem Datenschutzverstoß dann bußgeldpflichtig gemäß Art. 83 DS-GVO werden, wenn sie gemeinsam verantwortlich mit der den Verstoß behebenden Tochtergesellschaft gemäß Art. 26 DS-GVO ist. Legen Mutter- und Tochtergesellschaft gemeinsam Mittel und Zwecke der Datenverarbeitung fest und kann ein Datenschutzverstoß auch tatsächlich beiden zugerechnet werden, kann ein entsprechendes Bußgeld mit doppeltem Adressaten verhängt werden. Dies kommt dem Konstrukt der wirtschaftlichen Einheit durchaus nahe, wobei hier wohl die Haftung für Bußgelder nach den Vorgaben der Datenschutz-Grundverordnung nicht gesamtschuldnerisch ausfällt.

Hervorzuheben ist bei dieser Systematik, dass die gemeinsame Verantwortung und Zurechnung eines Datenschutzverstoßes auch tatsächlich feststehen muss. Ohne ein Konzernprivileg als Ausgleich zur umfassenden Haftung als Einheit, kann bei Beteiligungsformen von 100 % nicht wie im europäischen Kartellrecht automatisch von einer Einflussnahmemöglichkeit der Muttergesellschaft auf die Tochtergesellschaft ausgegangen werden, die eine Haftung begründet. Diese Vermutungsregelung greift nicht, was angesichts der erheblichen Kritik an dieser zu begrüßen ist. Im Kartellrecht wird bereits bemängelt, dass diese zu einer Verletzung der in Art. 6 EMRK und Art. 48 Abs. 1 GRC garantierten Unschuldsvermutung führe, da ein Nachweis für ein alleinverantwortliches Handeln der Tochtergesellschaft ein nahezu unüberwindbares Hindernis sei.⁴⁵

Abschließend ist somit festzuhalten, dass die systematischen Erwägungen gegen eine Ausdehnung der Haftung für Bußgelder auf eine wirtschaftliche Einheit im Datenschutzrecht sprechen.

2. Bußgeldrahmen

Vertritt man die Ansicht, dass der funktionale Unternehmensbegriff entsprechend EWG 150 DS-GVO maßgeblich für Bußgelder nach Art. 83 DS-GVO sein soll, könnte dies auch erhebliche Konsequenzen auf der Rechtsfolgenseite bei der Bemessung des Bußgeldes haben. Unmittelbar aus dem Wortlaut des Art. 83 Abs. 4-6 DS-GVO ergibt sich, dass bei der Bemessung des Bußgeldes auf den Umsatz des Unternehmens abzustellen ist.

37 Holländer, in: Beck'scher online-Kommentar Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Art. 83 Rn. 13.2.

38 Dannecker/Dannecker, NZWiSt 2016, 162 (166).

39 Vgl. auch Faust/Spittka/Wybitul, ZD 2016, 120 (124).

40 Vgl. zu den Normadressaten auch Bergt, in: Kühling/Buchner, die DS-GVO, 2017, Art. 83 Rn. 21.

41 In diesem Sinne auch Cornelius, NZWiSt 2016, 421 (425); Faust/Spittka/Wybitul, ZD 2016, 120 (122 ff.).

42 Faust/Spittka/Wybitul, ZD 2016, 120 (124).

43 Ebenso Cornelius, NZWiSt 2016, 421 (425); Faust/Spittka/Wybitul, ZD 2016, 120 (124); Gola, K&R 2017, 144 (146). Zum fehlenden Konzernprivileg in der DS-GVO im Einzelnen auch Voigt, CR 2017, 428 (429 f.).

44 Vgl. Cornelius, NZWiSt 2016, 421 (426), der einen Vorschlag zur datenschutzrechtlichen Einheit unterbreitet.

Würde man aufgrund des EWG 150 DS-GVO davon ausgehen, dass damit die wirtschaftliche Einheit gemeint ist, dürfte somit regelmäßig der Konzernumsatz herangezogen werden.

Es erscheint jedoch wenig sinnvoll, dass auf den Konzernumsatz bei der Bemessung der Höhe des Bußgeldes abgestellt werden soll, wenn ausschließlich eine Tochtergesellschaft für einen Datenschutzverstoß verantwortlich ist und bebußt werden soll. Regelmäßig würde die Gesellschaft mit einem Bußgeld belegt werden, welches ihre Finanzkraft erheblich übersteigt.⁴⁶ Bußgelder sollen abschreckend wirken, müssen gleichzeitig aber auch verhältnismäßig sein, vgl. Art. 83 Abs. 1 DS-GVO. Ein an eine einzelne Konzerngesellschaft gerichtetes Bußgeld würde den Grundsatz der Verhältnismäßigkeit⁴⁷ regelmäßig verletzen, wenn es anhand der Unternehmensgruppe bzw. des Konzernumsatzes bemessen wird. Heranzuziehen ist in solchen Fällen somit der Umsatz der einzelnen Gesellschaft.

In Fällen, in denen Gesellschaften einer Unternehmensgruppe als gemeinsam Verantwortliche für einen Datenschutzverstoß verantwortlich und damit bußgeldpflichtig werden, sollte das Bußgeld ebenfalls nicht in Bezug auf deren gemeinsamen Umsatz berechnet werden. Die gemeinsam Verantwortlichen haften nach den Vorgaben der Datenschutz-Grundverordnung nicht gesamtschuldnerisch für Bußgelder, so dass das Bußgeld individuell und im Hinblick auf den Beitrag am Datenschutzverstoß bemessen werden sollte. Eine andere Praxis müsste aufgrund der fehlenden Verhältnismäßigkeit als unzulässig angesehen werden.

IV. Fazit

Welcher Unternehmensbegriff – der des Art. 4 Nr. 18 DS-GVO oder der funktionale Unternehmensbegriff nach Art. 101 f. AEUV – im Rahmen von Art. 83 Abs. 4-6 DS-GVO künftig zur Anwendung kommen soll, werden wohl die Gerichte entscheiden müssen. Es sind jedoch ernstzunehmende Bedenken ersichtlich, warum Bußgelder nicht aufgrund des funktionalen Unternehmensbegriffs gegen eine wirtschaftliche Einheit zu verhängen sind. Sofern der europäische Ordnungsgeber eine andere Bußgeldpraxis anstrebt und insbesondere die wirtschaftliche Einheit haften sowie bei der Bemessung des Bußgeldes als Maßstab herangezogen werden soll, müsste eine Änderung direkt am Text der Datenschutz-Grundverordnung erfolgen. Dem einfachen Versuch, dies ggf. mit einem dem eigentlichen Wortlaut und Definitionen der Verordnung abweichenden EWG 150 DS-GVO zu erreichen, sollte aus Gründen der fehlenden Bestimmtheit eine Absage erteilt werden.

Sollte sich der Ordnungsgeber allem Aufwand zum Trotz kurzfristig zu Änderungen an der Datenschutz-Grundverordnung entscheiden, um mehr Rechtssicherheit für Bußgeldverfahren zu schaffen, spricht jedoch die Systematik des Datenschutzrechts gegen eine Ausweitung der Haftung auf die wirtschaftliche Einheit (wie sie ggf. EWG 150 DS-GVO entnommen werden könnte). Das Datenschutzrecht geht von einem Verantwortungsprinzip aus, und Bußgelder sollten als schärfstes Schwert der Aufsicht dementsprechend adressiert werden. Eine Muttergesellschaft kann zudem nach der Datenschutz-Grundverordnung schon für einen Verstoß durch eine Tochtergesellschaft bebußt werden, wenn beide gemeinsam verantwortlich sind und der Gesellschaftsmutter der Verstoß zugerechnet werden kann. Liegt der Verstoß allerdings allein im Verantwortungsbereich der Tochtergesellschaft und geschieht ein Datenschutzverstoß ohne Zutun der Muttergesellschaft, haftet diese selbstverständlich nicht.

Da bereits gewichtige Argumente gegen eine Ausdehnung der Haftung auf eine wirtschaftliche Einheit sprechen, sollte auch im Rahmen der Bußgeldbemessung der funktionale Unternehmensbegriff nicht herangezogen werden. Andernfalls drohen Szenarien, in denen einzelne Unternehmen eines Konzerns Bußgelder befürchten müssen, die am Umsatz des Konzerns bemessen und für das einzelne Unternehmen nicht leistbar sind. Dies würde einen vollkommen unzulässigen Verstoß gegen das Verhältnismäßigkeitsprinzip darstellen.



Dr. Niclas Krohm

ist Syndikusrechtsanwalt beim Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) im Bereich Datenschutz/Grundsatzfragen sowie als Rechtsanwalt für Schürmann Wolschendorf Dreyer Rechtsanwälte tätig.

45 Siehe zur Kritik insbesondere bei Dannecker/Dannecker, NZWiSt 2016, 162 (167 f) m.w.N.

46 So auch Faust/Spittka/Wybitul, ZD 2016, 120 (124).

47 Siehe weitgehend zum auch im europäischen Recht geltenden Grundsatz der Verhältnismäßigkeit in Bezug auf Bußgelder gegen Unternehmen, Martini/Wenzel, PinG 2017, 92 (94).

Dr. Tobias Jacquemain, LL.M.

Haftung privater Stellen bei Datenschutzverstößen

Im Falle eines Datenschutzverstoßes steht dem Betroffenen ein Recht auf Schadensersatz zu. Doch in der Praxis greift die Haftung fast nie. Woran sie scheitert und wie ein ersatzfähiger Schaden im Sinne der Datenschutz-Grundverordnung

(DS-GVO) zu bemessen ist, sind die zu beantwortenden Fragen, damit das bestehende Sanktionsdefizit im Datenschutz verringert werden kann.

I. Regulierungsmechanismen bestehen nur komplementär

Die Idee des geltenden Datenschutzrechts ist es zu gewährleisten, dass der Einzelne vor Risiken im Zusammenhang mit der Datenverarbeitung geschützt ist. Dieser Konzeption ist bereits eine systematische Nachrangigkeit des individuellen Rechtsschutzes immanent. Sind bei rechtswidrigem oder falschem Vorgehen keine Folgen für den Verursacher zu erwarten, läuft der zwingende Charakter durch Vorschriften leer, und das Datenschutzrecht wird mithin wertlos. Daher sehen sowohl das jetzige europäische Sekundärrecht als auch das deutsche Datenschutzrecht Rechtsbehelfe, Haftung und Sanktionen vor.¹ Selbstverständlich hält auch die DS-GVO als zukünftig zentrales Datenschutzrecht eine Reihe Rechtsfolgen bereit.

Zwei Tendenzen sind bei den Veränderungen vom Bundesdatenschutzgesetz (BDSG) hin zur DS-GVO in Bezug auf die Rechtsfolgen auszumachen: Die Strafen steigen enorm an, und der in seinen Rechten verletzte Einzelne wird gestärkt.² Das neue Sekundärrecht schafft eine beträchtliche Ausweitung der Instrumente zur Rechtsdurchsetzung. Dem Datensubjekt erwachsen daraus private und öffentlich-rechtliche Ansprüche. Der erkennbaren, grundsätzlichen Bestrebung der EU folgend, den Einzelnen mit Rechten und Ermächtigungen zur Verteidigung und Durchsetzung seiner Rechte in Anlehnung an den *homo oeconomicus* auszustatten,³ weist die DS-GVO dem Betroffenen eine Reihe „durchsetzbarer Rechte“⁴ zu. Neu ist hierbei der Rechtsbehelf gegen eine Aufsichtsbehörde nach Art. 78 DS-GVO. Ferner kann das Opfer eines Datenschutzverstoßes den Verantwortlichen gemäß Art. 79 DS-GVO in seinem Mitgliedstaat oder in dem der Niederlassung des Verantwortlichen verklagen. Die Instrumente zur Rechtsdurchsetzung sind im Ergebnis zwar umfangreicher geworden, aber aus privatrechtlicher Sicht nur graduell gewachsen. Eine Abkehr vom öffentlich-rechtlich geprägten Ansatz zur Sanktionierung geht damit nicht einher. Die Geldbuße bei Ordnungswidrigkeiten ist und bleibt die klassische Sanktion.

1. Sanktionen der Aufsichtsbehörden

Datenschutzverstöße können mit Wirksamwerden der DS-GVO für datenverarbeitende Stellen teuer werden. Als Grund wird dabei stets, aber vor allem ausschließlich auf die Verhängung von Bußgeldern verwiesen. Die Angst vor Kosten durch Datenschutzverstöße scheint sich allein auf die verwaltungsrecht-

liche Sanktion zu beschränken. Auch mit Wirksamwerden der DS-GVO bleibt die Regulierung behördlich geprägt. Die Rechtsdurchsetzung mittels behördlicher Aufsicht ist über das „one-stop-shop“-System⁵ und die verpflichtende Zusammenarbeit zwischen den Aufsichtsbehörden harmonisiert worden. Die DS-GVO ermächtigt die nationalen Ordnungsbehörden, Bußgelder in Höhe von bis zu 20 Millionen Euro zu verhängen, was gegenüber der bisherigen Obergrenze im deutschen Datenschutzrecht von 300.000 Euro eine drastische Erhöhung darstellt.⁶ Aus Betroffenenperspektive ist es als Vorteil zu bewerten, dass sich die Bußgelder durch die DS-GVO in ihrer Höhe zunehmend am Kartellrecht orientieren. Harte und damit kostenintensive Sanktionen sollen Unternehmen von Verstößen abhalten und ein Bewusstsein für Datenschutz schaffen. Die Millionengrenze kann sogar überschritten werden, weil Unternehmen auch mit „abschreckenden“⁷ Bußgeldern bis zu einer Höhe von 4 Prozent des globalen Umsatzes *per annum* bestraft werden können.

Das Recht lebt aber von seiner Anwendung. Wenn das Personal begrenzt ist, sind auch die Kontrollen begrenzt. Aufgrund der personell und materiell schwachen Ausstattung der Aufsichtsbehörden bleibt das in der Theorie scharfe Schwert der Geldbuße in der Praxis bisher nur selten benutzt: Bestätigt wird dieser Eindruck, wenn Datenschutz-

1 Zu den Folgen rechtswidriger Datenverarbeitung kann man auch die Betroffenenrechte auf Berichtigung, Löschung und Sperrung zählen. Gleichfalls kann man das Recht auf Schadensersatz oder Unterlassung zu den Rechten des Betroffenen fassen.

2 Vgl. Sloot, Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation, *International Data Privacy Law* 2014, 307 (319).

3 Franck/Purnhagen, *Homo Oeconomicus, Behavioural Sciences, and Economic Regulation: On the Concept of Man in Internal Market Regulation and its Normative Basis*, in: Mathis (Hrsg.), *Law and Economics in Europe: Foundations and Applications*, 2014, 329. Vgl. Sloot, Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation, *International Data Privacy Law* 2014, 307 (320).

4 EG. 13 DS-GVO. Vgl. dazu Sloot, Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation, *International Data Privacy Law* 2014, 307 (320).

5 Die Zuständigkeit der nationalen Aufsichtsbehörden ergibt sich nach dem Ort des Hauptsitzes eines Unternehmens. Was für einen lediglich national agierenden Unternehmer leicht nachvollziehbar ist, führt für international bzw. multi-national tätige Unternehmen zu dem Ergebnis, dass die Aufsichtsbehörde aus dem Mitgliedstaat der Hauptniederlassung auch für sämtliche Niederlassungen im EU-Ausland zuständig sein wird, um dem Unternehmer eine einheitliche Rechtsvollziehung zu gewährleisten.

6 Art. 83 Abs. 6 DS-GVO.

7 Art. 83 Abs. 9 S. 2 DS-GVO.

verstöße effektiver wettbewerbsrechtlich geahndet werden, anstatt das Datenschutzrecht dafür zu nutzen.⁸ Das mit 1,3 Millionen Euro höchste Bußgeld wurde erst 2014 vom Datenschutzbeauftragten Rheinland-Pfalz gegen den Debeka Krankenversicherungsverein verhängt.⁹ Ähnlich hoch, aber von mehr medialer Aufmerksamkeit begleitet, war die Sanktion der Berliner Aufsichtsbehörde im Jahr 2009. Hier kam es zu einem Bußgeld in Höhe von 1,12 Millionen Euro gegenüber der Deutschen Bahn.¹⁰ Viel häufiger bleibt es in der Praxis bei Ermahnungen, der Durchsetzung von Auskunftsansprüchen oder der Androhung von Bußgeldern, weil die finanzielle Sanktion nur als ultima ratio angesehen wird.

2. Strafrechtliche Sanktionen

Schwerwiegende Datenschutzverstöße können Straftatbestände erfüllen und sind mit bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe zu ahnden. Die Voraussetzungen zur Erfüllung eines solchen Tatbestands leiten sich aktuell noch aus § 43 BDSG ab.¹¹ Es bedarf hier des Vorsatzes, sich oder einem anderen einen Vermögensvorteil zu verschaffen oder jemanden bewusst damit schädigen zu wollen.¹² Straftatbestände, wie sie das BDSG kennt, können laut DS-GVO nicht mehr erfüllt sein, obwohl die Union mit Art. 83 Abs. 2 AEUV auch dafür eine Kompetenz besitzt.¹³ Strafrechtliche Sanktionen als Rechtsfolge für Verstöße können laut Art. 84 DS-GVO in Verbindung mit EG. 149 DS-GVO von den Mitgliedstaaten erlassen werden. Davon hat der deutsche Gesetzgeber mit § 42 BDSG-neu Gebrauch gemacht und knüpft dabei inhaltlich an die Straftatbestände des § 44 BDSG an. Für die Praxis weist die aktuell geltende Rechtsnorm jedoch bisher wenig Relevanz auf,¹⁴ und es bestehen keinerlei Gründe, dass sich dies mit dem BDSG-neu ändern wird.

3. Schadensersatz für Betroffene

Mittels der Effektivierung privatrechtlicher Haftung im Datenschutzrecht ließe sich zum Grundrechtsschutz des Einzelnen verhelfen, der bei den alternativen Rechtsfolgen des öffentlichen Rechts und des Strafrechts als Geschädigter außen vor bleibt. Die Verpflichtung zum Schadensersatz hingegen kann die Rechtsposition des Datensubjekts wieder herstellen oder es zumindest probieren. Es ist nicht einzusehen, weshalb demnächst Bußgelder in Millionen- oder gar Milliardenhöhe verhängt werden können, der Geschädigte aber zumeist leer ausgehen soll.¹⁵ Überdies spricht der generell zu verzeichnende Wechsel von staatlicher hin zu privater Datenverarbeitung für den Fokus auf das Privatrecht.¹⁶ Wenngleich der Schutz personenbezogener Daten als Abwehrrecht gegen staatliche Datenverarbeitung entstanden ist, so sind private Datenverarbeiter aus heutiger Sicht nicht minder gefährlich. Die rechtliche Verpflichtung zum Schadensersatz bei Datenschutzverstößen ist für die private Stelle finanziell spürbar und entfaltet dadurch eine präventive Funktion. Das Haftungsrecht schützt in der Konsequenz Grundrechte, weil es der ökonomischen Analyse des privatrechtlich gelagerten Datenschutzrechts nach aus dogmatischer Sicht dazu geeignet, einen Anreiz zum rechts-

konformen Verhalten zu entfalten.¹⁷ Der inzwischen vom Privatrecht dominierte Datenschutz verdient eine nähere Untersuchung seiner privatrechtlichen Rechtsfolge, die im Gegensatz zu Bußgeldern oder gar strafrechtlichen Sanktionen imstande ist, einen Ausgleich für den Betroffenen zu leisten.

In Deutschland ist das Recht auf Schadensersatz seit der Einführung des ersten Datenschutzgesetzes in Form der deliktischen Haftung nach bürgerlichem Recht existent und wurde im Jahr 1990 durch eine spezielle Rechtsnorm im BDSG aufgewertet. Auch das europäische Datenschutzrecht kennt den Schadensersatz sowohl als Betroffenenrecht als auch als Rechtsfolge von Beginn an. Die Grundverordnung normiert ein Haftungsinstitut zur Gewährung von Schadensersatz, welches erstmalig den Auftragsdatenverarbeitenden als Haftungsgegner benennt¹⁸ und die gesamtschuldnerische Haftung für Fälle, in denen mehrere Verantwortliche oder Auftragsverarbeitende für dieselbe Datenverarbeitung existieren, regelt.¹⁹ Als Rechtsschutzinstrument und Betroffenenrecht besitzt der Ersatzanspruch das Potenzial, das bestehende Sanktionsdefizit im Datenschutzrecht zumindest zu mindern und damit zur tatsächlichen Rechtsdurchsetzung beizutragen. In der Praxis spielt der Schadensersatz im Datenschutzrecht bis jetzt allerdings „kaum eine Rolle“²⁰, was die Gefahr birgt, dass das Grundrecht bei mindestens einer nicht effektiv durchsetzbaren

8 Mögliche Datenschutzverstöße der Facebook Inc., USA werden derzeit wettbewerbsrechtlich untersucht: Bundeskartellamt, Bundeskartellamt eröffnet Verfahren gegen Facebook wegen Verdachts auf Marktmissbrauch durch Datenschutzverstöße, Meldung v. 02.03.2016.

9 Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Bußgeldverfahren gegen die Debeka einvernehmlich abgeschlossen: Debeka akzeptiert Geldbuße und garantiert vorbildliche datenschutzkonforme Ausrichtung des Vertriebs, Pressemitteilung v. 29.12.2014.

10 Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutsche Bahn akzeptiert hohe Geldbuße und will künftig Vorbild im Datenschutz sein, Pressemitteilung v. 23.10.2009.

11 Ferner können auch Bestimmungen der StGB im Kontext des Persönlichkeitsschutzes Anwendung finden, siehe Weichert, Datenschutz – Grundrechtsschutz durch Verfahren, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 2008, Rn. 84.

12 § 44 Abs. 1 BDSG. Den objektiven und subjektiven Tatbestand darstellend Gola/Schomerus, BDSG, 2015, § 44, Rn. 5 ff. Zu den Tatbeständen im Detail Ehmann, in: Simitis (Hrsg.), BDSG, 2014, § 43, Rn. 53 ff.

13 Meyer, in: Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, 2015, Art. 83 AEUV, Rn. 71. Die Union hat dazu auch bereits konkrete Überlegungen angestellt: Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM (2010) 609 endg., 10; Kommission, Mitteilung „Auf dem Weg zu einer europäischen Strafrechtspolitik: Gewährleistung der wirksamen Durchführung der EU-Politik durch das Strafrecht“ v. 20.09.2011, KOM (2011) 573 endg., 3, 12, 14.

14 Thüsing/Pötters, Rechtsfolgen unerlaubter Datenverarbeitung, in: Thüsing (Hrsg.), Beschäftigtendatenschutz und Compliance, 2014, § 21, Rn. 27.

15 So auch Härting/Schneider, Das Ende des Datenschutzes – es lebe die Privatsphäre, CR 2015, 819 (827).

16 Sloot, Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation, International Data Privacy Law 2014, 307 (321).

17 Dazu ausführlich Jacquemain, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, 2017, 285 ff.

18 Art. 82 Abs. 2 DS-GVO.

19 Art. 82 Abs. 4 DS-GVO.

20 Gabel, in: Taeger/Gabel (Hrsg.), BDSG, 2013, § 7, Rn. 1; ebenso Becker, in: Plath (Hrsg.), BDSG, 2013, § 7, Rn. 1; Schneider, in: ders., Handbuch des EDV-Rechts, 2009, Kap. B, Rn. 361.

Rechtsfolge im Falle rechtswidrigen Handelns leerläuft. *Simitis* formulierte die folgende These als Begründung für die praktische Bedeutungslosigkeit, welche wohl auch noch für das zukünftige Haftungsinstitut in der DS-GVO seine Richtigkeit behalten wird: Die Unübersichtlichkeit und teilweise fehlende Eindeutigkeit bei der datenschutzrechtlichen Haftung hinterlässt den Eindruck, etwaige Ansprüche eines in seinen Grundrechten verletzten Betroffenen nach Möglichkeit kraft Gesetzes einzuschränken.²¹

II. Art. 82 DS-GVO wird zentrale Anspruchsgrundlage

Der Akt der Umsetzung ins nationale Recht entfällt mit dem Wechsel der Rechtsgrundlage zur Verordnung. Der Art. 82 DS-GVO stellt unmittelbar anwendbares Unionsprivatrecht dar.²² Mit der Wahl einer Verordnung geht ein Anwendungsvorrang einher. In der Konsequenz wird das bedeuten, dass die EG-Datenschutzrichtlinie (EG-DSRL) zwar mit Wirksamwerden der DS-GVO gemäß Art. 99 Abs. 1 DS-GVO aufgehoben wird, doch das im Zuge der Umsetzung der EG-DSRL geschaffene nationale Recht von unionsrechtlicher Seite unberührt bleibt und weiterbesteht. Der Vorranganspruch des Unionsrechts in Form der Verordnung gewinnt deswegen auch praktisch eine hohe Bedeutung, wenn aus deutscher Sicht zukünftig zwei Schadensersatzansprüche im Datenschutzprivatrecht (aus deutscher Sicht: § 83 BDSG-neu und Art. 82 DS-GVO) existieren werden. Das Recht auf Schadensersatz erhält seine Vollständigkeit sowohl durch den Rahmen der Unionsrechtsordnung, als auch des jeweiligen mitgliedstaatlichen Rechts. Nicht nur die Geltendmachung als solche, sondern auch haftungsausfüllende Aspekte wie Art und Umfang des Schadensersatzes werden deswegen weiterhin vom einzelstaatlichen Recht bestimmt.²³

1. Haftungsart

Die zukünftige Haftungsregel, Art. 82 DS-GVO, baut auf Art. 23 EG-DSRL auf und der Haftungstatbestand bleibt abgesehen von zwei Änderungen der Gleiche.²⁴ Gemeinsam ist dem gegenwärtigen und dem zukünftigen Haftungsregime die Schwierigkeit der Qualifizierung der Haftungsart. Die Einordnung des Art. 82 DS-GVO als Gefährdungshaftung ist genauso wie bei Art. 23 EG-DSRL auszuschließen.²⁵ Zwar fehlt im zukünftigen Haftungstatbestand die Rechtswidrigkeit als Voraussetzung, doch reicht dieser Umstand nicht, dass die Haftungsregel der DS-GVO bereits eine rechtswidrigkeitslose Gefährdungshaftung darstellt. Die ganzheitliche Betrachtung der Haftungsregel der Datenschutzverordnung legt die Absage der Qualifizierung als Gefährdungshaftung nahe. Die Exkulpationsmöglichkeit nach Art. 82 Abs. 3 DS-GVO in Verbindung mit einer Gefährdungshaftung würde den Haftungsausschluss auf außergewöhnliche, zufällige Ereignisse begrenzen. Das zentrale Argument gegen eine Qualifizierung der Gefährdungshaftung ist schlussendlich allein ausreichend und ganz leicht verständlich, dass sie nämlich von Seiten der Legislative tatbestandlich anzuordnen ist, was in Hinblick auf Art. 82 DS-GVO schlicht nicht gegeben ist. Schließlich ist als weiteres Indiz für die Ablehnung ebendieser Haftungsart noch hinzuzufügen, dass eine Gefährdungshaf-

tung in der Regel mit einer Zwanghaftpflichtversicherung einhergeht, die von der DS-GVO jedoch nicht gesetzlich angeordnet wird. Die IT-Haftpflichtversicherung ist wohl in größeren Unternehmen Standard, jedoch längst nicht flächendeckend vom Versicherungsschutz aller Unternehmen umfasst.

Es verbleiben der haftungsrechtlichen Systematik nach noch die Verschuldenshaftung und die vom Verschulden unabhängige Haftung. Der Wortlaut des Art. 82 DS-GVO setzt zur Anspruchsbegründung genauso wie das geltende Recht kein Verschulden und Vertretenmüssen voraus. Aufschluss über die Haftungsart gibt die Gesamtschau von Haftungs begründung (Art. 82 Abs. 2 DS-GVO) und Exkulpationsmöglichkeit (Art. 82 Abs. 3 DS-GVO). In der EG-DSRL wurde die Haftungsbe freiung noch fakultativ geschaffen (Art. 23 Abs. 2 EG-DSRL). Die Einordnung der Haftungsart bei der noch geltenden Datenschutzrichtlinie hing schlussendlich von der Ausgestaltung durch den nationalen Gesetzgeber ab und dabei insbesondere von der Wahl und Form einer Exkulpation in dem zur Umsetzung der EG-DSRL erlassenen innerstaatlichen Recht. Mit der DS-GVO entfällt die Umsetzungspflicht, und damit besteht die Möglichkeit zur Haftungsbe freiung zukünftig EU-weit. Die zukünftige Haftungsregel gewährt die Befreiung vom Schadensersatz, wenn der Anspruchsgegner nachweist, dass er „in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“.

Art. 82 Abs. 3 DS-GVO lässt sich weit interpretieren, so dass eine Vielzahl an Tatbeständen die Exkulpation erlaubt. Gründe zur Haftungsbe freiung können demnach weiter im Falle höherer Gewalt genauso wie im Fehlverhalten des Geschädigten lie-

21 Vgl. *Simitis*, in: ders. (Hrsg.), BDSG, 2014, § 7, Rn. 5. Noch schärfere Kritik übt ders., in: ders., Auf dem Weg zu einem neuen Datenschutzkonzept, DuD 2000, 714 (722) und spricht sogar von einer Schadensersatzpflicht als Fiktion.

22 Trotz der tatsächlichen Vorteile der Verordnung gegenüber der Richtlinie hinsichtlich der Rechtsvereinheitlichung kann und wird auch die DS-GVO keine komplette Harmonisierung des europäischen Datenschutzrechts normieren, welche die nationale Datenschutzregelung gänzlich überflüssig machen würde; Freiherr von dem Bussche; Zeiter; Brombach, Die Umsetzung der Vorgaben der EU-Datenschutz-Grundverordnung durch Unternehmen, DB 2016, 1359 (1364); Kuner, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, BNA Bloomberg Privacy and Security Law Report 2012, 6.2.2012, 1 (3); Spindler, Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937 (937).

23 In dieser Abhandlung richtet sich die Interpretation der supranationalen Haftungsinstitute im Datenschutzprivatrecht stellvertretend für sämtliche Zivilrechtsordnungen der Mitgliedstaaten nach deutschem Privatrecht.

24 Wenngleich auf den Kommissionsentwurf der DS-GVO bezogen, aber unverändert zutreffend Kosmides, Haftung für Datenschutzverstöße nach BDSG – Probleme des § 7 und europarechtliche Vorgaben, in: Conrad; Grützmaker (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, 2014, 534 (538).

25 Spindler, Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937 (947).

26 In den Fassungen der Kommission (DS-GVO-E) und des Europäischen Parlaments (Europäisches Parlament, Standpunkt festgelegt in erster Lesung am 12.03.2014 im Hinblick auf den Erlass der Verordnung (EU) Nr. .../2014 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Damit in Verbindung steht: Europäisches Parlament, Legislative Entschließung v. 12.03.2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung).) sind dieselben Befreiungsgründe, Fehlverhalten der betroffenen Person und höhere Gewalt, wie in EG. 55 EG-DSRL noch erwähnt, finden sich aber in der finalen Fassung nicht wieder.

gen.²⁶ Für den Ersatz des Schadens, der durch die nicht der DS-GVO entsprechende Verarbeitung verursacht wurde, ist in Art. 82 Abs. 2 DS-GVO weder ein Vertretenmüssen noch ein Verschulden verlangt. In seiner Gesamtheit setzt die Schadensersatznorm dann jedoch unausgesprochen ein widerlegliches Vertretenmüssen voraus, verbunden mit der Umkehr der Nachweispflicht zulasten des Verantwortlichen im Sinne des Art. 4 Abs. 1 Ziff. 7 DS-GVO. Die Begrifflichkeit der Verantwortlichkeit in Art. 82 Abs. 3 DS-GVO, auf welche die Haftung abstellt, begründet die Abkehr vom Verschulden hin zum Vertretenmüssen als Erfordernis zur Haftungsbegründung. Den Schadenserfolg hat die datenverarbeitende Stelle auch ohne Verschulden zu vertreten, die Zurechenbarkeit genügt dazu bereits. In der Praxis wird dieses Erfordernis der Verantwortlichkeit im Sinne des § 276 Abs. 1 BGB jedoch mangels abweichender Abrede oder gesetzlicher Anordnung mit dem Verschulden gleichzusetzen sein.²⁷ Einfache Fahrlässigkeit genauso wie Vorsatz können die Voraussetzung zur Haftung erfüllen. Es lässt sich deswegen resümieren, dass Art. 82 DS-GVO als eine Haftung mit vermutetem Verschulden samt Beweislastumkehr hinsichtlich der Verantwortlichkeit qualifiziert werden kann.²⁸

Damit verpasst die supranationale Legislative die Chance, ein Betroffenenrecht und einen Rechtsbehelf in seiner Wirkung zu stärken. Die mit der Datenverarbeitung verbundenen Gefahren für das grundrechtlich geschützte Persönlichkeitsrecht hätten aus rechtspolitischen Überlegungen heraus auch eine Gefährdungshaftung erlaubt.²⁹ Im Zuge der Implementierung der Haftung gemäß Art. 23 EG-DSRL ins nationale Recht bestand immerhin noch die Freiheit, eine rein verschuldensunabhängige, also eine schärfere Haftung zu normieren. Im Sinne des Funktionierens des Binnenmarkts und seines Wettbewerbs erscheint der in der DS-GVO gegangene Weg dennoch nachvollziehbar. Das vermutete Verschulden heilt zudem die für den Betroffenen grundsätzlich mangelhafte Transparenz bei der Datenverarbeitung, der die Schuldfrage deswegen nur schwer beweisen könnte. Ein tatsächlich effektiver Rechtsvollzug zum Schutz personenbezogener Daten bedarf dennoch spürbarer Mittel. Es ist offenkundig, dass der Ordnungsgeber das im Datenschutzrecht bestehende Sanktionsdefizit nicht primär durch Privatrecht zu lösen versucht.

2. Haftungsbegründung

Verglichen mit Art. 23 EG-DSRL fällt in Hinsicht auf die Haftungsregel der DS-GVO zunächst einmal auf, dass sich darin lediglich noch ein Haftungsgrund findet. Nur durch die nicht dieser Verordnung entsprechende Verarbeitung verursachte Schäden sind zu ersetzen. Dagegen beinhalteten die Fassungen des Europäischen Parlaments und der Kommission in Art. 77 Abs. 1 DS-GVO-E noch beide Haftungsgründe der EG-DSRL, was die Frage aufwirft, ob nun tatsächlich ausschließlich nicht mit der DS-GVO zu vereinbarende Datenverarbeitungen im Sinne des Art. 4 Abs. 1 Ziff. 2 DS-GVO haftungsauslösend sein können. Außen vor blieben in diesem Fall etwa Verstöße bei der etwaigen Benennung eines Datenschutzbeauftragten (Art. 37 DS-GVO) oder die Notifikation bei Datenschutzverstößen (Art. 33 f. DS-GVO), die nicht als Datenverarbeitung im Sinne der Verordnung zu qualifizieren sind.³⁰ Die deliktische Haftung

wäre in diesem Szenario als lückenhaft zu charakterisieren, wenn die unerlaubte Handlung ausschließlich in Verbindung mit einer Datenverarbeitung eine Ersatzpflicht auslöst. Doch genau diese Beschränkung auf Datenverarbeitungen wird von EG. 146 DS-GVO untermauert. Darin wird lediglich die Haftung auf diejenigen Datenverarbeitungen erweitert, „die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und nationalen Rechtsvorschriften zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang stehen“. Zusammengefasst ist der Haftungsgrund in Art. 82 DS-GVO jedenfalls verglichen mit dem bisherigen Schadensersatzanspruch im europäischen Datenschutzprivatrecht weitaus weniger offen formuliert. Doch im ersten Absatz der zukünftigen Haftungsregel wird deutlich, dass die Haftungsbegründung nicht derart begrenzt normiert ist. Der Ersatzanspruch nach Art. 82 DS-GVO besteht danach für jeden Schaden infolge eines „Verstoßes gegen diese Verordnung“. Bisher war die bloße Beeinträchtigung der informationellen Selbstbestimmung aus Betroffenensicht zu erdulden, da sie noch keine Rechtswidrigkeit indizierte.³¹ Allein der schädigende Verstoß gegen die DS-GVO genügt in Zukunft, um Schadensersatz verlangen zu können.

Von großer Bedeutung bleibt meines Erachtens die Würdigung des für die Haftungsbegründung ursächlichen Zusammenhangs. Ausgehend von der vorstehend konstatierten Haftung für vermutetes Verschulden wird für die haftungsbegründende Kausalität grundsätzlich ein Verschulden von Seiten des Schädigers verlangt. Jedoch ist die haftungsbegründende Kausalität, der Zusammenhang zwischen Tatbestand und Rechtsgutbeeinträchtigung, in Art. 82 DS-GVO gar keine notwendige Bedingung zur Haftungsbegründung. Die Norm verlangt stattdessen einen Kausalzusammenhang zwischen Tatbestand und Schaden („haftet für den Schaden, der durch die nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde“).³² Dieser ursächliche Zusammenhang für den haftungsbegründenden Tatbestand ist der Geschädigte sowohl darlegungs- als auch beweispflichtig. Auch wenn durch neue Pflichten wie die sog. Rechenschafts- und Nachweispflicht die Verantwortung des Verantwortlichen wächst, schafft dies keine grundsätzliche Umkehr der Beweislast weg vom Datensubjekt. Vielmehr geht die Beweislast aufgrund des Art. 82 Abs. 3 in Verbindung mit Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO nur

27 Grundmann, in: Krüger (Red.), Münchener Kommentar zum BGB, 2016, § 276, Rn. 10.

28 Zu diesem Schluss kommt auch Spindler, Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937 (947). Dem wohl zustimmend qualifizieren Larouche/Peitz/Purtova die Haftungsregel als „little more than a basic fault-based regime for privacy and data protection breaches, with a reversed burden of proof“, in: Larouche/Peitz/Purtova, Consumer privacy in network industries, 2016, 58.

29 Zu der Angemessenheit dieser Haftungsart im europäischen Datenschutzrecht vgl. Jacquemain, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, 2017, 136 ff.

30 Vgl. Gola/Piltz, Die Datenschutz-Haftung nach geltendem und zukünftigem Recht – ein vergleichender Ausblick auf Art. 77 DS-GVO, RDV 2015, 279 (284).

31 Gallwas, Schranken der Informationsfreiheit durch informationelle „Rechte anderer“ oder das „informationelle Drittverhältnis“, in: Conrad; Grützmaker (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, 2014, 347 (366).

32 Vgl. ferner Rat, Ratsdokument Nr. 8383/15 v. 13.05.2015, 3.

für das Verschuldensmoment auf den für die Verarbeitung Verantwortlichen oder den Auftragsdatenverarbeiter über.³³

3. Haftungsausfüllung

Das Problem bei der Haftung ist aber weniger die Haftungsbeurteilung als die Haftungsausfüllung. Für die DS-GVO ist das Vorliegen eines Schadens zwingend vorausgesetzt.³⁴ Die unzulässige Verarbeitung personenbezogener Daten ist jedenfalls ein Verfassungsverstoß;³⁵ ob dies gleichzeitig als ein Schaden im Sinne des Zivilrechts zu verstehen ist, muss individuell bewertet werden.

Ein Schaden ist nur im Rahmen des Schutzzwecks der DS-GVO (Art. 1 Abs. 2 DS-GVO) ersatzfähig. Mit der grundsätzlichen Anknüpfung des Art. 82 DS-GVO an Art. 23 EG-DSRL geht wohl auch in Zukunft das Erfordernis einer tatsächlichen Schädigung mit einer Rechtsgutbeeinträchtigung einher. Schäden in diesem Sinne setzen demzufolge die Rechtsgutbeeinträchtigung voraus, mit anderen Worten: Jeder ersatzfähige Schaden geht hier mit einer Rechtsgutbeeinträchtigung einher. Somit setzt nicht die haftungsbegründende, sondern die haftungsausfüllende Seite den Verletzungserfolg voraus.

Der unbestimmte Rechtsbegriff des Schadens ist autonom nach dem Unionsrecht auszulegen. EG 146 DS-GVO weist sogar explizit darauf hin. Der Schadensersatz nach Art. 82 DS-GVO umfasst materielle ebenso wie immaterielle Schäden. Damit hat sich die Version des Rats und hierbei die deutsche Delegation³⁶ durchgesetzt, wenngleich die Version des Europäischen Parlaments („damage including non-pecuniary damage“) inhaltlich dieses weite Verständnis teilt. Den Erwägungsgründen aller Entwürfe nach zeigt sich gerade in der englischen Sprachfassung, dass das Bestreben eines weiten Verständnisses („Any damage“) von allen legislativen Akteuren geteilt wird.

Auch hier ist die DS-GVO insoweit zu begrüßen, dass sie dieses umfassende Begriffsverständnis ausdrücklich normiert. Weitere Schwierigkeiten resultieren aus dem divergenten Umgang der Mitgliedstaaten bei der Entschädigung von Verletzungen des allgemeinen Persönlichkeitsrechts: Für manche ist bereits der Verletzungserfolg für einen Anspruch ausreichend, die anderen Mitgliedstaaten setzen dagegen einen Verletzungsschaden voraus. Es ist also davon abhängig, ob neben der Interessenverletzung ein schadensausfüllender Verlust Voraussetzung für einen ersatzfähigen Schaden ist. Diese Differenzierung entfällt bei den sog. *per se*-Schäden³⁷, die jedoch nicht in jeder nationalen Rechtsordnung als ersatzfähig erachtet werden. Das Erfordernis der haftungsausfüllenden Kausalität, des ursächlichen Zusammenhangs, zwischen Beeinträchtigung und Schaden, wäre damit hinfällig. Inwieweit auch *per se*-Schäden nach der Grundverordnung ersatzfähig sind, wird die Rechtspraxis entscheiden. Der explizite Verweis in den Erwägungsgründen auf ein Schadensverständnis im Sinne des Unionsrechts spricht dafür, wohingegen ein Ratsdokument³⁸ die Ersatzfähigkeit ebendieser Schäden ausdrücklich verneint.

Im Allgemeinen ist es bei unionsrechtlichen Schadensersatzansprüchen Aufgabe des Haftungsgläubigers, den Eintritt samt Höhe des Schadens nachzuweisen. Wie zuvor herausgestellt, ist für die Anspruchsbeurteilung die bloße Realisie-

rung des haftungsauslösenden Moments nicht ausreichend, sondern es muss tatsächlich ein Schaden bei einer Person vorliegen.³⁹ Dieses Erfordernis beinhalten alle Grundnormen des europäischen Haftungsrechts, wodurch eine Regel auszumachen ist, nach der zur Verletzung eines Rechts etwas Zusätzliches wie der Nachteil der Vermögensbilanz oder einer fiktiven Bilanz über immaterielle Interessen einer Person hinzukommen muss – ganz unabhängig davon, ob es sich um Verletzungen von Rechten oder Beeinträchtigungen durch unerlaubte Handlungen handelt.⁴⁰ In Hinsicht auf materielle Schädigungen ist diesem Erfordernis noch einfach gerecht zu werden. Immaterielle Schäden werden im Unionsrecht vielfach bei Vorliegen einer bestimmten Rechtsverletzung angenommen und ersetzt.⁴¹ Ein Hinweis der Kommission besagt hingegen, dass auch der immaterielle Schaden vom Betroffenen darzulegen ist und die Rechtsübertretung allein nicht ausreicht.⁴² Somit ist ausgeschlossen, ein Nichtübereinstimmen mit geltendem Recht durch die verantwortliche Stelle mit einer immateriellen Schädigung gleichzusetzen. Diesem Erfordernis zur Geltendmachung für den Immaterialschadensersatz kommt eine hohe Praxisrelevanz zu,⁴³ da sie den vom Datensubjekt zu leistenden Nachweis enorm erhöht. Meines Erachtens wird in dieser Voraussetzung der Hauptgrund liegen, dass Schadensersatzansprüche aus Betroffenensicht praktisch kaum durchzusetzen sind.

4. Schafft Art. 82 DS-GVO spürbare Veränderungen?

Die rechtliche Ausgestaltung der Haftungsregime im Datenschutzprivatrecht tritt zu den strukturellen Disparitäten er-

33 Kühling spricht hingegen insgesamt von einer „faktischen Beweislastumkehr“ in Kühling, Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen, NJW 2017, 1985 (1990).

34 Rat, Ratsdokument Nr. 9083/15 v. 27.05.2015, 18, Fn. 44.

35 Bamberger, in: Bamberger/Roth (Hrsg.), Beck'scher OK BGB, 2015, § 12, Rn. 161.

36 Rat, Ratsdokument Nr. 15076/13 v. 23.10.2013, 14, Fn. 28; ders., Ratsdokument Nr. 8383/15 v. 13.5.2015, 20, Fn. 44. Norwegen schlug dagegen vor, diese Konkretisierung in einem Erwägungsgrund vorzunehmen.

37 Bei sog. *per se*-Schäden entfällt die Differenzierung zwischen haftungsbegründender Interessenverletzung und schadensausfüllendem Verlust samt seiner Bewertung. Eine Verletzung der Rechte des Betroffenen ist mit dem immateriellen Schaden gleichgesetzt. Dazu Bar, *Damage without Loss*, in: Swadling/Jones (Hrsg.), *The Search for Principle*, 1999, 23 (37); Gerven, *Remedies for Infringements of Fundamental Rights*, *European Public Law* 2004, 261 (276 f.). Die Unionsgerichtsbarkeit geht bei der Unionshaftung bereits von diesem Verständnis des immateriellen Schadens aus, so Oskierski, *Schadensersatz im Europäischen Recht*, 2010, 311 f., 343 ff., 386. Vgl. auch Bar, *Gemeineuropäisches Deliktsrecht II*, 1999, Rn. 7, 20 ff.

38 Rat, Ratsdokument Nr. 15076/13 v. 23.10.2013, 14.

39 Kosmides, *Zivilrechtliche Haftung für Datenschutzverstöße*, 2010, 101; Rat, Ratsdokument Nr. 9083/15 v. 27.05.2015, 18, Fn. 44.

40 Bar, *Gemeineuropäisches Deliktsrecht II*, 1999, Rn. 5. Verschiedene Jurisdiktionen differenzieren zwischen rechtlich relevantem Schaden und ersatzfähigem Schaden. Auf diese Differenzierung soll hier und im Folgenden verzichtet werden.

41 Oskierski, *Schadensersatz im Europäischen Recht*, 2010, 168, 384. A. A., wonach immaterielle Schäden im Kontext des Art. 340 AEUV genauso wie materielle Schäden nachzuweisen sind: Jacob/Kottmann, in: Grabitz/Hilf (Hrsg.), *Das Recht der Europäischen Union*, 2015, Art. 340, Rn. 118.

42 Rat, Ratsdokument Nr. 9083/15 v. 27.05.2015, 18, Fn. 44.

43 Gola/Piltz, *Die Datenschutz-Haftung nach geltendem und zukünftigem Recht – ein vergleichender Ausblick auf Art. 77 DS-GVO*, RDV 2015, 279 (284).

schwerend hinzu und zeichnet für das Vollzugsdefizit des Schadensersatzanspruchs mitverantwortlich. Grundsätzlich sind die Haftungsinstitute im europäischen Datenschutzprivatrecht davon gekennzeichnet, dass sie hauptsächlich die Haftungsbegründung regeln. Eine große Verbesserung liegt in jedem Fall in der ausdrücklichen Erwähnung moralischer, also immaterieller Schäden als ersatzfähige Schäden im Sinne des Art. 82 Abs. 1 DS-GVO. Diese Anspruchsgrundlage wird zukünftig als *lex specialis* Vorrang gegenüber der konkurrierenden deliktischen Haftung im jeweiligen einzelstaatlichen Recht genießen, sie aber nicht verdrängen. Die deutsche Generalklausel zum Schutz des allgemeinen Persönlichkeitsrechts etwa, § 823 Abs. 1 BGB, wird auch weiterhin anwendbar sein. Jedoch ist Art. 82 DS-GVO neben ihrem bereichsspezifischen Vorteil auch aus rechtspraktischer Perspektive vorzuziehen. Ein maßgeblicher Vorzug darin liegt nämlich unter anderem in der zukünftig tatsächlich geltenden Beweislastumkehr hinsichtlich des Verschuldensmoments. Die größte Schwierigkeit im Zuge der Geltendmachung von Schadensersatz wird der vom Betroffenen zu leistende Nachweis darüber sein, dass tatsächlich eine immaterielle Schädigung vorliegt. Die Übertretung der DS-GVO allein wird dafür nicht ausreichen, vielmehr verlangt das zukünftige Recht eine durch die im datenschutzrechtlichen Sinne betroffene Person erlebte Benachteiligung. Denkbar erscheinen solche Beeinträchtigungen praktisch in Form von Ehrverletzungen, Verlust des Ansehens und ähnlicher emotional zu begründender Einbußen. An dieser Stelle gilt es grundlegend zu untersuchen, ob Art. 82 DS-GVO in der tatsächlichen Anwendung ein funktionales Instrument zur Geltendmachung einer Entschädigung in Geld sein kann. Immaterielle Schäden infolge unzulässiger Datenverarbeitung sind der zukünftigen Anspruchsgrundlage nach jedenfalls ausdrücklich zu kompensieren. Die künftige Haftungsregel in der DS-GVO knüpft den Ersatz nicht an eine schwerwiegende Verletzung, wie es § 823 Abs. 1 oder der nur für öffentliche Stellen geltende § 8 Abs. 2 BDSG machen. Im Umkehrschluss sind danach auch die bisher nicht ersatzfähigen kleineren, sozialadäquaten Eingriffe für einen Schadensersatz ausreichend, um sie in Geld zu entschädigen.

Besondere Relevanz gewinnt mit der unmittelbaren Anwendbarkeit der DS-GVO das für die vollständige Geltung ergänzende Zivilrecht der Mitgliedstaaten. Die hiesige Rechtsprechung verlangt für den Immaterialschadensersatz bei zivilrechtlichen Persönlichkeitsverletzungen unverändert eine schwere Verletzung. Das noch geltende BDSG ist mittels § 1 Abs. 1 BDSG mit dem Persönlichkeitsrecht verknüpft. Dieser Schutzzweck korrespondiert mit Art. 1 Abs. 1 EG-DSRL („Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.“), da er im Zuge der Implementierung der Richtlinie aus dem Jahr 1995 zu keiner Änderung des Schutzzwecks des BDSG führte. Wenn nun mit der DS-GVO laut Art. 1 Abs. 2 DS-GVO die „Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ geschützt werden, ist der Persönlichkeitsschutz darunter auch weiterhin zu subsumieren. Es ist aber nicht die Geldentschädigung bei Persönlichkeitsverletzungen, die eine schwerwiegende Verletzung

voraussetzt, sondern die Geldentschädigung bei Persönlichkeitsverletzungen nach § 823 Abs. 1 BGB i. V. m. Art. 2 Abs. 1 u. Art. 1 Abs. 1 GG. Der Ersatz immaterieller Schäden in Form einer Geldentschädigung auf Grundlage des zukünftigen Datenschutzrechts in Form der DS-GVO hängt jedenfalls nicht von der Intensität der Beeinträchtigung ab. Gerade mit der ab 2018 in der gesamten Union unmittelbar geltenden DS-GVO wird diese Unvollkommenheit besonders deutlich, wenn sich die Voraussetzungen zum Schadensersatzanspruch nach Sekundärrecht richten und die haftungsausfüllende Kausalität, der Schaden sowie sein Umfang durch jeweils anzuwendendes nationales Recht zu bestimmen sind. Das Zusammenwirken der DS-GVO mit dem BDSG-neu ist aufgrund der mangelnden Spezifik der supranationalen Anspruchsgrundlagen einerseits unerlässlich, andererseits verdünnt sie sich durch autonome Auslegung unbestimmter Rechtsbegriffe durch Unionsrecht. Zusammengefasst ist das supranationale Haftungsregime als unvollkommen zu bewerten. Die Europäisierung des privatrechtlichen Datenschutzes trifft dadurch auf zu viele verschiedene nationale Eigenheiten in der jeweiligen Zivilrechtsordnung, um einen einheitlichen Rechtsvollzug zu ermöglichen.

III. Ohne Schaden kein Schadensersatz

Datenschutz schützt nicht nur die Privatsphäre des Einzelnen, sondern schafft einen noch weitergehenden Schutzgehalt. Die notwendige Verknüpfung zwischen ideeller und kommerzieller Seite des Datenschutzrechts als allgemeines Persönlichkeitsrecht wird durch den Gedanken der Selbstbestimmung hergestellt.⁴⁴ Das allgemeine Persönlichkeitsrecht vermag diesen Dualismus also inzwischen abzubilden, das Schadensersatzrecht noch nicht.

1. Was ist der ersatzfähige Schaden?

Der Schutzzweck des Datenschutzrechts erschöpft sich schon seit langem nicht mehr allein im Schutz ideeller Werte wie Würde, Persönlichkeit oder Integrität, sondern ist gerade auch auf das Austarieren wirtschaftlicher Interessen gerichtet. Für das informationelle Selbstbestimmungsrecht gilt insoweit das Gleiche wie auch für das allgemeine Persönlichkeitsrecht; auch Letzteres mag früher rein ideell verstanden worden sein, hat sich jedoch im Laufe der Zeit zu einem Recht fortentwickelt, das neben ideellen auch Vermögensinteressen des Einzelnen umfasst.⁴⁵

Solcherlei Vermögensinteressen stehen beim Umgang mit personenbezogenen Daten oftmals sogar im Vordergrund. In der digitalen Welt haben sich personenbezogene Daten zu einer Art von Währung entwickelt und werden als wirtschaftliches Tauschobjekt genutzt. Damit agiert der Ein-

44 Zustimmung Graf von Westerholt, Wettbewerbsrecht und Datenschutzrecht – ein ungeklärtes Verhältnis, in: Straus (Hrsg.), Aktuelle Herausforderungen des geistigen Eigentums: FS für Beier, 1996, 561 (567).

45 Der Dualismus des Persönlichkeitsschutzes, gleichzeitig ideelle Interessen als auch Vermögensrechte zu schützen, ist in der Rechtswissenschaft ebenso wie in der Judikatur wiederzufinden. Söder, in: Gersdorf/Paal (Hrsg.), Beck'scher OK Informations- und Medienrecht, 2015, § 823 BGB, Rn. 127; Hubmann, Das Persönlichkeitsrecht, 1967, 133 f., 283 f. BGH, Urteil v. 20.03.1968, NJW 1968, 1773 (1774) – Mephisto; BGH, Urteil v. 08.05.1956, BGHZ 20, 346 – Paul Dahlke.

zelle aber bei einer Datenpreisgabe nicht mehr nur als „Person“, sondern auch als Marktteilnehmer.

a) Materielle Schäden

Liegen Vermögensschäden vor, so kann der in negativer Weise Betroffene ebendiesem, in einem Geldbetrag bestimmtem Ausgleich zivilrechtlich einfordern. Eine negative Veränderung des fiktiven Vermögensstatus als Folge rechtswidriger Verarbeitung personenbezogener Daten ist ebenso theoretisch wie auch praktisch denkbar. Die Kreditwirtschaft wird gerne als Beispiel für rein materielle Schäden als Folge unzulässiger Datenverarbeitung angeführt, da sie schon aus ihrem Geschäftsmodell heraus eine pekuniäre Bestimmbarkeit mit sich bringt. Dieser numerisch genau bestimmbare, also nach der konkreten Berechnung ermittelte Schaden ist grundsätzlich ersatzfähig.⁴⁶ Ein fehlerhaftes und deshalb unzulässiges Credit Reporting zur Bonitätsbewertung kann für den Betroffenen einen klar bestimmbaren Verlust in seiner Vermögensbilanz zur Folge haben. Die Differenz zwischen der wegen der negativen Bewertung höheren Zinslast und einer der tatsächlichen Solvenz des Kreditnehmers entsprechenden Zinslast ist der Vermögensschaden, der sich auf Euro und Cent genau bestimmen lässt.⁴⁷ Diese objektive Wertbestimmbarkeit würde jede prozessuale Durchsetzung von Schadensersatzansprüchen in der Rechtspraxis von vornherein als viel Erfolg versprechender erscheinen lassen als die Geltendmachung von immateriellen Schadensersatzforderungen. Bei der Durchsetzung eines Ersatzes für den Vermögensschaden ist der Klagegegenstand bzw. der Streitwert klar bestimmbar. In dem hier skizzierten Szenario aus dem Kreditwesen ist primär die Vermögenslage betroffen, eine Persönlichkeitsrechtsverletzung liegt im Binnenverhältnis zwischen der Kreditanstalt und dem Kunden, der hier das Datensubjekt darstellt, auf den ersten Blick nicht nahe.

b) Immaterielle Schäden

aa) Fehlende Bemessungskriterien im Datenschutzrecht

In den meisten Fällen der Nichtbeachtung von datenschutzrechtlichen Pflichten bleibt es allein bei einer Grundrechtsverletzung. Die größte, mit dem Ersatz immaterieller Schäden verbundene Schwierigkeit liegt meines Erachtens darin, einen solchen Schaden pekuniär zu erfassen. Schlussendlich wird die Determinierung der Schadenshöhe gerade von immateriellen Schäden ein Richterrecht bleiben. Gleichwohl versteht sich bereits die EG-DSRL als Instrument zur Angleichung der Rechtsvorschriften (EG. 8 EG-DSRL), und die DS-GVO als unionsweit unmittelbar geltender Rechtsakt bezweckt erst recht die unionsweit kohärente und einheitliche Anwendung (EG. 10 DS-GVO). Diese legislativen Bemühungen um Kohärenz verlangen meinem Verständnis nach einen möglichst von Einheitlichkeit geprägten Umgang mit dem Schadensersatzanspruch im Datenschutzprivatrecht. Dies gelingt am besten durch möglichst umfassende und detaillierte Vorgaben im Rechtsakt. Auf Seiten des haftungsausfüllenden Tatbestands verbleibt der ersatzfähige Schaden jedoch ohne anzuwendende Kriterien zur Determinierung der Schadenshöhe. Im Sinne des unionsweiten, möglichst einheitlichen Rechtsvollzugs bleiben konkretisierende Vorgaben in Form von Leitlinien, Mitteilungen oder gar

Rechtsakten wünschenswert. Eine solche Weiterentwicklung und Spezifizierung der Haftungsregime durch die supranationale Ebene wäre erstrebenswert, um die Klärung nicht dem nationalen Recht zwangsweise zu überlassen und damit die einheitliche Rechtsanwendung zu behindern.

bb) Datenschutzverstoß = unerlaubte Kommerzialisierung personenbezogener Daten?

Aus den bei Datenschutzverstößen vorherrschend auftretenden immateriellen Schäden sollen im Sinne der Messbarkeit von Schäden Vermögensschäden werden, da Letztere eine Quantifizierbarkeit des Schadensumfangs mit sich bringen. Grundsätzlich besteht bei der ökonomischen Bestimmung von aus Datenschutzverstößen resultierenden immateriellen Schäden die Problematik der Bewertung von nichtkörperlichen Persönlichkeitsrechten. In deren Schutzzumfang kann zweifellos auch ein wirtschaftlicher, in Geld ausdrückbarer Wert einbezogen sein. Das Immaterialgüterrecht ist der beste Beleg dafür, dass sowohl die ökonomischen als auch die ideellen Interessen des Rechteinhabers geschützt sein können. Auch das Recht auf informationelle Selbstbestimmung schützt beide Interessensdimensionen des von der Datenverarbeitung Betroffenen.⁴⁸ Die informationelle Selbstbestimmung schützt nicht nur vor Preisgabe der eigenen Daten, sondern mithin auch vor deren Kommerzialisierung durch Dritte. Eine richterliche Rechtsfortbildung, welche die vermögenswerten Bestandteile des zivilrechtlichen Schutzes personenbezogener Daten als Konkretisierung des allgemeinen Persönlichkeitsrechts ausdrücklich anerkennt, erscheint wahrscheinlich. Wie dies praktisch gelingen kann, hat die BVerfG-Entscheidung in der Rechtssache „Blauer Engel“⁴⁹ bewiesen. Der Datenschutz, der im Persönlichkeitsrecht wurzelt, kann seinen Vermögenswert bereits heute nicht mehr verneinen. Mit der Möglichkeit der Verwertung erhält das Datenschutzrecht eine immaterialgüterrechtliche Komponente.⁵⁰ Diese Entwicklung ist bisweilen noch im Anfangsstadium und wird sich in der nächsten Zeit mit Sicherheit fortsetzen. Das Recht steht vor der Aufgabe, sich dieser Entwicklung im Kontext der Verarbeitung personenbezogener Daten anzupassen. Genau das hat die Gerichtsbarkeit hinsichtlich des Rechts am eigenen Bild, ebenfalls eine Ausprägung des Persönlichkeitsrechts, geschafft: „Es wurde (...) im Interesse der Wirksamkeit des Schutzes dem der ideellen Interessen ein ideell gebundener Schutz von Vermögensinteressen hinzugefügt.“⁵¹ Befürchtungen, dass eine solche Entwicklung pauschal zur Kommerzialisierung des Datenschutzrechts führt, kann entgegengetreten werden, da die informationelle Selbstbestimmung ein Persönlichkeitsrecht bleibt. Inwieweit der Schutz der Daten ein eigentumsartiges Recht umfasst, ist hier nicht zu beantworten. Für

46 Bergmann/Möhrle/Herb, Datenschutzrecht, 2012, § 7 BDSG, Rn. 11.

47 Vgl. LG Paderborn, Urteil v. 05.03.1981, MDR 1981, 581.

48 Dazu ausführlich Jacquemain, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, 2017, 257 ff. Zustimmung Buchner, Informationelle Selbstbestimmung im Privatrecht, 2006, 217.

49 BVerfG, Beschluss v. 22.08.2006, NJW 2006, 3409 – Blauer Engel.

50 Jacquemain, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, 2017, 266 ff.

51 BVerfG, Beschluss v. 22.08.2006, NJW 2006, 3409 (3410) – Blauer Engel.

den zu bejahenden deliktsrechtlichen Schutz des Rechts des Betroffenen auf Schutz seiner personenbezogenen Daten, der kommerzielle Interessen umfasst, bedarf es keiner Ausschließlichkeitsrechte an Daten oder einer personellen Zuweisung. Lediglich das materielle Interesse am Recht auf Schutz personenbezogener Daten muss dafür besser bemessbar werden.

Die unerlaubte Kommerzialisierung personenbezogener Daten durch eine private datenverarbeitende Stelle stellt aufgrund der damit einhergehenden Beeinträchtigung des kommerziellen Interesses des Rechts auf informationelle Selbstbestimmung einen materiellen Schaden dar. In der Konsequenz können Schäden aus Datenschutzvergehen mitunter als ersatzfähige Vermögensschäden erfasst werden, die sich genau bemessen lassen. Das Immaterialgüterrecht hält entsprechende Instrumente zur konkreten Schadensberechnung bereit, die auch im Datenschutzrecht anwendbar sind.⁵² Insbesondere das Urheberrecht könnte dem privaten Rechtsschutz im Datenschutzrecht als Vorbild dienen.⁵³ Damit würden zumindest manche Datenschutzverstöße tatsächlich zu materiellen Schäden umgewandelt und damit in ihrem Umfang ermittelbar. Der pekuniäre Wert eines personenbezogenen Datums ist demnach im kommerziell motivierten Verletzungsfall der ersatzfähige Schaden. Daneben können auch die ideellen Interessen des Rechts des Betroffenen auf Schutz seiner personenbezogenen Daten verletzt sein, was zu einem Anspruch auf Immaterialschadensersatz führt. Die Rechtsdurchsetzung auf Ersatz solcher Doppelverletzungen⁵⁴ sollte sich dabei im Sinne der Praktikabilität ausschließlich auf den materiellen ersatzfähigen Schaden beschränken, solange die Verletzung des allgemeinen Persönlichkeitsrechts nicht überwiegt.

cc) Bemessungskriterien für Persönlichkeitsverletzungen aus Datenschutzverstößen

Kann ein Datenschutzverstoß nicht als unerlaubte Kommerzialisierung der auf den Geschädigten bezogenen Daten qualifiziert werden, bleibt nur noch seine Einordnung als Verletzung ausschließlich ideeller Interessen des deliktisch geschützten Persönlichkeitsrechts. Die Frage, ob jede datenschutzrechtliche Übertretung automatisch eine Verletzung des allgemeinen Persönlichkeitsrechts bedeutet,⁵⁵ steht in enger Verbindung mit der Frage, ob nur schwere Verletzungen dieser Art ersatzfähig sind. Allein der schädigende Verstoß gegen die DS-GVO genügt in Zukunft, um Schadensersatz verlangen zu können. Somit ist die Intensität der Beeinträchtigung allein für die Determinierung einer Entschädigungshöhe von Relevanz und nicht für die Anerkennung eines Schadensersatzanspruchs. Tatsächlich ist jeder Schaden nach der DS-GVO zukünftig ersatzfähig, er sollte aber dennoch ein Mindestmaß überschreiten.⁵⁶ Der in der Rechtspraxis auftretenden Schwierigkeit, eine Intensität zu bestimmen, lässt sich nicht mit einer Art Rechenformel begegnen. Indes lassen sich Kriterien definieren, die für eine Einordnung der Schwere als Grundlage dienen können. Die Qualifizierung der Eingriffsintensität ist maßgeblich bedingt durch die Reichweite derer, die von der Verletzung Kenntnis erlangen, aber auch durch die Dauer der Beeinträchtigung, das Verschulden des Schädigers und vor allem durch den Kontext der Datenver-

arbeitung.⁵⁷ Wenngleich die genannten und weitere ungenannte Parameter nicht trennscharf zu definieren sind, folglich keine formelle Gewichtung zugewiesen bekommen können und auch keine Quantifizierbarkeit der Persönlichkeitsverletzung erlauben, so kann damit dennoch ein qualitatives Richtmaß definiert werden. Die festgestellte Intensität der Beeinträchtigung des Rechts auf informationelle Selbstbestimmung gibt Orientierung für die Entschädigungshöhe. Unstrittig ist, dass schwere Verletzungen zu einer höheren Geldentschädigung führen müssen als minder schwere. Daraus lässt sich erkennen, dass eine ordinale Einordnung des Verstoßes mithilfe solcher Leitlinien möglich wird. Existiert im Idealfall zusätzlich noch eine Tabelle für Entschädigungshöhen bei Datenschutzverstößen auf Grundlage von Fallrecht, liefert die Übertragung der ordinalen Einordnung numerische Ober- und Untergrenzen für eine Geldentschädigung als Rechtsfolge. Die Determinierung einer Entschädigungshöhe wäre mithilfe eines solchen numerischen Rahmens maximal objektiviert. Schlussendlich muss die Geldentschädigung für immaterielle Schäden der Funktion der Haftung im Datenschutzprivatrecht entsprechend auch in ihrer Höhe präventiven Ansprüchen genügen.

52 Buchner, Informationelle Selbstbestimmung im Privatrecht, 2006, 304 mit zahlreichen Nachweisen für gegenteilige Auffassungen. Sein späterer Doktorand Lindhorst folgt dieser Auffassung in Lindhorst, Sanktionsdefizite im Datenschutzrecht, 2009, 69 f. Weichert bejaht dies indirekt, indem er neben dem konkreten Schaden auch die Schadensermittlung über die Lizenzgebühr für gangbar betrachtet, Weichert, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463 (1466). Scheja/Haag plädieren für die Schadensberechnung durch Lizenzanalogie, Scheja/Haag, Datenschutzrecht, in: Leupold/Glossner (Hrsg.), Münchener Anwaltshandbuch IT-Recht, 2013, Rn. 371. Gegen die Lizenzanalogie als Rechtsfolge, weil der Betroffene im Datenschutzrecht nicht über einen „kommerzialisierbaren Persönlichkeitswert“ verfügt, argumentiert Schröder, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, 2007, 131.

53 Dazu ausführlich Jacquemain, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, 2017, 273 ff. Ein Plädoyer für ein Datenverwertungsrecht nach dem Vorbild ökonomischer property rights gibt Purtova, Property rights in personal data: a European perspective, 2012. Schwartmann/Hentsch postulieren einen Verwertungsschutz nach dem Vorbild des Urheberrechts, lehnen jedoch die pauschale Übertragung urheberrechtlicher Konzepte auf personenbezogene Daten begründet ab, in: Schwartmann/Hentsch, Eigentum an Daten. Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV 2015, 221 (224, 230). Ein solches Verwertungsrecht ist von der von Kilian stets angeführten Verfügungsbefugnis abzugrenzen. Eine weitere Alternative: Für ein Verständnis des Persönlichkeitsrechts als Intellectual Property Right: Pinckaers, From Privacy toward a new intellectual property rights in person, 1996.

54 Zustimmend, dass es Doppelverletzungen ideeller und kommerzieller Interessen geben kann: Wandtke, Ökonomischer Wert von persönlichen Daten, MMR 2017, 6 (9); Reber, Marlene Dietrich. Eine Prozessgeschichte zu den ideellen und kommerziellen Bestandteilen des (postmortalen) Persönlichkeitsrechts, ZUM 2004, 708 (714); Wagner, in: Habersack (Red.), Münchener Kommentar zum BGB, 2013, § 823, Rn. 246.

55 Dafür spricht nach jetzigem Recht: BGH, Urteil v. 22.05.1984, BGHZ 91, 233 (239 f.) – AEG-Aktionär: „Jede durch das Bundesdatenschutzgesetz nicht gedeckte Übermittlung personenbezogener Daten stellt eine Verletzung dieses Rechts [das allgemeine Persönlichkeitsrecht des Klägers] dar.“ Dagegen Klippel, Deliktsrechtliche Probleme des Datenschutzes, BB 1983, 407 (414); Ehmann, Informationsschutz und Informationsverkehr im Zivilrecht, AcP 188 (1988), 230 (378) unter Berufung auf BGH, Urteil v. 17.12.1985, NJW 1986, 2505 – Zulässige Speicherung personenbezogener kreditrelevanter Daten über Ein-Mann-GmbH-Gesellschafter. Inwiefern dieses Urteil Ehmanns These stützt, bleibt unklar, eher stärkt es Buchner, der richtigerweise eine Abwägung der schutzwürdigen Interessen verlangt; s. dazu Buchner, Informationelle Selbstbestimmung im Privatrecht, 2006, 300.

56 So verlangt es das Schadensverständnis im unionsrechtlichen Sinne, Oskierski, Schadensersatz im Europäischen Recht, 2010, 385.

57 Ein Vorschlag für Bemessungskriterien für Persönlichkeitsverletzungen aus Datenschutzverstößen in: Jacquemain, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, 2017, 328 ff.

Das Normieren einer Haftung wirkt zwar bereits generalpräventiv, doch auch auf Mikroebene bedarf es als Rechtsfolge für die einzelnen Delikte spürbarer Entschädigungssummen, um der individuellen Prävention Rechnung zu tragen.

IV. Fazit

Der Mangel an erfolgreich durchgesetzten Schadensersatzansprüchen lässt sich mit Sicherheit nicht auf die immerzu vollständige Einhaltung sämtlicher datenschutzrechtlicher Anforderungen zurückführen. Geschriebenes Datenschutzrecht und gelebte Datenverarbeitung haben heute nur noch wenig miteinander gemein. Der Einzelne im Datenschutzprivatrecht steht häufig international agierenden Unternehmen gegenüber, was zu einem hohen Ungleichgewicht zwischen Betroffenen und verantwortlicher Stelle führt. Doch gerade zivilrechtliche Bestimmungen vermögen es ihrer Funktion nach, Disparitäten grundsätzlich auszugleichen. Es gelingt in der Praxis jedoch nicht, das materielle Recht zu effektivieren. Eine solche Effektivierung der Rechtsdurchsetzung könnte aber eine Antwort auf unstrittig bestehende Sanktionsdefizit im Schutzbereich individueller Freiheit darstellen. Zivilrechtliche Durchsetzungsmechanismen, die unser Recht kennt, kommen mit dem dagegen immer noch neuartigem Datenschutzrecht nicht zurecht. An sich ist dieses datenschutzrechtliche Vollzugsdefizit alles andere als eine neue Erkenntnis, gleichwohl hat sich daran aber bislang nur wenig geändert und wird es auch nicht durch die DS-GVO. Eine individuelle Rechtsdurchsetzung findet im Datenschutzrecht bis heute so gut wie gar nicht statt, und auch die behördliche Rechtsdurchsetzung wird gemeinhin als nur wenig effektiv eingeschätzt.

Was das Haftungsrecht in seiner theoretischen Natur zu leisten vermag, stößt in der Rechtspraxis auf seine Unzulänglichkeiten. Sind Datenschutzverstöße nicht gleichzeitig als Medienrechtsdelikte zu qualifizieren, lässt sich konsta-

tieren, dass die Schadenshöhe für den Einzelnen zu gering ist, um sie prozessual geltend zu machen. Stellt der Wert personenbezogener Daten bei der unrechtmäßigen Kommerzialisierung von personenbezogenen Daten den ersatzfähigen materiellen Schaden dar, wird er für den Einzelnen immer noch keine nennenswerte Größe erreichen, die eine Durchsetzung wirtschaftlich erscheinen ließ. Persönlichkeitsrechtliche Verletzungen führen vor Gericht nur im Einzelfall zu finanziell hohen Geldentschädigungen, obwohl die Billigkeit als Maßstab durchaus häufiger das Feststellen spürbarer Erträge erlauben würde. Je weiter die Kommerzialisierung von Daten voranschreitet, desto stärker wird der in der Information enthaltene wirtschaftliche Wert auch die ideelle Dimension repräsentieren. Eine Höherbewertung des ersatzfähigen Schadens – gerade bei Doppelverletzungen ideeller und kommerzieller Interessen – erscheint geboten. Ließe sich der kartellrechtliche Charakter, der zu der Erhöhung der Bußgeldhöhen geführt hat, auch auf das Privatrecht übertragen, kämen spürbare Entschädigungshöhen auf die privaten Stellen zu. Der Individualrechtsschutz kann im Ergebnis nur eine bescheidene Präventivwirkung entfalten. In der Konsequenz scheitert die privatrechtliche Rechtsdurchsetzung meistens an dem dafür nötigen Aufwand, spätestens aber an den dabei anfallenden Kosten.



Dr. Tobias Jacquemain, LL.M.

ist promovierter Datenschutzrechtler und veröffentlicht im Datenschutz ebenso wie im Europäischen Wirtschaftsrecht.

RA Dr. Christian Rolf/Katharina Siewert

Überlegungen zu den Rechtsgrundlagen des künftigen Beschäftigtendatenschutzes

Der Countdown für das Inkrafttreten der DS-GVO¹ tickt. Erst sah es so aus, als ob der Gesetzgeber die Öffnungsklausel des Artikel 88 DS-GVO nicht mehr nutzen wird, um eine Regelung zur Datenverarbeitung im Beschäftigungskontext zu schaffen. Nicht wenige Autoren beschäftigten sich vorsorglich mit der Frage, ob § 32 BDSG a.F. unter der DS-GVO weiter gelten kann².

Das zeugt von wenig Vertrauen in den deutschen Gesetzgeber. Gleichwohl ist es gelungen, mit § 26 BDSG n.F. eine Regelung auf den Weg zu bringen, die dem § 32 BDSG a.F. entspricht³. Dieser Beitrag widmet sich einigen Fragen, die sich im Hinblick auf das Verhältnis der DS-GVO und der Neuregelung des § 26 BDSG stellen.

I. DS-GVO als primäre Rechtsgrundlage

Feststeht: Ab dem 25. Mai 2018 gilt die DS-GVO, die trotz ihrer neuartigen Bezeichnung („Grund“) eine Verordnung nach Artikel 288 Abs. 2 Satz 2 AEUV ist. Sie gilt, auch zwischen Privaten, unmittelbar und zwingend und bedarf keiner Umsetzung. Mitgliedsstaatliches Recht, das die unmittelbare Geltung der Verordnung beeinträchtigt, findet keine Anwendung. Dies verbietet grundsätzlich auch mitgliedstaatliche Regelungen, welche die Bestimmungen der Verordnung nur wiederholen, da die Rechtsquelle (Verordnung oder nationales Recht?) dadurch intransparent wird⁴. Von Letzterem erteilt die DS-GVO ausweislich des Erwägungsgrundes Nr. 8 nur einen Dispens, soweit „dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen“. Über die Auslegung der Verordnung wacht nach Artikel 267 AEUV der EuGH. Die DS-GVO ist damit die primäre Rechtsquelle des Datenschutzes⁵.

II. Nur noch abgeleitete Kompetenz des deutschen Gesetzgebers

Der deutsche Gesetzgeber hat wegen der unmittelbaren Wirkung der DS-GVO keine originäre Regelungskompetenz mehr⁶ und die deutsche Gerichtsbarkeit kein Auslegungsmonopol. Die DS-GVO könnte wegen ihres zwingenden Anwendungsbefehls den Beschäftigtendatenschutz alleine regeln. Die Mitgliedsstaaten können, sie müssen aber nicht von einer Öffnungsklausel Gebrauch machen. Würde die DS-GVO den Beschäftigtendatenschutz regeln, entspräche die Rechtslage in etwa dem alten BDSG vor Einführung des § 32 BDSG. Regelungen über Arbeitsverhältnisse waren in § 28 BDSG geregelt, ergänzende Vorschriften kamen etwa für den internationalen Datentransfer und die Betroffenenrechte zur Anwendung. Dieses Normprogramm würde auch die DS-GVO bieten. Und mehr: Mit der Erweiterung in Artikel 88 Abs. 1 DS-GVO auf Kollektivvereinbarungen bestünde eine ausdrückliche Norm dafür, dass auch eine Kollektivvereinbarung Rechtsgrundlage der Datenverarbeitung sein kann, was in der deutschen Rechtsprechung allerdings auch anerkannt ist⁷.

Für den Beschäftigtendatenschutz findet sich die Öffnungsklausel in Art. 88 Abs. 1 DS-GVO. Es heißt dort bekanntlich, dass die Mitgliedstaaten „durch Rechtsvorschriften oder durch

Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen“ können. Die allgemeine Regelung ist jetzt also die DS-GVO. Zu einer Abweichung für den Beschäftigtendatenschutz kommt es nur, soweit der mitgliedstaatliche Gesetzgeber im Rahmen des Art. 88 DS-GVO eine spezifizierende Regelung erlässt bzw. eine Kollektivregelung eine solche Spezifizierung enthält. Mit anderen Worten: Der Mitgliedsstaat muss von seiner (abgeleiteten) Kompetenz auch Gebrauch machen, sonst bleibt es bei der DS-GVO.

III. Anmeldung nach Art. 88 Abs. 3 DS-GVO

Hinzu tritt eine, wenn auch umstrittene formelle Voraussetzung. Nach Art. 88 Abs. 3 DS-GVO muss der Mitgliedsstaat die aufgrund der Öffnungsklausel erlassenen Rechtsvorschriften

1 Art. 99 Abs. 2 DS-GVO: 25.05.2018.

2 Etwa Kutzki, öAT 2016, 115, 117; Ehmann/Selmayr/Selk, DS-GVO, 2016, Art. 88 Rn. 156; Kort, NZA-Beilage 2016, 62, 66; Kort, NZA-Beilage 2016, 62, 63; Gola/Pöppers/Thüsing, RDV 2016, 57, 60.

3 Die Entwurfsbegründung, BT-Drs. 18/11325, S. 97 spricht davon, dass die spezialgesetzliche Regelung des § 32 BDSG a.F. fortgeführt wird.

4 EuGH vom 28.03.1985, C-272/83.

5 Gola, BB 2017, 1462, 1462: „Grundgesetz“ des Datenschutzes; Kort, NZA-Beilage 2016, 62, 63: es kommt dafür auch nicht auf die Öffnungsklausel des Art. 88 DS-GVO an; Ehmann/Selmayr/Heberlein, DS-GVO, Art. 6 Rn. 31.

6 Ebenso Kort, NZA-Beilage 2016, 62, 63: „Die DS-GVO gibt vielmehr den Mitgliedsstaaten aufgrund der Öffnungsklausel des Art. 88 Abs. 1 DS-GVO einen weiten Regelungsspielraum, setzt jedoch auch einen Regelungsrahmen für den Beschäftigtendatenschutz auf der Basis ihrer übrigen Regelungen.“; Gola/Pöppers/Thüsing, RDV 2016, 57, 57.

7 BAG, 27.05.1986, 1 ABR 48/84b; 25.09.2013, 10 AZR 270/12; 14.05.2014, 1 ABR 2/13; offen gelassen von BAG 17.11.2016, 2 AZR 730/15.

der Kommission mitteilen, also die Vorschriften praktisch notifizieren, die aufgrund der Öffnungsklausel gelten. Die Rechtsfolge einer unterlassenen Mitteilung ist streitig. Einige Autoren meinen, dass die Mitteilung zwar für die Geltung der nationalen Regelung zwingend ist, aber auch nach dem 25. Mai 2018 erfolgen könnte.⁸ Andere sehen darin eher eine Ordnungsvorschrift, die die Geltung der erlassenen Normen nicht berühren soll⁹. Allerdings finden sich Stimmen, die den Gesetzgeber vor einem Versäumnis warnen, denn es droht ein Verlust der Rechtsetzungskompetenz, wenn keine Mitteilung bis zum 25. Mai 2018 erfolgt¹⁰. Hier ist jetzt gesetzgeberisches Risikomanagement gefordert. Die besseren Gründe sprechen dafür, die Mitteilung nach Art. 88 Abs. 3 DS-GVO sehr ernst zu nehmen. Denn wenn Art. 88 Abs. 3 DS-GVO einen Sinn haben soll, dann doch die Pflicht des Mitgliedsstaates, klarzustellen, welche Normen „spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigungskontext“ sind. Andernfalls bliebe dies unklar. Und das ist genau das, was der unmittelbaren Geltung einer Verordnung entgegensteht. Versäumt ein Mitgliedsstaat die Mitteilung insgesamt, droht damit aus unserer Sicht der Verlust der entsprechenden Norm als im Rahmen des Art 88 Abs. 1 DS-GVO erlassen. Auch dann bleibt es bei der DS-GVO.

IV. Wie hat der deutsche Gesetzgeber die Kompetenz genutzt?

Das ist erst einmal der Rahmen, in dem sich der Mitgliedsstaat Deutschland befand, als § 26 BDSG n.F. erlassen wurde. Ob dies so ganz reflektiert wurde, ist offen. Es hat den Anschein, als habe der Gesetzgeber nicht die Öffnungsklausel einer Verordnung genutzt, sondern weiterhin angenommen, eine Richtlinie umzusetzen. Die Unsicherheit zeigt sich an § 1 Abs. 5 BDSG n.F., wonach das BDSG n.F. nicht gelten soll, soweit die DS-GVO unmittelbar gilt. Diese Vorschrift ist eigentlich sinnlos. Das BDSG muss seinen Geltungsanspruch nicht zu Gunsten der DS-GVO zurücknehmen, sondern umgekehrt, die DS-GVO geht nach Art. 288 AEUV automatisch vor.

1. Inhaltliche Umsetzung

Im Beschäftigtendatenschutz kann der Gesetzgeber die in Art. 88 Abs. 1, 2 DS-GVO genannten Gegenstände regeln. Die Aufzählung ist nicht abschließend, aber Art. 88 DS-GVO gibt eine inhaltliche Begrenzung vor¹¹. Der Gesetzgeber hat inhaltlich die Regelung des § 32 BDSG a.F. fortgeführt¹². Sich darauf zu verlassen, dass ein Fortschreiben des § 32 BDSG a.F. als tragfähige Regelung des Beschäftigtendatenschutzes reicht, birgt allerdings Risiken. Dies lässt sich am Beispiel einer aktuellen Entscheidung des BAG vom 22. September 2016¹³ zur heimlichen Videoüberwachung sehen:

Das BAG billigt in dieser Entscheidung die heimliche Videoüberwachung in Folge seiner ständigen Rechtsprechung unter Geltung des § 32 Abs. 1 BDSG als ultima ratio, wenn andere Aufklärungsmethoden des Arbeitgebers versagen, um den Verdacht eines Vertragsbruchs durch den Arbeitnehmer aufzuklären. Geregelt ist die heimliche Videoüberwachung in § 26 BDSG n.F.

nicht, obwohl Art. 88 Abs. 2 DS-GVO „Überwachungsmaßnahmen“ als mögliche Regelungsgegenstände der mitgliedstaatlichen Spezifizierung nennt. Die heimliche Videoüberwachung könnte im Rahmen der DS-GVO auf Probleme stoßen, da Art. 13, 14 DS-GVO Informationspflichten gegenüber den Betroffenen aufstellen¹⁴. Zwar erlaubt Art. 23 Abs. 1 DS-GVO Ausnahmen durch mitgliedstaatliche Regelungen. Auch eine solche findet sich im Entwurf des BDSG n.F. indes nicht. Will man die heimliche Videoüberwachung also weiterhin gemäß den Erkenntnissen der Rechtsprechung halten, muss man sich darauf verlassen, dass dies entweder (heimlich) in § 26 BDSG n.F. mitgeregelt ist oder durch die DS-GVO selbst legitimiert wird. Beides ist sehr zweifelhaft. Schwerer wiegt indes Folgendes: Die Videoüberwachung führte im Ausgangsfall zur Überführung eines Mitarbeiters, gegen den kein Verdacht einer Straftat bestand, wie von § 32 Abs. 1 Satz 2 BDSG a.F. und jetzt § 26 Abs. 1 Satz 2 BDSG n.F. gefordert. Das BAG billigte jedoch die Verwertung dieses „Zufallsfundes“ und setzte sich dabei nach eigenem Bekunden über den Wortlaut § 32 BDSG einfach hinweg¹⁵: „Soweit der Wortlaut der Bestimmung ein anderes Verständnis nahelegen könnte, ist er ‚verunglückt‘. Diese Regelung solle ... die von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern.“

Wenn § 26 BDSG n.F. nur den bisherigen § 32 BDSG a.F. fortführt, fragt sich, ob damit auch die bisherige Rechtsprechung fortgeführt werden soll. Wenn das nicht der Fall ist, wäre die vom BAG vertretene Auslegung *contra legem* nicht mehr möglich. Ist das aber der Fall, enthält § 26 BDSG im Rahmen der Öffnungsklausel des Art. 88 DS-GVO eine Vorschrift, von der bekannt ist, dass sie nach Auslegung der Gerichte nicht das meint, was sie regelt. Das ist vor dem Hintergrund, dass in letzter Instanz der EuGH darüber entscheidet, ob § 26 BDSG eine zulässige Öffnungsklausel ist, fragwürdig. Es besteht die Gefahr, dass der EuGH nicht anerkennt, dass im Rahmen von Art. 88 DS-GVO auch solche Grundsätze einbezogen / mitgeregelt sind, die sich, entgegen dem Wortlaut der mitgliedstaatlichen Regelung, aus der nationalen Rechtsprechung ergeben. Der Wortlaut von Art. 88 DS-GVO nennt nur Rechtsvorschriften und nicht Gerichtsentscheidungen. Besser wäre es gewesen, die durch die Rechtsprechung veranlasste Korrektur schlicht im Gesetz zu regeln.

2. Mitteilung

Das Problem setzt sich dann bei Art 88. Abs. 3 DS-GVO fort, nämlich bei der Meldepflicht. Es stellt sich nach Art. 88 Abs. 3 DS-GVO die Frage, welche Normen des deutschen Rechts jetzt

8 So Kort, NZA-Beilage 2016, 62, 66 unter d); Körner, NZA 2016, 1383, 1385; Ehmann/Selmayr/Selk, DS-GVO, 2017, Art. 88 Rn. 136.

9 So etwa Riesenhuber, BeckOK Datenschutzrecht, Art. 88 Rn. 95.

10 Gola, DS-GVO, Art. 88 Rn. 17; ders. zusammen mit Pötters und Thüsing, RDV 2016, 57, 59.

11 Gola/Pötters/Thüsing, RDV 2016, 57, 59.

12 So ausdrücklich: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/79 und zur Umsetzung der Richtlinie (EU) 2016/680 Drucksache 18/11655, Bl. 97.

13 BAG, 22.09.2016 – 2 AZR 848/15.

14 Darauf weist Gola/Schulz, DS-GVO, Art. 6 Rn. 162 hin.

15 BAG, ebenda; anders LAG Baden-Württemberg, 20.7.2016, 4 Sa 61/15.

eigentlich als Spezifizierung des Beschäftigtendatenschutzes gemeldet werden (sollen). Wie gesagt, kann man diese Frage ignorieren, wenn man sich auf den Standpunkt stellt, dass Art. 88 Abs. 3 DS-GVO auch bei einem Versäumnis die (nicht mitgeteilten) Vorschriften unberührt lässt, was nach unserem Verständnis aber riskant wäre. Varianten:

a) Enge Variante: Nur § 26 BDSG n.F. als Spezifizierung

Der Gesetzgeber könnte nur § 26 BDSG n.F. als Spezifizierung nach Art. 88 Abs. 3 DS-GVO verstehen und der Kommission mitteilen. Wäre allein § 26 BDSG n.F. die Spezifizierung, würden sämtliche anderen Normen des BDSG n.F. und des sonstigen deutschen Rechts keine Regelung zum Beschäftigtendatenschutz treffen können, da der Gesetzgeber insoweit nicht von der Öffnungsklausel des Art. 88 DS-GVO Gebrauch gemacht hat. Es gelten dann die Regelungen der DS-GVO.

b) Oder eine weite Variante?

Die Alternative läge darin, dass das BDSG n.F. in seiner Gesamtheit als Spezifizierung nach Art. 88 Abs. 1, 3 DS-GVO zu melden wäre, mit der Folge, dass solche Regelungen des BDSG n.F. zur Anwendung kommen, die den Beschäftigtendatenschutz betreffen. Zumindest für die in den §§ 32ff. BDSG n.F. bestimmten Betroffenenrechte wäre naheliegend, dass diese auch für Arbeitnehmer gelten sollen. Das kann man noch ausdehnen und andere Rechtsvorschriften des Bundes über den Datenschutz im Sinne von § 1 Abs. 2 BDSG n.F. zu Spezifizierung nach Art. 88 Abs. 1 DS-GVO erklären, die dann – wie unter der alten Rechtslage (§ 1 Abs. 3 BDSG a.F.) – den Regelungen des BDSG vorgehen. Diskutiert wird dies etwa für § 80 Abs. 2 Satz 2 Hs. BetrVG, wonach der Betriebsrat in die Listen über die Bruttolöhne und -gehälter Einblick nehmen darf¹⁶. Folge wäre, dass alles, was datenschutzrechtliche Relevanz im Beschäftigungskontext hat, als Spezifizierung gemeldet werden könnte. Diesen Weg scheint etwa Österreich gehen zu wollen. Geplant ist, das Arbeitsverfassungsgesetz, das eine Kodifikation des Arbeitsrechts enthält, als „Vorschrift im Sinne des Art. 88 DS-GVO mitzuteilen“¹⁷. Es ist aber fraglich, ob eine solche Pauschalmeldung von Art. 88 DS-GVO erlaubt ist. Denn die Mitteilung eines nicht näher spezifizierten Teiles einer mitgliedstaatlichen Rechtsordnung kann kaum gleichzeitig eine Spezifizierung im Sinne des Art. 88 DS-GVO sein¹⁸. Fraglich ist auch, ob Art. 88 DS-GVO nur solche Vorschriften als mitteilungsfähig und -pflichtig ansieht, die „im Kern“ Datenschutzfragen im Beschäftigungskontext regeln¹⁹. Zu einen führt das zu schwierigen Abgrenzungsfragen, ob eine mitgliedstaatliche Bestimmung nun im Kern oder eher am Rande die Datenverarbeitung im Beschäftigungskontext regelt. Zum anderen lässt sich Art. 88 DS-GVO die Pflicht des Mitgliedsstaates entnehmen, zu erklären, welche Bestimmungen seiner Rechtsordnung aufgrund der Öffnungsklausel gelten sollen²⁰. Andernfalls wäre der Rechtsrahmen wieder unklar, was mit der unmittelbaren Geltung der DS-GVO nach Art. 288 Abs. 1 AEUV nicht vereinbar ist²¹: Es gäbe dann Bestimmungen, welche die Datenerhebung unmittelbar im Rahmen der Öffnungsklausel regeln, Bestimmungen, die

zwar nicht nach Art. 88 Abs. 3 DS-GVO gemeldet sind, aber gleichwohl datenschutzrechtliche Relevanz im Beschäftigungskontext haben, und für alles andere gelten die Regelungen der DS-GVO. Ein Rechtsgrundlagenchaos wäre unvermeidbar, was Art. 288 AEUV kaum erlaubt.

Der Gesetzgeber hat diese Frage bisher nicht beantwortet. Einer kryptischen Formulierung der Entwurfsbegründung lässt sich entnehmen, dass sich der Gesetzgeber vorbehält, „Fragen des Datenschutzes im Beschäftigungsverhältnis innerhalb dieser Vorschrift [§ 26 BDSG n.F.] oder im Rahmen eines gesonderten Gesetzes“ zu regeln²². Ob nach dem Ablauf der Meldefrist nach Art. 88 Abs. 3 DS-GVO ein neues Beschäftigtendatenschutzgesetz im Rahmen der Öffnungsklausel erlassen werden könnte, ist aber gerade offen.

Vielleicht war § 26 BDSG ein guter Mittelweg. Der Gesetzgeber hat sich die Modifizierung des § 26 BDSG n.F. vorbehalten, was möglich erscheint, da Art. 88 Abs. 3 DS-GVO eine „spätere Änderung“ zulässt. Daher könnte es mit § 26 BDSG n.F. gelungen sein, einen Platzhalter zu erlassen, der spätere Änderungen flexibel aufnimmt²³. Das Problem einer Regelung des Beschäftigtendatenschutzes wurde dann fristwährend vertagt.

Zu den zahlreichen Aufrufen, die Gelegenheit des Art. 88 DS-GVO zu nutzen, um endlich ein eigenständiges – perfektes – Beschäftigtendatenschutzgesetz zu schaffen, das Fragen umfassend beantwortet, sei nur angemerkt: Wie die DS-GVO selbst ist auch das BDSG n.F. das Ergebnis eines Abstimmungsprozesses widerstreitender Gruppen. Mit anderen Worten: Auf mehr kann man sich eben nicht verständigen. Hinzu kommt ein weiteres Moment. In einer wirtschaftlich fast täglich vermehrten digitalisierten Welt kommt dem Umgang mit Daten zentrale Bedeutung zu. Jeder Regulator, ob europäisch oder national, wird der technischen Entwicklung immer hinterherlaufen. Allein der DS-GVO ging ein 5-jähriger Abstimmungsprozess voraus²⁴. Das entspricht auf der technischen Seite ungefähr dem Zeitraum, um Prototypen autonom fahrender Autos bis zur Serienreife zu entwickeln²⁵. Und während sich die Zeiträume, in denen Gesetze gemacht werden, immer weiter verlängern, verkürzen sich die Zeiträume technischer Innovationen mit zunehmender Geschwindigkeit. Das bedeutet: eine up-to-date Regelung schafft der Gesetzgeber nie.

16 Gola, BB 2017, 1462, 146; anders BAG, 14.01.2014 – 1 ABR 54/12, NZA 2016, 738 ff., gestützt auf § 32 BDSG.

17 Der Gesetzesentwurf für ein Datenschutzanpassungsgesetz sieht mit § 29 öDSG-E folgende Regelung vor: „Das Arbeitsverfassungsgesetz (ArbVG), BGBl. Nr. 22/1974, ist eine Vorschrift im Sinne des Art. 88 DSGVO. Die dem Betriebsrat nach dem ArbVG zustehenden Befugnisse bleiben unberührt.“

18 Ebenso Kort, NZA-Beilage 2016, 62, 66, der eine Öffnung zugunsten des bisherigen BDSG nicht für zulässig hielt; Aufschluss gibt hier auch der Erwägungsgrund Nr. 10 der DS-GVO. Danach können die Mitgliedsstaaten Regelungen für besondere Verarbeitungssituationen treffen; ebenso Ehmann/Selmayr/Selk, Art. 88 Rn. 167f.

19 So Gola/Pötters/Thüsing, RDV 2016, 57, 59.

20 Oben unter 3.

21 Oben, Fn. 3.

22 Oben, Fn 11.

23 Gola/Pötters/Thüsing, RDV 2016, 57, 60 hatten vorgeschlagen, notfalls § 32 BDSG a.F. zu melden, um auf diese Weise wenigstens von der Öffnungsklausel Gebrauch gemacht zu haben.

24 Kutzki, öAT 2016, 115, 115.

25 Vgl. in Bezug auf den Prototypen des selbstfahrenden Autos von Google <http://www.zeit.de/mobilitaet/2014-12/auto-google-autonom-fahren>, aufgerufen am 16.08.2017.

V. Fazit: Schlägt jetzt die Stunde der Betriebsvereinbarung ?

Man wird mit der neuen Regelung arbeiten können, und zwar vor allem wegen der Möglichkeit, Spezifizierungen im Beschäftigtenkontext durch Betriebsvereinbarungen zu erlassen. Dies ist auch schon bisher anerkannt, in jüngster Zeit verstärkt²⁶. Der Wortlaut ist missverständlich. Art. 88 Abs. 1 DS-GVO indiziert, dass auch hier der Mitgliedsstaat die Spezifizierung regelt, was streng genommen nur auf für allgemeinverbindlich erklärte Tarifverträge zuträfe. Der Erwägungsgrund Nr. 155 hilft hier zur Klärung, denn dort heißt es, dass der Mitgliedsstaat „oder“ Kollektivvereinbarungen Rechtsquelle spezifischerer Vorschriften für die Verarbeitung personenbezogener Daten im Beschäftigungskontext sein können. § 26 Abs. 4 BDSG n.F. wiederholt dies nochmals, auch wenn das eigentlich nicht erforderlich wäre, denn die Rechtsmacht zur Regelung personenbezogener Daten im Beschäftigungskontext erhalten die jeweiligen Parteien der Kollektivvereinbarung unmittelbar aus Art. 88 DS-GVO. Die Betriebsvereinbarung unterliegt nicht der Meldepflicht des Art. 88 Abs. 3 DS-GVO, denn diese richtet sich nur an Mitgliedsstaaten und nicht an Sozialpartner. Inhaltlich besteht zwar Streit, was die Betriebsparteien dürfen²⁷. Diese Frage ist allerdings wohl eher theoretischer Natur, da Art. 88 DS-GVO Vorgaben macht, die in etwa dem des BDSG und des BetrVG (§ 75 BetrVG) entsprechen²⁸. Interessant an der Betriebsvereinbarung als Grundlage der Datenverarbeitung im Beschäftigungsverhältnis ist nicht nur, dass sie eine maßgeschneiderte Lösung bietet, sondern unter Umständen gerade darin liegt, dass sie Versäumnisse der gesetzlichen Regelung des § 26 BDSG n.F. ausgleichen kann. Man kann sich nämlich sehr gut vorstellen, etwa die Grundsätze der heimlichen Videoüberwachung in einer Betriebsvereinbarung zu konkretisieren. Als von Art. 88 DS-GVO anerkanntes Regelungsinstrument wäre eine solche Regelung zulässig, auch wenn man zum Schluss

kommt, dass der deutsche Gesetzgeber mangels ausdrücklicher Regelung in § 26 BDSG n.F. dafür keine gesetzliche Rechtsgrundlage geschaffen hat. Ebenso wäre eine Regelung zur Weitergabe von Mitarbeiterdaten im Konzern möglich, was im Erwägungsgrund Nr. 48 der DS-GVO angelegt ist.

Es bleibt daher zum einen zu hoffen, dass der Gesetzgeber der Mitteilungspflicht nachkommt und zum anderen, dass Gerichte ein praktikables Verständnis entwickeln, um die Neuregelung handhabbar zu machen.



Dr. Christian Rolf

ist Partner im Frankfurter Büro von Willkie Farr & Gallagher LLP. Er ist auf das gesamte Arbeits- und Dienstvertragsrecht spezialisiert, u. a. auf Mitarbeiterdatenschutz und Compliance sowie Vergütung von Führungskräften und berät bei sämtlichen Aspekten von Transaktionen und Übernahmen.



Katharina Siewert

ist wissenschaftliche Mitarbeiterin bei Willkie Farr & Gallagher LLP. Sie studierte in Gießen und Zürich und promoviert an der Justus Liebig Universität Gießen im Wirtschaftsstrafrecht.

26 Was schon unter dem BDSG a.F. anerkannt war: BAG, 27.05.1986, 1 ABR 48/84; 25.09.2013, 10 AZR 270/12; 15.04.2014, 1 ABR 2/13; LAG Düsseldorf 25.10.2016, 8 TaBV 62/16; offen gel. BAG, 17.11.2016, 2 AZR 730/25.

27 Kort, NZA-Beilage 2016, 62, 66: nur geringe Abweichung nach unten.

28 In diese Richtung Wybitul, ZD 2016, 203, 207.

Bitte
vormerken

41. DAFTA

„Perspektiven des Datenschutzrechts 2018 –
Anforderungen und Praxis“

16 – 17.11.2017 in Köln

36. RDV-FORUM

15.11.2017 in Köln

Kurzbeiträge

Aus den aktuellen Berichten der Aufsichtsbehörden (32): Beschäftigtendatenschutz und Datenschutzkontrolle

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter*

Mindestlohngesetz und Datenschutz

Das ULD Schleswig-Holstein befasst sich in seinem 36. TB, 2015/1016, Ziff. 5.2), mit Fragen zur Einhaltung datenschutzrechtlicher Vorschriften im Zusammenhang mit der Erfüllung der Vorgaben nach dem Mindestlohngesetz (MiLoG). Nach § 20 MiLoG sind Arbeitgeber mit Sitz im In- oder Ausland verpflichtet, ihren im Inland beschäftigten Arbeitnehmerinnen und Arbeitnehmern ein Arbeitsentgelt mindestens in Höhe des Mindestlohns zu zahlen. Ordnungswidrig handelt derjenige Arbeitgeber, der Werk- oder Dienstleistungen in erheblichem Umfang ausführen lässt, indem er als Unternehmer einen anderen Unternehmer oder Nachunternehmer beauftragt, von dem er weiß oder fahrlässig nicht weiß, dass dieser entgegen dem MiLoG den Mindestlohn nicht erbringt. Hinzu tritt eine verschuldensunabhängige Haftung des Arbeitgebers als Generalunternehmer für Auftrag nehmende Unternehmen und weitere Nachunternehmer. Als weitere Sanktion droht dem Arbeitgeber im Fall eines Verstoßes seiner Auftragnehmer ein Ausschluss von der Vergabe öffentlicher Aufträge.

Zur Begrenzung des Haftungsrisikos wurden von den Datenschutzaufsichtsbehörden Vertragsstrafenregelungen und Bürgschaften vorgeschlagen, die der Generalunternehmer mit seinen Auftragnehmern vereinbaren könnte. Entsprechende Leitlinien wurden vom Bundesarbeitsgericht in einer Entscheidung zum Recht der Arbeitnehmerentsendung entwickelt (BAG, Beschluss vom 06.11.2002, Az.: 5 AZR 617/01). Weiterhin wird empfohlen, dass hinsichtlich der Beauftragung weiterer Subunternehmer ein Zustimmungsvorbehalt für den Generalunternehmer vereinbart wird. In Betracht kommt auch, sich von Forderungen Beschäftigter der Subunternehmer auf Zahlung des Mindestlohns freistellen zu lassen.

Wichtig ist aus datenschutzrechtlicher Sicht, dass der Generalunternehmer in diesem Kontext keine Befugnis hat, die Personalakten der Beschäftigten bei seinen Auftragnehmern einzusehen. Die Einsicht in die Personalakten bezieht sich auf ein höchstpersönliches Recht, das nach der Rechtsprechung des BAG nur vom Beschäftigten selbst wahrgenommen werden darf. Ebenso darf dem Generalunternehmer kein umfassender Zugriff auf die automatisierten Personalsysteme bei den Auftragnehmern gestattet werden. Die Datenschutzaufsichtsbehörden halten eine Übermittlung nicht anonymisierter Verdienstbescheinigungen für unzulässig, da auch Angaben zur

Konfessionszugehörigkeit, zum Familienstand, zur Steuerklasse, zur Anzahl der Kinder, zum vollständigen Geburtsdatum und zur Privatanschrift enthalten sein können. Als Lösung bietet sich eine stichprobenartige Kontrolle geschwärzter Verdienstbescheinigungen an. Näheres ergibt sich aus dem Beschluss der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18./19. März 2015, der unter folgendem Link abrufbar ist: www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89_DSK-MindestlohngesetzUndDatenschutz.pdf;

Zur Thematik äußert sich auch der Unabhängiges Datenschutzzentrum Saarland, 26. TB, 2015/16, Ziff. 12.8, wobei er stichprobenartige Kontrollen von hinsichtlich überflüssiger Angaben geschwärzten Gehaltsbescheinigungen für unbedenklich ansieht.

Weitergabe von Beschäftigtendaten zum Nachweis der Sozialauswahl

Ein weiterer Fall im Rahmen des Beschäftigtendatenschutzes betraf die Weitergabe von Beschäftigtendaten im Rahmen eines Personalabbaukonzepts (ULD-SH, 36. TB, Ziff. 5.5.7). Zum Nachweis der Sozialauswahl hatte ein Arbeitgeber den Kündigungsschreiben eine Liste der zur Entlassung vorgesehenen Arbeitnehmer beigelegt. Auf dieser Liste waren neben dem Namen der Betroffenen u. a. deren Geburtsdatum, Familienstand und Staatsangehörigkeit vermerkt. Der Arbeitgeber vertrat die Auffassung, dass er aufgrund der Vorgaben nach § 1 Abs. 3 Kündigungsschutzgesetz (KSchG) zum Nachweis der Sozialauswahl neben dem Namen auch die Qualifikation und die Sozialdaten der als vergleichbar angesehenen Mitarbeiter offenzulegen hatte. Er begründete dies damit, dass er im Falle eines arbeitsgerichtlichen Verfahrens diese Daten hätte ebenfalls offenlegen müssen. Daher habe man nicht nur eine Namensliste, sondern auch die Kriterien der Auswahl und deren Erfüllung übermittelt.

Das ULD stellt dazu fest, dass zunächst § 1 Abs. 5 Satz 1 KSchG lediglich die bloße Namensliste und keine Informationen, die darüber hinausgehen, vorsieht. Weitergehende Informationen habe nach § 1 Abs. 3 Satz 1 2. Hs. KSchG der Arbeitgeber dem Arbeitnehmer nur auf Verlangen mitzuteilen. Nur insoweit gehe die Norm den allgemeinen Regeln

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

gen des Bundesdatenschutzgesetzes (BDSG) gemäß § 1 Abs. 3 Satz 1 BDSG vor. Die unaufgeforderte Übermittlung einer Liste mit den Namen der zur Entlassung vorgesehenen Arbeitnehmer, deren Wohnort, Geschlecht, Staatsangehörigkeit, Familienstand, Anzahl der Kinder, Geburtsdatum, Alter, Anstellungsstatus, Schwerbehinderung, Vertragsbeginn und Beruf erfolgte daher ohne Rechtsgrundlage. Das ULD hat in diesem Fall einen Verstoß durch Übermittlung personenbezogener Daten ohne vorheriges Verlangen festgestellt.

Umgang mit privaten Daten auf dem Dienstrechner beim Ausscheiden aus dem Unternehmen

Ein weiterer vom ULD behandelter Fall (36. TB, Ziff 5.5.8) betrifft den Umgang mit erlaubterweise auf dem Dienstrechner gespeicherten privaten personenbezogenen Daten der Beschäftigten bei ihrem Ausscheiden aus dem Unternehmen. Das ULD empfiehlt, dass, wenn sich ein Unternehmen entscheidet, die private Nutzung von Dienstgeräten zuzulassen, eine Betriebsvereinbarung regeln sollte, dass private Daten als solche zu kennzeichnen und besser noch in einem gesonderten Bereich abzulegen sind.

Bei einer Speicherung der privaten Daten in einer gesonderten oder gekennzeichneten Ablage ist eine Einsichtnahme durch das Unternehmen grundsätzlich nicht zulässig, da diese Daten für die Beendigung des Beschäftigungsverhältnisses nicht erforderlich sind. Die gekennzeichneten Daten müssen dem Beschäftigten zugeleitet werden. Soweit die Zuordnung einzelner Dateien unklar ist, kann schrittweise eine Einsichtnahme durch die Personalabteilung in Beisein des Betriebsrats, des Datenschutzbeauftragten und bestenfalls auch des Beschäftigten erfolgen. Die Erforderlichkeit der Einsichtnahme ist für jede Datei gesondert zu prüfen.

Grundsätzlich sei die Ablage privater, persönlicher Daten auf einem Dienstrechner aber immer problematisch und zu vermeiden. Das ULD rät ggf. zu einer technischen Containerlösung mit einem verschlüsselten Datenbereich in speziellen Verzeichnissen oder zu einer Verschlüsselung der einzelnen Dateien, wenn eine Erlaubnis zur Speicherung privater Informationen auf dem Dienstrechner erteilt wird.

Keine juristischen Personen als betriebliche Datenschutzbeauftragte nach dem BDSG

Das ULD S—H. (36. TB, Ziff. 5.3) lehnt die Bestellung juristischer Personen, wie etwa eine GmbH oder eine AG, als betriebliche Datenschutzbeauftragte aus folgenden Erwägungen ab. Zunächst besteht das gesetzliche Erfordernis, dass die als bestellte Person die erforderliche Zuverlässigkeit und Fachkunde besitze, was sich im Kern nur auf natürliche Personen beziehen könne, da nur diese ihre erworbene Fachkunde etwa in Form von Nachweisen zu einer abgeschlossenen Berufsausbildung und einer absolvierten Fortbildung erbringen können. In diesem Kontext ist zu bemerken, dass auch Personengesellschaften, wie die OHG oder die KG, nicht als betriebliche Datenschutzbeauftragte be-

stellt werden können. Letzterem wird teilweise entgegnet, dass nach den Vorschriften der Wirtschaftsprüferordnung offene Handelsgesellschaften und Kommanditgesellschaften als Wirtschaftsprüfungsgesellschaften anerkannt werden, wenn sie wegen ihrer Treuhandtätigkeit als Handelsgesellschaften in das Handelsregister eingetragen worden sind. Nach den Vorschriften des Handelsgesetzbuchs können Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften als Abschlussprüfer agieren. Damit hat der Gesetzgeber eine deutliche Aussage getroffen, die im BDSG für die betrieblichen Datenschutzbeauftragten gerade fehlt. Eine entsprechende Einsetzung von Personengesellschaften wurde im BDSG nicht normiert.

Andererseits lege der Wortlaut des § 4f BDSG auch deshalb nahe, dass nur eine Bestellung natürlicher Personen in Betracht kommt, weil die Aussagen zum Benachteiligungsverbot, zur Unterstellung des betrieblichen Datenschutzbeauftragten beim Leiter der nichtöffentlichen Stelle, zur entsprechenden Anwendung der Vorschrift zur Kündigung von Arbeitsverhältnissen (§ 626 BGB) bezüglich des Widerrufs der Bestellung, zur Übernahme von Fortbildungskosten zur Erhaltung der für die Aufgaben erforderlichen Fachkunde (§ 4f Abs. 3 BDSG) sowie zur Geltendmachung eines Zeugnisverweigerungsrechts (§ 4f Abs. 4a BDSG) hierfür sprechen. Gerade die Geltendmachung eines Zeugnisverweigerungsrechts gilt speziell für natürliche Personen. Zeugen sollen bekanntlich vor einem Gewissenskonflikt bewahrt bleiben. Die Zeugnisverweigerung erfolgt wegen persönlicher Gründe, die bei einer natürlichen Person vorhanden sein können. Letzteres gilt etwa nach Maßgabe von § 383 Abs. 1 ZPO.

Ebenso beurteilt die BfDI, 26. TB, 2015/2016, Ziff. 1.8, die Rechtssituation, indem, wenn eine Person außerhalb der verantwortlichen Stelle bestellt werden soll (§ 4f Abs. 2 S. 3 BDSG), es sich nur um eine natürliche Person, nicht aber eine juristische Person oder eine Partnerschaftsgesellschaft handeln kann.

Betroffene, die sich vertraulich an die Person des Beauftragten für den Datenschutz wenden möchten, könnten bei einer juristischen Person oder einer Partnergesellschaft als externem Datenschutzbeauftragten zudem nicht sicher sein, dass die Person, der das Anliegen vorgetragen wird, sie tatsächlich vertritt und auch weiterhin als Organ der juristischen Person tätig sein wird, zumal sich die Zusammensetzung der natürlichen Personen als Organe einer juristischen Person ändern kann. Zuletzt ist eine juristische Person nicht in der Lage, verschwiegen zu sein (§ 4f Abs. 4 BDSG); dies können nur natürliche Personen.

Auch die DS-GVO geht nach Auffassung der BfDI grundsätzlich von dem Verständnis aus, dass nur natürliche Personen die Anforderungen an Fachkunde und Eignung erfüllen können. In Leitlinien der Artikel-29-Gruppe werde zwar akzeptiert, dass ein externer Datenschutzbeauftragter auch eine juristische Person sein könne. Allerdings müsse dann jede (natürliche) Person, die innerhalb dieser Organisation Funktionen des Datenschutzbeauftragten wahrnimmt, sämtliche Voraussetzungen für die Benennung eines Datenschutzbeauftragten erfüllen. Dabei sollten in einem Team klare Verantwortlichkeiten festgelegt und eine Person als primärer Ansprechpartner festgelegt werden.

Gebühren für Amtshandlungen der Saarländischen Aufsichtsbehörde

Mit der Verordnung zur Änderung der Verordnung über den Erlass eines Allgemeinen Gebührenverzeichnisses vom 6. April 2016 (Amtsbl. S. 246) wurde im Allgemeinen Gebührenverzeichnis unter Ziffer 240 ein eigener Gebührentatbestand geschaffen, der es ermöglicht, für Amtshandlungen der saarländischen Aufsichtsbehörde nach dem Bundesdatenschutzgesetz (BDSG) Verwaltungsgebühren zu erheben (vgl. Unabhängiges Datenschutzzentrum Saarland, 26. TB, 2015/16, Ziff. 23.1. Das Gebührenverzeichnis sieht u.a. für datenschutzrechtliche Kontrollmaßnahmen einen Gebührenrahmen von 50-5.000 Euro vor, wenn diese mit einem besonderen Prüfungsaufwand einhergehen. In Fällen, in denen die verantwortlichen Stellen nachweislich kooperieren, um datenschutzkonforme Zustände herzustellen, kann auf die Festsetzung einer Gebühr aus Billigkeitsgründen ganz verzichtet werden. Für Anordnungen zur Beseitigung festgestellter Datenschutzverstöße oder technischer oder organisatorischer Mängel nach § 38 Abs. 5 Satz 1 BDSG können ebenfalls 50-5.000 Euro festgesetzt werden. Auch die Beratung betrieblicher Datenschutzbeauftragter oder anderer

nicht-öffentlicher Stellen kann mit einer Gebühr zwischen 200-10.000 Euro veranschlagt werden, wenn es sich nicht bloß um einfache Auskünfte handelt. Durch die Gebührenfreiheit für einfache Auskünfte sollen die verantwortlichen Stellen auch weiterhin dazu ermuntert werden, bei konkreten datenschutzrechtlichen Fragestellungen mit der Aufsichtsbehörde Rücksprache zu halten und deren Expertise und Rechtsrat einzuholen. Gleichwohl ist eine Gebührenerhebung für Beratungsleistungen trotz der gesetzlich vorgesehenen Beratungsaufgabe der Landesbeauftragten für Datenschutz dann angemessen, wenn diese Beratung im Sinne einer umfassenden Rechtsberatung und datenschutzrechtlichen Bewertung eigener Datenverarbeitungsprozesse in Anspruch genommen wird. Die sich aus einer solchen umfassenden Beratung ergebenden Vorteile für die Unternehmen sind wirtschaftlicher Art und verschaffen den entsprechenden Stellen erhebliche Wettbewerbsvorteile. Auf der einen Seite vermeiden die verantwortlichen Stellen durch die Einschaltung externer Dienstleister und Beratungsunternehmen entstehende Kosten. Gleichzeitig verringern sie das Risiko von gegen das Unternehmen geführten Verwaltungs- und Bußgeldverfahren wegen unzulässiger Datenverarbeitung und gerichtlicher Inanspruchnahme durch etwaig Betroffene.

Gehaltsdaten für Benchmarks übermitteln – zulässig?

Dr. Niels Lepperhoff, Düsseldorf*

Die Mehrheit der Arbeitnehmer hat sich wohl mal gefragt, wie ihr Gehalt im Vergleich zu dem anderer ausfällt. Auch Personalabteilungen beschäftigten sich mit der Frage nach einer angemessenen Vergütung. Da ist es naheliegend, sich Gehaltsvergleiche, sogenannte Gehaltsbenchmarks, anzusehen und diese auch für Gehaltsverhandlungen heranzuziehen. Diese Gehaltsbenchmarks können naturgemäß nicht ohne die Lieferung von individuellen Gehaltsdaten erstellt werden. Die Anbieter von Gehaltsbenchmarks brauchen eine Vielzahl an Datensätzen, um eine aussagekräftige Übersicht bieten zu können. Für sie wäre es daher ideal, wenn Arbeitgeber die Gehaltsdaten aller Mitarbeiter übermitteln würden. Den Arbeitgebern kann im Gegenzug ein finanzieller Vorteil oder der Zugang zur Gehaltsbenchmark geboten werden. Es stellt sich die Frage, auf welcher Rechtslage eine solche Weitergabe denkbar wäre und ob es durch Anonymisierung der Gehaltsdaten möglich wäre, die Notwendigkeit einer Rechtsgrundlage zu umgehen.

I. Einleitung

Zahlen wir unter- oder überdurchschnittliche Gehälter? Diese und ähnliche Fragen stellen sich Personalleiter. Zur Beantwortung

wird u.a. auf Anbieter von Gehaltsbenchmarks zurückgegriffen. Solche Benchmarks geben Auskunft über die Gehaltsspannbreiten in einer Branche. Dabei wird je nach Benchmark neben weiteren Kriterien auch nach Qualifikation, Position, Geschlecht und Alter unterschieden. Um solche Benchmarks erstellen zu können, sind die Anbieter auf personenbezogene Gehaltsdaten angewiesen. Personalleiter stehen deshalb vor der Frage, ob sie die Gehaltsdaten ihrer Mitarbeiter zum Aufbau eines Benchmarks an die Anbieter übermitteln dürfen. Ob eine solche Übermittlung zu einer Preisreduktion oder einem anderweitigen wirtschaftlichen Vorteil führt, ist für die datenschutzrechtliche Frage der Zulässigkeit grundsätzlich unerheblich und wird deshalb nicht weiter betrachtet.

Aufgrund der Verarbeitung für eigene Zwecke durch den Anbieter des Benchmarks scheidet eine Auftragsverarbeitung aus. Im Folgenden wird die Zulässigkeit beleuchtet. Mit Blick auf

* Der Autor ist Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (einem Gemeinschaftsunternehmen des BvD e.V. und der GDD e.V.). Er verfügt über langjährige Erfahrung als externer Datenschutzbeauftragter und berät sowohl deutsche als auch internationale Unternehmen. Daneben ist er Inhaber eines Lehrauftrags des Masterstudienganges „Medienrecht und Medienwirtschaft“ an der Technischen Hochschule Köln.

die sehr überschaubare Geltungsdauer des BDSG-alt konzentriert sich die Betrachtung auf die DS-GVO i.V.m. BDSG-neu¹.

Im Folgenden wird davon ausgegangen, dass im Arbeitsvertrag keine einer Übermittlung entgegenstehenden Vertraulichkeitsklauseln vereinbart worden sind.

An die Prüfung, ob ein Personenbezug vorliegt (Abschnitt 2), schließt sich die Diskussion zur Zulässigkeit an (Abschnitt 3).

Wenn die Übermittlung an einen Empfänger in einem Drittstaat stattfinden soll, muss dort regelmäßig gemäß Art. 44 DS-GVO zusätzlich ein angemessenes Datenschutzniveau vorliegen. Dies gilt auch, wenn der Vertragspartner in der EU niedergelassen ist, die Daten aber bspw. an ein Webportal übermittelt werden, das in einem Drittstaat betrieben wird. Unterauftragnehmer des Anbieters sind ebenfalls zu berücksichtigen. Da sich für die vorliegende Fragestellung keine Besonderheit bzgl. der Drittstaatenthematik ergibt, wird auf eine Erörterung verzichtet.

II. Personenbezug der übermittelten Daten

Als Ziele eines solchen Benchmarks stellen sich u.a. dar,

- die Gehaltsentwicklung bestimmter Personen über längere Zeiträume nachzuzeichnen und
- einen Vergleich zwischen Personen mit gleichen demographischen und qualifikatorischen Eigenschaften zu ermöglichen.

Um diese Ziele zu erreichen, müssen neben den eigentlichen Gehaltsdaten (Bruttogehalt, Dienstwagennutzung, Arbeitsstunden usw.) weitere Angaben zur Person, Position und Qualifikation übermittelt werden. Gewünscht werden bspw. die folgenden Angaben:

- Land des Arbeitsorts,
- Name des Arbeitgebers,
- Postleitzahl der Betriebsstätte,
- Abteilungsname,
- Bezeichnung der Position,
- Geschlecht,
- Geburtsdatum,
- Ausbildung,
- Hierarchiestufe und
- Fachrichtung.

Nach Art. 4 Abs. 1 DS-GVO liegt ein Personenbezug bereits dann vor, wenn die natürliche Person bestimmbar ist. Auch wenn der Name des Mitarbeiters nicht enthalten ist, so reichen die übrigen Angaben für den Empfänger grundsätzlich aus, um den Personenbezug herzustellen. Insbesondere bei Positionen mit Kundenkontakt reicht dazu häufig die Webseite des Arbeitgebers aus, da sie neben Namen auch die Abteilung, die Position und meistens das Geschlecht durch den Namen verrät. Als weitere Hilfsmittel kommen Xing und LinkedIn in Frage, deren Nutzung für die Anbieter ohne nennenswerte Hürden legal möglich ist. Damit sind die übermittelten Daten für den Anbieter personenbezogen.²

III. Rechtsgrundlagen für eine Übermittlung

Die Übermittlung vom Arbeitgeber an den Benchmark-Anbieter gliedert sich in zwei Phasen, die jeweils eine legitimierende Rechtsgrundlage benötigen:

1. Entnahme der Daten aus der Personalakte bzw. dem Personalinformationssystem und
2. Übermittlung an den Benchmark-Anbieter.

Ob die Daten in der Personalakte in Papierform vorliegen oder in einem elektronischen Personalinformationssystem gespeichert sind, ist unerheblich. § 26 Abs. 7 BDSG-neu bezieht auch Verarbeitungen außerhalb eines Dateisystems mit ein. Im Folgenden wird deshalb abkürzend von Personalakte gesprochen.

Findet sich für eine der Phasen keine Rechtsgrundlage, ist die Übermittlung in Gänze unzulässig. Grundsätzlich kommen die üblichen Rechtsgrundlagen für die Übermittlung vom Arbeitgeber an den Benchmark-Anbieter in Betracht:

- Einwilligung (Abschnitt 3.1)
- Notwendig zur Durchführung des Arbeitsverhältnisses (Abschnitt 3.2)
- Interessensabwägung (Abschnitt 3.3)

1. Einwilligung

Eine wesentliche Voraussetzung für die Wirksamkeit von Einwilligungen ist die Freiwilligkeit ihrer Erteilung (Art. 7 Abs. 4 und Erw. 43 DS-GVO sowie § 26 Abs. 2 BDSG-neu). Mit dem expliziten Abstellen der DS-GVO auf die Ungleichgewichte zwischen Betroffenen und Unternehmen in Erw. 43 verändert sich die Rechtslage, geprägt u.a. durch Entscheidungen des BAG, nicht grundlegend.³ Die Tatsache des Arbeitsverhältnisses schließt damit für Arbeitnehmer nicht per se die Möglichkeit aus, in eine Übermittlung an den Anbieter einzuwilligen.

§ 26 Abs. 2 BDSG-neu sieht die Gewährung eines rechtlichen oder wirtschaftlichen Vorteils für den Betroffenen als ein Kriterium an, das für eine Freiwilligkeit spricht. Ein solcher Vorteil wäre eine Bezahlung der Mitarbeiter für die Entnahme und Übermittlung.

Das zweite Kriterium des § 26 Abs. 2 BDSG-neu, die gleichlautenden Interessen von Arbeitnehmern und Arbeitgebern, setzt voraus, dass die Interessen an der Übermittlung gleichlaufen. Das kann bei einer Aufteilung der Bezahlung der Fall sein. Es kommt jedenfalls auf die Gestaltung im Einzelfall an, da generell davon auszugehen ist, dass der Mitarbeiter kein Interesse an einer Übermittlung hat, wenn er von dieser nicht profitiert.

Die Übermittlung an den Anbieter lässt sich damit durchaus auf eine Einwilligung stützen, sofern die übrigen Anforderungen des Art. 7 DS-GVO insbesondere hinsichtlich der anzugebenden Informationen erfüllt werden.⁴ Gleichwohl sollte im Einzelfall geprüft werden, dass keine Konstellation vorliegt, die gegen die Freiwilligkeit spricht.

2. Durchführung des Arbeitsverhältnisses

§ 26 Abs. 1 BDSG-neu regelt die Zulässigkeit einer Datenverarbeitung im Beschäftigungsverhältnis unter Nutzung der Öff-

¹ BDSG in der Fassung der Fassung vom 30.06.2017 (BGBl. I S. 2097).

² Gemäß des EUGH-Urteils zur dynamischen IP-Nummer (C 582/14, Rn. 49) reicht für die Bestimmbarkeit der Person aus, dass mittels Zusatzinformationen der Personenbezug rechtlich zulässig hergestellt werden könnte.

³ Schulz, Art. 7, Rn. 76, in: Gola, DS-GVO Kommentar.

⁴ So sieht Gola/Wronka, Handbuch Arbeitnehmerdatenschutz, 2013, Rn. 887 die Einwilligung im ähnlich gelagerten Fall der Übermittlung an Versicherungen als zulässig an.

nungsklausel in Art. 88 Abs. 1 DS-GVO. Insofern tritt § 26 Abs. 1 BDSG-neu an Stelle von Art. 6 Abs. 1 lit b DS-GVO.

§ 26 Abs. 1 S. 1 BDSG-neu erlaubt u.a. die Datenverarbeitung, sofern diese für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Der Bezugspunkt ist der Arbeitsvertrag. Eine Datenverarbeitung, die für die Durchführung eines Arbeitsvertrags notwendig ist, wäre zulässig. Dieses trifft zweifelsohne auf die Festlegung des Gehaltes zu. Eine Analyse, ob ein Gehalt marktüblich ist, mag aus Sicht des Arbeitgebers für die Gehaltsfestsetzung während des Beschäftigungsverhältnisses hilfreich sein, notwendig ist sie indes nicht, da das Gehalt auch ohne Benchmark verhandelt werden kann. Ein Arbeitgeber könnte sich etwa an Tarifverträgen orientieren oder einfach das vom Mitarbeiter geforderte Gehalt akzeptieren. Somit ist die Entnahme aus der Personalakte und Übermittlung an den Anbieter für die Durchführung des Beschäftigungsverhältnisses nicht notwendig. Dies gilt folgerichtig auch, wenn der Erhalt des Benchmarks an eine Datenübermittlung gekoppelt wäre.

Eine Notwendigkeit zur Entnahme und Übermittlung könnte vorliegen, wenn die Gehaltsfestsetzung oder -entwicklung im Arbeitsvertrag an den Benchmark des Anbieters gekoppelt wird und dieser ausschließlich den Unternehmen zur Verfügung gestellt wird, die ihrerseits Gehaltsdaten übermitteln. Eine solche Konstruktion dürfte in der Praxis eher die Ausnahme darstellen.

3. Interessensabwägung

Art. 6 Abs. 1 lit. f DS-GVO erlaubt eine Datenverarbeitung, sofern diese für berechtigte Interessen des Arbeitgebers oder eines Dritten, hier des Anbieters, erforderlich ist und die berechtigten Interessen der Betroffenen an einer Unterlassung der Datenverarbeitung nicht überwiegen. Ein denkbare berechtigtes Interesse seitens des Arbeitgebers wäre es, wenn durch die Datenübermittlung ein Zugang zu der Benchmark erlangt wird.

Seitens des Anbieters wäre das Einsammeln von personenbezogenen Gehaltsdaten zur Erstellung und Verkauf der Benchmarks ein berechtigtes Interesse. Allerdings kann ein Anbieter auch Mitarbeiter direkt ansprechen und um deren Daten bitten. Der Weg über den Arbeitgeber ist deshalb eher praktisch denn notwendig. Da die berechtigten Inter-

essen der betroffenen Mitarbeiter überwiegen, kann die Erörterung der Notwendigkeit dahingestellt bleiben.

Die berechtigten Interessen des Unternehmens bzw. des Anbieters sind gegen die berechtigten Interessen der Beschäftigten abzuwägen. Generell besteht das Gebot, Daten in der Personalakte vertraulich zu behandeln. Dieses ergibt sich aus der höchstrichterlichen Rechtsprechung⁵. Diese Rechtsprechung stützt sich teilweise auf verfassungsrechtliche Überlegungen, die auch im Lichte der DS-GVO grundsätzlich Bestand haben. Die Vertraulichkeit steht einer Entnahme aus der Personalakte sowie der Übermittlung regelmäßig entgegen.⁶ Da Art. 6 Abs. 1 lit f DS-GVO keine wesentlichen materiellen Unterschiede zu dem bisherigen die Interessensabwägung regelnden § 28 Abs. 1 Nr. 2 bzw. Abs. 2 Nr. 2 a) BDSG aufweist, lässt sich die bestehende Auslegung sinngemäß mit der gebotenen Vorsicht übertragen.

Negative Konsequenzen für Betroffene, wenn bspw. Ex-Ehepartner die Gehaltshöhe zum Gegenstand von Forderungen machen, sprechen auch im Einzelfall gegen eine Übermittlung. Dieses wird durch die aus der Erfahrung bekannten Erwartung der Mitarbeiter auf eine vertrauliche Behandlung der Gehaltsdaten gestützt. Deshalb spricht einiges dafür, dass in der Praxis eine Einzelfallbetrachtung geboten erscheint.

Erhalten Empfänger oder Unterauftragnehmer in Drittländern die personenbezogenen Daten, sprechen weitere Gründe gegen eine Übermittlung.

Selbst wenn die Daten vor der Übermittlung anonymisiert werden würden, wäre die Entnahme aus der Personalakte weiterhin personenbezogen und damit regelmäßig unzulässig.

IV. Fazit

Das Gebot der Vertraulichkeit der Personalakte setzt der Datenverarbeitung des Arbeitgebers weiterhin Grenzen. Auch wenn bei einer Teilnahme an einem Gehaltsbenchmark durch Lieferung personenbezogener Gehaltsdaten der Mitarbeiter wirtschaftliche Vorteile für Unternehmen oder der Bezug des Benchmarks winken, lässt sich neben der Einwilligung durch die Arbeitnehmer keine weitere legitimierende Rechtsgrundlage erkennen.

⁵ Gola/Wronka, Handbuch Arbeitnehmerdatenschutz, 6. Aufl. 2013, Rn. 139.

⁶ Für den in der Eingriffstiefe vergleichbaren Fall des Bankgeheimnisses siehe Simitis, Bundesdatenschutzgesetz, 8. Aufl., § 28 Rn. 99.

Rechtsprechung

Zur Zulässigkeit einer allgemeinen Schweigepflichtentbindung gegenüber einem Versicherer

(Bundesgerichtshof, Urteil vom 5. Juli 2017 – IV ZR 121/15 –)

- § 213 VVG steht der Zulässigkeit so genannter allgemeiner Schweigepflichtentbindungen nicht entgegen. Der Versicherer darf im Rahmen seiner Leistungsprüfung dem Versicherten die Erteilung einer solchen Erklärung aber regelmäßig nicht abverlangen (Fortführung des Senatsurteils vom 22. Februar 2017 – IV ZR 289/14, r+s 2017, 232).**
- Auch nach Inkrafttreten des § 213 VVG ist in Fällen der Datenerhebung ohne ausreichende Rechtsgrundlage, insbesondere bei Nichtbeachtung der Vorgaben des § 213 Abs. 2 Satz 2, Abs. 3 und 4 VVG, sachlich-rechtlich zu prüfen, ob der Versicherer nach § 242 BGB gehindert ist, sich auf die Ergebnisse seiner Ermittlungen zu berufen und insbesondere darauf gestützt von dem Gestaltungsrecht der Arglistanfechtung Gebrauch zu machen (Fortführung des Senatsurteils vom 28. Oktober 2009 – IV ZR 140/08, r+s 2010, 55).**

Tatbestand:

Die Klägerin verlangt – soweit im Revisionsverfahren noch von Interesse – als Versicherte vom beklagten Versicherer Leistungen aus einer Berufsunfähigkeits-Zusatzversicherung nebst Erstattung vorgerichtlicher Rechtsverfolgungskosten.

Im Juni 2004 beantragte der Ehemann der Klägerin bei der Beklagten eine Risikolebensversicherung, in welche die seinerzeit 44-jährige Klägerin als versicherte Person einbezogen werden sollte. Der Versicherungsantrag enthält detaillierte Angaben zu Vorerkrankungen des Ehemanns, während auf der den Gesundheitszustand der Klägerin betreffenden Antragsseite lediglich Körpergröße und Gewicht angegeben und sämtliche weitere Fragen (mit Ausnahme der nicht beantworteten Frage nach Medikamenteneinnahme innerhalb des letzten Jahres) verneint sind. Der Antrag trägt Unterschriften der Klägerin. Die Beklagte stellte einen Versicherungsschein mit Wirkung ab dem 1. September 2004 aus.

Im November 2004 beantragte der Ehemann als Versicherungsnehmer eine Berufsunfähigkeits-Zusatzversicherung zur genannten Lebensversicherung, in welche die Klägerin, die seinerzeit als Postzustellerin arbeitete, ebenfalls als versicherte Person einbezogen werden sollte. In dem auf den 15. November 2004 datierten Antragsformular sind unter der Überschrift „Gesundheitsangaben“ zahlreiche Fragen, unter anderem nach Behandlungen und Untersuchungen des Bewegungsapparates während der zurückliegenden zehn Jahre, diagonal durchgestrichen und mit dem handschriftlichen Zusatz versehen: „Hauptantrag wurde im Sep. 2004 gestellt. Der gesundheitliche Zustand hat sich nicht verändert und es ist nichts neues dazugekommen. Gesundheitsfragen siehe Hauptantrag“. Darunter befinden sich die Unterschriften der Eheleute. Der daraufhin erstellte Versicherungsschein nennt als Versicherungsbeginn ebenfalls den 1. September 2004 und als Leistungsdauer für die Berufsunfähigkeitsrente zehn Jahre.

Die Klägerin bezieht wegen einer psychischen Erkrankung, in deren Folge sie nach ihrer Behauptung seit Mai 2011 bedingungsgemäß berufsunfähig ist, seit November 2011 eine Rente wegen voller Erwerbsminderung. Im Januar 2012 zeigte sie die Erkrankung der Beklagten an. Wenig später beantragte sie [auf einem Vordruck der Beklagten] Versicherungsleistungen und unterzeichnete unter anderem eine von der Beklagten vorformulierte Schweigepflichtentbindungserklärung mit folgendem Wortlaut:

„Ich ermächtige den Versicherer, zur Nachprüfung und Verwertung der von mir über meine Gesundheitsverhältnisse gemachten Angaben alle Ärzte, Krankenhäuser und sonstige Krankenanstalten, bei denen ich in Behandlung war oder sein werde, sowie andere Personenversicherer über meine Gesundheitsverhältnisse bei Vertragsschluss zu befragen; dies gilt auch für die Zeit vor der Antragsannahme. ...“

Anfragen der Beklagten bei gesetzlichen Krankenversicherern und verschiedenen Ärzten ergaben, dass die Klägerin ab dem Jahr 2001 wegen einer Erkrankung an der Kniescheibe und Wirbelsäulenbeschwerden ärztlich behandelt und zweimal über mehrere Wochen krankgeschrieben, zudem im Jahre 2004 wegen Schmerzen im Ellenbogen behandelt und vom 4. bis 13. November 2004 krankgeschrieben worden war.

Mit Schreiben vom 27. April 2012 focht die Beklagte ihre Annahme der Berufsunfähigkeits-Zusatzversicherung wegen Verletzung der vorvertraglichen Anzeigepflicht an und erklärte sich für leistungsfrei. Daraufhin kündigte der Ehemann der Klägerin den Hauptvertrag.

Die Klägerin hat sich darauf berufen, beim Ausfüllen des ersten Versicherungsantrags infolge einer Magen-Darm-Verstimmung mehrfach die Toilette aufgesucht zu haben. Ihr seien daher keine Gesundheitsfragen gestellt, sondern sie sei am Ende nur zur Unterschrift aufgefordert worden. Das Antragsformular habe ein Mitarbeiter der Beklagten zuvor ausgefüllt. Beim zweiten Antrag habe ebenfalls ein Mitarbeiter der Beklagten die Gesundheitsfragen mit der Bemerkung gestrichen, es könne auf den Hauptantrag Bezug genommen werden. Die Ellenbogenerkrankung sei folgenlos geblieben. Die Klägerin vertritt im Übrigen die Auffassung, mit der von der Beklagten geforderten, weit gefassten Schweigepflichtentbindungserklärung sei ihr Recht auf informationelle Selbstbestimmung verletzt worden.

Die Beklagte behauptet, die Gesundheitsfragen beider Anträge seien der Klägerin ordnungsgemäß unterbreitet worden. Zudem habe sich auch der Ehemann der Klägerin bei der Antragstellung arglistig verhalten.

Das Landgericht hat die Klage auf Versicherungsleistungen abgewiesen. Die hiergegen gerichtete Berufung der Klägerin ist erfolglos geblieben. Mit der durch den Senat insoweit zugelassenen Revision verfolgt die Klägerin ihr Klagebegehren auf Zahlung von Berufsunfähigkeitsrente und damit verbundene Nebenforderungen weiter.

Aus den Gründen:

Das Rechtsmittel führt im Umfang seiner Zulassung zur Aufhebung des Berufungsurteils und Zurückverweisung der Sache an das Berufungsgericht.

I. Dieses hat die von der Beklagten erklärte Arglistanfechtung durchgreifen lassen. Die durch Anfragen bei Versicherern und Ärzten gewonnenen Erkenntnisse der Beklagten über Vorerkrankungen der Klägerin seien verwertbar. Soweit sich die Klägerin mit Blick auf die Entscheidung des Bundesverfassungsgerichts vom 23. Oktober 2006 (VersR 2006, 1669) darauf berufe, ihre Schweigepflichtentbindungserklärung sei zu weit gefasst gewesen, betreffe

die genannte Entscheidung den Streitfall nicht, weil die Erklärung hier nicht formularmäßig erfolgt sei. Zudem seien die Vorerkrankungen der Klägerin unstreitig, so dass sich die Frage eines Verwertungsverbots nicht stelle.

Die Vorerkrankungen der Klägerin seien gefahrerheblich und mithin offenbarungspflichtig gewesen. Bei einer Postzustellerin seien Erkrankungen der Knie, der Wirbelsäule und des Ellenbogens für das zu versichernde Risiko von maßgeblicher Bedeutung. Unstreitig hätte die Beklagte den Versicherungsantrag bei Kenntnis dieser Erkrankungen nicht angenommen.

Nach dem Vortrag der Klägerin könne zwar für den Antrag auf die Lebensversicherung (Hauptantrag) noch nicht von einer Anzeigepflichtverletzung ausgegangen werden, weil sie die dortigen Gesundheitsfragen möglicherweise nicht zur Kenntnis genommen habe. Eine zumindest bedingt vorsätzliche Falschbeantwortung der Gesundheitsfragen habe jedoch bei Beantragung der Zusatzversicherung vorgelegen. Lebensnah könne der diesbezügliche Vortrag der Klägerin nur dahingehend verstanden werden, dass auf die Gesundheitsfragen des Hauptantrags Bezug genommen worden sei. Angesichts der großflächigen Durchstreichung der Gesundheitsfragen und des ins Auge fallenden Hinweises „Gesundheitsfragen s. Hauptantrag“ hätten die Klägerin und ihr Ehemann den Zusatzantrag nicht unterschreiben können, ohne dass sich ihnen die Bezugnahme auf Gesundheitsfragen aufgedrängt hätte.

Die Klägerin habe auch arglistig gehandelt. Sie habe den handschriftlichen Zusatz mit dem Verweis auf den Hauptantrag gelesen und erkannt, dass Eintragungen zu ihrer gesundheitlichen Verfassung gefehlt hätten, obwohl sie für ihre Berufstätigkeit relevante Erkrankungen gehabt habe. Insoweit sei ihr klar gewesen, etwas für den Versicherer und den Versicherungsvertrag Wichtiges zu verschweigen. Dieses Schweigen sei mithin darauf gerichtet gewesen, den Versicherer trotz ihrer Vorerkrankungen zu einer Vertragsannahme ohne Risikoausschlüsse zu bewegen.

Auch der Ehemann der Klägerin habe – als Versicherungsnehmer – die Beklagte arglistig getäuscht. Ihm seien die Erkrankungen der Klägerin bei lebensnaher Betrachtung bekannt gewesen; spätestens bei Stellung des Zusatzantrags habe ihm klar sein müssen, dass Gesundheitsfragen betreffend seine Frau zu keiner Zeit beantwortet worden seien. Die Aufrechterhaltung dieses Irrtums sei nur damit zu erklären, dass er die Antragsannahme nicht habe gefährden wollen.

Einer Vernehmung des Ehemanns der Klägerin als Zeugen habe es nicht bedurft, weil sich die arglistige Täuschung schon aus dem Vortrag der Klägerin ergebe.

II. Das hält rechtlicher Nachprüfung nicht stand.

1. Rechtsfehlerhaft hat es das Berufungsgericht versäumt zu prüfen, ob die von der Beklagten zur Frage vorvertraglicher Anzeigepflichtverletzungen des Versicherungsnehmers und der Versicherten durchgeführte Erhebung von Gesundheitsdaten der Klägerin bei ihren gesetzlichen Krankenversicherern und Ärzten gegen die Vorgaben der verfassungsgerichtlichen Rechtsprechung zum Recht des Versicherten auf informationelle Selbstbestimmung sowie des § 213 VVG verstößt und es der Beklagten infolgedessen möglicherweise nach Treu und Glauben verwehrt ist, sich auf die hierdurch gewonnenen Erkenntnisse im Rahmen der erklärten Arglistanfechtung zu berufen.

a) Das Berufungsgericht hätte zunächst der Frage der Rechtmäßigkeit der Datenerhebung durch die Beklagte nachgehen müssen.

aa) Dabei hat es entgegen der Auffassung der Revision im Ausgangspunkt noch richtig erkannt, dass die weite Fassung der von der Beklagten vorformulierten und von der Klägerin unterzeichneten Schweigepflichtentbindung für sich genommen keinen rechtlichen Bedenken begegnet. Denn das Gesetz setzt, wie sich aus

§ 213 VVG ergibt, die Zulässigkeit so genannter allgemeiner Schweigepflicht entbindungen voraus.

Zwar sah der Gesetzentwurf zur Reform des Versicherungsvertragsrechts ursprünglich in § 213 VVG – E vor, dass die Erhebung personenbezogener Gesundheitsdaten nur zulässig sein sollte, soweit die betroffene Person im Einzelfall eine Einwilligung nach § 4a BDSG erteilt hat (BT-Drucks. 16/3945 S. 40). Diese Fassung der Vorschrift wurde aber nicht Gesetz. Vielmehr ordnet das am 1. Januar 2008 in Kraft getretene Versicherungsvertragsgesetz in § 213 Abs. 2 Satz 1 VVG an, dass die – auch danach für die Datenerhebung des Versicherers notwendige – Einwilligung des Betroffenen schon vor Abgabe der Vertragserklärung erteilt werden kann. Nach der dieser Normfassung zugrundeliegenden Beschlussempfehlung des Rechtsausschusses lässt die Regelung damit die „einmalige Einwilligung in eine Datenerhebung bei Abgabe der Vertragserklärung weiterhin zu“ (BT-Drucks. 16/5862 S. 100). Das Recht der betroffenen Person auf wirkungsvollen informationellen Selbstschutz soll danach nicht durch eine obligatorische Einzelfalleinwilligung, sondern dadurch erreicht werden, dass der Betroffene gemäß § 213 Abs. 2 Satz 2 VVG stets vorab über eine geplante Datenerhebung zu unterrichten ist und dieser widersprechen sowie darüber hinaus nach § 213 Abs. 3 VVG jederzeit verlangen kann, dass eine Erhebung nur bei Einzelfalleinwilligung erfolgt (BT-Drucks. 16/5862 aaO).

Dementsprechend sieht auch ein Teil der obergerichtlichen Rechtsprechung und das Schrifttum die Erteilung allgemeiner, vom Einzelfall gelöster Schweigepflichtentbindungen – unabhängig davon, ob sie vor Vertragsschluss oder später erfolgen – als grundsätzlich zulässig an (OLG Brandenburg NJW – RR 2014, 1501, 1502; Höra, in: Bruck/Möller, VVG 9. Aufl. § 213 VVG Rn. 48 f.; HK – VVG/Muschner, 3. Aufl. § 213 Rn. 28; Rixecker, in: Langheid/Rixecker, VVG 5. Aufl. § 213 Rn. 16; Eichelberg, in: Looschelders/Pohlmann, VVG 3. Aufl. § 213 Rn. 8; MünchKomm – VVG/Eberhardt, 2. Aufl. § 213 Rn. 85; Klär/Heyers, in: PK – VVG, 3. Aufl. § 213 Rn. 4; Voit, in: Pröls/Martin, VVG 29. Aufl. § 213 Rn. 38; Spuhl, in: Marlow/Spuhl, Das Neue VVG kompakt 4. Aufl. Rn. 1462; Schneider, in: Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch 3. Aufl. § 1a Rn. 41; Neuhaus/Kloth, NJOZ 2009, 1370, 1376; Notthoff, ZfS 2008, 243, 248; a.A. OLG Jena VersR 2011, 380, 382). Eine Differenzierung danach, von wem die Erklärung formuliert oder ob sie formularmäßig erteilt wurde, erfolgt dabei nicht (Höra, in: Bruck/Möller aaO Rn. 49; Rixecker, in: Langheid/Rixecker aaO; vgl. auch Plath, BDSG/DS-GVO 2. Aufl. § 4a BDSG Rn. 37 [zur Einwilligung nach § 4a Abs. 1 BDSG]).

Ein abweichendes Normverständnis ist auch nach dem Beschluss des Bundesverfassungsgerichts vom 23. Oktober 2006 (VersR 2006, 1669) nicht geboten. Danach begegnet es verfassungsrechtlichen Bedenken, eine versicherungsvertragliche Obliegenheit als wirksam anzusehen, nach welcher der Versicherungsnehmer gehalten ist, eine vom Versicherer geforderte umfassende Schweigepflichtentbindung zu erteilen, wenn ihm damit die tatsächliche Möglichkeit und Zumutbarkeit informationellen Selbstschutzes genommen wird (aaO Rn. 33, 53 f.). Demgegenüber ist eine entsprechende Entbindungserklärung nicht zu beanstanden, wenn dem Versicherten zu deren Erteilung Alternativen freigestellt waren, die ihm die Wahrung seiner Rechte ermöglichen (aaO Rn. 61). Im Anschluss daran hat der Senat in seiner jüngsten Rechtsprechung betont, dass der Versicherungsnehmer dem Versicherer eine unbeschränkte Schweigepflichtentbindung erteilen kann. Denn als Träger des Rechts auf informationelle Selbstbestimmung steht es ihm frei, Daten anderen gegenüber zu offenbaren (Senatsurteil vom 22. Februar 2017 – IV ZR 289/14, r+s 2017, 232 Rn. 49 [zur Veröffentlichung in BGHZ vorgesehen]).

bb) Das Berufungsgericht hat allerdings nicht berücksichtigt, dass der Versicherer im Rahmen seiner Leistungsprüfung dem Versicherten die Erklärung einer solchen allgemeinen Schweigepflichtentbindung regelmäßig nicht abverlangen darf.

Gemäß § 31 Abs. 1 VVG hat der Versicherungsnehmer bei der Erhebung von Daten durch den Versicherer grundsätzlich nur insoweit mitzuwirken, als diese zur Prüfung des Leistungsfalls relevant sind (Senatsurteil vom 22. Februar 2017 aaO Rn. 29, 45). Im Falle eines geringen Kenntnisstands des Versicherers kann dies eine gestufte, einem Dialog vergleichbare Datenerhebung erforderlich werden lassen, in deren Rahmen sich die Erhebungen des Versicherers zunächst auf solche Informationen zu beschränken haben, die ihm einen Überblick über die zur Beurteilung des Versicherungsfalls einschließlich des vorvertraglichen Anzeigeverhaltens des Versicherungsnehmers relevanten Umstände ermöglichen (Senatsurteil vom 22. Februar 2017 aaO Rn. 46 f.).

Dementsprechend ist der Versicherungsnehmer aufgrund seiner gesetzlichen Obliegenheit aus § 31 Abs. 1 VVG auch nur insofern gehalten, inhaltlich begrenzte Schweigepflichtentbindungen zu erklären, als das Erhebungsbegehren des Versicherers jeweils zulässigerweise reicht (vgl. Senatsurteil vom 22. Februar 2017 aaO Rn. 47 f.). Dabei ist es ihm zwar unbenommen, zur Beschleunigung der Leistungsprüfung sogleich eine unbeschränkte Entbindungserklärung zu erteilen. Hierüber und über die andernfalls schrittweise zu erfüllende Obliegenheit hat ihn der Versicherer aber eingangs der Erhebungen zu informieren (Senatsurteil vom 22. Februar 2017 aaO Rn. 49). Diese Grundsätze gelten für die Mitwirkungsobliegenheit des bezugsberechtigten Versicherten nach § 31 Abs. 2 VVG entsprechend.

cc) Hat die Beklagte von der Klägerin entgegen diesen Vorgaben gleichwohl verlangt, die fragliche allgemeine Schweigepflichtentbindung zu erteilen, und ist die Klägerin dem nachgekommen, so ist die auf dieser Grundlage durchgeführte Datenerhebung rechtswidrig, weil es an einer wirksamen Einwilligung der betroffenen Person im Sinne des § 213 Abs. 1 Halbsatz 2 VVG fehlte.

Nach der genannten Vorschrift ist die Erhebung von Gesundheitsdaten durch den Versicherer nur zulässig, soweit die betroffene Person eine Einwilligung erteilt hat. Hierfür genügt ihr bloßes Einverständnis nicht ohne weiteres. Wie das Bundesverfassungsgericht in seinem Beschluss vom 23. Oktober 2006 (VersR 2006, 1669) betont hat, gebietet die aus dem allgemeinen Persönlichkeitsrecht folgende Schutzpflicht den zuständigen staatlichen Stellen, die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen (aaO Rn. 29, 33). Dieser Schutz, der im Rahmen der Leistungsprüfung des Versicherers durch die Grundsätze des Senatsurteils vom 22. Februar 2017 (IV ZR 289/14, r+s 2017, 232) gewährleistet wird, kann dem Betroffenen nicht unter Berufung auf eine nur scheinbare Freiwilligkeit der Preisgabe bestimmter Informationen wieder genommen werden (vgl. BVerfG aaO Rn. 33).

Kommt eine allgemeine Schweigepflichtentbindung dementsprechend zustande, dass der Versicherer diese im Rahmen der Leistungsprüfung verlangt, anstatt sie lediglich als Alternative zur andernfalls schrittweise zu erfüllenden Mitwirkungsobliegenheit anzubieten, kann sie eine Datenerhebung nach § 213 Abs. 1 VVG nicht rechtfertigen. Denn das Einverständnis des Betroffenen, der regelmäßig nicht um die Begrenzung der ihn treffenden Mitwirkungsobliegenheit weiß und sich einem darüber hinausreichenden Verlangen ausgesetzt sieht, dessen Erfüllung aus seiner Sicht mit der Gewährung der – für ihn bisweilen existentiellen – Versicherungsleistung verknüpft ist, stellt sich nur als scheinbar freiwillig dar, nachdem

ihm die freie Entscheidung über die ihm zustehenden Wahlmöglichkeiten zu keiner Zeit eröffnet worden ist.

dd) Hat die Klägerin die im Streit stehende Erklärung dagegen erteilt, ohne dass die Beklagte dies verlangt hätte, aber auch ohne von dieser auf die Möglichkeit der schrittweisen Erteilung inhaltlich beschränkter Schweigepflichtentbindungen hingewiesen worden zu sein, so hätte das Berufungsgericht hinsichtlich der Rechtmäßigkeit der hierauf beruhenden Datenerhebung darüber hinaus prüfen müssen, ob dabei die weiteren Vorgaben des § 213 VVG beachtet wurden.

Die Beklagte hätte die Klägerin insofern vor der Erhebung der Gesundheitsdaten nach § 213 Abs. 1 VVG unterrichten sowie darauf hinweisen müssen, dass sie der Erhebung widersprechen kann (§ 213 Abs. 2 Satz 2, Abs. 4 VVG). Zudem wäre die Klägerin auf ihr Recht hinzuweisen gewesen, jederzeit verlangen zu können, dass eine Datenerhebung nur erfolgt, wenn jeweils in die einzelne Erhebung eingewilligt worden ist (§ 213 Abs. 3 und 4 VVG).

Hätte die Beklagte der Klägerin die entsprechenden Informationen nicht erteilt, so wäre die auf Grundlage der allgemeinen Schweigepflichtentbindung durchgeführte Datenerhebung gleichfalls als rechtswidrig anzusehen (vgl. Höra, in: Bruck/Möller, VVG 9. Aufl. § 213 Rn. 64; bei fehlendem Hinweis auf Widerspruchsrecht: Klär/Heyers, in: PK-VVG, 3. Aufl. § 213 Rn. 37; Neuhaus/Kloth, NJOZ 2009, 1370, 1386).

ee) Nach alldem hat es das Berufungsgericht rechtsfehlerhaft unterlassen aufzuklären, wie es zur Abgabe der allgemeinen Schweigepflichtentbindung durch die Klägerin kam und – gegebenenfalls – wie die hierauf erfolgte Datenerhebung ablief. Hätte sich die Datenerhebung der Beklagten insofern als rechtswidrig dargestellt, wäre weiter zu prüfen gewesen, welche Gesundheitsdaten auf Grundlage der fraglichen Erklärung erhoben wurden, nachdem von der Klägerin – worauf die Revision hinweist – neben der allgemeinen, noch weitere „individuell-konkrete“ Entbindungserklärungen erteilt worden waren.

Allerdings wären auch diese nach den vorgenannten Maßstäben zu überprüfen gewesen. Denn allein der Umstand, dass in ihnen möglicherweise nur einzelne Auskunftstellen benannt waren, macht sie noch nicht hinreichend konkret, wenn sie nicht ansatzweise erkennen ließen, welche Informationen der Versicherer mit ihrer Hilfe erheben könnte (vgl. BVerfG VersR 2013, 1425, 1428).

ff) Die fehlende Prüfung kann nicht durch das Revisionsgericht erfolgen, da es an den hierfür erforderlichen tatrichterlichen Feststellungen fehlt. Für das Revisionsverfahren ist daher zu unterstellen, dass die Datenerhebung der Beklagten zumindest teilweise rechtswidrig war.

b) Im Falle einer – unterstellt – rechtswidrigen Datenerhebung wäre in einem zweiten Schritt zu klären, ob die Beklagte daran gehindert war, sich auf das Ergebnis der rechtswidrigen Ermittlungen zu berufen und die Anfechtung der Berufsunfähigkeitszusatzversicherung nach § 123 BGB zu erklären.

aa) Nach der Senatsrechtsprechung zur Rechtslage vor Inkrafttreten des neuen Versicherungsvertragsgesetzes ist in Fällen der Datenerhebung ohne ausreichende Rechtsgrundlage sachlich-rechtlich zu prüfen, ob der Versicherer nach § 242 BGB gehindert ist, sich auf die Ergebnisse seiner Ermittlungen zu berufen und insbesondere darauf gestützt von dem Gestaltungsrecht der Arglistanfechtung Gebrauch zu machen (Senatsurteil vom 28. Oktober 2009 – IV ZR 140/08, r+s 2010, 55 Rn. 19 ff.; Senatsbeschlüsse vom 25. Mai 2011 – IV ZR 191/09, VersR 2011, 1249 Rn. 7 f.; vom 21. September 2011 – IV ZR 203/09, VersR 2012, 297 Rn. 8).

Dabei führt nicht jedes rechts- oder pflichtwidrige Verhalten des Versicherers stets oder auch nur regelmäßig zur Unzulässig-

keit der hierdurch ermöglichten Wahrnehmung seiner Rechte. Vielmehr ist zunächst danach zu fragen, ob er die tatsächlichen Voraussetzungen der Rechtsausübung, wie z.B. die Erlangung der erforderlichen Tatsachenkenntnis, gerade durch das beanstandete Verhalten zielgerichtet geschaffen hat, denn ein solch treuwidriges Verhalten kann dazu führen, ihm die Ausnutzung der so gewonnenen Rechtsstellung zu versagen. Lässt sich ein zielgerichtet-treuwidriges Handeln im vorgenannten Sinne nicht feststellen, ist alsdann durch eine umfassende Abwägung der maßgeblichen Umstände des Einzelfalls zu entscheiden, ob und inwieweit dem Versicherer die Ausübung seiner Rechtsposition nach Treu und Glauben verwehrt sein soll. Dies gilt umso mehr, wenn beiden Seiten ein Rechtsverstoß zur Last fällt (vgl. zum Vorstehenden: Senatsurteil vom 28. Oktober 2009 aaO Rn. 21; Senatsbeschlüsse vom 25. Mai 2011 aaO Rn. 8; vom 21. September 2011 aaO Rn. 7).

bb) Ob diese Grundsätze nach Inkrafttreten des § 213 VVG fortgelten, ist umstritten.

Einige Stimmen im Schrifttum lehnen dies aus unterschiedlichen Gründen ganz oder teilweise ab. Nach einer Ansicht darf der Versicherer rechtswidrig erlangte Daten bei der Leistungsprüfung und insbesondere zur Begründung der Leistungsablehnung nicht verwenden, da angesichts der klaren Regelung in § 213 VVG für eine Abwägung kein Raum mehr sei (Voit, in: Prölss/Martin, VVG 29. Aufl. § 213 Rn. 49 f.; vgl. auch Rixecker, in: Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch 3. Aufl. § 46 Rn. 209; Höra, r+s 2008, 89, 93; Notthoff, ZfS 2008, 243, 247). Andere meinen, es sei dem Betroffenen verwehrt, sich auf den Verstoß des Versicherers zu berufen, wenn er selbst in rechtswidriger Weise gegen vorvertragliche Anzeigepflichten verstoßen habe, nachdem § 213 VVG keine entsprechende Rechtsfolge normiere und der Betroffene in diesen Fällen keinen Schutz verdiene (HK-VVG/Muschner, 3. Aufl. § 213 Rn. 87 und 90 f.; Klär, in: PK-VVG, 2. Aufl. § 213 Rn. 41; Kalis, in: Bach/Moser, Private Krankenversicherung, 5. Aufl. § 213 VVG Rn. 76 f.; Fricke, VersR 2009, 297, 304 f.; vgl. auch: Neuhaus, Berufsunfähigkeitsversicherung, 3. Aufl. P Rn. 90, 97; Neuhaus/Kloth, NJOZ 2009, 1370, 1388; ähnlich zur Rechtslage vor Inkrafttreten des § 213 VVG: OLG Saarbrücken, VersR 2009, 1478, 1481).

Die überwiegende Meinung hält demgegenüber an den Grundsätzen der bisherigen Senatsrechtsprechung auch nach Inkrafttreten des § 213 VVG fest (OLG Brandenburg NJW-RR 2014, 1501, 1502; OLG Jena VersR 2011, 380, 382; OLG Saarbrücken VersR 2013, 1157, 1162; D. Wendt, in: FAKomm-VersR, § 213 VVG Rn. 34; Rixecker, in: Langheid/Rixecker, VVG 5. Aufl. § 213 Rn. 25 f.; MünchKomm-VVG/Eberhardt, 2. Aufl. § 213 Rn. 139 ff.; Klär/Heyers, in: PK-VVG, 3. Aufl. § 213 Rn. 49; Schneider, in: Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch 3. Aufl. § 1a Rn. 41a; Spuhl, in: Marlow/Spuhl, Das Neue VVG kompakt, 4. Aufl. Rn. 1477; Britz, Die Erhebung personenbezogener Gesundheitsdaten durch Versicherungsunternehmen bei Dritten gemäß § 213 VVG unter Berücksichtigung des Gendiagnostikgesetzes, 2011 S. 252-257; Washausen, Der Gesundheitsdatenschutz im Privatversicherungsrecht, 2016 S. 242-249; Looschelders, JR 2010, 530, 531).

cc) Die letztgenannte Auffassung trifft zu.

§ 213 VVG regelt für den Fall einer rechtswidrigen Datenerhebung keine Sanktionen (vgl. Karczewski, r+s 2012, 521, 525). Daraus lässt sich indes weder folgern, dass nach dem Willen des Gesetzgebers jeder Verstoß rechtlich folgenlos bleiben soll, noch dass eine Missachtung der rechtlichen Erfordernisse stets dazu führen muss, dass der Versicherer die von ihm gewonnenen Daten nicht verwenden dürfte. Vielmehr hat sich an der – insbesondere

auch verfassungsrechtlich geschützten – Interessenlage der Beteiligten und dem Gebot, ihren Grundrechten nach dem Prinzip der praktischen Konkordanz Geltung zu verschaffen (vgl. zur Auslegung von § 31 VVG: Senatsurteil vom 22. Februar 2017 – IV ZR 289/14, r+s 2017, 232 Rn. 41), mit dem Inkrafttreten des § 213 VVG, der dieselben verfassungsrechtlichen Vorgaben umsetzen sollte, die bereits Grundlage der früheren Senatsrechtsprechung waren (Senatsurteil vom 28. Oktober 2009 aaO Rn. 19 ff.; Senatsbeschlüsse vom 25. Mai 2011 aaO Rn. 7 f.; vom 21. September 2011 aaO Rn. 8), nichts geändert.

Damit bleibt es bei den bisherigen Grundsätzen, wobei jedoch zu berücksichtigen ist, dass der Senat den betroffenen Versicherern in seinen bisherigen Entscheidungen noch zugutegehalten hat, dass ihr jeweiliges Verlangen nach einer weit gefassten Schweigepflichtentbindungserklärung vor der Entscheidung des Bundesverfassungsgerichts vom 23. Oktober 2006 (VersR 2006, 1669) gestellt worden war und seinerzeit einer allgemein – auch vom Senat – gebilligten Praxis entsprochen hatte (vgl. Senatsurteil vom 28. Oktober 2009 aaO Rn. 28; Senatsbeschluss vom 21. September 2011 aaO Rn. 15). Das lässt sich auf die Datenerhebung nach Inkrafttreten des § 213 VVG, der gerade die vorgenannte verfassungsgerichtliche Rechtsprechung berücksichtigen sollte (vgl. Senatsurteil vom 13. Juli 2016 – IV ZR 292/14, r+s 2016, 472 Rn. 41), nicht übertragen (vgl. Rixecker, in: Langheid/Rixecker aaO Rn. 26; Voit, in: Prölss/Martin aaO Rn. 50; Washausen aaO S. 247 f.; Karczewski aaO).

dd) Das bedeutet für den Streitfall:

(1) Es kommt darauf an, aus welchen Gründen die Beklagte den rechtlichen Anforderungen an eine zulässige Datenerhebung nicht genügt hat.

Anders als das Berufungsgericht meint, spielt insofern keine Rolle, dass die Ermittlungsergebnisse der Beklagten nicht im Streit stehen. Vielmehr ist auch im Fall unstreitig verschwiegener Vorerkrankungen zu klären, ob sich die Verwendung der diesbezüglichen Erkenntnisse des Versicherers bei der Ausübung von Gestaltungsrechten wie Rücktritt oder Anfechtung als unzulässige Rechtsausübung darstellt, wobei der Einwand aus § 242 BGB keine Einrede, sondern ein von Amts wegen zu beachtender Einwand ist (Senatsbeschlüsse vom 25. Mai 2011 aaO Rn. 7; vom 21. September 2011 aaO Rn. 8, jeweils m.w.N.).

Mangels der insofern erforderlichen Feststellungen kann der Senat nicht selbst entscheiden, ob sich die Beklagte die für ihre Arglistanfechtung erforderliche Tatsachenkenntnis gerade durch ein gegebenenfalls zu beanstandendes Verhalten zielgerichtet geschaffen hat.

(2) Lässt sich ein zielgerichtet-treuwidriges Handeln der Beklagten im vorgenannten Sinne nicht feststellen, ist weiter mittels einer Abwägung der Fallumstände zu klären, ob sich das Verhalten der Beklagten anderweitig als treuwidrig darstellt und das Interesse der Klägerin am Schutz ihrer Gesundheitsdaten oder das aner kennenswerte Interesse der Beklagten an einer Offenlegung risikorelevanter Vorerkrankungen überwiegt.

Auch diese dem Tatrichter vorbehaltene Abwägung kann der Senat nicht selbst vornehmen, weil das Berufungsgericht insoweit keine ausreichenden Feststellungen getroffen hat. Insbesondere steht das Ergebnis der Abwägung nicht deshalb fest, weil im Falle eines erwiesenen arglistigen Verhaltens des Versicherungsnehmers bei Vertragsschluss dessen Schutzbedürfnis an der Geheimhaltung seiner Gesundheitsdaten regelmäßig aufgehoben wäre. Denn das schüfe einen Anreiz für den Versicherer, im Versicherungsfall ohne Rücksicht auf das Grundrecht auf informationelle Selbstbestimmung – und nunmehr auch die Regelung in § 213 VVG – Gesund-

heitsdaten mit dem Ziel zu erheben, ein arglistiges Verhalten des Versicherungsnehmers nachzuweisen (Senatsbeschluss vom 21. September 2011 aaO Rn. 14 m.w.N.). Vielmehr bleibt eine vom Versicherer aufgedeckte Arglist des Versicherungsnehmers lediglich ein – wenn auch meist gewichtiger – in die Güterabwägung einfließender Umstand (Senat aaO).

c) Der Senat kann demnach nicht ausschließen, dass die bislang unterbliebene Prüfung nach den obenstehenden Maßstäben zu einem für die Klägerin günstigeren Ergebnis führt. Die Sache bedarf deshalb neuer Verhandlung und Entscheidung.

2. Soweit die Revision die Annahme des Berufungsgerichts beanstandet, sowohl die Klägerin als auch ihr Ehemann hätten Vorerkrankungen der Klägerin jedenfalls bei Stellung des Zusatzantrags arglistig verschwiegen, deckt sie keine Rechtsfehler des Berufungsurteils auf. Die gegen die zugrunde liegenden Feststellungen erhobenen Verfahrensrügen – auch die Rügen der Verletzung des Rechts auf rechtliches Gehör – hat der Senat geprüft und für nicht durchgreifend erachtet. Von einer näheren Begründung wird insoweit nach § 564 Satz 1 ZPO abgesehen.

Dynamische IP-Adresse als personenbezogenes Datum

(Bundesgerichtshof, Urteil vom 16. Mai 2017 – VI ZR 135/13 –)

- a) **Die dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, stellt für den Anbieter ein personenbezogenes Datum im Sinne des § 12 Abs. 1 und 2 TMG in Verbindung mit § 3 Abs. 1 BDSG dar (Fortführung von EuGH NJW 2016, 3579).**
- b) **§ 15 Abs. 1 TMG ist entsprechend Art. 7 Buchst. f der Richtlinie 95/46 EG dahin auszulegen, dass ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf (Fortführung von EuGH aaO).**

Sachverhalt:

Der Kläger macht gegen die beklagte Bundesrepublik Deutschland einen Unterlassungsanspruch wegen der Speicherung von Internetprotokoll-Adressen (im Folgenden: IP-Adressen) geltend. IP-Adressen sind Ziffernfolgen, die vernetzten Computern zugewiesen werden, um deren Kommunikation im Internet zu ermöglichen. Beim Abruf einer Internetseite wird die IP-Adresse des abrufenden Computers an den Server übermittelt, auf dem die abgerufene Seite gespeichert ist. Dies ist erforderlich, um die abgerufenen Daten an den richtigen Empfänger zu übertragen.

Zahlreiche Einrichtungen des Bundes betreiben allgemein zugängliche Internetportale, auf denen sie aktuelle Informationen bereitstellen. Mit dem Ziel, Cyber-Angriffe abzuwehren und die

strafrechtliche Verfolgung von Angreifern zu ermöglichen und dadurch eine Abschreckungswirkung zu erreichen, werden bei einer Vielzahl dieser Portale alle Zugriffe in Protokolldateien festgehalten. Darin werden jeweils der Name der abgerufenen Datei bzw. Seite, in Suchfelder eingegebene Begriffe, der Zeitpunkt des Abrufs, die übertragene Datenmenge, die Meldung, ob der Abruf erfolgreich war, und die IP-Adresse des zugreifenden Rechners über das Ende des jeweiligen Nutzungsvorgangs hinaus gespeichert.

Der Kläger rief in der Vergangenheit verschiedene solcher Internetseiten auf. Mit seiner Klage begehrt er, die Beklagte zu verurteilen, es zu unterlassen, die IP-Adresse des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet – mit Ausnahme eines bestimmten Portals, für das der Kläger bereits einen Unterlassungstitel erwirkt hat – übertragen wird, über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist.

Das Amtsgericht hat die Klage abgewiesen. Auf die Berufung des Klägers hat das Berufungsgericht das erstinstanzliche Urteil unter Zurückweisung des weitergehenden Rechtsmittels teilweise abgeändert. Es hat die Beklagte verurteilt, es zu unterlassen, die IP-Adresse des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet – mit Ausnahme eines Internetportals – übertragen wird, in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, sofern der Kläger während eines Nutzungsvorgangs seine Personalien, auch in Form einer die Personalien ausweisenden E-Mail-Anschrift, angibt und soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist.

Aus den Gründen:

Das Berufungsgericht, dessen Urteil unter anderem in ZD 2013, 618 veröffentlicht ist, hat im Wesentlichen ausgeführt, analog § 1004 Abs. 1 Satz 2 BGB und gemäß § 823 BGB, Art. 1 Abs. 1, Art. 2 Abs. 1 GG, § 4 Abs. 1 BDSG, § 12 Abs. 1 TMG bestehe der geltend gemachte Unterlassungsanspruch nur insoweit, als er Speicherungen von IP-Adressen in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs betreffe und der Kläger während eines Nutzungsvorgangs seine Personalien angebe.

In diesem Fall sei die dynamische IP-Adresse des Klägers ein personenbezogenes Datum. Die Bestimmung der Person müsse gerade für die verarbeitende Stelle technisch und rechtlich möglich sein und dürfe keinen Aufwand erfordern, der außer Verhältnis zu dem Nutzen der Information für diese Stelle stehe. Danach sei in Fällen, in denen der Nutzer seinen Klarnamen offen lege, ein Personenbezug dynamischer IP-Adressen zu bejahen, weil die Beklagte den Klarnamen mit der IP-Adresse verknüpfen könne.

Die Verwendung des Datums über das Ende des Nutzungsvorgangs hinaus sei nach § 12 Abs. 1 TMG unzulässig, da nicht von einer Einwilligung des Klägers auszugehen sei und ein Erlaubnistatbestand nicht vorliege. § 15 Abs. 1 TMG greife jedenfalls deshalb nicht, weil die Speicherung der IP-Adresse über das Ende des Nutzungsvorgangs hinaus für die Ermöglichung des Angebots (für den jeweiligen Nutzer) nicht erforderlich sei. Der Begriff der Erforderlichkeit sei eng auszulegen und umfasse nicht den sicheren Betrieb der Seite.

Ein weitergehender Unterlassungsanspruch bestehe nicht. Soweit der Kläger seinen Klarnamen nicht angebe, könne nur der Zugangsanbieter die IP-Adresse einem bestimmten An-

schlussinhaber zuordnen. In den Händen der Beklagten sei die IP-Adresse hingegen – auch in Verbindung mit dem Zeitpunkt des Zugriffs – kein personenbezogenes Datum, weil der Anschlussinhaber bzw. Nutzer für die Beklagte nicht bestimmbar sei. Maßgeblich sei, dass der Zugangsanbieter die IP-Adressen nur für einen begrenzten Zeitraum speichern und nur in bestimmten Fällen an Dritte übermitteln dürfe. Dass die Beklagte im Zusammenhang mit einem strafrechtlichen Ermittlungsverfahren oder der Verfolgung von Urheberrechtsverletzungen unter bestimmten Voraussetzungen an die für die Herstellung des Personenbezugs erforderlichen Informationen gelangen könnte, sei unerheblich, weil das Interesse an der Verfolgung von Straftaten und Urheberrechtsverletzungen das Persönlichkeitsrecht des Betroffenen regelmäßig überwiege. Es komme auch nicht auf die theoretische Möglichkeit an, dass der Zugangsanbieter der Beklagten unbefugt Auskunft erteile. Denn eine illegale Handlung könne nicht als normalerweise und ohne großen Aufwand durchzuführende Methode angesehen werden.

Die Beurteilung des Berufungsgerichts hält revisionsrechtlicher Überprüfung nicht stand.

A) Revision des Klägers

Die Revision des Klägers hat Erfolg.

Nach den vom Berufungsgericht bisher getroffenen Feststellungen kann nicht ausgeschlossen werden, dass der Kläger von der Beklagten nach § 1004 Abs. 1 BGB analog, § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG, § 4 Abs. 1 BDSG, § 12 Abs. 1 TMG beanspruchen kann, es zu unterlassen, die für den Abruf ihrer Internetseiten durch den Kläger übermittelten IP-Adressen in Verbindung mit der Zeit des jeweiligen Abrufs über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen. Bei dem Speichern der (hier allein in Frage stehenden dynamischen) IP-Adresse kann es sich um einen nach dem Datenschutzrecht unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht des Klägers in seiner Ausprägung als Recht auf informationelle Selbstbestimmung handeln. Hierzu wird das Berufungsgericht weitere Feststellungen zu treffen haben.

1. Ein Unterlassungsanspruch scheidet nicht daran, dass die gespeicherten (dynamischen) IP-Adressen mangels Bestimmbarkeit des Anschlussinhabers für die Beklagte keine personenbezogenen Daten im Sinne von § 12 Abs. 1 TMG darstellen.

a) Nach § 12 Abs. 1 TMG darf der Diensteanbieter personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

Diese Vorschrift ist anwendbar, da die in Rede stehenden Portale als Telemedien (§ 1 Abs. 1 Satz 1 TMG), die Beklagte als Diensteanbieter (§ 2 Satz 1 Nr. 1 TMG) und der Kläger als Nutzer (§ 11 Abs. 2 TMG) anzusehen sind.

b) Personenbezogene Daten sind nach der auch für das Telemediengesetz maßgeblichen (KG, K&R 2011, 418; Moos, in: Taeger/Gabel, BDSG, 2. Aufl., § 12 TMG Rn. 5) Legaldefinition in § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener)“.

Die von der Beklagten gespeicherten dynamischen IP-Adressen des Klägers sind jedenfalls im Kontext mit den weiteren in den Protokolldateien gespeicherten Daten als Einzelangaben über sachliche Verhältnisse anzusehen, da die Daten Aufschluss darüber geben, dass zu bestimmten Zeitpunkten bestimmte Seiten bzw. Dateien über das Internet abgerufen wurden (vgl. Simitis/Dammann, BDSG, 8. Aufl., § 3 Rn. 10; Sachs, CR 2010, 547, 548). Diese sachlichen Verhältnisse waren solche des Klägers; denn er war Inhaber

des Anschlusses, dem die IP-Adressen zugewiesen waren (vgl. BGH, Urteil vom 12. Mai 2010 – I ZR 121/08, BGHZ 185, 330 Rn. 15), und er rief die Internetseiten im Übrigen auch selbst auf. Da die gespeicherten Daten aus sich heraus keinen unmittelbaren Rückschluss auf die Identität des Klägers zuließen, war dieser zwar nicht „bestimmt“ im Sinne des § 3 Abs. 1 BDSG (vgl. Schulz, in: Roßnagel, BeckRTD-Komm., § 11 TMG Rn. 22; Gola/Schomerus, BDSG, 12. Aufl., § 3 Rn. 10), er war jedoch „bestimmbar“.

c) Die Bestimmbarkeit einer Person setzt voraus, dass grundsätzlich die Möglichkeit besteht, ihre Identität festzustellen (Buchner, in: Taeger/Gabel, BDSG, 2. Aufl., § 3 Rn. 11; Plath/Schreiber, in: Plath, BDSG, 2. Aufl., § 3 Rn. 13). Umstritten war, ob bei der Prüfung der Bestimmbarkeit ein objektiver oder ein relativer Maßstab anzulegen ist (vgl. zum damaligen Meinungsstand Senatsbeschluss vom 28. Oktober 2014 – VI ZR 135/13, VersR 2015, 370 Rn. 23 ff.).

aa) Der erkennende Senat hat daher mit dem vorgenannten Beschluss dem Gerichtshof der Europäischen Union (im Folgenden: Gerichtshof) gemäß Art. 267 AEUV unter anderem folgende Frage zur Auslegung des Unionsrechts vorgelegt:

„Ist Art. 2 Buchstabe a der 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) – Datenschutz-Richtlinie – dahin auszulegen, dass eine Internetprotokoll-Adresse (IP-Adresse), die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?“

bb) Der Gerichtshof hat mit Urteil vom 19. Oktober 2016 – C-582/14, NJW 2016, 3579 die Frage wie folgt beantwortet:

„Art. 2 Buchst. a der 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 ist dahin auszulegen, dass eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.“

Zur Begründung hat der Gerichtshof im Wesentlichen ausgeführt (aaO, Rn. 40 ff.), bereits aus dem Wortlaut von Art. 2 Buchst. a der Richtlinie 95/46 EG gehe hervor, dass nicht nur eine direkt identifizierbare, sondern auch eine indirekt identifizierbare Person als bestimmbar angesehen werde. Die Verwendung des Begriffs „indirekt“ durch den Unionsgesetzgeber deute darauf hin, dass es für die Einstufung einer Information als personenbezogenes Datum nicht erforderlich sei, dass die Information für sich genommen die Identifizierung der betreffenden Person ermögliche. Zudem heiße es im 26. Erwägungsgrund der Richtlinie 95/46 EG, dass bei der Entscheidung, ob eine Person bestimmbar sei, alle Mittel berücksichtigt werden sollten, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Da dieser Erwägungsgrund auf die Mittel Bezug nehme, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem „Dritten“ eingesetzt werden könnten, sei sein Wortlaut ein Indiz dafür, dass es für die Einstufung eines Datums als „personenbezogenes Datum“ im Sinne von Art. 2 Buchst.

a der Richtlinie 95/46 EG nicht erforderlich sei, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befänden. Dass über die zur Identifizierung des Nutzers einer Website erforderlichen Zusatzinformationen nicht der Anbieter von Online-Mediendiensten verfüge, sondern der Internetzugangsanbieter dieses Nutzers, vermöge daher nicht auszuschließen, dass die von einem Anbieter von Online-Mediendiensten gespeicherten dynamischen IP-Adressen für ihn personenbezogene Daten im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 EG darstellten. Die Möglichkeit, eine dynamische IP-Adresse mit den Zusatzinformationen zu verknüpfen, über die der Internetzugangsanbieter verfüge, stelle ein Mittel dar, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden könne. Das vorlegende Gericht weise in seiner Vorlageentscheidung zwar darauf hin, dass das deutsche Recht es dem Internetzugangsanbieter nicht erlaube, dem Anbieter von Online-Mediendiensten die zur Identifizierung der betreffenden Person erforderlichen Zusatzinformationen direkt zu übermitteln, doch gebe es offenbar – vorbehaltlich der vom vorlegenden Gericht insoweit vorzunehmenden Prüfungen – für den Anbieter von Online-Mediendiensten rechtliche Möglichkeiten, die es ihm erlaubten, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, damit diese die nötigen Schritte unternehme, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten. Der Anbieter von Online-Mediendiensten verfüge somit offenbar über Mittel, die vernünftigerweise eingesetzt werden könnten, um mit Hilfe Dritter, und zwar der zuständigen Behörde und dem Internetzugangsanbieter, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen.

cc) Auf dieser Grundlage ist das Tatbestandsmerkmal „personenbezogene Daten“ des § 12 Abs. 1 und 2 TMG in Verbindung mit § 3 Abs. 1 BDSG richtlinienkonform dahingehend auszulegen, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt.

Denn die Beklagte verfügt über rechtliche Mittel, die vernünftigerweise eingesetzt werden können, um mit Hilfe Dritter, und zwar der zuständigen Behörde und des Internetzugangsanbieters, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen (vgl. Gerichtshof aaO Rn. 47). Die Beklagte kann – im Falle einer bereits eingetretenen Schädigung – Strafanzeige bei den Strafverfolgungsbehörden erstatten; im Falle der drohenden Schädigung kann sie die zur Gefahrenabwehr zuständigen Behörden einschalten. Nach § 100j Abs. 2 und 1 StPO, § 113 TKG (vgl. BVerfGE 130, 151) können die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden zu diesem Zweck von Internetzugangsanbietern bei Vorliegen bestimmter Voraussetzungen Auskunft verlangen, entsprechendes gilt für die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden, die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der genannten Stellen. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden. Dadurch können die gewonnenen Informationen zusammengeführt und der Nutzer bestimmt werden (vgl. Gerichtshof aaO Rn. 49 a.E.).

2. Auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen lässt sich nicht beurteilen, ob zugunsten der Beklagten ein Erlaubnistatbestand im Sinne von § 15 Abs. 1 TMG eingreift.

a) Handelt es sich bei der IP-Adresse im Zusammenhang mit den Daten des Zugriffs um personenbezogene Daten, ist die Speicherung über den Zugriff hinaus nach § 12 Abs. 1 TMG nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

b) Eine Einwilligung des Nutzers liegt hier nicht vor. Es kommt aber eine Erlaubnis nach § 15 Abs. 1 TMG in Betracht. Danach darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind dabei insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

c) Fraglich war, ob die Voraussetzungen des § 15 Abs. 1 TMG auch dadurch erfüllt sein können, dass die Maßnahmen des Diensteanbieters über den konkreten Nutzungsvorgang hinaus „erforderlich“ sind, um Cyberangriffe („Denial-of-Service“-Attacks) abzuwehren und damit die Inanspruchnahme von Telemedien (allgemein) zu ermöglichen. Eine solche Auslegung wäre mit dem Wortlaut der Vorschrift vereinbar gewesen. Denn die behaupteten „Denial-of-Service“-Attacks führen dazu, dass das Telemedium nicht mehr erreichbar und seine Inanspruchnahme somit nicht mehr möglich ist. Allerdings wurde in der Literatur überwiegend die (enge) Auffassung vertreten, dass die Datenerhebung und -verwendung nur erlaubt sei, um ein konkretes Nutzungsverhältnis zu ermöglichen und die Daten, soweit sie nicht für Abrechnungszwecke benötigt werden, mit dem Ende des jeweiligen Nutzungsvorgangs zu löschen seien (vgl. zum damaligen Meinungsstand Senatsbeschluss vom 28. Oktober 2014 – VI ZR 135/13, aaO Rn. 38). Dieses enge Verständnis des § 15 Abs. 1 TMG hätte einer Erlaubnis zur Speicherung der IP-Adressen zur (generellen) Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit von Telemedien entgegengestanden.

aa) Der erkennende Senat hat dem Gerichtshof der Europäischen Union gemäß Art. 267 AEUV deshalb folgende weitere Frage zur Auslegung des Unionsrechts vorgelegt:

„Steht Art. 7 Buchstabe f der Datenschutz-Richtlinie einer Vorschrift des nationalen Rechts entgegen, wonach der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden darf, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Telemediums durch den jeweiligen Nutzer zu ermöglichen und abzurechnen, und wonach der Zweck, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann?“

bb) Der Gerichtshof hat mit Urteil vom 19. Oktober 2016 – C-582/14, aaO die Frage wie folgt beantwortet:

„Art. 7 Buchst. f der Richtlinie 95/46 ist dahin auszulegen, dass er einer Regelung eines Mitgliedstaats entgegensteht, nach der ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die konkrete Inanspruchnahme der Dienste durch den betreffenden Nutzer zu ermöglichen und abzurechnen, ohne dass der Zweck, die generelle Funktionsfähigkeit der Dienste zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann.“

cc) Danach wäre die Auslegung des § 15 Abs. 1 und 4 TMG in dem oben angesprochenen engen Sinne mit Art. 7 Buchst. f der Richtlinie 95/46 EG unvereinbar. § 15 Abs. 1 TMG ist entsprechend Art. 7 Buchst. f der Richtlinie 95/46 EG dahin auszulegen, dass ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf.

Nach Art. 7 Buchst. f der Richtlinie 95/46 EG ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie „erforderlich [ist] zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 [der Richtlinie] geschützt sind, überwiegen“.

Art. 5 der Richtlinie 95/46 EG erlaubt den Mitgliedstaaten zwar, nach Maßgabe des Kapitels II und damit des Art. 7 die Voraussetzungen näher zu bestimmen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist, doch kann von dem Ermessen, über das die Mitgliedstaaten nach Art. 5 verfügen, nur im Einklang mit dem von der Richtlinie verfolgten Ziel der Wahrung eines Gleichgewichts zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre (vgl. Gerichtshof aaO Rn. 58) Gebrauch gemacht werden. Die Mitgliedstaaten dürfen nach Art. 5 der Richtlinie in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten keine anderen als die in Art. 7 der Richtlinie aufgezählten Grundsätze einführen und auch nicht durch zusätzliche Bedingungen die Tragweite der sechs in Art. 7 vorgesehenen Grundsätze verändern (vgl. in diesem Sinne EuGH Slg 2011, I – 12181 Rn. 33 ff. ASNEF und FECEMD).

Im vorliegenden Fall hätte § 15 TMG, wenn er in der angesprochenen engen Weise ausgelegt würde, eine geringere Tragweite als der in Art. 7 Buchst. f der Richtlinie 95/46 EG aufgestellte Grundsatz.

Während nämlich in Art. 7 Buchst. f der Richtlinie allgemein auf die „Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden“, Bezug genommen wird, würde § 15 TMG dem Diensteanbieter die Erhebung und Verwendung personenbezogener Daten eines Nutzers nur gestatten, soweit dies erforderlich ist, um die konkrete Inanspruchnahme elektronischer Medien zu ermöglichen und abzurechnen. § 15 TMG stünde daher einer zur Gewährleistung der Inanspruchnahme von Online-Mediendiensten dienenden Speicherung personenbezogener Daten über das Ende eines Zugriffs auf diese Dienste hinaus allgemein entgegen. Andererseits haben die Einrichtungen des Bundes, die Online-Mediendienste anbieten, ein berechtigtes Interesse daran, die Aufrechterhaltung der Funktionsfähigkeit der von ihnen allgemein zugänglich gemachten Internetseiten über ihre konkrete Nutzung hinaus zu gewährleisten.

Der Gerichtshof weist weiter darauf hin, dass Art. 7 Buchst. f der Richtlinie 95/46 EG einen Mitgliedstaat daran hindert, kategorisch und ganz allgemein die Verarbeitung bestimmter Kategorien personenbezogener Daten auszuschließen, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen. Ein Mitgliedstaat kann daher für diese Kategorien das Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen nicht abschließend vor-

schreiben, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt (vgl. in diesem Sinne EuGH Slg 2011, I-12181 Rn. 47 ff. ASNEF und FECEMD).

d) Diese Abwägung kann im Streitfall auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen nicht (abschließend) vorgenommen werden. Das Berufungsgericht hat keine hinreichenden Feststellungen dazu getroffen, ob die Speicherung der IP-Adressen des Klägers über das Ende eines Nutzungsvorgangs hinaus erforderlich ist, um im konkreten Fall die generelle Funktionsfähigkeit der jeweils in Anspruch genommenen Dienste zu gewährleisten. Die Beklagte verzichtet nach ihren eigenen Angaben bei einer Vielzahl der von ihr betriebenen Portale mangels eines „Angriffsdrucks“ darauf, die jeweiligen IP-Adressen der Nutzer zu speichern. Demgegenüber fehlen entsprechende Feststellungen dazu, wie hoch das Gefahrenpotential bei den übrigen Online-Mediendiensten des Bundes ist, welche der Kläger in Anspruch nehmen will. Dazu gehören etwa Feststellungen zu Art, Umfang und Wirkung von bereits erfolgten und etwa drohenden Cyber-Angriffen wie „Denial-of-Service“-Attacken sowie zu der Bedeutung der betroffenen Telemedien.

Erst wenn entsprechende Feststellungen hierzu getroffen sind, wird das Berufungsgericht die nach dem Urteil des Gerichtshofs gebotene Abwägung zwischen dem Interesse der Beklagten an der Aufrechterhaltung der Funktionsfähigkeit ihrer Online-Mediendienste und dem Interesse oder den Grundrechten und Grundfreiheiten des Klägers nachzuholen haben. Dabei wird auch der Gesichtspunkt der Generalprävention gebührend zu berücksichtigen sein. Die Parteien werden dabei Gelegenheit haben, gegebenenfalls ergänzend vorzutragen.

Allerdings dürfte der mit der Speicherung der Daten eines Nutzers über das Ende eines Nutzungsvorgangs hinaus verbundene Eingriff in das allgemeine Persönlichkeitsrecht – in seiner Ausprägung als Recht auf informationelle Selbstbestimmung – nach den bisherigen Feststellungen eher gering wiegen. Denn die Stellen der Beklagten, die die IP-Adressen des Klägers gespeichert haben, hätten den Kläger nicht ohne weiteres identifizieren können. Nach den bisher getroffenen Feststellungen ist davon auszugehen, dass ihnen – die Nichtangabe der Personalien vorausgesetzt – keine Informationen vorlagen, die dies ermöglicht hätten. Anders als es bei statischen IP-Adressen der Fall sein kann, lässt sich die Zuordnung dynamischer IP-Adressen zu bestimmten Anschlüssen keiner allgemein zugänglichen Datei entnehmen (vgl. Gerlach, CR 2013, 478, 480). Der Zugangsanbieter des Klägers durfte den Stellen der Beklagten, welche die IP-Adressen speichern (sog. verantwortliche Stellen), keine Auskunft über dessen Identität erteilen, weil es dafür keine gesetzliche Grundlage gibt (§ 95 Abs. 1 Satz 3 TKG). Die Befugnisse der zuständigen Stellen im Sinne des § 113 Abs. 3 TKG (etwa die Staatsanwaltschaft im Rahmen eines Ermittlungsverfahrens nach § 100j StPO) zur Feststellung der Identität sind an enge Voraussetzungen gebunden, bei deren Vorliegen das Interesse des Nutzers an der Wahrung seiner Anonymität zurücktreten könnte.

B) Revision der Beklagten

Die Revision der Beklagten hat ebenfalls Erfolg und führt auch insoweit zur Aufhebung des Berufungsurteils und zur Zurückverweisung der Sache an das Berufungsgericht.

1. Das Berufungsgericht ist zwar zutreffend davon ausgegangen, dass die dynamische IP-Adresse des Klägers in Verbindung mit dem Zeitpunkt des Nutzungsvorgangs (erst recht) ein personenbezogenes Datum im Sinne von § 12 Abs. 1 TMG darstellt, wenn der Kläger während eines Nutzungsvorgangs seine Personalien angibt und die Beklagte den Klarnamen mit der IP-Adresse verknüp-

fen kann. Dies begegnet nach den vorstehenden Ausführungen keinerlei Zweifel.

2. Jedoch steht das vom Berufungsgericht befürwortete enge Verständnis des § 15 Abs. 1 TMG nicht in Einklang mit Art. 7 Buchstabe f der Datenschutz-Richtlinie. § 15 Abs. 1 TMG muss richtlinienkonform dahin ausgelegt werden, dass der von dem Diensteanbieter verfolgte Zweck, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung personenbezogener Daten des Nutzers auch über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann, wenn, soweit und solange die Verwendung zu diesem Zweck erforderlich ist. Das Berufungsgericht wird auf der Grundlage der noch zu treffenden Feststellungen die erforderliche Abwägung auch für den Fall nachzuholen haben, in dem der Nutzer während eines Nutzungsvorgangs seine Personalien angibt.

Anforderungen an eine Einwilligung

(Oberlandesgericht Karlsruhe, Beschluss vom 28. Juni 2017 – 1 Rb 8 Ss 540/16 –)

- 1. Das in § 4a Abs. 1 Satz 3 Bundesdatenschutzgesetz aufgestellte Erfordernis einer schriftlichen Zustimmung zur Weitergabe von Daten erfüllt eine Schutz- und Warnfunktion für den zu einer Einwilligung Aufgeforderten, der nicht übereilt zustimmen, sondern die Chance erhalten soll, sich seiner Entscheidung bewusst zu werden. Der Ausnahmecharakter der Vorschrift gebietet eine restriktive Auslegung.**
- 2. Die Einwilligung im datenschutzrechtlichen Sinne ist von der rechtfertigenden Einwilligung im ordnungswidrigkeitrechtlichen Sinne zu unterscheiden. Eine solche Rechtfertigung kommt aber nur in Betracht, wenn der Einwilligende nach den objektiven Umständen imstande ist, Bedeutung und Tragweite des Rechtsgutsverzichts zu beurteilen.**

Sachverhalt:

Das Amtsgericht hat den Betroffenen – einen niedergelassenen Arzt – mit Urteil vom 02.05.2016 wegen eines vorsätzlichen Verstoßes gegen das Bundesdatenschutzgesetz in zwei Fällen zu zwei Geldbußen von je 500 EUR verurteilt, weil er am 25.02.2014 im Rahmen seiner Arztpraxis in W. bei R. auf Veranlassung von dessen Arbeitgeber ein Drogenscreening durchgeführt und das Ergebnis dieser Untersuchung an diesen weitergeleitet hatte, ohne dass der Patient zuvor sein schriftliches Einverständnis mit der Untersuchung und der Datenweitergabe erklärt hatte. Hiergegen wendet sich der Betroffene mit der Rechtsbeschwerde, mit welcher er die Verletzung sachlichen Rechts rügt. Die Generalstaatsanwaltschaft Karlsruhe hat auf Aufhebung des Urteils angetragen.

Aus den Gründen:

Dem zulässigen Rechtsmittel kann ein – zumindest vorläufiger – Erfolg nicht versagt bleiben.

1. Entgegen der Bewertung der Verteidigung liegt ein zur Einstellung des Verfahrens führendes Hindernis nicht vor. Dass gegen den Verfolgten ein berufsrechtliches Verfahren geführt und dieses gegen Zahlung einer Geldbuße eingestellt worden

war, bewirkt einen Strafklageverbrauch nicht, da berufsgerichtliche Sanktionen lediglich disziplinarischen und keinen bestrafenden Charakter haben (BVerfGE 21, 378, 384 ff.; BVerfGE 27, 180, 184 f.) und die Ahndung im Rahmen des ärztlichen Berufsrechts anhand spezifischer Sonderregelungen erfolgt, die außerhalb des Strafrechts liegen (Rehborn, GesR 2004, 170, 174).

2. Jedoch hält die gerichtliche Beweiswürdigung einer rechtlichen Überprüfung nicht stand, denn diese ist lückenhaft. Aus den Urteilsgründen ergibt sich insoweit lediglich, dass der Zeuge R. mit der auf Veranlassung seines früheren Arbeitgebers bei ihm zuvor durchgeführten Vorsorgeuntersuchung G 25 einverstanden gewesen war und sein Einverständnis auch schriftlich erklärt hatte. Bezüglich der nachfolgenden Abgabe einer Urinprobe lässt sich den Urteilsgründen aber lediglich entnehmen, dass der Patient durch eine Arzthelferin auf die Notwendigkeit der Abgabe einer Urinprobe zur Durchführung eines Drogenscreenings hingewiesen, eine solche Untersuchung ohne Einholung einer schriftlichen Einverständniserklärung sodann durchgeführt und das insoweit positive Ergebnis an den Arbeitgeber des Untersuchten weitergeleitet worden war. Aus den Feststellungen ergibt sich aber nicht, ob sich der Betroffene zu der Aufforderung zur Abgabe einer Urinprobe gegenüber der Arzthelferin geäußert hat und er ob er ggf. in Kenntnis der Bedeutung einer solchen Erklärung mit der Durchführung eines Drogentest einverstanden gewesen war.

a. Nach § 43 Abs. 2 Nr. 1 BDSG, der vorliegend auch für den Betroffenen zur Anwendung kommt (§ 1 Abs. 2 Nr. 3 BDSG), handelt ordnungswidrig, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (§ 3 Abs. 1 BDSG). Besondere Arten personenbezogener Daten sind dabei Angaben über die Gesundheit (§ 3 Abs. 9 BDSG). Unter Erheben ist das Beschaffen von Daten über den Betroffenen zu verstehen (§ 3 Abs. 3 BDSG), wohingegen unter den Begriff des Verarbeitens das Speichern und Übermitteln personenbezogener Daten fällt (§ 3 Abs. 4 BDSG). Speichern ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung (§ 3 Abs. 4 Satz 2 Nr. 1 BDSG), Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden (§ 3 Abs. 4 Satz 2 Nr. 3 a BDSG). Dabei ist unerheblich, ob der Täter die Daten durch Angestellte hat erheben lassen, denn verantwortliche Stelle ist insoweit jede Person, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 Abs. 7 BDSG). Vorliegend steht danach aufgrund der auch in subjektiver Hinsicht getroffenen Feststellungen des Amtsgerichts fest, dass der Betroffene durch die Auswertung des durchgeführten Drogenscreenings, die Erfassung der Daten und die Weitergabe dieser an den Arbeitgeber personenbezogene Daten des Zeugen R. erhoben und verarbeitet hat.

b. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten war vorliegend auch nicht zulässig, da weder das Bundesdatenschutzgesetz noch eine andere Rechtsvorschrift dies erlaubt oder angeordnet hatte und außerdem auch keine datenschutzrelevante Zustimmung des Betroffenen vorlag (§ 4 Abs. 1 BDSG). Dass die vom Zeugen R. im Rahmen der G 25 Untersuchung erteilte schriftliche Zustimmung zur Datenweiter-

gabe an seine Arbeitgeber auch die Erhebung und Verarbeitung der Daten aus dem Drogenscreening erfasst hätte, ist den Urteilsgründen nicht zu entnehmen. Eine solche schriftliche Einwilligung ist jedoch erforderlich, soweit nicht wegen besondere Umstände eine andere Form angemessen ist (§ 4a Abs. 1 Satz 3 BDSG). Hiervon ist jedoch nicht auszugehen, da die Schriftform eine Schutz- und Warnfunktion für den zu einer Einwilligung Aufgeforderten erfüllt (Beck-OK-BDSG/Kühling, 18. Edition vom 1.11.2016, § 4a Rn. 49). Dieser soll nicht übereilt zustimmen, sondern die Chance erhalten, sich seiner Entscheidung bewusst zu werden (Beck-OK-BDSG/Kühling, a.a.O.). Der Ausnahmecharakter der Vorschrift gebietet daher eine restriktive Auslegung (Beck-OK-BDSG/Kühling, a.a.O.). Auch sind besondere und eine andere Form rechtfertigende Umstände, wie etwa eine besondere Eilbedürftigkeit im Interesse des Betroffenen, vorliegend nicht ersichtlich.

Da der Betroffene nach den getroffenen Feststellungen auch um das Schriftformerfordernis wusste, ist auch die Annahme einer vorsätzlichen Tatbestandsverwirklichung nicht zu beanstanden (§ 43 Abs. 2 Nr. 1 BDSG), Anhaltspunkte für das Vorliegen eines Tatbestandsirrtums liegen nicht vor (§ 11 Abs. 1 OWiG).

3. Jedoch ist die Einwilligung im datenschutzrechtlichen Sinne (§ 4 Abs. 1 BDSG) von der rechtfertigenden Einwilligung im ordnungswidrigkeitrechtlichen Sinne zu unterscheiden. Zwar schützen Ordnungswidrigkeitentatbestände zumeist nicht unmittelbar individuelle Rechtsgüter, sondern Allgemeininteressen (Göhler/Gürtler, OWiG, 16. Auflage 2012, Vor § 1 Rn. 22; vgl. OLG Hamm NStZ 1985, 275), jedoch ist es der Zweck des Bundesdatenschutzgesetzes, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG). Das allgemeine Persönlichkeitsrecht stellt ein anerkanntes individuelles Rechtsgut dar (siehe nur Beck-OK-StGB/Momsen/Savic, 32. Edition vom 1.9.2016, § 32 Rn. 19), so dass eine rechtfertigende Einwilligung grundsätzlich möglich ist (ebenso Kohlhaas/Erbs/Amb, Strafrechtliche Nebengesetze, 211. Ergänzungslieferung, 11/2016, § 4a BDSG Rn. 2), und zwar unbeschadet eines datenschutzrechtlichen Schriftformerfordernisses (§ 4a Abs. 1 Satz 3 BDSG), zumal ein Verstoß hiergegen letztendlich nur zu einem Anspruch auf Löschung der Daten führt (Kohlhaas/Erbs/Amb a.a.O.).

4. Ob die Voraussetzungen einer solchen rechtfertigenden Einwilligung (vgl. hierzu KK-OWiG/Rengier, 4. Auflage 2014, Vor § 15 Rn. 13) hier gegeben waren, hat das Amtsgericht aber weder festgestellt noch sich näher damit auseinandergesetzt. Insoweit wird sich die Tatrichterin in der neuen Hauptverhandlung insbesondere mit der Frage zu befassen haben, ob eine mündliche rechtfertigende Einwilligung überhaupt ausdrücklich oder zumindest konkludent erklärt wurde oder ob der Zeuge R. lediglich den Anweisungen der Arzthelferin Folge geleistet hat. Auch muss der Einwilligende nach seiner Reife imstande gewesen sein, Bedeutung und Tragweite des Rechtsgutsverzichts zu beurteilen, weshalb das Amtsgericht neben den intellektuellen Fähigkeiten des Patienten und den äußeren Umständen der Erklärung in seine Abwägung auch wird einstellen müssen, ob der Zeuge um die möglichen Folgen einer solches „Drogenscreenings“ wusste oder solche in Kauf genommen hat bzw. ob er hierüber und etwaige Verweigerungsrechte zuvor durch die Arzthelferin oder auf sonstige Weise, etwa im Rahmen der G 25 Untersuchung, ausdrücklich aufgeklärt worden war.

Presserechtlicher Auskunftsanspruch gegenüber Staatsanwaltschaft (Ls)

(Verwaltungsgerichtshof Baden-Württemberg, Beschluss vom 4. August 2017 – 1 S 1307/17 –)

1. Die Staatsanwaltschaften dürfen die Medien über strafrechtliche Verfahren unter Nennung des Namens des Beschuldigten grundsätzlich nur in Fällen schwerer Kriminalität oder bei Straftaten informieren, die die Öffentlichkeit besonders berühren.
2. Wenn eine Befugnis der Staatsanwaltschaft zur Information der Medien unter Namensnennung besteht, indiziert dies – wenn nicht Umstände des Einzelfalls anderes gebieten – die Pflicht der Staatsanwaltschaft, den Medien auf Anfrage zur Person des Beschuldigten Auskunft zu geben.
3. Der Grundsatz, dass eine Nennung des Namens des Beschuldigten der Staatsanwaltschaft nur gestattet ist bei Fällen schwerer Kriminalität und bei Straftaten, die die Öffentlichkeit besonders berühren, gilt in gleicher Weise für die allgemeine Medieninformation der Staatsanwaltschaft durch Pressemitteilung wie für die Auskunftserteilung nach § 4 LPresseG auf Anfrage eines einzelnen Pressevertreters.

Keine Taxifahrerüberwachung im Minutentakt (Ls)

(Arbeitsgericht Berlin, Urteil vom 10. August 2017 – 41 Ca 12115/16 –)

Wenn in einem Taxi nach einer Standzeit von drei Minuten ein akustisches Signal erfolgt, nach dessen Ertönen der Taxifahrer innerhalb von 10 Sekunden eine Taste zu drücken hat, um Vergütung für die Standzeit zu erhalten, ist das eine mit § 32 BDSG unvereinbare Mitarbeiterkontrolle.

(Nicht amtlicher Leitsatz)

Mitbestimmung bei Einrichtung und Betrieb einer Smartphone-App mit Kundenfeedbackfunktion

(Arbeitsgericht Heilbronn, Beschluss vom 8. Juni 2017 – 8 BV 6/16 –)

1. Eine vom Arbeitgeber betriebene Smartphone-Applikation, die es den Nutzern ermöglicht, ein Kundenfeedback abzugeben, das auch Angaben zu Leistung und Verhalten der Mitarbeiter enthalten könnte, ist

keine technische Überwachungseinrichtung im Sinne von § 87 Abs. 1 Nr. 6 BetrVG, wenn der Arbeitgeber weder zur Abgabe derartiger Angaben auffordert, noch diese programmgemäß technisch weiterverarbeitet.

- 2. Eine im Kern selbständige Erhebung von Daten iSv § 87 Abs. 1 Nr. 6 BetrVG durch eine technische Einrichtung ist dann nicht gegeben, wenn diese Daten der Einrichtung durch Dritte ohne eigenes Zutun – insbesondere ohne hierauf gerichtete Aufforderung der Kunden durch den Arbeitgeber – zuwachsen.**
- 3. Eine programmgemäße technische Datenverarbeitung ist nicht gegeben, wenn die bei der technischen Einrichtung eingehenden Daten anschließend ausschließlich manuell selektiert und an die Stellen weitergeleitet werden, für die die Informationen bestimmt sind. Anders kann dies dann beurteilt werden, wenn die eingehenden Daten durch die technische Einrichtung mittels einer eigenen Auswertungssoftware weiterverarbeitet werden können.**

Sachverhalt:

Die Beteiligten streiten über ein Mitbestimmungsrecht des Gesamtbetriebsrats beim Betreiben einer Smartphone-App durch die Antragsgegnerin.

Die Arbeitgeberin betreibt bundesweit ein Lebensmitteleinzelhandelsunternehmen. Das Unternehmen besteht aus 10 Betrieben, in denen ca. 1.100 Arbeitnehmer beschäftigt werden. Der Antragsteller ist der für das Unternehmen zuständige Gesamtbetriebsrat. Insgesamt entsenden acht Betriebsratsgremien ihre Mitglieder in den Gesamtbetriebsrat; der Sitz des Unternehmens befindet sich in N.

Die Unternehmensgruppe K stellt über die gängigen App-Stores eine kostenfreie Applikation mit dem Namen „K – Angebote und mehr“ zum Download und zur Nutzung bereit.

Diese Applikation (im Folgenden: App) wird von der K Informationssysteme GmbH & Co. KG entwickelt und veröffentlicht. Die App bietet den Kunden der Arbeitgeberin sowie der anderen Vertriebsunternehmen in ihrer aktuellen Version u. a. Rezeptideen, Informationen über die aktuellen Angebote der K SB-Warenhäuser, die Möglichkeit des Anlegens einer Einkaufsliste sowie eine Funktion zum Auffinden des nächst gelegenen K SB-Warenhauses.

Darüber hinaus bietet die App ein sogenanntes „Filial-Feedback“ an. Dieses ermöglicht den Kunden Rückmeldungen zu den Filialen der Arbeitgeberin. Vor Abgabe des Feedbacks wird der Nutzer in der jeweiligen App aufgefordert, eine konkrete Filiale auszuwählen. Im nachfolgenden Formularfeld kann der Nutzer zu der Filiale dann zunächst einen positiven oder negativen Smiley auswählen sowie optional einen Freitext senden. In der früheren Version der App bestand zudem eine Fotofunktion, mittels derer wahlweise Fotos direkt aufgenommen und anschließend versendet oder aber bereits gespeicherte Fotos an die Arbeitgeberin versendet werden konnten. Diese Funktion wurde mittlerweile unstrittig gelöscht. Die bei den älteren App-Versionen, welche noch im Umlauf sind, übermittelten Fotos werden von den jeweiligen Backend-Schnittstellen der App verworfen und an kein System weitergegeben.

Die im Freitextfeld der App eingegebenen Kundenkommentare werden sodann ausschließlich an die K Dienstleistungs GmbH & Co. KG (im Folgenden: Dienstleistungs-KG) weitergeleitet. Dort werden die Kommentare von Mitarbeitern gesichtet und manuell einzelnen Themenbereichen zugeordnet. Bei der Dienstleistungs-KG gehen hierbei Kundenrückmeldungen nicht nur im Wege der App ein, sondern auch per E-Mail mittels des Kontaktformulars auf der Inter-

netseite des Unternehmensverbundes, ferner handschriftliche Briefe sowie telefonische Kundenrückmeldungen. Die Weiterverarbeitung erfolgt dann dergestalt, dass die Rückmeldungen, die das Warenortiment der Arbeitgeberin betreffen, an den Bereich Einkauf, welcher unternehmensübergreifend arbeitet, weitergeleitet werden. Ferner werden sämtliche Kundenrückmeldungen mit Bezug auf eine bestimmte Filiale einmal pro Woche an den Hausleiter dieser Filiale weitergegeben, unabhängig davon, ob es sich um Rückmeldungen per E-Mail, Brief, Telefonat oder per App handelt.

Streitig ist zwischen den Beteiligten, ob die Arbeitgeberin die Rückmeldungen, die sie über die App gewinnt, verlässlich anonymisiert, indem Namen und Zeitstempel entfernt werden, sofern die Rückmeldung einen Mitarbeiterbezug aufweist.

Mit anwaltlichen Schreiben vom 18.07.2016 wurde die Arbeitgeberin mit Frist bis zum 29.07.2016 aufgefordert, das Filial-Feedback für sämtliche Betriebe des Unternehmens in der App zu deaktivieren und Verhandlungen mit dem Gesamtbetriebsrat zum Abschluss einer Gesamtbetriebsvereinbarung hinsichtlich der Anwendung der App aufzunehmen.

Mit E-Mail vom 28.07.2016 bestritt die Arbeitgeberseite das Bestehen eines Mitbestimmungsrechtes und lehnte Verhandlungen hierüber zwecks Abschlusses einer Gesamtbetriebsvereinbarung ab.

Mit Beschluss vom 05.09.2016 setzte das Arbeitsgericht Heilbronn auf Antrag des Gesamtbetriebsrates einen Einigungsstellenvorsitzenden ein und setzte die Zahl der Beisitzer fest. Diese Entscheidung wurde durch das Landesarbeitsgericht Baden-Württemberg (Aktenzeichen 21 TaBV 12/16) am 13.01.2017 bestätigt.

Die erste Sitzung der Einigungsstelle ist terminiert auf den 20.06.2017.

Der Gesamtbetriebsrat ist der Auffassung, dass der Betrieb der App eine mitbestimmungspflichtige Angelegenheit im Sinne von § 87 Abs. 1 Nr. 6 BetrVG darstelle. Durch den Betrieb der Seite ohne seine Zustimmung verletze die Arbeitgeberin sein Mitbestimmungsrecht, weshalb er Unterlassung verlangen könne.

Das Mitbestimmungsrecht ergebe sich daraus, dass die App eine technische Einrichtung darstelle, die es der Arbeitgeberin ermögliche, sowohl das Verhalten als auch die Leistung der Arbeitnehmer zu kontrollieren und mittels der durch die App gewonnenen Daten zu überwachen. Über die Feedbackfunktion hätten die Kunden die Möglichkeit, Kommentare zu Leistung und Verhalten der einzelnen Mitarbeiter abzugeben. Da die Mitarbeiter der Arbeitgeberin verpflichtet seien, Namensschilder zu tragen, sei die Identifizierung der betroffenen Mitarbeiter jederzeit durch Namensnennung möglich. Eine Identifikation sei zudem möglich über Angaben zu Datum und Uhrzeit in Kombination mit den Einsatzplänen der jeweiligen Filialen. Eine wirksame Anonymisierung durch die Dienstleistungs-KG werde bestritten, zumal diese im gleichen Gebäude angesiedelt sei wie die Antragsgegnerin und die Ausgestaltung der Vertragsbeziehungen unklar sei.

Der Gesamtbetriebsrat beantragt zuletzt:

1. Der Antragsgegnerin wird aufgegeben, es zu unterlassen, die Funktion Filial-Feedback in der App „K – Angebote und mehr“ für das Unternehmen und seine Betriebe ohne Zustimmung des Antragstellers oder den die Zustimmung ersetzenden Spruch der Einigungsstelle zu nutzen und zur Nutzung bereitzustellen.

Hilfsweise für den Fall des Unterliegens mit Antrag Ziffer 1 wird folgender Antrag Ziffer 2 gestellt:

2. Der Antragsgegnerin wird aufgegeben, es zu unterlassen, ohne Zustimmung des Antragstellers oder den die Zustimmung ersetzenden Spruch der Einigungsstelle, die mittels der Filial-Feedback-Funktion in der App „K – Angebote und mehr“ gewonnenen und ihr übermittelten Daten zu erfassen, zu speichern und zu nutzen.

3. Für jeden Fall der Zuwiderhandlung gegen die Verpflichtung aus Antrag Ziffer 1 bzw. Antrag Ziffer 2 wird der Antragsgegnerin ein Ordnungsgeld in Höhe von bis zu EUR 10.000,00 angedroht.

Die Arbeitgeberin beantragt die Zurückweisung der Anträge.

Die Arbeitgeberin ist der Auffassung, dass der Betrieb der App samt der Funktion Filialfeedback insbesondere nach Löschung der Fotofunktion nicht der Mitbestimmung des Gesamtbetriebsrats gemäß § 87 Abs. 1 Nr. 6 BetrVG unterliege. Dies sei darauf zurückzuführen, dass keine Information automatisiert von der App erhoben werde. Diese übermittle lediglich Daten, die von Dritten eingegeben würden. Die App stelle letztlich nur einen weiteren Übertragungsweg für Kundenrückmeldungen dar, ebenso wie das Kontaktformular auf der Internetseite der Arbeitgeberin, und fungiere damit lediglich als elektronischer Briefkasten. Zudem erfolge auch keine technische Datenverarbeitung, da alle gewonnenen Daten anschließend manuell sortiert und einfallabhängig an die betroffenen Filialen bzw. in der Hauptsache an den Einkauf weitergereicht würden. Damit stelle die App keine technische Einrichtung dar, die programmgemäß personenbezogene Arbeitnehmerdaten verarbeite. Auch ein öffentlicher Überwachungsdruck werde nicht erzeugt, da sämtliche Kundenrückmeldungen ausschließlich der Dienstleistungs-KG übersandt würden und nicht öffentlich einsehbar seien.

Zudem würden die Daten, welche Mitarbeiter der Arbeitgeberin betreffen, zuverlässig durch die Dienstleistungs-KG anonymisiert, indem die Original-Meldung überschrieben werde, soweit diese Namen von Mitarbeitern oder Daten enthalte, die einen Rückschluss auf einen konkreten Mitarbeiter erlauben würden.

Hinsichtlich der weiteren Vorbringens der Parteien wird ergänzend Bezug genommen auf die gewechselten Schriftsätze sowie die Verhandlungsprotokolle.

Aus den Gründen:

Die Anträge des Gesamtbetriebsrats sind zulässig, jedoch unbegründet.

I. Zulässigkeit

Die Anträge sind zulässig.

1. Der Rechtsweg zu den Gerichten für Arbeitsachen ist eröffnet gemäß § 2a Abs. 1 Nr. 1 ArbGG, da es sich im vorliegenden Fall um eine betriebsverfassungsrechtliche Streitigkeit handelt.

Das Arbeitsgericht Heilbronn ist gemäß §§ 82 Abs. 1 S. 2 ArbGG zuständig, da der Sitz der Arbeitgeberin sich in Neckarsulm befindet.

2. Die Anträge sind auch hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO.

Es handelt sich um Unterlassungsanträge, die die eigentliche Streitfrage so zur Entscheidung stellen, dass diese mit Rechtskraftwirkung endgültig entschieden werden kann. Es wird deutlich, welche Handlungen die Arbeitgeberin zu unterlassen hat, nämlich über die K Informationssysteme GmbH & Co. KG den Kunden die App-Funktion Filial-Feedback zur Nutzung bereit zu stellen sowie die hieraus gewonnenen Daten selber zu nutzen. Hierbei ist die Unterlassungsverpflichtung nicht notwendig darauf beschränkt, bestimmte eigene Handlungen zu unterlassen. Sie kann vielmehr auch beinhalten, dass der Verpflichtete innerhalb seines Organisationsbereiches aktiv auf Dritte einwirken muss, um den Eintritt eines bestimmten Erfolgs zu verhindern (BAG 29. April 2004 – 1 ABR 30/02 Rn. 112). Der Antrag erfasst auch alle Applikationen „K-Angebote und mehr“, unabhängig davon, für welche Betriebsysteme diese entwickelt werden.

3. Das Verfahren wurde durch wirksamen Beschluss des Gesamtbetriebsrats vom 12./13.07.2016 eingeleitet; auch das Vorliegen der Prozessvollmacht des Verfahrensbevollmächtigten des Antragstellers ist mittlerweile nicht mehr streitig.

II. Begründetheit

Die Anträge des Gesamtbetriebsrats sind unbegründet.

1. Der Antragsteller hat keinen Anspruch darauf, dass die Antragsgegnerin es unterlässt, die Funktion Filial-Feedback ohne seine Zustimmung bzw. ohne diesen ersetzenden Spruch der Einigungsstelle zu nutzen und zur Nutzung bereitzustellen.

a) Nach der gefestigten Rechtsprechung des Bundesarbeitsgerichts steht dem hier gem. § 50 Abs. 1 BetrVG zuständigen Gesamtbetriebsrat bei Verletzung seiner Mitbestimmungsrechte aus § 87 BetrVG ein Anspruch auf Unterlassung der mitbestimmungswidrigen Maßnahmen zu. Dieser Anspruch setzt keine grobe Pflichtverletzung des Arbeitgebers im Sinne von § 23 Abs. 3 BetrVG voraus (BAG 3. Mai 1994 – 1 ABR 24/93). Der Unterlassungsanspruch wird zwar in § 87 BetrVG nicht ausdrücklich geregelt; Unterlassungsansprüche können aber als selbständige, einklagbare Nebenleistungsansprüche auch ohne gesetzliche Normierung bestehen. Der Anspruch ergibt sich bei sozialen Angelegenheiten im Sinne von § 87 BetrVG aus der besonderen Rechtsbeziehung, die zwischen Arbeitgeber und Betriebsrat besteht.

b) Ein Mitbestimmungstatbestand nach § 87 Abs. 1 Nr. 6 BetrVG ist vorliegend nicht gegeben.

aa) Nach der genannten Vorschrift hat der Betriebsrat bzw. Gesamtbetriebsrat u. a. mitzubestimmen bei der Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. „Überwachung“ im Sinne dieser Vorschrift ist ein Vorgang, durch den Informationen über das Verhalten oder die Leistung von Arbeitnehmern erhoben und – jedenfalls in der Regel – aufgezeichnet werden, um sie der späteren Wahrnehmung zugänglich zu machen. Die Informationen müssen auf technische Weise ermittelt und dokumentiert werden, so dass sie zumindest für eine gewisse Dauer verfügbar bleiben und vom Arbeitgeber herangezogen werden können (BAG 27. Januar 2004 – 1 ABR 7/03 Rn. 27; BAG 10. Dezember 2013 – 1 ABR 43/12 Rn. 20).

Die Überwachung muss aber durch die technische Einrichtung selbst bewirkt werden. Dazu muss diese aufgrund ihrer technischen Natur unmittelbar, d. h. wenigstens in ihrem Kern, die Überwachung vornehmen, indem sie das Verhalten oder die Leistung der Arbeitnehmer kontrolliert. Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG setzt daher voraus, dass die technische Einrichtung selbst und automatisch die Daten über bestimmte Vorgänge verarbeitet, wobei es jedoch ausreicht, wenn lediglich ein Teil des Überwachungsvorgangs mittels einer technischen Einrichtung erfolgt (BAG 15. Dezember 1992 – 1 ABR 24/92 Rn. 32; BAG 10. Dezember 2013 – 1 ABR 43/12 Rn. 20).

So wird die durch Computer ermöglichte technische Überwachung in drei Phasen automatisierter Personaldatenverarbeitung gegliedert, von denen jede das Mitbestimmungsrecht des Betriebsrats auslösen kann, nämlich die Erhebung von Verhaltens- und Leistungsdaten, das Verarbeiten (Sichten, Ordnen, Inbeziehungsetzen) und die Beurteilung der Daten (Vergleich der Verhaltens-/Leistungsangabe mit der Vorgabe). Ausreichend für das Vorliegen eines Mitbestimmungsrechtes ist es, wenn lediglich ein Teil des Überwachungsvorgangs mittels einer technischen Einrichtung erfolgt (BAG 15. Dezember 1992 – 1 ABR 24/92 Rn. 32).

Für den Fall, dass die technische Einrichtung die Verhaltens- bzw. Leistungsdaten der Mitarbeiter nicht selbst erhebt, ist für das Vorliegen eines Mitbestimmungstatbestandes nach § 87 Abs. 1 Nr. 6 BetrVG erforderlich, dass diese Daten programmgemäß durch die technische Einrichtung zu Aussagen über Verhalten oder Leistung einzelner Arbeitnehmer verarbeitet werden. Dies ist seit der Entscheidung des Bundesarbeitsgerichts zum Technikerberichts-system

(BAG 14. September 1984 – 1 ABR 23/82 Rn. 52) sowie den Folgeentscheidungen (z. B. BAG 23. April 1985 – 1 ABR 39/81 Rn. 38 zum TÜV-Berichtssystem) und vom 11. März 1986 (BAG 11. März 1986 – 1 ABR 12/84 Rn. 21) sowie vom 15. Dezember 1992 (BAG 15. Dezember 1992 – 1 ABR 24/92 Rn. 30) Gegenstand ständiger Rechtsprechung zu dieser Frage; das Schrifttum ist dem großteils beigetreten (GK-BetrVG/ Wiese, § 87 Rn. 527 f.; Fitting, 28. Aufl., § 87 Rn. 238 ff.; aA HSWGNR/Worzalla, 8. Aufl. § 87 Rn. 370).

Hintergrund dieser Grundentscheidung ist, dass bei der programmgemäßen technischen Auswertung auch manuell erhobener Daten notwendigerweise ein Kontextverlust der Daten eintritt, weil der ursprüngliche Erhebungszusammenhang verloren geht und das Vergessen von Daten ausgeschlossen wird, so dass die Sammlung von Informationen über den Arbeitnehmer für diesen nicht wahrnehmbar, weil anonym und ohne Möglichkeit einer wirksamen Gegenkontrolle vorgenommen wird. Jedenfalls die notwendige Selektion der Daten und der damit verbundene Kontextverlust sowie die unbegrenzt mögliche Erstreckung der Verarbeitung auf alle Daten einschließlich solcher, die weit zurückliegen und einen gegenwärtigen Aussagewert möglicherweise nicht mehr haben, können Einsichten in Leistung und Verhalten von Arbeitnehmern möglich machen, die einmal bei herkömmlicher Überwachung nicht gegeben waren und zum anderen einer persönlichen, individualisierenden Beurteilung entbehren, was den Arbeitnehmer zu einem bloßen Beurteilungsobjekt machen kann (BAG 14. September 1984 – 1 ABR 23/82).

Auch in der aktuellen Rechtsprechung des BAG (z. B. vom 13. Dezember 2016 – 1 ABR 7/15 Rn. 22) stellt das Bundesarbeitsgericht darauf ab, ob die manuell gewonnenen Daten von der technischen Einrichtung selbst weiterverwertet werden. Es kommt daher in Bezug auf das Betreiben einer Facebook-Seite zu dem Ergebnis, dass aufgrund der (zum Zeitpunkt der Entscheidung) fehlenden Auswertungsmöglichkeiten durch die Facebook-eigene Software der Betrieb einer solchen Internetplattform nicht mitbestimmungspflichtig ist, obwohl der Betrieb einer solchen Website stets auch Kommentare von Nutzern erlaubt (vgl. Rn. 33 der genannten Entscheidung), welche im Gegensatz zu Benutzer-Postings auch nicht deaktiviert werden können.

bb) Bei der von der Arbeitgeberin über die K Informationssysteme GmbH & Co. KG zur Verfügung gestellten Smartphone-Applikationen handelt es sich nicht um eine technische Einrichtung, die zur Überwachung der Leistung und des Verhaltens der bei ihr beschäftigten Arbeitnehmer bestimmt ist.

Zwar stellt die Applikation eine technische Einrichtung dar. Allerdings ermöglicht die bereitgestellte Funktion „Kundenfeedback“ nicht eine Überwachung des Verhaltens und der Leistung der beschäftigten Mitarbeiter, da diese die Daten nicht im Kern selbst erhebt oder aber programmgemäß verarbeitet.

(1) Die streitgegenständliche App erhebt die Daten nicht selbständig. Datenerhebung ist nach der gesetzlichen Definition von § 3 Abs. 3 Bundesdatenschutzgesetz das Beschaffen von Daten über den Betroffenen, vorliegend also über die Mitarbeiter, deren Persönlichkeitsrecht gegenüber der Arbeitgeberseite durch § 87 Abs. 1 Nr. 6 BetrVG geschützt werden soll. Das Erheben besteht damit in einer Aktivität, durch die die erhebende Stelle Kenntnis von den betreffenden Daten erhält oder die Verfügungsmacht über diese begründet. Jedoch erfüllt nicht jedes Erhalten oder Empfangen von Daten die Voraussetzungen des Beschaffens in diesem Kontext. Vielmehr muss zu der objektiven Tatsache der Begründung der Verfügungsgewalt über die Daten ein aktives Handeln kommen, das von einem entspre-

chenden, der erhebenden Stelle zuzurechnenden Willen der handelnden Person getragen ist (Simitis/ Dammann BDSG § 3 Rn. 102). Das vom Begriff des Beschaffens geforderte aktive und subjektive Element fehlt, wenn Daten einer Stelle durch Dritte ohne eigenes Zutun zuwachsen. Hält der Informationsempfänger elektronische oder herkömmliche Empfangsvorrichtungen wie Briefkästen, Faxgeräte, E-Mail-Accounts oder Websites mit Eingabemöglichkeit vor und werden diese zur Mitteilung personenbezogener Daten benutzt, so liegt darin kein Erheben der damit empfangenen Daten, es sei denn, die Benutzer wurden aufgefordert, für bestimmte Zwecke bestimmte Daten zu liefern (Simitis/Dammann BDSG § 3 Rn. 104).

Dies ist vorliegend nicht gegeben, weil die Arbeitgeberin die Kunden gerade nicht zu einem Feedback über das Verhalten und die Leistung der Mitarbeiter auffordert. Zwar verkennt die Kammer nicht, dass die Aufforderung zu einem „Feedback“ den Kunden auch dazu verleiten kann, Kommentare über Verhalten und Leistung von Mitarbeitern abzugeben; im Fokus dieser Aufforderung steht dies jedoch nicht. So hat die Arbeitgeberin nachvollziehbar behauptet, dass 99 % der Kundenrückmeldungen sich auf das Warensortiment und ähnliche Bedingungen der betreffenden Filiale beziehen und nur 1 % mitarbeiterbezogen sei.

(2) Die streitgegenständliche App verarbeitet die mitarbeiterbezogenen Daten, die von Kunden eingegeben werden, auch nicht etwa programmgemäß zu Aussagen über Verhalten und Leistung der Betroffenen. Im Gegensatz zu EDV-Systemen, bei denen Leistungsdaten manuell eingegeben, jedoch programmgemäß zusammengestellt, in Beziehung zueinander gesetzt und damit zu Aussagen über Leistung oder Verhalten von Arbeitnehmern zusammengefasst werden (wie z.B. beim Technikerberichtssystem in der BAG-Entscheidung vom 14. September 1984), stellt die streitgegenständliche App lediglich eine weitere Übermittlungsmöglichkeit für Rückmeldungen durch Dritte dar. Sie verarbeitet selber derartige Daten ebenso wenig wie das Kontaktpostfach der Arbeitgeberin auf der Unternehmens-Website und stellt daher lediglich eine Form des elektronischen Briefkastens dar.

Die weitere Nutzung der Daten erfolgt hingegen nicht technisch mit der Gefahr des Kontextverlustes, sondern ausschließlich manuell dadurch, dass Informationen durch Mitarbeiter der Dienstleistungs-KG selektiert und an die entsprechenden Hausleiter der Betriebe weitergeleitet werden. Dafür, dass die App selber die entsprechenden Daten kategorisiert oder auch eine Auswertungsmöglichkeit zur Verfügung stellt, bestehen keinerlei Anhaltspunkte. Die Gefahr des Kontextverlustes und der anonymen Überwachung gerade durch die technische Einrichtung ist damit nicht gegeben. Die Möglichkeit, dass Kunden dem Arbeitgeber Daten über Verhalten oder Leistung seiner Mitarbeiter zukommen lassen, wird durch § 87 Abs. 1 Nr. 6 BetrVG ebenso wenig erfasst, wie eine Überwachung der Arbeitnehmer durch Testkäufer oder Hausdetektive.

cc) Da es bereits an einer Überwachungsmöglichkeit durch die technische Einrichtung fehlt, kam es nicht streitentscheidend auf die Frage der wirksamen Anonymisierung durch die K Dienstleistungs-KG an.

2. Auch der vom Gesamtbetriebsrat gestellte Hilfsantrag unterlag der Zurückweisung, da die App keine mitbestimmungspflichtige technische Einrichtung darstellt, da diese die Arbeitnehmerdaten weder erhebt noch programmgemäß verarbeitet.

3. Der Antrag auf Androhung eines Ordnungsgeldes ist mangels Stattgabe der Unterlassungsanträge zur Entscheidung nicht angefallen.

Zulässigkeit von On-Board-Kameras

(Verwaltungsgericht Göttingen, Urteil vom 31. Mai 2017 – 1 A 170/16 –)

Die Aufzeichnung von Verkehrsverstößen anderer Verkehrsteilnehmer mit durch im eigenen PKW installierte On-Board-Kameras erfolgt weder für ausschließlich persönliche oder familiäre Tätigkeiten (§ 38 Absatz 5 i.V.m. § 27 Absatz 1 Satz 2 BDSG) noch ist diese Videoüberwachung nach § 6b Absatz 1 Nr. 3 BDSG gerechtfertigt.

Sachverhalt:

Der Kläger wendet sich gegen eine datenschutzaufsichtliche Anordnung der Beklagten.

Der Kläger zeigte im Laufe der vergangenen Jahre ca. 50.000 Verkehrsordnungswidrigkeiten bei Ordnungsbehörden, Polizei und Staatsanwaltschaft an. In seinem Pkw sind an Front- und Heckscheibe Onboard-Kameras, sogenannte Dashcams (aus dem Englischen: dashboard – Armaturenbrett – und cam – Kamera –) installiert, mit denen er den vorausfahrenden und nachfolgenden Straßenverkehr aufzeichnen kann. Erstmals im Jahr 2014 führte die Beklagte gegen den Kläger ein Ordnungswidrigkeitenverfahren nach dem Bundesdatenschutzgesetz wegen der Beobachtung und Aufzeichnung des Straßenverkehrs mit Dashcams. Das Verfahren wurde durch Beschluss des Amtsgerichts M. aus formalen Gründen eingestellt (Az.: S. Owi T. Js U. (V.). Am 29.10.2014 teilte die Beklagte dem Kläger mit, dass sie erneut ein Ordnungswidrigkeitenverfahren und ein datenschutzrechtliches Untersagungsverfahren gegen ihn einleiten würde, falls er wieder Dashcams zur Dokumentation von Verkehrsordnungswidrigkeiten einsetzen würde.

Im November 2014 zeigte der Kläger beim Landkreis W. unter Vorlage von Bildaufnahmen einer Dashcam Verkehrsordnungswidrigkeiten vom 31.10. (Bl. 5 ff., 19, 19a Beiakte B zu 1 A 83/15), 04. (Bl. 21-23 Beiakte B zu 1 A 83/15), 10. (Bl. 24 ff. Beiakte B zu 1 A 83/15), 19. (Bl. 31, 32 Beiakte B zu 1 A 83/15) und 26.11.2014 (Bl. 33-35a Beiakte B zu 1 A 83/15) an. Daraufhin leitete die Beklagte ein aufsichtsbehördliches Kontrollverfahren gegen den Kläger ein und forderte ihn mit Schreiben vom 01.12.2014 (Bl. 11 ff. Beiakte B zu 1 A 83/15) auf, acht Fragen zur Verwendung der Dashcams zu beantworten. Nachdem der Kläger trotz Zwangsgeldandrohung die erbetenen Auskünfte bis zum 09.01.2015 nicht erteilt hatte, hörte ihn die Beklagte mit Schreiben desselben Datums zum Erlass einer beabsichtigten datenschutzaufsichtlichen Anordnung nach § 38 Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG) an.

Nachdem die Beklagte davon Kenntnis erlangt hatte, dass der Kläger beim Landkreis W. weitere Verkehrsordnungswidrigkeiten vom 02.05. (Bl. 61a -64 Beiakte 001) und 22.06.2016 (Bl. 68 Beiakte 001) unter Vorlage von Bildaufnahmen einer Dashcam angezeigt hatte, erließ sie nach erneuter Anhörung am 24.06.2016 eine datenschutzaufsichtliche Anordnung. In dieser gab sie dem Kläger auf,

1.1 die Verwendung von Onboard-Videokameras jeden Typs (sogenannte Dashcams bzw. Actioncams) in von ihm im öffentlichen Verkehr als Fahrer oder Beifahrer genutzten Kraftfahrzeugen so zu gestalten, dass eine Erhebung und Verarbeitung personenbezogener Daten anderer Verkehrsteilnehmer mit diesen Videokameras anlässlich der widmungsgemäßen Nutzung von öffentlichen Verkehrsflächen ausgeschlossen ist,

1.2 auf in seinem Besitz befindlichen Datenträgern gespeicherte Daten über im öffentlichen Straßenverkehr erhobene Videosequenzen, die aus der Verwendung von Onboard-Videokameras stammen und die nicht ausschließlich persönlichen und familiären Zwecken dienen, innerhalb einer Frist von sieben Tagen nach Bekanntgabe der Verfügung zu löschen,

1.3 ihr die in Ziff. 1.2 angeordnete Löschung innerhalb von zwei Wochen nach Unanfechtbarkeit der Verfügung schriftlich zu bestätigen (Ziff. 1.3).

Darüber hinaus drohte sie dem Kläger zu Ziffern 1.1 bis 1.3 Zwangsgelder an. Zu Ziffern 1.1 und 1.2 drohte sie Zwangsgelder in Höhe von 5.000 (Ziffer 3.1) bzw. 1.000 Euro (Ziffer 3.2) an, wenn der Kläger den Verfügungen nicht innerhalb von drei bzw. sieben Tagen nach Bekanntgabe nachkomme. Zu Ziffer 1.3 drohte sie ein Zwangsgeld in Höhe von 100 Euro, wenn er der Anordnung nicht innerhalb von zwei Wochen nach Unanfechtbarkeit des Bescheids nachkomme. In Ziffer 2 ordnete sie die sofortige Vollziehung der Anordnungen zu Ziffern 1.1 und 1.2. an.

Zur Begründung der Anordnung zu Ziffer 1.1 führte die Beklagte aus, der Anwendungsbereich des Bundesdatenschutzgesetzes sei eröffnet. Die Aufnahmen der Kameras hätten den Zweck, Verkehrsunfälle oder Ordnungswidrigkeiten zu dokumentieren und seien keiner persönlichen oder familiären Tätigkeit des Klägers i. S. v. § 1 Abs. 2 Nr. 3 BDSG zuzuordnen. Die Aufnahme anderer Verkehrsteilnehmer mit einer Videokamera stelle eine Erhebung, die Speicherung der erhobenen Videobilder auf einer SD-Karte eine Verarbeitung und die Verwendung der Aufnahmen bei Straf- und Ordnungswidrigkeitenanzeigen eine Übermittlung personenbezogener Daten dar und sei deshalb grundsätzlich nach § 4 Abs. 1 BDSG verboten. Die Videoüberwachung durch den Kläger sei auch nicht nach der datenschutzrechtlichen Ausnahмовorschrift des § 6b Abs. 1 Nr. 3 BDSG zulässig. Insbesondere sei sie nicht zur Wahrnehmung berechtigter Interessen erfolgt. Solche Interessen müssten konkret benannt werden. Hierfür würde der vom Kläger angegebene Zweck der Videoüberwachung „Selbstschutz, Eigentumschutz, Beweissicherung“ nicht ausreichen. § 6b BDSG lasse keine permanente Videoüberwachung zur abstrakten Gefahrenvorsorge zu. Um konkrete Unfälle dokumentieren zu können, reiche es aus, von dem konkreten Unfall Aufnahmen zu machen. Einer permanenten Aufnahme des gesamten Verkehrsgeschehens bedürfe es hierfür gerade nicht. Aber selbst wenn die vom Kläger praktizierte permanente Videoüberwachung seinen berechtigten Interessen dienen würde, würden die schutzwürdigen Interessen der Betroffenen, nicht in den Fokus der Onboard-Kameras des Klägers zu geraten, demgegenüber überwiegen. Die Anordnung sei ermessensgerecht. Der Kläger habe keine nachvollziehbaren Interessen, die über die Beschaffung von Beweisen im Falle eines Unfalls hinausgingen, vorgetragen. Die heimliche Videoüberwachung sei auch mit Blick auf § 6b Abs. 2 BDSG rechtswidrig, denn danach seien der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Eine Einschränkung der Anordnung auf bestimmte Kameras sei mangels Mitwirkung des Klägers nicht möglich gewesen. Sie entspräche im Übrigen auch nicht dem Zweck, jegliche Erhebung und Verarbeitung personenbezogener Daten anderer Verkehrsteilnehmer zu unterbinden. Dasselbe gelte, soweit die Anordnung zu Ziffer 1.1 auf jegliches vom Kläger genutztes Kraftfahrzeug erstreckt worden sei. Nicht ausgeschlossen sei jedoch, dass der Kläger die Dashcams für vom Bundesdatenschutzgesetz nicht erfasste persönliche Zwecke im Sinne des § 1 Abs. 2 Nr. 3 BDSG auch künftig weiter verwende. Ihm sei lediglich die permanente Videoüberwachung des Straßenverkehrs untersagt, sowie die Löschung der unzulässig erhobenen und gespeicherten Aufnahmen aufgegeben worden.

Die Anordnung der Löschung stütze die Beklagte auf § 35 Abs. 2 Satz 2 Nr. 1 BDSG.

Am 07.07.2016 hat der Kläger Klage erhoben.

Aus den Gründen:

Die Klage ist unbegründet.

Rechtsgrundlage für die Anordnungen der Beklagten zu Ziffern 1.1-1.3 ist § 38 Absatz 5 Satz 1 BDSG. Danach kann zur Gewährleistung der Einhaltung des Bundesdatenschutzgesetzes und ande-

rer Vorschriften über den Datenschutz die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Die Aufsichtsbehörden im Sinne von § 38 Absatz 5 BDSG werden von den Landesregierungen oder den von ihnen ermächtigten Stellen bestimmt (Absatz 6). In Niedersachsen sind dies I. oder AA. J. (§ 22 Absatz 6 Satz 1 NDSG) und damit die Beklagte.

Der Kläger hat gegen § 6b BDSG verstoßen. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen (Nr. 1.), zur Wahrnehmung des Hausrechts (Nr. 2.) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist (Nr. 3) und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Es kann dahin gestellt bleiben, ob auch bei einem Verstoß gegen § 6b BDSG die Aufsichtsbehörde nach § 38 Absatz 5 Satz 1 BDSG nur dann einschreiten darf, wenn der Anwendungsbereich der Vorschrift gemäß § 27 Abs. 1 Satz 1 BDSG eröffnet ist. Danach ist der Anwendungsbereich von § 38 Abs. 5 Satz 1 BDSG eröffnet, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch u.a. nicht-öffentliche Stellen (Nr. 1). Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt (Satz 2).

Dagegen erfasst § 6b BDSG die reine Beobachtung selbst. Die Möglichkeit einer dateimäßigen oder automatisierten Auswertung personenbezogener Daten wird dabei nicht verlangt. Damit ist allein die Videoüberwachung öffentlich zugänglicher Räume datenschutzrechtlich relevant, unabhängig davon, ob es zu einer anschließenden Speicherung von Bildmaterial kommt (BT-Drucksache 14/4329, Seite 38; Gola/Schomerus, BDSG, 12. Aufl. 2015, § 6b Rn. 1; Bergmann/Möhrle/Herb, Datenschutzrecht, Loseblattsammlung Stand September 2016, § 6b Rn. 1 ff.). Vor diesem Hintergrund stellt die als „lex specialis“ bezeichnete Vorschrift einen Fremdkörper in der Systematik des Bundesdatenschutzgesetzes dar. Sie regelt ausschließlich, wann eine Videoüberwachung öffentlich zugänglicher Räume zulässig ist und unter welchen Voraussetzungen die Verarbeitung oder Nutzung von bei der Videoüberwachung „erhobenen“ Daten zulässig ist. Die Begriffsdefinitionen in §§ 1-3 BDSG sind dabei nicht ohne weiteres übertragbar. So ist nach § 3 Absatz 3 BDSG unter „erheben“ das Beschaffen von Daten über den Betroffenen zu verstehen. Dabei ist ein zielgerichtetes Beschaffen der Daten notwendig. Bei zufälligen Beobachtungen gewonnene Daten oder Daten, die der verantwortlichen Stelle unaufgefordert zugeleitet würden, würden die Daten nicht beschafft. Dagegen wird in § 6b BDSG davon ausgegangen, dass auch die bei einer reinen Beobachtung gewonnenen Daten „erhoben“ werden, wenn es in Absatz 3 der Vorschrift heißt, „Die Verarbeitung oder Nutzung“ von nach Absatz 1 erhobenen Daten ist zulässig,....“ (vgl. Gola/Schomerus, a.a.O., § 3 Rn. 24, § 6b Rn. 3 und 10; Becker in: Plath, BDSG/DS-GVO, 2. Aufl. 2016, § 6b Rn. 1; s. auch Bergmann/Möhrle/Herb, Datenschutzrecht, a.a.O., § 3 Rn. 62 ff).

Auf diese Unterschiede kommt es hier jedoch im Ergebnis nicht an, weil der Kläger mit seinen Videokameras nicht nur i. S. v. § 6b BDSG beobachtet, sondern darüber hinaus personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt und dafür erhoben hat und die Erhebung,

Verarbeitung oder Nutzung der Daten nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgte. Der Anwendungsbereich des § 38 Absatz 5 BDSG ist nach § 27 Absatz 1 Satz 1 BDSG damit eröffnet.

Personenbezogene Daten sind gemäß § 3 Absatz 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmaren natürlichen Person (Betroffener). Automatisierte Verarbeitung wird in § 3 Absatz 2 BDSG als Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen bezeichnet. Nicht-öffentliche Stellen sind gemäß § 2 Absatz 4 Satz 1 BDSG u. a. natürliche Personen, die nicht hoheitliche Aufgaben wahrnehmen. Diese Voraussetzungen sind hier gegeben.

Die mittels der Dashcams vom Kläger erstellten Aufnahmen enthalten personenbezogene Daten i. S. d. § 3 Abs. 1 BDSG. Unter den Begriff der „persönlichen oder sachlichen Verhältnisse“ einer Person fallen unzweifelhaft Aufnahmen von Personen, aber auch GPS-Standortdaten (Plath/Schreiber, in: Plath, BDSG/DS-GVO, 2. Aufl. 2016, § 3 BDSG, Rn. 8) und Kfz-Kennzeichen (Schaffland/Wiltfang, BDSG, Stand Mai 2016, § 3, Rn. 14). Eine Person ist bestimmt, wenn sie ohne weitere Identifikationsmerkmale klar zu erkennen ist. Auf welche Weise der Betroffene identifiziert werden kann, ist unerheblich. Bestimmbar ist eine Person, wenn auf sie Rückschlüsse möglich sind und sie damit individualisierbar ist (zu Vorstehendem: Schaffland/Wiltfang, a. a. O., § 3, Rn. 17). Auf den in den Verwaltungsvorgängen enthaltenen Ausdrücken der übermittelten Aufnahmen (Bl. 6, 22, 22a, 23, 28, 28a, 30, 31a, 35 und 35a der Beiakte B VG GÖ zu 1 A 83/15 sowie Bl. 62-64, 68 Beiakte 001) sind teilweise (Werbe-) Aufschriften auf Pkws lesbar (Bl. 6, 19, 19a Beiakte B VG GÖ zu 1 A 83/15,) sowie Gesichter und Kfz-Kennzeichen (Bl. 35, 35a Beiakte B a.a.O.; Bl. 62, 63, 64, 68 Beiakte 001) erkennbar. Auf den Aufnahmen werden darüber hinaus die Längen- und Breitengrade und der Zeitpunkt ihrer Entstehung angegeben, so dass der genaue Aufenthaltsort zumindest bestimmbarer Personen zu einem bestimmten Zeitpunkt ermittelt werden könnte. Personenbezogene Daten enthalten auch die 20 Videodateien, die der Kläger beim ehemaligen Landkreis W. im Zusammenhang mit Verkehrsordnungswidrigkeitenanzeigen eingereicht hat. Denn auf den Videos sind Fahrzeuge, Kfz Kennzeichen, selten auch Fahrzeugführer erkennbar. Sie enthalten Datums- und Zeitangaben und GPS-Daten.

Diese personenbezogenen Daten werden mittels einer Datenverarbeitungsanlage (vgl. EuGH, Urteil vom 11.12.2014 – C 212/13 -, Leitsatz Nr. 2; Nds. OVG Lüneburg, Urteil vom 29. 09.2014 – 11 LC 114/13 -, Rn. 29, jeweils juris) vom Kläger als nicht-öffentliche Stelle im Sinne des § 2 Absatz 4 Satz 1 BDSG erhoben und bei Bedarf verarbeitet und genutzt.

Das Verarbeiten umfasst gem. § 3 Abs. 4 Satz 1 BDSG u. a. das Speichern (§ 3 Abs. 4 S. 2 Nr. 1 BDSG) personenbezogener Daten. Der Kläger speichert die personenbezogenen Daten (zunächst) auf einem Datenträger ab. Dass der Kläger die Daten nach eigener Darstellung regelmäßig überspielt, ist unerheblich. Überdies nutzt der Kläger die personenbezogenen Daten gem. § 3 Abs. 5 BDSG durch die Vorlage bei der Polizei, der Ordnungswidrigkeitenbehörde und der Staatsanwaltschaft. Der Kläger erhebt die personenbezogenen Daten i. S. d. § 3 Abs. 3 BDSG auch hierfür, da er sie sich durch den absichtlichen Betrieb der Kameras beschafft, d. h. Verfügungsmacht über sie erhält (vgl. Plath/Schreiber in: Plath, a. a. O., § 3 BDSG, Rn. 30).

Der Kläger ist als natürliche Person überdies eine nicht-öffentliche Stelle i. S. d. § 2 Abs. 4 BDSG, da er keine hoheitlichen Aufgaben der öffentlichen Verwaltung wahrnimmt.

Die Anwendung des § 38 Abs. 5 BDSG ist nicht gem. § 27 Abs. 1 Satz 2 BDSG ausgeschlossen, da die Erhebung, Verarbeitung und Nutzung der Daten nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Zwar unterfällt die private Videoüberwachung grundsätzlich der Ausnahme für persönliche und familiäre Tätigkeiten. Werden jedoch öffentliche Räume, zum Beispiel Teile einer Straße oder ein Nachbargrundstück miterfasst, dient sie nicht mehr „ausschließlich“ persönlicher oder familiärer Tätigkeit, mit der Folge der Anwendbarkeit des Bundesdatenschutzgesetzes (Schaffland/Wiltfang, a. a. O., § 1, Rn. 22a; EuGH, Urteil vom 11.12.2014 – C-212/13 –, juris, Rn. 33). Der Kläger nutzt die Kameras, wie den dem Gericht vorliegenden Aufnahmen zu entnehmen ist, unstrittig zumindest auch, um Verkehrsordnungswidrigkeiten anderer Verkehrsteilnehmer unabhängig von einer eigenen Betroffenheit im öffentlichen Verkehrsraum zu dokumentieren. Soweit er sich dahin eingelassen hat, die Kameras zum Selbst- und Eigentumsschutz sowie zur Beweissicherung angeschafft zu haben, stellen diese Zwecke selbst bei einer möglichen eigenen Betroffenheit des Klägers von Verkehrsordnungswidrigkeiten grundsätzlich keinen ausschließlich privaten oder familiären Zweck dar. Werden Erhebung und Verarbeitung personenbezogener Daten unter dem erklärten Zweck vorgenommen, sich Beweismittel in möglichen straf- oder zivilgerichtlichen Verfahren zu beschaffen und die Aufnahmen im Bedarfsfall bei Behörden vorzulegen, wird dadurch der persönliche und familiäre Bereich verlassen (VG Ansbach, Urteil vom 12.08.2014 – AN 4 K 13.01634 –, juris, Rn. 44). Das weitere Vorbringen des Klägers, die Kameras zum weit überwiegenden Großteil für private oder familiäre Zwecke zu nutzen, ist schon wegen der festgestellten Nutzung zu anderen Zwecken unerheblich. Soweit er behauptet, Zweck des Einsatzes der onboard-Kameras sei nicht die Videoüberwachung von Verkehrsteilnehmern gewesen, sondern die Aufzeichnung von Fahrstrecken für zukünftige Motorradtouren mit seiner Frau, geben die vorliegenden Aufnahmen hierfür nichts her.

Ein Ausschluss des § 38 Abs. 5 BDSG ergibt sich auch nicht aus § 27 Abs. 2 BDSG. Danach gelten die Vorschriften des Dritten Abschnitts (Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen, §§ 27 bis 38a) nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind. Diese Ausnahmevorschrift kommt hier deshalb nicht zum Tragen, weil es vorliegend um Daten aus Datenverarbeitungsanlagen geht.

Der Betrieb der zwei Videokameras und die gleichzeitige Speicherung der erhobenen Bilddaten ist nicht durch § 6b BDSG gerechtfertigt. § 6b BDSG verdrängt für die hier vorliegende Videoüberwachung öffentlich zugänglicher Räume als abschließende *lex specialis* (s. o.) die allgemeineren Vorschriften der §§ 28, 29 BDSG (vgl. Nds. OVG Lüneburg, Urteil vom 29.09.2014, Rn. 36, a.a.O.).

Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) unter näher definierten alternativen Voraussetzungen zulässig (§ 6b Abs. 1 BDSG); die Verarbeitung und Nutzung derartiger Daten ist dabei unter in Absatz 3 dieser Vorschrift näher bestimmten Bedingungen erlaubt.

Die Videoüberwachung des Klägers unterfällt dem Regelungsgehalt des § 6 b BDSG.

Die vom Kläger genutzten Dashcams unterfallen dem Begriff der „optisch-elektronischen Einrichtung“. Die Norm erfasst aufgrund ihres nicht einschränkenden Wortlauts nicht nur ortsfeste, sondern auch mobile Geräte (so auch Becker, in: Plath, a. a. O., § 6b BDSG,

Rn. 12; OLG Stuttgart, Beschluss vom 04.05.2016 – 4 Ss 543/15 –, juris, Rn. 12, m. w. N.). Bei den Verkehrsräumen, für die eine Beobachtung in Rede steht, handelt es sich unzweifelhaft um öffentlich zugängliche Räume. Alle dem öffentlichen Verkehr gewidmeten Flächen sind öffentlich zugängliche Räume i. S. d. § 6b Abs. 1 BDSG (Becker, in: Plath, a.a.O., § 6b BDSG, Rn. 9).

Der Kläger hat mit seinen Dashcams auch den öffentlichen Verkehrsraum im Sinne von § 6b BDSG beobachtet. Unter diesem Merkmal ist die Sichtbarmachung von Geschehnissen und Personen mithilfe dazu geeigneter technischer Einrichtungen von einer gewissen Dauer – und damit eine Form des Überwachens – zu verstehen. Soweit streitig ist, ob hierunter auch bloße Kamera-Monitor-Systeme als „verlängertes Auge“ ohne nachfolgende Aufzeichnung oder Auswertung fallen (s. Nds. OVG Lüneburg, Urteil vom 29.09.2014, a.a.O. mit weiteren Hinweisen), kommt es vorliegend hierauf nicht an. Denn der Kläger hat Bildaufzeichnungen für einen bestimmten Zeitraum gespeichert, um die Möglichkeit der anlassbezogenen nachträglichen Inaugenscheinnahme der gespeicherten Videoaufnahmen zu gewährleisten. Bei den gespeicherten Daten handelt es sich um personenbezogene Daten (s.o.), so dass der notwendige Personenbezug nach § 6b Absatz 1 BDSG gegeben ist.

Die Beobachtung erfolgte auch für eine gewisse Dauer, was sich bereits anhand der Anzahl der vorliegenden Bildaufnahmen zeigt. Der Kläger hat auch nicht lediglich Einzelaufnahmen von Bildern per Videotechnik – „shot“ – (vgl. VG Schwerin, Beschluss vom 18.06.2015 – 6 B 1637/15 SN –, Rn. 30, juris) gemacht, sondern sich immer wieder mit eingeschalteten Dashcams im Straßenverkehr bewegt und dabei aufgezeichnet, so dass auch insoweit eine Videoüberwachung im Sinne von § 6b Absatz 1 BDSG vorliegt.

So hat er direkt nach der Einstellung des wegen des Vorwurfs einer unzulässigen Dashcamnutzung geführten Ordnungswidrigkeitenverfahrens innerhalb des kurzen Zeitraums von einem Monat vom 01.11.2014 bis zum 30.11.2014 fünf Verkehrsordnungswidrigkeiten mit seinen Dashcams dokumentiert und angezeigt. Dabei waren die von ihm angezeigten Rotlichtverstöße (Bl. 6, 19, 19a, 22-23 der Beilakte B VG GÖ zu 1 A 83/15) unzweifelhaft durch Videos dokumentiert. Denn auf den hierzu übersandten Aufnahmen ist ein Screenshot eines geöffneten Programms zum Abspielen und Bearbeiten von Videos zu erkennen. Auch die vom Kläger angeführten Fälle mit eigener Betroffenheit lassen den Schluss zu, dass er die Kameras anlasslos aufzeichnen lässt. Soweit er geschildert hat, ihm sei im Dezember 2015 in einer Kurve ein Fahrzeug mit sehr hoher Geschwindigkeit auf seiner Fahrspur entgegen gekommen, darf davon ausgegangen werden, dass die Dashcam des Klägers unabhängig von diesem Anlass betrieben wurde. Anders ist, zumindest ohne weitere Darlegung, nicht verständlich, aus welchem Grund eine sich derart unvorhersehbar ereignende Situation aufgezeichnet wurde. Dass der Kläger regelmäßig mit eingeschalteten Dashcams den Straßenverkehr anlasslos aufgezeichnet hat, ergibt sich insbesondere aus dem vom Landkreis Z. übersandten Datenträger mit Videodateien (Beilakten 003 und 004), die der Kläger beim ehemaligen Landkreis W. im Zusammenhang mit Verkehrsordnungswidrigkeitenanzeigen eingereicht hat. Die 20 Videodateien beinhalten Aufnahmen einzelner Verkehrsvorgänge im Zeitraum 17.03.2014 bis einschließlich Juni 2016, die der Kläger als Verkehrsverstöße angezeigt hat. Auf den Videos sind die Fahrzeuge, die Kfz Kennzeichen, selten auch die Fahrzeugführer erkennbar. Die Videos enthalten eine Datums- und Zeitangabe und GPS-Daten. Diesen Inhalt der Videos hat der Kläger in der mündlichen Verhandlung nicht bestritten.

Unter Berücksichtigung des Anzeigeverhaltens des Klägers in der Vergangenheit mit 50.000 Anzeigen von Verkehrsverstößen

in den letzten Jahren und seines ausgeprägten Interesses an der Verfolgung von Verkehrsordnungswidrigkeiten geht das Gericht davon aus, dass es sich bei den vorliegenden Videoaufnahmen lediglich um den Ausschnitt einer umfassenden Videoüberwachung des gesamten Verkehrsgeschehens durch den Kläger handelt. Die zumindest regelmäßige Aufzeichnung des Verkehrsgeschehens dient dem Kläger offensichtlich dazu, möglichst jeden Verkehrsverstoß in seiner Fahrumgebung erfassen und anschließend unter Vorlage von Beweismaterial anzeigen zu können. Seine Behauptung, er schalte seine Dashcams nur ein, wenn er selbst während des Autofahrens einen Verkehrsverstoß wahrnehme, ist lebensfremd und entspricht nicht seinem offensichtlichen Anliegen an einer umfassenden Verfolgung von Verkehrsverstößen. Dementsprechend hat der Kläger in der mündlichen Verhandlung am 31.05.2017 angegeben, dass er in der Vergangenheit nachträglich die Aufnahmen der Dashcam ausgewertet habe, um dabei ggfs. passende Aufnahmen zu von ihm im Straßenverkehr beobachteten Verkehrsverstößen zu finden. Eine Beobachtung des öffentlichen Verkehrsraums im Sinne von § 6b Abs. 1 BDSG durch den Kläger liegt damit vor. Daran würde auch nichts ändern, wenn – wie der Kläger in dem Verkehrsordnungswidrigkeitenverfahren vor dem Amtsgericht M. (S. OWi T. Js X. (Y.)) behauptet hat – einzelne der angezeigten und dokumentierten Verkehrsverstöße, insbesondere die Verkehrsverstöße vom 02.05. und 22.06.2016 (Bl. 62-64 und 68 Beiakte 001), nicht aus einer Videoaufzeichnung stammen würden, sondern es sich um Einzelbildauslösungen ohne vorherigen Monitorbetrieb handeln würde. Unerheblich ist darüber hinaus, dass auf einzelnen vorgelegten Aufnahmen weder das Kraftfahrzeugkennzeichen noch die Insassen der Fahrzeuge zu erkennen sind (vgl. Bl. 6, 19, 19a, 22, 22a, 23 Beiakte B zu 1 A 83/15). Denn auch dann liegt immer noch eine genügende Anzahl von ausreichend aussagekräftigen Videoaufnahmen vor, die die Annahme rechtfertigen, der Kläger überwache mit seinen Dashcams den öffentlichen Verkehrsraum.

Die Beobachtung ist nicht gem. § 6b Abs. 1 Nr. 1 bis Nr. 3 BDSG zulässig. Eine Zulässigkeit nach Nr. 1 und Nr. 2 scheidet offensichtlich aus. Die Videoüberwachung des Straßenverkehrs ist auch nicht nach Nr. 3 zur Wahrnehmung berechtigter Interessen des Klägers für konkret festgelegte Zwecke erforderlich.

Soweit der Kläger vorgetragen hat, die Kameras dienten seinen berechtigten Interessen wie Selbst- und Eigentumsschutz und einer diesbezüglichen Beweissicherung, kann dies den Einsatz der Kameras allenfalls in solchen Einzelfällen rechtfertigen, aber nicht die hier in Rede stehende anlasslose und regelmäßige Videoüberwachung des Straßenverkehrs. Soweit der Kläger behauptet hat, Zweck des Einsatzes der onboard-Kameras sei nicht die Videoüberwachung von Verkehrsteilnehmern gewesen, sondern die Aufzeichnung von Fahrstrecken für zukünftige Motorradtouren mit seiner Frau, geben die Videoaufnahmen dafür nichts her (s.o.). Der Kläger verfolgt mit seiner Praxis, andere Verkehrsteilnehmer zu beobachten und Verkehrsvorgänge aufzuzeichnen, um im Fall von Verkehrsverstößen Beweismaterial zu haben, keine schützenswerten eigenen Interessen, sondern tritt als Sachwalter öffentlicher Interessen auf. Die öffentliche Aufgabe der Gewährleistung eines gesetzeskonformen Straßenverkehrs obliegt ausschließlich den Straßenverkehrsbehörden und der Polizei, nicht aber privaten Dritten (so bereits Urteil der beschließenden Kammer vom 09.05.2012, Az. 1 A 114/11, Bl. 6 d. Urteilsabdruck, unveröffentlicht; Nds. OVG, Beschluss vom 23.09.2013 – 13 LA 144/12 –, juris, Rn. 10).

Aber selbst wenn man hier ein schutzwürdiges Interesse des Klägers nach § 6b BDSG annehmen würde, würden jedenfalls Anhaltspunkte bestehen, dass die schutzwürdigen Interessen der an-

deren Verkehrsteilnehmer (auch Fußgänger) mit ihrem Recht auf informationelle Selbstbestimmung die Interessen des Klägers auf Selbst- und Eigentumsschutz ohne konkrete Gefährdung überwiegen (§ 6b Absatz 1, 2. Halbsatz BDSG, vgl. VG Ansbach, a.a.O., Rn. 59). Denn für diese besteht die Gefahr, dass sie aufgrund der Anzeigen des Klägers mit im Rahmen der Videoüberwachung gewonnenen Bildaufnahmen zu Unrecht mit Ordnungswidrigkeitenverfahren überzogen werden. Die Aufgabe der Verfolgung von Ordnungswidrigkeiten oder Straftaten obliegt aber nicht dem Kläger (s.o.), sondern den hierfür zuständigen Behörden (vgl. auch § 6b Abs. 3 Satz 2 BDSG).

Ein Verstoß gegen § 6b BDSG liegt auch deshalb vor, weil der Kläger den Umstand der Beobachtung nicht gem. § 6b Abs. 2 BDSG durch geeignete Maßnahmen erkennbar gemacht hat.

Soweit der Kläger den Straßenverkehr mit seinen Dashcams nicht nur beobachtet, sondern darüber hinaus auch Aufzeichnungen verarbeitet und genutzt hat, war ihm dies nicht nach § 6b Abs. 3 Satz 1 BDSG erlaubt. Danach ist die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Diese Vorschrift kann nur so verstanden werden, dass sie ausschließlich die Verarbeitung oder Nutzung von Daten aus einer nach Absatz 1 zulässigen Videoüberwachung regelt. Daran fehlt es hier. Der Anwendungsbereich der Norm ist deshalb gar nicht eröffnet.

Demnach lagen die Eingriffsvoraussetzungen nach § 38 Absatz 5 Satz 1 BDSG vor, weil der Kläger gegen § 6b BDSG verstoßen hat.

Die von der Beklagten mit Blick hierauf getroffenen Anordnungen nach Ziffern 1.1-1.3 sind sowohl geeignet, erforderlich als auch verhältnismäßig im engeren Sinne, um zukünftig solche Verstöße zu verhindern.

Die Anordnung zu Ziffer 1.1 genügt noch dem Bestimmtheitsgebot des § 37 Abs. 1 VwVfG. Dieses verlangt, dass der maßgebliche Regelungsgehalt des Verwaltungsaktes zweifelsfrei zum Ausdruck kommt. Dabei ist nicht nur der Tenor, sondern auch die Begründung des Bescheids zu berücksichtigen.

Allein dem Wortlaut von Ziffer 1.1 lässt sich noch nicht entnehmen, in welcher Weise dem Kläger die Verwendung von Dashcams untersagt wird. Danach hat er die Nutzung von Dashcams in Kraftfahrzeugen so zu beschränken, dass eine Erhebung und Verarbeitung personenbezogener Daten anderer Verkehrsteilnehmer mit den Videokameras ausgeschlossen ist. Soweit der Kläger meint, ihm werde damit ausnahmslos die Verwendung seiner Dashcams im öffentlichen Straßenverkehr untersagt, ergibt sich aus der Begründung des Bescheids, dass dies nicht richtig ist. Denn danach wird ihm ausschließlich die „von ihm praktizierte permanente Videoüberwachung“ (s. S. 5 unten) vorgeworfen und ihm wird „lediglich die permanente Videoüberwachung des Straßenverkehrs untersagt“ (s. S. 7 unten). Ausdrücklich nicht ausgeschlossen wird, dass er die Dashcams für vom Bundesdatenschutzgesetz nicht erfasste persönliche Zwecke i.S.d. § 1 Absatz 2 Nr. 3 BDSG (identisch mit § 27 Absatz 1 Satz 2 BDSG) auch künftig weiter verwende (s. S. 7 unten). Nicht geregelt ist dagegen, ob der Kläger außerhalb der Videoüberwachung im Sinne von § 6b Abs. 1 BDSG seine Dashcams zur Aufnahme einzelner Fotos im Straßenverkehr verwenden darf. Ein solches – von der Beklagten wohl beabsichtigtes – Verbot ist Ziffer 1.1 auch unter Berücksichtigung der Begründung des Bescheids nicht zu entnehmen. Dort ist ausschließlich von einem Verbot der Videoüberwachung die Rede. An keiner Stelle wird dem Kläger darüber hinaus untersagt, mit den Dashcams einzelne Fotos zu machen. Demnach ist der Anordnung zu Ziffer 1.1 unter Berücksichtigung der Ausführungen im Bescheid nur mit ausreichender

Bestimmtheit zu entnehmen, dass dem Kläger die Nutzung von Dashcams in Fahrzeugen untersagt wird, soweit er mit den Kameras – wie in der Vergangenheit geschehen – anlasslos und mit gewisser Dauer den Straßenverkehr beobachtet und dabei mit den Kameras in unzulässiger Weise personenbezogene Daten anderer Verkehrsteilnehmer erhebt, verarbeitet und nutzt.

Ermessensfehler sind nicht ersichtlich. Die Anordnung ist geeignet zur Wiederherstellung datenschutzkonformer Zustände. Die Anordnung ist überdies erforderlich. Dem steht nicht entgegen, dass die Anordnung keine Ausnahme für eine Nutzung zu familiären oder persönlichen Zwecken enthält. Wie vom Kläger selbst vorgetragen, unterfällt eine solche Nutzung bereits nicht dem Anwendungsbereich des Bundesdatenschutzgesetzes und damit nicht dem Regelungsbereich der Beklagten. Diese war deshalb nicht zur Aufnahme einer entsprechenden Einschränkung verpflichtet. Im Übrigen hat sie in den Gründen des Bescheids klargestellt, dass eine Nutzung zu familiären und persönlichen Zwecken weiterhin möglich sei (s.o.). Nicht zu beanstanden ist auch, dass die Beklagte ihre Anordnung auf die Verwendung von Onboard-Videokameras jeden Typs und auch auf vom Kläger lediglich als Beifahrer genutzte Fahrzeuge erstreckt hat. Hätte sie hierauf verzichtet, bestünden Regelungslücken, die vom Kläger zu einer weiteren unzulässigen Videoüberwachung des Straßenverkehrs ausgenutzt werden könnten.

Die Anordnung ist auch angemessen. Die Beklagte hat zutreffend festgestellt, dass das schutzwürdige Interesse der zukünftig von den Beobachtungen und Aufzeichnungen betroffenen Verkehrsteilnehmer, nicht heimlich beobachtet und aufgenommen zu werden, höher zu bewerten ist, als das Interesse des Klägers, weiterhin Dashcams – in datenschutzwidriger Weise – zu nutzen.

Die Anordnung unter Ziff. 1.2 des Bescheides ist ebenfalls rechtmäßig. Sie beschränkt sich nach ihrem Wortlaut und auch unter Berücksichtigung der Begründung des Bescheids auf die Löschung gespeicherter Videodateien. Vom Kläger wird ausschließlich die Löschung von „Videosequenzen“ und nicht auch von Bilddateien verlangt. Ermächtigungsgrundlage für die Anordnung ist § 38 Abs. 5 Satz 1 BDSG in Verbindung mit § 35

Abs. 2 Satz 2 Nr. 1 BDSG. Danach kann die Beklagte als zuständige Aufsichtsbehörde zur Gewährleistung der Einhaltung der Vorschriften des Bundesdatenschutzgesetzes die Löschung unzulässig gespeicherter personenbezogener Daten anordnen. Die Speicherung der personenbezogenen Daten durch den Kläger ist aus den beschriebenen Gründen unzulässig. Soweit sich der Kläger auf ein berechtigtes Interesse an der Speicherung einzelner Beweisequenzen berufen hat, hat er dieses Interesse in keiner Weise substantiiert. Im Übrigen verlangt die Beklagte nur die Löschung von Daten aus den im Straßenverkehr erhobenen Videosequenzen, die nicht ausschließlich persönlichen und familiären Zwecken dienen. Solche persönlichen und familiären Zwecke hat der Kläger bisher allerdings nicht substantiiert geltend gemacht.

Auch die Anordnung zu Ziffer 1.3, mit der der Kläger zur schriftlichen Bestätigung der angeordneten Löschung innerhalb von zwei Wochen nach Unanfechtbarkeit des Bescheids verpflichtet wird, begegnet keinen rechtlichen Bedenken. Diese Anordnung steht in unmittelbarem Zusammenhang mit der Anordnung zu Ziffer 1.3 und findet ihre Rechtsgrundlage in § 38 Absatz 5 Satz 1 BDSG.

Die gemäß § 70 NVwVG i. V. m. § 65 Abs. 1 Nr. 2, Abs. 2, 67 Abs. 1, 70 Nds. SOG erfolgte Androhung von Zwangsgeldern in den Ziffern 3.1, 3.2 und 3.3 ist ebenfalls nicht zu beanstanden. Den Androhungen liegen rechtmäßige Verwaltungsakte zu Grunde. Die Höhe der angedrohten Zwangsgelder ist ebenfalls nicht zu beanstanden. Sie bewegen sich im unteren Bereich des Rahmens nach § 67 Absatz 1 Nds. SOG von mindestens 5 und höchstens 50.000 Euro.

Da die Beklagte dem Kläger ausschließlich die Videoüberwachung nach § 6b BDSG und nicht auch die datenschutzwidrige Aufnahme von Einzelbildern mittels Videotechnik im Straßenverkehr untersagt hat, war die Rechtmäßigkeit eines solchen Verbots nicht (mehr) zu prüfen. Damit war auch kein Raum für die Prüfung, ob diese Art der Datenerhebung, -verarbeitung und -nutzung nach § 4 Absatz 1 i.V.m. § 29 BDSG (Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung) gerechtfertigt wäre.

Berichte, Informationen, Sonstiges

Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation

Arbeitspapier zum Thema E-Learning-Plattformen

61. Meeting, 24.–25. April 2017, Washington D.C. (USA)

Einführung

1. E-Learning-Plattformen erfreuen sich weltweit wachsender Beliebtheit. Sie ermöglichen die Einrichtung eines „virtuellen Kursraumes“, in dem Lehrkräfte Lernmaterialien zur Verfügung stellen und Leistungsüberprüfungen durchführen können. Zudem fördern viele dieser Plattformen kollaboratives Lernen und ermöglichen die Kommunikation zwischen Lernenden und Lehrenden. E-Learning-Plattformen werden immer stärker in das Curriculum eingebunden, so dass ihre Nutzung schon bald gang und gäbe sein wird.

2. Bis vor Kurzem beschränkte sich die Leistungsbeurteilung der Lernenden und die damit verbundene Datenerhebung fast ausschließlich auf Prüfungsergebnisse und Anwesenheit. Mit dem zunehmenden Einsatz von E-Learning-Plattformen wächst die Menge an personenbezogenen Daten, die über die Lernenden zur Verfügung stehen. Diese reichen von Informationen über die Nutzung von Lernmaterialien und die Bearbeitung von Aufgaben (beispielsweise die Zeit, die investiert oder benötigt wurde, um die Aufgabe durchzulesen) bis hin zur Unterrichts- /Kursteilnahme und sonstigen bildungsbezogenen Aktivitäten (z. B. Benotung). Je stärker der Unterricht auf virtuellen Kursräumen oder elektronischen Geräten basiert, desto spezifischere und umfassendere digitale Daten werden über die Lernenden sowie ihr Verhalten und ihre Leistungen generiert. Zudem könnte die große Menge an digitalen Daten über Schüler und Studierende sowie deren Verhalten die Nachfrage nach einer verstärkten Datennutzung im Bildungsbereich ankurbeln, z. B. in Form von „Learning Analytics“¹.

3. Auf Universitärebene bieten viele Einrichtungen – oft in Partnerschaft mit Privatunternehmen – bereits sogenannte „Massive Open Online Courses“ (MOOCs) an, bei denen sich Teilnehmerinnen und Teilnehmer für Universitätskurse einschreiben können, die online abgehalten werden. Solche Kurse finden nicht in traditionellen Kursräumen statt, und mit ihnen geht häufig eine grenzüberschreitende Erhebung von personenbezogenen Daten der Teilnehmerinnen und Teilnehmer einher². Die digitalen Plattformen erfassen jede einzelne Interaktion zwischen dem/der Lernenden, der Lehrkraft und der Lernumgebung. Häufig wird weder den Lernenden noch den Lehrkräften klar sein, was mit den erhobenen Daten genau geschieht.

4. Die Sensibilität der digitalen Daten von Schülern und Studierenden sollte keinesfalls unterschätzt werden. Personenbezogene Daten zum Lernverhalten können als besonders sensibel angesehen werden, da diese Daten Informationen zu den Interessen und Fähigkeiten der Lernenden, ihrer Merkfähigkeit, ihrer Schnelligkeit bei der Aufgabenbearbeitung und ihrer Lernbereitschaft umfassen. Im Rahmen von Datenanalysen könnten diese Daten auch genutzt werden, um Prognosen in Bezug auf die berufliche Zukunft und Karrierechancen der Lernenden zu treffen³. In einigen Staaten der USA beispielsweise werden Daten aus dem primären und sekundären Bildungsbereich – also vom Kindergarten bis zum 12. Schuljahr („K 12“) – mit Arbeitnehmerdaten verknüpft⁴. Bestimmte E-Learning-Plattformen nutzen die von den Schülern und Studierenden erfassten Daten für neuartige Analysen (z. B. um Legasthenie prognostizieren zu können) und in einigen Fällen für kommerzielle Zwecke⁵. Durch die zunehmende Digitalisierung von Schüler- und Studierendendaten und den Einsatz neuer Analysetechniken sind die Lernenden einer allgegenwärtigen Beobachtung ausgesetzt, die die Grundrechte der Privatsphäre und der geistigen Freiheit massiv bedrohen können.

5. In den meisten Fällen werden die Daten, die im Zusammenhang mit E-

Learning-Plattformen verarbeitet werden, nicht bei der Schulverwaltung gespeichert. Viele Bildungseinrichtungen beauftragen externe Cloudanbieter mit der Speicherung und Verarbeitung der Schüler- und Studierendendaten. Cloudgestützte Plattformen bergen jedoch zusätzliche Datenschutz- und Sicherheitsrisiken⁶. Ein besonderes Problem kann sich aus der Kontrollverteilung zwischen den Lehranstalten und den Anbietern von E-Learning-Plattformen ergeben.⁷ Die Anbieter legen nämlich oft standardmäßige Geschäftsbedingungen fest, die ihnen mitunter sehr viel Spielraum für die Nutzung der Daten zu ihren eigenen Zwecken einräumen – und die oftmals nicht mit der Bildungsmission der Ein-

1 Learning Analytics kann bezeichnet werden als „das Messen, Sammeln, Analysieren und Auswerten von Daten über Lernende und ihren Kontext mit dem Ziel, das Lernen und die Lernumgebung zu verstehen und zu optimieren“, Learning and Academic Analytics, G. Siemens, 5. August 2011, <http://www.learninganalytics.net/?p=131>.

2 Steve Kolowich: „Are MOOC-Takers ‚Students‘? Not When It Comes to the Feds Protecting Their Data“, THE CHRONICLE OF HIGHER EDUCATION, 3. Dezember 2014, <http://chronicle.com/article/Are-MOOCtakers-Students-/150325>.

3 Singapur beispielsweise arbeitet an der Entwicklung einer „Total Online Learning Solution“, die Aus- und Weiterbildungs- mit Lerndaten kombiniert. Jedem Schüler wird bereits im Kindergarten ein sogenannter „Learning Record Store“ zugewiesen, der alle Lerndaten erfasst; vgl. Frankfurter Allgemeine Zeitung (FAZ) vom 28. Januar 2016, S. 9: „Fürs Überleben lernen wir. Was Unternehmen aus Lerndaten ableiten können“.

4 Siehe beispielsweise National Center for Education Statistics: „SLDS Topical Webinar Summary: Linking K12 Education Data to Workforce“, 28. August 2014; https://nces.ed.gov/programs/slds/pdf/Linking_K12_Education_Data_to_Workforce_August2014.pdf.

5 Niederländische Datenschutzaufsichtsbehörde (College bescherming persoonsgegevens): Fall z2013-00795, 14. Juli 2014. Schlussfolgerungsbericht: „Onderzoek CBP naar de verwerking van persoonsgegevens door Snappet“ (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf).

6 Vgl. Arbeitspapier Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes – „Sopot Memorandum“ – 51. Sitzung, 23.–24. April 2012, Sopot (Poland), S. 1–3; https://datenschutzberlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf.

7 Ariel Bogle: What the Failure of inBloom Means for the Student-Data Industry, SLATE, 24. April 2014; http://www.slate.com/blogs/future_tense/2014/04/24/what_the_failure_of_inbloom_means_for_the_student_data_industry.html.

richtung vereinbar sind. Zudem könnten bestimmte Anbieter nicht gewillt sein, wesentliche Pflichten zu erfüllen (z. B. im Zusammenhang mit der Datensicherheit) oder sich an Beschränkungen zu halten (beispielsweise in Verbindung mit grenzüberschreitenden Datenübermittlungen), was jedoch unerlässlich ist, um das erforderliche Maß an Schutz gewährleisten zu können.

Umfang

6. Im Rahmen dieses Dokuments wird „E-Learning“ als Nutzung technischer Instrumente und Medien verstanden, die die Kommunikation von Wissen, die Wissensentwicklung sowie die Interaktion zwischen Lehrkräften, Lernenden und Lehranstalten technisch unterstützt. E-Learning-Plattformen beziehen in der Regel eine Vielzahl von Geräten (z. B. Computer und Tablets), Datenverarbeitungssowie Nutzungsmodellen (Präsenzschulungen, Onlinekurse usw.) und Akteuren (beispielsweise Lernende, Bildungseinrichtungen, Plattformanbieter und Anwendungsanbieter) ein.

7. Dieses Arbeitspapier beleuchtet die größten Datenschutzrisiken, die E-Learning-Plattformen für die Lernenden bergen, und stellt Empfehlungen für Lehranstalten, Anbieter von E-Learning-Plattformen und Datenschutzbehörden bereit. Mögliche Datenschutzrisiken für Lehrkräfte im Zusammenhang mit der Nutzung von E-Learning-Plattformen (z.B. Leistungsbewertung von Lehrkräften) werden nicht berücksichtigt. Im Zentrum dieses Arbeitspapiers steht die zunehmende Nutzung von E-Learning-Plattformen in der Primar- und Sekundarbildung.

Datenschutzrisiken für die Lernenden

Unrechtmäßige Verarbeitung und fehlende Transparenz

8. In Gesetzen im Schul- und Bildungsbereich werden neue technologische Trends bei Lernverfahren sowie der erweiterte Umfang und die umfassenderen Zwecke der Datenverarbeitung im Zusammenhang mit E-Learning und Learning Analytics oft nicht hinreichend berücksichtigt. Ob die Einwilligung als gültige Rechtsgrundlage angesehen werden könnte, ist ebenfalls fraglich. Eine wirksame Einwilligung muss freiwillig erteilt werden, was im Bildungskontext

nur schwer garantiert werden kann – vor allem, wenn die Nutzung von E-Learning-Plattformen verpflichtend ist. Deshalb könnte die Erfassung und Analyse von Schüler- und Studierendendaten in einigen Rechtssystemen ohne die nötige Rechtsgrundlage erfolgen, wenn die Gesetzgeber die Rechte zum Schutz der Privatsphäre und die Datenschutzrechte bei der Datenverarbeitung im Rahmen von E-Learning-Plattformen und Learning Analytics nicht ausreichend abgesichert haben.

9. Die Erhebung oder Nutzung von Schüler- und Studierendendaten erfolgt unter Umständen ohne Wissen der Lehrkräfte, Bildungseinrichtungen, Eltern oder Lernenden. Darüber hinaus sind den Lernenden, Eltern oder Lehrkräften die an der Datenverarbeitung beteiligten Akteure meist nicht bekannt. Der Mangel an Transparenz wirkt sich direkt auf die Frage der Rechtmäßigkeit der Verarbeitung und des Grundsatzes der Verarbeitung nach Treu und Glauben aus.

Übermäßige Datenerhebung

10. Die Lernenden könnten von einer übermäßigen Erhebung personenbezogener Daten betroffen sein. Es könnten sehr persönliche oder sensible Informationen über sie erfasst sein, wie etwa Standortinformationen, Gesundheitszustand, Schlafverhalten oder Aktivitäten in sozialen Netzwerken⁸. Sportlehrer könnten beispielsweise Tracking- und Auswertungstools einsetzen, die auch gesundheitsbezogene Gewohnheiten und Verhaltensweisen außerhalb des Unterrichts überwachen. Bildungseinrichtungen könnten bei ihren Anstrengungen zur Bekämpfung von Cybermobbing versucht sein, die Aktivitäten der Schüler und Studierenden in sozialen Netzwerken zu beobachten. Mit solchen Aktivitäten würden sie unangemessen in das Privatleben der Schüler und Studierenden eingreifen. In diesen Zusammenhängen ist es wichtig, den Verhältnismäßigkeitsgrundsatz zu beachten, insbesondere wenn es um Maßnahmen geht, die sich auf Aktivitäten von Schülern und Studierenden außerhalb des Bildungskontextes erstrecken.

11. Im Zusammenhang mit Learning Analytics kann der Umfang an Informationen, die über die Lernenden angefordert werden, sogar noch größer sein.

Bestimmte Analysetools nutzen Informationen über Aktivitäten in sozialen Netzwerken, Protokolle von Online-Spielen, Online-Communitys und von physiologischen Sensoren erfasste Daten, wie etwa Eye-Tracking- oder Motion-Capture-Daten. Hierbei können Datensätze zu kognitiver Entwicklung, sozialem Lernen, Diskursverläufen, Interaktionen in einem Netzwerk, Lernpfade in Kursen, Ausbau von Kompetenzen und Verhalten bei der Suche nach Hilfe von Interesse sein⁹.

Profiling und automatisierte Entscheidungsfindung

12. Die Art und Menge der mithilfe von E-Learning-Plattformen erfassten Daten erleichtert statistische Analysen und die Erstellung von Profilen. Dies kann zur Folge haben, dass die Lernenden zunehmend auf Grundlage von Gruppenprofilen und nicht mehr aufgrund ihrer individuellen Entwicklung bewertet werden.

13. Bildungseinrichtungen haben zudem keine Kontrolle über die Algorithmen, die im Rahmen von Learning-Analytics-Verfahren genutzt werden, und sie überlassen es den Anbietern der E-Learning-Plattformen festzulegen, was die Clickstream-Daten der Schüler und Studierenden über ihren Wissensstand aussagen. Das bedeutet, dass die Lehrkräfte Entscheidungen auf Grundlage von Interpretationen treffen müssen, die sie nicht überprüfen können.

14. E-Learning-Anbieter und andere Unternehmen nutzen die von den Lernenden erfassten Daten, um subjektive Einschätzungen über deren „Geselligkeit“ und „Enthusiasmus“ zu treffen¹⁰. Die menschlichen Tätigkeiten innewohnende Fehleranfälligkeit bei der Datenerzeugung und auch Systementwicklung können zu ungerechten Ergebnissen für die Lernenden führen, insbesondere für Angehörige von Gruppen, die bereits in der Vergangenheit Diskriminierungen

8 Khaliah Barnes: Student Data Collection Is Out of Control, N.Y. TIMES, 25. September 2014; <http://www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning/student-datacollection-is-out-of-control>.

9 „Editorial: Datasets for Learning Analytic“, Journal of Learning Analytics, 3 (3), 307–311, 2016; <http://dx.doi.org/10.18608/jla.2016.32.15>.

10 Natasha Singer: Deciding Who Sees Students' Data, N.Y. TIMES, 5. Oktober 2013; <http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html?pagewanted=all>.

erlebt haben. Folgerungen und Beurteilungen in Bezug auf die Lernenden, die nichts mit akademischer Leistung zu tun haben, könnten die Betroffenen stigmatisieren und ihre Bildungschancen einschränken.

15. Eltern, Schüler und Studierende haben unter Umständen weder Zugriff auf die Daten, die für die Entscheidungsfindung herangezogen werden, noch auf Informationen über den Prozess der Entscheidungsfindung (Funktionsweise der Analysen) oder die Schlussfolgerungen, die den in Bezug auf den Lernenden getroffenen Entscheidungen zugrunde liegen (z. B. bei der Benotung oder Feststellung potenzieller Lernschwierigkeiten). Dies gilt vor allem für den Einsatz von proprietären Algorithmen, deren Methodik undurchschaubar ist, oder für Systeme, die selbstlernend konzipiert sind, so dass selbst die Entwickler des Systems möglicherweise nicht mehr nachvollziehen können, wie eine bestimmte Beurteilung zustande kommt.

16. Problematisch ist es zudem, wenn es an Mechanismen fehlt, die die Beachtung von Treu und Glauben im Entscheidungsfindungsprozess gewährleisten und die Lernenden und Eltern die Möglichkeit geben, die Beurteilungen anzufechten¹¹.

Schleichende Funktionserweiterung

17. Privatunternehmen, die mithilfe von E-Learning-Plattformen Daten über die Lernenden erheben, könnten diese Informationen außerhalb des Bildungsbereichs für Data-Mining-Zwecke nutzen¹². So könnten die Daten beispielsweise genutzt werden, um in der Welt außerhalb der Bildungseinrichtung Entscheidungen über die Zukunftschancen der Lernenden zu treffen, z. B. in Bezug auf Beruf, Wohnmöglichkeiten und Kreditwürdigkeit¹³.

Unzureichende Sicherheit

18. Bildungseinrichtungen und Anbieter von E-Learning-Plattformen könnten es versäumen, die von den Lernenden erfassten Daten angemessen zu schützen¹⁴. Schüler- und Studierendendaten sind immer wieder von Datenlecks betroffen, unabhängig davon, ob sie von der Bildungseinrichtung selbst gespeichert oder an private Anbieter bzw. staatliche Stellen übermittelt werden¹⁵. Derartige Datenlecks können beispielsweise durch die Nutzung unsicherer An-

meldeverfahren, eine schlechte Konfiguration der Plattform oder anderweitiges menschliches Versagen verursacht werden. Lernende, Lehrkräfte und Administratoren könnten zudem motiviert sein, Sicherheitsvorkehrungen für ihre eigenen Daten (oder die Daten anderer) zum Zwecke des Missbrauchs zu umgehen (z. B. zur Änderung von Noten).

Mangelnde Rechenschaft

19. Gibt es keine klare Verteilung der Rollen und Verantwortlichkeiten an die im Zusammenhang mit dem Einsatz einer E-Learning-Plattform beteiligten diversen Akteure, könnte dies dazu führen, dass weder die Bildungseinrichtungen noch die Anbieter von E-Learning-Plattformen die notwendigen Maßnahmen ergreifen, um Datenschutz- und Datensicherheitsrisiken zu minimieren.

20. Für die Eltern und Lernenden gibt es ggf. keinen zentralen Ansprechpartner, der sich um die Risiken des Schutzes der Privatsphäre und des Datenschutzes kümmert.

Anpassungszwang

21. Das Wissen, dauerhaft beobachtet zu werden, und die Angst vor einem künftigen Missbrauch oder vor der Offenlegung der Daten können eine abschreckende Wirkung haben und die schöpferische Entfaltung und Ausdrucksfähigkeit während der geistigen Entwicklung eines Kindes behindern. Die Lernenden fühlen sich unter Umständen gezwungen, traditionelle Normen zu befolgen, und schrecken vor der Entwicklung innovativer Ideen zurück, da sie befürchten, ihre unkonventionelle Herangehensweise könnte dokumentiert und ihnen dann später irgendwann vorgehalten werden.

Empfehlungen für Bildungseinrichtungen und Anbieter von E-Learning-Plattformen

22. Trotz der Herausforderungen, die die Nutzung von E-Learning-Plattformen in Bezug auf den Datenschutz mit sich bringt, ist es möglich, diese Arten von Plattformen zu nutzen, ohne bedeutende datenschutzrechtliche Grundsätze zu verletzen. Die Arbeitsgruppe gibt Bildungseinrichtungen und E-Learning-Anbietern die folgenden Empfehlungen, um den beschriebenen Datenschutz- und Sicherheitsrisiken vorzubeugen.

23. Bildungsanstalten sollten bei der Auswahl von E-Learning-Plattformen darauf achten, dass die Anbieter ausreichende Garantien vorsehen, die sicherstellen, dass die Privatsphäre und die Datenschutzrechte der Lernenden in angemessenem Maße geschützt sind.

24. Sowohl Bildungseinrichtungen als auch Plattformanbieter sollten sich über die für sie geltenden rechtlichen Rahmenbedingungen des Datenschutzes sowie über vorhandene Orientierungshilfen informiert halten, die beispielsweise von Datenschutzbehörden herausgegeben werden¹⁶.

11 Siehe Marc Rotenberg und Khaliah Barnes: Student and Data Privacy, N.Y. TIMES, 3. Mai 2014; <http://www.nytimes.com/2014/05/04/business/students-and-data-privacy.html>.

12 Google beispielsweise gab zu, E-Mails von Lernenden gelesen zu haben, die das Unternehmen über seine beliebte Plattform Google Apps for Education erfasst hatte. Vgl. Benjamin Herold: Google Under Fire for Data-Mining Student Email Messages, EDUCATION WEEK, 26. März 2014; <http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html>.

13 In den USA werden beispielsweise bereits Rabatte für gute Leistungen angeboten: So werden anhand der Noten der Lernenden Rabatte bei Autoversicherungen berechnet. Siehe beispielsweise STATE FARM: Coverage Options That Fit You; <https://www.statefarm.com/insurance/auto/discounts>.

14 Siehe z. B. Natasha Singer: Uncovering Security Flaws in Digital Education Products for School Children, N.Y. TIMES, 8. Februar 2015, auf Seite B1, verfügbar unter: <http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html>; D.C. Special Education Students' Confidential Info Was Publicly Accessible for Years, WTOP (4. Februar 2015, 5:15 Uhr Ortszeit), <http://wtop.com/dc/2015/02/d-c-special-education-students-confidential-info-publicly-accessible-years/>; Benjamin Herold: Danger Posed by Student-Data Breaches Prompts Action, EDUCATION WEEK, 22. Januar 2014; http://www.edweek.org/ew/articles/2014/01/22/18dataharm_ep.h33.html.

15 Natasha Singer: Data Security Is a Classroom Worry, Too, N.Y. TIMES, 22. Juni 2013, auf Seite BU1, verfügbar unter: <http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html>.

16 So hat die spanische Datenschutzbehörde z. B. vor Kurzem einen Bericht veröffentlicht, in dem die Ergebnisse einer amtlichen Untersuchung von Cloud-Diensten im Bildungsbereich zusammengefasst sowie für alle relevanten Akteure eine Reihe von Empfehlungen bereitgestellt wird. Dabei wird auf Themen wie Sicherheit, Speicherort, Vertragsklauseln, die Beziehung zwischen verantwortlicher Stelle und Auftragsverarbeiter sowie Informationen für Benutzer, Cloud-Dienste und mobile Apps eingegangen. Vgl. http://www.agpd.es/portalwebAGPD/canal/documentacion/publicaciones/comun/Guias/Inspeccion_cloud_edu_cacion.pdf (in spanischer Sprache). Zudem hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder jüngst eine Orientierungshilfe für die Nutzung von E-Learning-Plattformen in Schulen herausgegeben, vgl. https://datenschutz-berlin.de/attachments/1220/OH_Lernplattform_neu.pdf.

25. Bildungseinrichtungen müssen die Einwilligung der Eltern einholen, sofern erforderlich.

26. Bildungseinrichtungen und Anbieter von E-Learning-Plattformen sollten nur so viele Daten von Schülern und Studierenden erheben, wie zur Erreichung des spezifischen Zweckes notwendig ist.

27. Bildungseinrichtungen und E-Learning-Anbieter sollten sicherstellen, dass die Zwecke, zu denen sie Daten erheben, klar festgelegt sind. „Bildungszwecke“ und „Bildungsqualität“ sind beispielsweise sehr schwammige Begriffe, die eine übermäßige Datenerhebung zulassen. Eine gezieltere Erfassung z. B. kann dadurch erreicht werden, dass spezifiziert wird, dass die Datenerhebung erforderlich ist, um „die Lesekompetenz von Fünftklässlern zu fördern“ oder „die Leistung von Oberstufenschülern in Physik zu verbessern“.

28. Bildungseinrichtungen und Anbieter von E-Learning-Plattformen sollten ihre jeweiligen Rollen, Verantwortlichkeiten und Rechte klar zuweisen. Bildungseinrichtungen sollten sicherstellen, dass in der Vereinbarung mit dem E-Learning-Anbieter festgelegt wird, dass dieser Schüler- und Studierendendaten nur gemäß den Anweisungen der Bildungseinrichtung verarbeiten darf. Auch Themen wie Datensicherheit, Ort der Datenverarbeitung und die Möglichkeit, unabhängige Audits durchzuführen, sollten berücksichtigt werden¹⁷.

29. Anbieter von E-Learning-Plattformen sollten Schüler- und Studierendendaten nur für die explizit von der Bildungseinrichtung genehmigten Zwecke erheben, nutzen oder übermitteln. Zudem sollten Plattformanbieter die von Schülern und Studierenden erhobenen Daten nicht länger aufbewahren, als es für die Erfüllung der zulässigen Bildungszwecke erforderlich ist¹⁸.

30. Studierende und Eltern haben ein Recht auf leicht zugängliche und klare Informationen über Datenschutz- und Sicherheitspraktiken. Bildungseinrichtungen und E-Learning-Anbieter sollten Informationen über die Kategorien der erhobenen Daten, die Zwecke, zu denen die Daten verarbeitet werden, die an der Verarbeitung beteiligten Akteure, die

Dauer der Datenspeicherung und getroffene Sicherheitsvorkehrungen öffentlich bereitstellen.

31. Bildungseinrichtungen müssen sicherstellen, dass sie die volle Kontrolle über Bewertungen oder Beurteilungen im Zusammenhang mit Studierenden behalten, insbesondere im Falle automatisierter Entscheidungsfindung.

32. Bildungseinrichtungen, Plattformanbieter und andere beteiligte Unternehmen sollten bei der Nutzung von Algorithmen und Profilen, die die Entscheidungsfindung beeinflussen könnten, auf lückenlose Transparenz achten. Studierende und Eltern müssen über alle verwendeten Systeme zur automatisierten Entscheidungsfindung oder über sonstige regelbasierte Systeme sowie über die den Entscheidungen zugrundeliegenden Schlussfolgerungen aufgeklärt werden.

33. Algorithmen, Protokolle, Designs und Implementierungen sollten für externe Überprüfungen und/oder Tests zur Verfügung gestellt werden. Offene Audits oder Prüfungen, die von vertrauenswürdigen Instanzen durchgeführt werden, können Gewissheit darüber bringen, dass die E-Learning-Technologie tatsächlich alle versprochenen Merkmale aufweist und keine ungerechten oder diskriminierenden Ergebnisse abliefern.

34. Bildungseinrichtungen und Anbieter von E-Learning-Plattformen sollten datenschutzfördernde Techniken (Privacy Enhancing Technologies (PET)) einbauen, die die Erhebung personenbezogener Daten von Schülern und Studierenden auf ein Minimum beschränken oder ganz verhindern. Wenn möglich, sollten Daten gemäß den Grundsätzen der Datenminimierung, des Datenschutzes durch Technik und der datenschutzfreundlichen Voreinstellungen pseudonymisiert, anonymisiert oder gelöscht werden. Bildungseinrichtungen sollten in Betracht ziehen, die Nutzung der Plattform nur unter Verwendung eines Pseudonyms zu erlauben und die echten Namen der Lernenden nicht an den Plattformanbieter weiterzugeben.

35. Bei der Erhebung von Schüler- und Studierendendaten sollten die Datenverantwortlichen die Aufbewahrungs-

fristen für die verschiedenen Kategorien von Daten explizit festlegen und anwenden, um zu gewährleisten, dass die Daten nicht länger als nötig gespeichert werden.

36. Lernende und Eltern sind berechtigt, Zugang zu den Schüler- bzw. Studierendendaten und zu anderen gespeicherten personenbezogenen Daten (z. B. Informationen zum Verhalten) zu erhalten und zu korrigieren, unabhängig davon, wer die Informationen erhebt oder verwaltet.

37. In Bezug auf automatisierte Einzelentscheidungen sollten die Lernenden Zugang zu der Entscheidung und die ihr zugrundeliegenden Schlussfolgerungen erhalten. Es müssen spezifische Verfahren vorgesehen sein, die zu einer Überprüfung von Entscheidungen durch einen Menschen führen, wenn eine andere Sicht eingebracht, Gegendarstellungen vorgebracht oder Entscheidungen angefochten werden.

38. Die Bildungseinrichtungen sollten Situationen vermeiden, in denen sich die Betroffenen gefangen fühlen, etwa wenn die Verarbeitung personenbezogener Daten durch Plattformanbieter eine Black-Box für Schüler und Studierende darstellt, die den Betroffenen keinerlei Transparenz und Kontrolle bietet. Anbieter von E-Learning-Plattformen sollten die Portabilität von Daten in strukturierten, maschinenlesbaren und offenen Formaten ermöglichen (z. B. im Falle eines Schulwechsels).

39. Schüler und Studierende treffen gelegentlich – ohne sich ausreichend informiert zu haben – schlechte Entscheidungen, die sie im Erwachsenenalter beeinträchtigen können. Das Konzept des Rechts auf Vergessenwerden wurde bereits in einigen gesetzlichen Regelwerken berücksichtigt, um die negativen Konsequenzen schlech-

17 Nähere Informationen finden Sie im Arbeitspapier Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes – „Sopot Memorandum“ – der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation, 51. Sitzung, 23.–24. April 2012, Sopot (Poland), S. 3–6; https://datenschutzberlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf.

18 Siehe auch Student Privacy Pledge: „K-12 School Service Provider Pledge to Safeguard Student Privacy“; <https://studentprivacypledge.org/wp-content/uploads/2014/09/Student-Privacy-Pledge-V1.pdf>.

ter Entscheidungen zu minimieren. Bildungseinrichtungen sollten die Schüler und Studierenden über ihre Rechte aufklären und ihr Bewusstsein für mehr Achtsamkeit bei der Veröffentlichung und Weitergabe personenbezogener Daten schärfen. E-Learning-Anbieter sollten Tools integrieren, die eine effektive Ausübung des Rechts auf Vergessenwerden ermöglichen.

40. Bildungseinrichtungen und Plattformanbieter sollten die Daten von Schülern und Studierenden nur in der Form erheben, nutzen und übermitteln, wie es der Kontext zulässt, in dem die Lernenden die Daten bereitstellen. Daten, die sich auf die Nutzung der E-Learning-Plattform beziehen, sollten für keine unvereinbaren anderen Zwecke verwendet oder zur Verfügung gestellt werden.

41. Bildungseinrichtungen sollten eine Datenschutz-Folgenabschätzung und eine Risikoanalyse durchführen, bevor sie eine E-Learning-Plattform einsetzen, sowie die auf Grundlage der dabei ermittelten Ergebnisse notwendigen technischen und organisatorischen Maßnahmen treffen, bevor und solange sie die Dienste einer solchen Plattform in Anspruch nehmen. Die technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit sollten kontinuierlich überwacht und optimiert werden.

42. Bildungseinrichtungen und E-Learning-Anbieter sollten eine Zweifaktor-Authentifizierung beim Anmeldevorgang für Administratoren und Lehrkräfte verwenden, um dem Missbrauch durch gestohlene Passwörter vorzubeugen. Es sollten Richtlinien für Zugriffskontrolle und Protokollierun-

gen festgelegt und durchgesetzt werden, um sicherzustellen, dass der Zugriff auf personenbezogene Daten angemessen verwaltet und kontrolliert wird. Der Zugang zu personenbezogenen Daten sollte auf dem sogenannten „Need-to-know-Prinzip“ (Kenntnis nur bei Bedarf) basieren.

43. E-Learning-Anbieter sollten Bildungseinrichtungen, Studierende, Schüler und deren Eltern sowie die zuständigen Aufsichtsbehörden im Falle einer Datenschutzverletzung gemäß der jeweils geltenden gesetzlichen Meldepflicht benachrichtigen¹⁹.

Empfehlungen für Datenschutzbehörden

44. Datenschutzbehörden sollten ihre Anstrengungen zur Bewusstseins-schärfung verstärken und Bildungseinrichtungen beraten. So könnten sie beispielsweise die Anwendung von Grundsätzen des Datenschutzes durch Technik bei E-Learning-Anbietern fördern und gleichzeitig ihre Aufsichts- und Kontrolltätigkeiten intensivieren (z. B. durch Durchführung von groß angelegten Datenschutzprüfungen, sogenannten „Privacy Sweeps“).

45. Die für den Datenschutz zuständigen Behörden sollten die Implementierung von Verhaltensregeln und Datenschutz-Zertifizierungsverfahren sowie die Erstellung eines angemessenen Rahmenwerks und geeigneter Tools für Datenschutz-Folgenabschätzungen unterstützen, um die Entwicklung datenschutzfreundlicher Lösungen zu fördern.

Empfehlungen für politische Entscheidungsträger

46. Wo es an klaren gesetzlichen Regelungen für die Erhebung, Verarbei-

tung und Nutzung von Schüler- und Studierendendaten fehlt, sollten solche Regeln festgelegt werden.

47. Werden in bestehenden Gesetzen neue technologische Trends bei Lernverfahren sowie der erweiterte Umfang und die umfassenderen Zwecke der Datenverarbeitung im Zusammenhang mit E-Learning sowie die darauf basierenden Entscheidungen nicht hinreichend berücksichtigt, sollten die Gesetze dahingehend überarbeitet werden²⁰.

48. Außerdem sollten politische Entscheidungsträger dafür sorgen, dass der Datenschutz zum Bestandteil von Studienprogrammen und Lehrplänen wird²¹.

19 Siehe beispielsweise die Festlegungen der OECD bezüglich des Meldens von Datenschutzverstößen im „The OECD Privacy Framework“, OECD 2013, verfügbar unter: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

20 EPIC hat ein Rahmenwerk mit dem Titel „Student Privacy Bill of Rights“ entworfen, das auf traditionellen Datenschutzgesetzen aufbaut. Vgl. EPIC: Student Privacy Bill of Rights, <https://epic.org/privacy/student/bill-of-rights.html>. Das Rahmenwerk „Student Privacy Bill of Rights“ hat zahlreiche Bestimmungen aus der Richtlinie 95/46/EG und der Konvention Nr. 108 des Europarates übernommen, einschließlich der Zweckbestimmung, den Anforderungen an die Datensicherheit und der Pflicht zur Gewährleistung der Richtigkeit von Daten für diejenigen, die die Daten speichern. Siehe Khaliah Barnes: Why a ‘Student Privacy Bill of Rights’ is Desperately Needed, WASHINGTON POST, 6. März 2014; <https://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/>.

21 ICDPPC 38, „Resolution for the Adoption of an International Competency Framework on Privacy Education“, Marrakesch 2016; <https://icdppc.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacyeducation.pdf>.

Literaturhinweise

Eßer/Kramer/von Lewinski (Hrsg.) DS-GVO / BDSG – Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze, Heymanns Kommentare, 5. Aufl. 2017, 2404 S., gebunden, 149,- €.

Der von Eßer/Kramer/von Lewinski herausgegebene Praxiskommentar, der 2014 unter der Bezeichnung Auernhammer ein erfolgreiches Comeback gefeiert hat, wurde jetzt um eine Kommentierung der DS-GVO ergänzt. Sie umfasst etwa ein Drittel des nunmehr 2267 Seiten umfassenden Gesamtwerkes, das sich nunmehr in drei Teile gliedert: Die Kommentierung der neuen Datenschutz-Grundverordnung, das noch geltende Bundesdatenschutzgesetz inkl. Ausblick, wo sich künftig welche Regelung in der DS-GVO wiederfinden wird, und in die sogenannten Nebengesetze wie das Telemediengesetz und das Telekommunikationsgesetz. Darüber hinaus gibt der Titel eine Einführung in die EU-Datenschutzrichtlinie für Polizei und Justiz. Insgesamt 16 Kenner des Datenschutzrechts in Wissenschaft und Praxis waren an der Überarbeitung beteiligt.

Nicht berücksichtigt werden konnte die nunmehr verabschiedete und zeitgleich mit der DS-GVO Geltung erlangende Neufassung des BDSG. Eine digitale Vollkommentierung des neuen BDSG ist für 2018 angekündigt und soll Bestandteil der Onlineausgabe des Kommentars auf Jurion werden.

Bei allen Veränderungen bleibt das Wesentliche des Klassikers aber gleich: Der Leser findet weiter in bewährter Qualität und wissenschaftlicher Gründlichkeit die gewohnte praxisgerechte Hilfestellung, die aber auch zu recht aufzeigt, dass manche Regelungen der Verordnung interpretationsfähig sind und in ihrer Anwendung von den entscheidenden Worten der Europäischen Datenschutzausschusses bzw. letztendlich des EuGH abhängen. Auch zu deren Meinungsbildung sollte der Kommentar ein Beitrag sein. Gleiches

wird der Fall sein für die Neuauflagen der bereits erschienenen und erst noch angekündigten DS-GVO/BDSG n.F.

(Prof. Peter Gola)

Schaffland/Wiltfang, **Datenschutz-Grundverordnung (DS-GVO)/ Bundesdatenschutzgesetz (BDSG)**, bearbeitet von Schaffland/Holthaus/Schaffland, Schmidt, Erich (Verlag), Loseblattwerk, 2017, 2650 S., Kommentar mit Abonnement, 112,- €.

Auch der Schaffland/Wiltfang hat sich mit geänderten dreiköpfigen Autorenteam der DS-GVO angenommen und in seiner Loseblattsammlung Kommentierungen zunächst bis zu den Art. 36 vorgelegt.

Indem EU-, Bundes- und Landesdatenschutzrecht systematisch integriert und laufend aktualisiert wird, bietet Ihnen das Werk

- eine umfassende und fundierte Kommentierung der DS-GVO, startend mit einer umfangreichen Grundlieferung, die in mehreren Folgeupdates zügig erweitert wird,
- die Fortführung der bewährten Kommentierung zum BDSG bis zum 25. Mai 2018,
- eine sukzessive umfassende Kommentierung des dann geltenden BDSG (neu),
- einschlägige Regelungstexte der Landesdatenschutzgesetze und Auszüge aus vom BDSG tangierten Gesetzen.

Neben einer leicht verständlichen Synopse zu bisherigem und neuem Recht enthält es Wertungen zu Auswirkungen der DS-GVO auf die künftige Rechtslage – unter Beachtung des neuen BDSG. Innerhalb der DS-GVO-Erläuterungen werden neues Recht und die bisherige Rechtslage übersichtlich gespiegelt.

(Schriftleitung)

Lutz Orgelmann, Die rechtlichen Grenzen der Nutzung von E-Books. Eine vergleichende Untersuchung aus Sicht des Verbrauchers unter Berücksichtigung der Besonderheiten des Kulturguts Buch, Schriften zum Bürgerlichen Recht (BR), Band 473, Duncker & Humblodt, Berlin, 2017, 282 S. Print: 89,90 €, E-Book: 79,90 €, Print & E-Book: 107,90 €.

Das Kulturgut Buch befindet sich in einem ständigen Wandel. Nach der Erfindung des Buchdrucks durch Gutenberg dürfte das E-Book die größte Revolution darstellen. Das Werk des Autors kann nunmehr über das Internet ohne Datenträger verbreitet werden.

Nach dem Willen des Gesetzgebers besteht ein erhebliches öffentliches Interesse an einer gesicherten Versorgung der Bevölkerung mit diesem besonderen Gut. Dabei stellen das Urheberrecht und die Vertragsbedingungen der Anbieter über Generationen anerkannte und gewollte Umgangsformen mit diesem Werk in Frage. Niemand hegt Zweifel daran, dass ein klassisches Buch verliehen, verschenkt oder an ein Antiquariat veräußert werden darf. Auf das E-Book ist diese Wertung nicht ohne weiteres übertragbar.

Die Arbeit untersucht umfassend die urheberrechtlichen Fragestellungen, um auf dieser Grundlage das Vertragsverhältnis zwischen Kunde und Anbieter unter Berücksichtigung des Verbraucherrechts zu beleuchten.

(Schriftleitung)

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.

Abel, Ralf. B., Lösch- und Sperrkonzepte nach der DS-GVO, Ping 2017, S. 177

Der Beitrag geht der Frage nach, für welche Zeitdauer personenbezogene Daten unter der Regie der DS-GVO gespeichert und ggf. verwendet werden dürfen. Ergebnis ist, dass die DS-GVO für alle Verarbeitungsvorgänge die Festlegung abstrakter oder konkreter Speicherfristen fordert, die den Dokumentations- und Transparenzpflichten unterliegen.

Bergt, Matthias, Sanktionierung von Verstößen gegen die Datenschutz-Grundverordnung, DuD 2017, S. 555

Aufgezeigt wird, wie unter der DS-GVO Datenschutzverstöße künftig sanktioniert werden, um dem Datenschutzrecht mehr Durchsetzungskraft zu verhelfen.

Gola, Peter/Klug, Christoph, Die Entwicklung des Datenschutzrechts im ersten Halbjahr 2017, NJW 2017, S. 2593

Die Autoren geben ihren seit Erscheinen des BDSG erscheinenden Übersichtsaufsatz vor.

Hartung, Jürgen/Büttgen, Lisa, Die Auftragsverarbeitung nach der DS-GVO, DuD 2017, S. 549

Ausführlich belegt wird u.a., dass die Privilegierungswirkung der Datenweitergabe an den Auftragsdatenverarbeiter auch unter der DS-GVO fortbesteht.

Marschall, Kevin, Meldepflichten nach der DS-GVO, Datenschutz Praxis, 8/2017, S. 1

Der Beitrag gibt übersichtliche Hinweise wie bei Datenschutzpannen nach der DS-GVO zu verfahren ist.

Lachenmann, Matthias, Neue Anforderungen an die Videoüberwachung, ZD 2017, S. 407

Der Autor beleuchtet kritisch die Neuregelungen zur Videoüberwachung in der DS-GVO und dem BDSG 2018, wobei er § 4 als europarechtswidrig bewertet.

Lantwien, Tobias, Risikoberuf Datenschutzbeauftragter?, ZD 2017, S. 411

Der Autor geht Haftungsmöglichkeiten des DSB nach der DS-GVO nach und kommt zu dem Ergebnis, dass die bisherigen nur eingeschränkt bestehenden zivil- und strafrechtlichen Haftungsmöglichkeiten nicht vergrößert werden.

Moos, Flemming, Die Entwicklung des Datenschutzrechts im Jahr 2016, K&R 2017, S. 566

Dieser Beitrag gibt im Anschluss an den Aufsatz in K&R 2016, 220 ff. einen Überblick über bedeutsame Entwicklungen im Bereich des Datenschutzrechts während des Jahres 2016. Die Darstellung beschränkt sich – wie üblich – auf besonders praxisrelevante Entwicklungen auf gesetzgeberischer und regulatorischer Ebene sowie auf wichtige einschlägige Judikatur.

Ruppert, Felix, Der neue strafrechtliche Geheimnisschutz – Der Weg in die Zukunft des IT-Outsourcings?, K&R 2017, S. 609

Der Beitrag analysiert den Gesetzesentwurf der Bundesregierung zur Neuregelung des strafrechtlichen Geheimnisschutzes hinsichtlich der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, den der Bundestag am 29.06.2017 in einer durch den Rechtsausschuss geänderten Fassung angenommen hat. Die Regelungen haben Gewicht, da mit dem technischen Fortschritt der Trend zum IT-Outsourcing ungebrochen ist.

Schätzle, Daniel, Zum Koppelungsverbot der Datenschutz-Grundverordnung, Ping 2017, S. 203

Der Autor will unter Aufzeigen der bisherigen Literatur die Frage beantworten, warum auch die DS-GVO kein absolutes Koppelungsverbot kennt.

Strubel, Michael, Anwendungsbereich des Rechts auf Datenübertragbarkeit, ZD 2017, S. 355

Untersucht wird die Reichweite der Anwendbarkeit des Art. 20 DS-GVO unter Berücksichtigung der dazu ergangenen weitreichenden Guidelines der Art. 29-Gruppe.



Digitalisiertes Kinderzimmer: Verzaubertes Spielzeug auf dem Vormarsch

Kill Cayla

Der Friedhof der Kuscheltiere hat eine neue Bedeutung. Wer vor eine paar Monaten Puppe Cayla gekauft hat, der muss sie jetzt zerstören. Sie enthält nämlich Mikrophon und Antenne und wurde von der Bundesnetzagentur als verbotene „versteckte, sendefähige Anlage“ eingestuft. Auf das besitzen oder vertreiben von Wanzen, die vor-täuschen Spielzeuge zu sein, stehen bis zu zwei Jahre Knast. Eltern müssen die Puppe nun zerstören und das Gemetzel dokumentieren. Alternativ kann Cayla gegen offiziellen Vernichtungsnachweis zum gemeindlichen Recyclinghof. Das reicht für ein kleines Kindertrauma. Die Puppe einfach an den Händler zurück zu geben ist unzulässig. Halten wir fest: Vertrieb und Besitz eines Kinderspielzeugs, das man in Deutschland legal erwerben kann,

sind strafbar. Niemand kümmert sich darum, als die Wunderpuppe in den Handel kommt, obwohl man damit wirbt, dass sie hören und sprechen kann. Monate später fällt auf, dass eine versteckte Sendeanlage auch dann strafbar ist, wenn sie in einer Puppe versteckt ist. Bevor die Puppe auf den Markt kam stand aber schon im Gesetz, dass der Besitz von in Alltagsgegenständen versteckten Sendeanlagen strafbar ist. In Zeiten, in denen sprechende Haushaltsgegenstände Mode sind, ist Cayla kein Einzelfall. Was unterscheidet sie von Siri, Cortana und den vielen anderen „Sprachassistenten“ in Lautsprechern und Handys? Man kann sich fragen, ob diese überhaupt noch in Alltagsgegenständen „versteckt“ sind. Bei Licht betrachtet, hält aber auch Cayla nicht geheim, dass sie sendet

und empfängt. Immerhin ist das die einzige Eigenschaft, die sie zu einer besonderen Puppe macht. Zumindest Eltern muss klar sein, worum es geht. Sie können sich fragen, ob sie ihre Kinder mit funkenden Wanzen spielen lassen sollen. Vor allem aber müssen Unternehmen prüfen, ob ihr Geschäft strafbar sein kann, bevor sie ihre Geräte in den Handel bringen und Behörden müssen von Anfang an besser auf hörende und sprechende Puppen aufpassen.



DS-GVO: Jetzt handeln und Haftungsrisiken vermeiden



Forgó/Helfrich/Schneider
Betrieblicher Datenschutz
2. Auflage. 2017. LX, 1332 Seiten.
In Leinen € 209,-
ISBN 978-3-406-69541-4

Mehr Informationen:
www.beck-shop.de/bjzdai

Das Handbuch

bietet Unternehmen sowie deren Beratern **fundierte, praxisorientierte Hilfestellungen zur Umsetzung** notwendiger Datenschutz- und Datensicherheits-Mechanismen nach der neuen Datenschutz-Grundverordnung (DS-GVO). Bei Nichteinhaltung der neuen Regelungen drohen drastische Bußgelder und Haftungsrisiken für die Unternehmensleitung.

Die 2. Auflage

- erläutert die wichtigsten Neuerungen durch die DS-GVO
- stellt die Unterschiede des geltenden und des neuen Rechts dar
- liefert ausführliche Orientierung für die rechtzeitige Umsetzung der datenschutzrechtlichen Anforderungen
- zeigt konkret den Handlungsbedarf und die Handlungsspielräume auf
- berücksichtigt die aktuelle Rechtsprechung, u.a. »Wegfall von Safe Harbor«, US-EU-Privacy-Shield.

Die Herausgeber

sind herausragende Experten des Datenschutzrechts: Prof. Dr. Nikolaus **Forgó**, Prof. Dr. Marcus **Helfrich** und Prof. Dr. Jochen **Schneider**.

Besonders hilfreich

für Geschäftsführer, Rechtsabteilungen und deren Berater, Unternehmensberatungen, Rechtsanwälte sowie interne und externe Datenschutz- und Datensicherheitsbeauftragte.

Datenschutz- und Informationsfreiheitsrecht PLUS | PREMIUM Neu



Datenschutz- und Informationsfreiheitsrecht PLUS

ZD – Zeitschrift für Datenschutz, Gola/Schomerus, BDSG, Simitis BDSG und Paal/Pauly, **Datenschutz-Grundverordnung**, dazu der **BeckOK Datenschutzrecht**: diese und weitere wichtige Informationsquellen stehen Ihnen auch online zur Verfügung – übersichtlich, zitierfähig und zu günstigen Preisen. Dazu vieles, was die Arbeit im Datenschutzrecht erleichtert: Rechtsprechung in Hülle und Fülle, sorgfältig aktualisierte Gesetzestexte und konkrete Lösungen für die Unternehmenspraxis.

Infos: www.beck-shop.de/yqaxb

► schon ab € 57,-/Monat
(zzgl. MwSt., 6-Monats-Abo)

4 Wochen kostenlos testen

Datenschutz- und Informationsfreiheitsrecht PREMIUM | Neu

Manchmal muss es im Datenschutz- und Informationsfreiheitsrecht eben etwas mehr sein. Für diesen Fall bietet Ihnen das Aufbaumodul PREMIUM weitere renommierte Werke wie etwa **Gola, Datenschutz-Grundverordnung**, **Ehmann/Selmayr, Datenschutz-Grundverordnung** oder **v.d. Bussche/Voigt, Konzerndatenschutz**. Ein Muss für Spezialisten und eine große Hilfe für jeden Praktiker.

Infos: www.beck-shop.de/btpihm

► schon ab € 89,-/Monat
(zzgl. MwSt., 6-Monats-Abo)

► Einführungspreis bis 31.01.2018: schon ab € 75,-/Monat
(zzgl. MwSt., 6-Monats-Abo)