

Zeitschrift für  
Datenschutz-,  
Informations- und  
Kommunikationsrecht

# RDV

2/2015

Recht der Datenverarbeitung

Herausgegeben von

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

## Aufsätze

SCHWARTMANN/OHR, Datenschutzrechtliche Perspektiven des Einsatzes intelligenter Fahrzeuge

JASPERS/FRANCK, Connected Car und Beschäftigtendatenschutz

GENNEN, Vertragsgestaltung bei Connected Car-Lösungen

## Kurzbeiträge

GOLA, Aus den aktuellen Berichten der Aufsichtsbehörden (18): Erhebung von Daten zu Zwecken der Werbung durch Krankenkassen

WEHMEYER, Neue Rechtsprechung: Vertragsstrafenklauseln in Adressverträgen

LEONHARDT, Konzerninterner Datenaustausch in der Praxis – Ergebnisse der Online-Befragung

## Rechtsprechung

Aus dem Inhalt

BVerfG, Zur Reichweite „spruchrichterlicher Tätigkeit“ (Ls)

BGH, Anspruch des Kindes auf Auskunft über die Identität des anonymen Samenspenders (Ls)

BGH, Datenerhebung bei Minderjährigen zur Mitgliederwerbung einer Krankenkasse im Rahmen eines Gewinnspiels

BAG, Bewerberdaten für den örtlichen Betriebsrat bei zentralem Online-Recruitment-Center

OVG NRW, Zur Einsichtnahme in das Dienstverhältnis betreffende behördeninterne E-Mails

31. Jahrgang  
April 2015  
Seiten 57–110



Gesellschaft für Datenschutz  
und Datensicherheit e.V.



[www.rdv-online.de](http://www.rdv-online.de)

### Inhaltsverzeichnis

#### Editorial

57

#### Veranstaltungen

58

#### Aufsätze

Prof. Rolf SCHWARTMANN/Sara OHR  
Datenschutzrechtliche Perspektiven des Einsatzes  
intelligenter Fahrzeuge

59

RA Andreas JASPERS/Dr. iur. Lorenz FRANCK  
Connected Car und Beschäftigtendatenschutz

69

Prof. Klaus GENNEN  
Vertragsgestaltung bei Connected Car-Lösungen

74

#### Kurzbeiträge

Prof. Peter GOLA  
Aus den aktuellen Berichten der Aufsichtsbehörden  
(18): Erhebung von Daten zu Zwecken der Werbung  
durch Krankenkassen

82

Stefan WEHMEYER  
Neue Rechtsprechung: Vertragsstrafenklauseln  
in Adressverträgen

84

Andreas LEONHARDT  
Konzerninterner Datenaustausch in der Praxis  
– Ergebnisse der Online-Befragung

86

#### Rechtsprechung

Zur Reichweite „spruchrichterlicher Tätigkeit“ (Ls)  
(BVerfG, Beschluss vom 02.12.2014)

89

Anspruch des Kindes auf Auskunft über die  
Identität des anonymen Samenspenders (Ls)  
(BGH, Urteil vom 28.01.2015)

89

Datenerhebung bei Minderjährigen zur Mitglieder-  
werbung einer Krankenkasse im Rahmen eines  
Gewinnspiels  
(BGH, Urteil vom 22.01.2014)

89

Frage nach der Gewerkschaftszugehörigkeit  
(BAG, Urteil vom 18.11.2014)

92

Bewerberdaten für den örtlichen Betriebsrat bei  
zentralem Online-Recruitment-Center  
(BAG, Beschluss vom 21.10.2014)

95

Zur Einsichtnahme in das Dienstverhältnis  
betreffende behördeninterne E-Mails  
(OVG NRW, Beschluss vom 07.01.2015)

97

Kein einstweiliger Rechtsschutz gegen Umsetzung  
auf den Posten des Behördlicher Datenschutzbe-  
auftragten (Ls)  
(OVG NRW, Beschluss vom 07.10.2014)

100

Unzulässige Drohung mit Schufa-Einmeldung  
– Kosten der Abmahnung  
(LG Darmstadt, Urteil vom 16.10.2014)

100

Anspruch auf förmliche Rücknahme einer  
Abmahnung (Ls)  
(LAG Niedersachsen, Urteil vom 20.11.2014)

101

Kein Abwehrrecht von Mietern gegen als Attrappen  
bekannte Videokameras im Hauseingangsbereich (Ls)  
(AG Berlin-Schönefeld, Urteil vom 30.07.2014)

101

Posttraumatische Belastungsstörungen als Dienst-  
unfall nach Einsicht in Personalakte (Ls)  
(VerwG Aachen, Urteil vom 11.12.2014)

101

#### Berichte, Informationen, Sonstiges

36. Internationale Datenschutzkonferenz  
auf Mauritius (GÜRTLER)

102

Schluss mit den datenschutzrechtlichen Missständen  
beim Umgang mit Krankengeldbeziehern!

104

Datenschutzverstoß als Wettbewerbsverstoß

104

Auftraggeberhaftung für den „Mindestlohn“ aus  
Datenschutzsicht

104

BITKOM kritisiert Verbandsklagerecht beim Daten-  
schutz: Stellung des Datenschutzbeauftragten  
wird geschwächt

105

Akzeptanz des vernetzten Autos

106

#### Literaturhinweise

##### Buchbesprechungen

*Gregor Thüsing*, Beschäftigtendatenschutz und  
Compliance (REDAKTION)

107

*Beatrice Lederer*, Open Data – Informationsöffentlich-  
keit unter dem Grundgesetz (REDAKTION)

107

*Marc Oskan*, Die schlichte Einwilligung im Urheber-  
recht – Eine Untersuchung unter Berücksichtigung  
der Vorschabilder-Rechtsprechung des BGH  
(DEUMELAND)

107

*Wolfgang Däubler*, Gläserne Belegschaften  
(WRONKA)

108

*Oliver Busch*, Realtime Advertising – Digitales  
Marketing in Echtzeit: Strategien, Konzepte und  
Perspektiven (SCHRIFTFLEITUNG)

108

##### Neuerscheinungen

Aufsätze

109

#### Nachgefasst

110

## Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

Prof. Dr. Rolf SCHWARTMANN, Fachhochschule Köln

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

## in Kooperation mit der

Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

## Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

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

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

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

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

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

Prof. Dr. Karl 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 Bundesarbeitsgericht a.D.

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

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

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

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

---

**Beilagenhinweis** GDD-Mitteilungen 2/2015, Tagungsbericht 38. DAFTA, Sachregister 2014

---

## Manuskripte

Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an die Schriftleitung erbeten. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Sie können nur zurückgesandt werden, wenn Rückporto beigefügt ist. 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 Mikroverfilmung vorbehalten. Sie erstrecken sich auch auf die veröffentlichten Gerichtsentscheidungen und ihre 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

Geschäftsführer: Dr. Karl Ulrich

Leitung: Hans-Günter Böse

HRB 337678

## Satz

alka mediengestaltung gmbh

Ottostraße 6, 53332 Bornheim-Sechtem

## Druck

AZ Druck und Datentechnik GmbH

Heisinger Straße 16, 87437 Kempten

## Anzeigenverwaltung

DATAKONTEXT GmbH, Frechen

Thomas Reinhard-Rief

Hultschiner Straße 8

D-81677 München

Telefon: (089) 21 83-89 35

Fax: (089) 21 83-96 02 33

E-Mail: reinhard@datakontext.com

www.datakontext.com

Geschäftsführer: Dr. Karl Ulrich

Leitung: Hans-Günter Böse

HRB 337678

Zeitschrift für  
Datenschutz-, Informations-  
und Kommunikationsrecht  
Schriftleitung:  
Prof. Peter Gola, Königswinter  
(federführend)  
RA Dr. Georg Wronka, Bonn  
RA Andreas Jaspers, Bonn  
Redaktion: Birgit Koppitsch  
31. Jahrgang 2015 Heft 2  
Seiten 57–110

# RDV

## Recht der Datenverarbeitung

31. Jahrgang · April 2015 · Seiten 57–110

## Editorial

### Zertifizieren statt spionieren

Die Welt um uns herum ist voll von Spionen, auch in unseren Autos. Moderne Fahrzeuge enthalten eine Vielzahl von Sensoren. Sie erheben und übermitteln etwa an den Hersteller Daten über den Fahrzeugzustand, die Umgebung und Position des Autos und das Fahrverhalten. Vermehrt werden auch Daten erhoben, die sich unmittelbar auf den Fahrer beziehen, wie seine Alkoholisierung, sein Gesundheitszustand oder seine Gemütslage. Sie leiten weiter, ob der Airbag aktiviert ist, der Gurt geschlossen sowie ob und mit wie viel Gewicht die Sitze belegt sind. Diese Daten lassen Rückschlüsse auf persönliches Verhalten zu, das im Zweifel gegen den Fahrer verwendet werden kann. So wurden etwa schon Mängelansprüche während der Gewährleistung unter Hinweis darauf zurückgewiesen, dass die vom Achslastsensor aufgezeichnete Überschreitung der zulässigen Last auf der Hinterachse überschritten war.

Die aus dem Fahrzeug gesendeten Daten ermöglichen durch die Übertragung der Fahrzeug-Identifizierungsnummer (FIN) eine Zuordnung der Informationen zum Fahrer. Sie lassen selbst dann eine Aussage über die Persönlichkeit des Fahrers zu, selbst wenn man das nicht vermutet. Wer etwa auf einer Flanierstraße mit offener Fensterscheibe, nicht angeschnallt im Wechsel beschleunigt und abbremst und dabei eine bestimmte Musik hört,

der ist auch für die Werbewirtschaft hinreichend gekennzeichnet. Man kann ihn vermutlich mit sportlichen Felgen oder Auspuffanlagen und vielleicht sogar mit einem Angebot für einen Saunaclub eher beglücken, als mit einer Heizdecke. So etwas nennt man Scoring, also das Bilden von Kaufprofilen. Wer sich angesichts dessen Sorgen um seine Privatsphäre macht, der sieht keine grünen Männchen, sondern ist in der Realität angekommen.

Viele wollen Abstandsassistent & Co. aber nicht mehr missen. Wer seinen Fuhrpark oder seine Mietwagenflotte mit aktuellen Modellen bestücken will, der kommt nicht an kommunizierenden Autos vorbei.

Nun sind die Datenschützer in der Automobilindustrie aufgerufen, ihre Verantwortung für einen verantwortungsvollen Umgang mit smarten Autos zu übernehmen. Das gilt für Hersteller sowie für Zulieferer. Zum Glück hat uns gerade die Automobilindustrie schon vorgelebt, wie man Sicherheit in Autos verbaut. Jeder Zulieferer der vom Cupholder für einen Kaffeebecher bis zur Lampenfassung an einen führenden Automobilhersteller liefern will, muss hohe Zertifizierungsanforderungen erfüllen. Dieses System ist aufwendig. Zugleich bringt es Fahrzeuge hervor, die weltweit Qualitätsmaßstäbe setzen. Dieser Ansatz muss auf den Einsatz von kommunizierender Technik im Fahrzeug übertragen

werden. Wer zum Beispiel eine intelligente Software zur LKW-Routenplanung anbietet, muss unter Zugrundlegung eines transparenten Standards festgelegte Vorgaben für Datenschutz und Datensicherheit einhalten. Die Zertifizierung solcher Standards kann nur durch eine unabhängige Stelle erfolgen. So ist sichergestellt, dass Routenplanungen für LKWs, die mit der Umwelt und anderen Fahrzeugen auf Basis von Big Data-Anwendungen kommunizieren, sicheren Standards entsprechen. Wenn die Datenverarbeitungsvorgänge offengelegt werden, sind sie verantwortbar. Zertifiziert und transparent handelnde Spione sind keine Spione, sondern Helfer.

*Rolf Schwartmann*



**Prof. Dr. Rolf Schwartmann**

Leiter der Kölner Forschungsstelle für Medienrecht an der Fachhochschule Köln, Mitherausgeber der Fachzeitschrift RDV sowie Vorstandsvorsitzender der GDD e.V., Bonn

Termin	Thema	Ort	Kontakt
28.04.2015	Grundlagen der Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
27.-28.04.2015	Datenschutz Management – Teil 3	Köln	GDD e.V. und DATAKONTEXT
28.04.2015	Grundlagen der Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
05.05.2015	Umsetzung des neuen Datenschutzstandards bei Dienstleistern	Köln	GDD e.V. und DATAKONTEXT
06.05.2015	Die Datenpanne! Wie Sie den Albtraum vermeiden oder managen können	Stuttgart	GDD e.V. und DATAKONTEXT
07.05.2015	Moderne Unternehmenskommunikation: E-Mail- und Internet Einsatz	Düsseldorf	GDD e.V. und DATAKONTEXT
11.05.2015	Prüfung von SAP-Systemen durch Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
11.-12.05.2015	ARGE Datenschutz International	Köln	GDD e.V. und DATAKONTEXT
18.05.2015	Cloud Computing: Leit- und Richtlinien für Datenschutz und IT-Sicherheit	Köln	GDD e.V. und DATAKONTEXT
19.05.2015	Repetitorium GDDcert.	Köln	GDD e.V. und DATAKONTEXT
19.05.2015	Data Leakage Prevention	Köln	GDD e.V. und DATAKONTEXT
19.05.2015	Datenschutz im Gesundheitswesen	Berlin	GDD e.V. und DATAKONTEXT
27.05.2015	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Köln	GDD e.V. und DATAKONTEXT
27.05.2015	Personaldatenverarbeitung und HR-Prozesse	Stuttgart	GDD e.V. und DATAKONTEXT
09.06.2015	Was der Datenschutzbeauftragte von der IT-Sicherheit wissen muss!	Köln	GDD e.V. und DATAKONTEXT
08.-12.06.2015	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Hamburg	GDD e.V. und DATAKONTEXT
19.06.2015	Die häufigsten Datenschutz-Schwachstellen und wie man sie vermeiden kann	Köln	GDD e.V. und DATAKONTEXT
03.-05.08.2015	GDD-Sommer-Workshop	Timmendorfer Strand	GDD e.V. und DATAKONTEXT
02.09.2015	Datenschutzaudit leicht gemacht	Köln	GDD e.V. und DATAKONTEXT
08.09.2015	Die Datenpanne! Wie Sie den Albtraum vermeiden oder managen können	Köln	GDD e.V. und DATAKONTEXT
09.09.2015	Personaldatenverarbeitung und HR-Prozesse	Düsseldorf	GDD e.V. und DATAKONTEXT
14.-16.09.2015	Das SAP-System für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
14.-18.09.2015	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
22.-23.09.2015	Datenschutz Kompakt	Köln	GDD e.V. und DATAKONTEXT
24.09.2015	Grundlagen der Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT

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

# Aufsätze

Rolf Schwartzmann/Sara Ohr

## Datenschutzrechtliche Perspektiven des Einsatzes intelligenter Fahrzeuge

### A. Einleitung

Der Einsatz intelligenter, vernetzender Technik in Fahrzeugen ist ein bedeutendes rechtliches Thema für die Wirtschaft.<sup>1</sup> Der Vorstandsvorsitzende der Volkswagen AG Winterkorn hat es auf den Punkt gebracht: „Autos erzeugen die meisten Daten der Welt. (...) Und auf diese Daten sind natürlich alle scharf. Mithilfe von Autos kann man zum Beispiel den besten Wetterbericht der Welt machen: Außentemperaturfühler, Regensensoren, Radsensoren für Glätte, alles Informationen in Echtzeit.“<sup>2</sup> Während die Wirtschaft unter den Stichworten Industrie 4.0 und Internet der Dinge kreativ und in rasanter Geschwindigkeit vernetzte Produkte und Dienstleistungen auf den Markt bringt, versucht das Recht, hier namentlich das Datenschutzrecht, diese Entwicklungen juristisch zu fassen.

Dabei gilt es, bei der Nutzung personenbezogener Daten aus Autos, neben Privatheit und Datenschutz auch die Datensicherheit zu wahren. Daten sind nämlich Sicherheitsrisiken, sowohl für den einzelnen Fahrer als auch für den Straßenverkehr. Schließlich kann man sie manipulieren, „hacken“ und zu kriminellen Zwecken missbrauchen.

Der Autofahrer im Jahr 2015 möchte sein Auto nicht mehr nur als Fortbewegungsmittel verwenden. Er möchte sein Smartphone und seine Wearables nutzen, um sie mit dem Fahrzeug zu vernetzen. Dabei soll die Nutzung von Apps genauso möglich sein, wie der Zugriff auf eine Cloud. Mails abzurufen und Netzdienste von Facebook bis YouTube zu nutzen, ist kein Problem mehr. Zudem kann man über Endgeräte nach Wahl standortunabhängig ein Fahrzeug steuern, seinen Wartungszustand oder die Tankfüllung abfragen.

### I. Gesetzliche Vorgaben

#### 1. Verfassungsrechtliche Vorgaben

Zugleich gilt auch in Zeiten autonom kommunizierender Fahrzeuge nach wie vor die dem Gedanken der Selbstbestimmung entstammende Maxime des Bundesverfassungsgerichts aus der Volkszählungsentscheidung, wonach der Einzelne wissen soll, wer, was, bei welcher Gelegenheit über ihn weiß.<sup>3</sup> Für jeden Verkehrsteilnehmer folgt hieraus ein grundsätzlicher Anspruch auf spurenfreie Mobilität.<sup>4</sup> Die Freiheit, sich selbstbestimmt zu bewegen und zu verhalten, wäre wesentlich eingeschränkt, wenn der Einzelne stets mit der Aufzeichnung und Auswertung seiner Daten rechnen müsste.<sup>5</sup> Justizminister Maas hat diesen Rechtsgedanken kürzlich auf vernetzte Autos übertragen. „Verbraucherinnen und Verbraucher müssen (...) die Hoheit über die Sammlung, Weitergabe und Verwertung ihrer Daten behalten. Es darf keinen „gläsernen Autofahrer“ geben.“<sup>6</sup> Diese Forderung ist rechtlich alternativlos. Sie ist aber schwer umsetzbar.

Im Hinblick auf die Vernetzung von Fahrzeugen ebenfalls von Bedeutung ist das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme. Von dieser weiteren Ausprägung des allgemeinen Persönlichkeitsrechts wird der Einzelne vor heimlichen Zugriffen auf wesentliche Teile seiner Lebensgestaltung geschützt, die ein aussagekräftiges Profil seiner Persönlichkeit bieten können.<sup>7</sup>

Daten, die auf dem Telekommunikationsweg übertragen werden, sind ferner über Art. 10 Abs. 1 GG geschützt. Das

Telekommunikationsgeheimnis greift jedoch nur bis zum Abschluss eines Kommunikationsvorgangs. Bleiben die Daten hieran anschließend gespeichert, unterliegen sie dem Schutz des Rechts auf informationelle Selbstbestimmung.<sup>8</sup>

#### 2. Einfachgesetzliche Vorgaben

Nach dem Recht auf informationelle Selbstbestimmung, das § 4 Abs. 1 BDSG im Rahmen des einfachen Rechts umsetzt, ist jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur erlaubt, wenn der Betroffene (§ 3 Abs. 1 BDSG) – also derjenige, der geschützte Informationen preisgibt – hierin einwilligt oder eine gesetzliche Vorschrift einen Dritten oder den Staat zum Umgang mit den Daten ermächtigt.

1 Aus diesem Grund wurde und wird es in dieser Zeitschrift verstärkt behandelt. Vgl. nur Lüdemann/Jürgens/Ortmann, RDV 2014, 3; Lüdemann/Sengstacken, RDV 2014, 177; Kremer, RDV 2014, 240; Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302; Gennen, RDV 2015, in diesem Heft; Jaspers/Franck, RDV 2015, in diesem Heft.

2 Interview im Stern Nr. 10/2015, S. 78.

3 BVerfGE 65, 1, 42.

4 Weichert, SVR 2014, 201, 203.

5 BVerfG, NJW 1984, 419, 422.

6 Vgl. unter <http://www.bmfv.de/SharedDocs/Reden/DE/2015/20150215-Safer-Internet-Day-2015.html?nn=1477162> (letzter Abruf: 06.03.2015).

7 BVerfG, NJW 2008, 822, 827.

8 Durner, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, 72. Ergänzungslieferung 2014, Art. 10 Rn. 56.

### a) TMG und BDSG

Auf einfachgesetzlicher Ebene kommen für die Legitimation zur Erhebung, Verarbeitung und Nutzung von Kfz-Daten die Vorschriften des TMG sowie des BDSG in Betracht. Während für Bestands- oder Nutzungsdaten, die zur Ermöglichung der Inanspruchnahme der jeweiligen Dienste oder zu Abrechnungszwecken erforderlich sind, das TMG einschlägig ist,<sup>9</sup> richtet sich der Umgang mit Inhaltsdaten nach dem BDSG. Auch wenn es sich bei den Inhaltsdaten tendenziell um die persönlichkeitsensibelsten Angaben handelt, ist eine genaue Abgrenzung nicht immer leicht zu treffen. Gerade den Nutzungsdaten kann angesichts der vielfältigen Vernetzungsfunktionen moderner Fahrzeuge ein hoher – im Einzelfall gegenüber Inhaltsdaten sogar erhöhter – Sensibilitätsgrad zukommen.<sup>10</sup> Selbst datenschutzrechtlich wenig relevant erscheinende Fahrzeugeinstellungen wie die Sitzposition können durch die Zusammenführung mit anderen Daten – etwa dem Beschleunigungs- und Bremsverhalten oder den Fahrtzeiten – ein hinreichend detailliertes Personenprofil ermöglichen, welches sodann die Zuordnung zu einer jedenfalls bestimmbaren Person erlaubt.<sup>11</sup> Streiten lässt sich daher bereits über den Anwendungsbereich des BDSG anhand der Frage, wann Daten personenbezogen sind.

### b) IVSG und TKG

Einen weiteren datenschutzrechtlichen Erlaubnistatbestand enthält § 3 S. 2 des Gesetzes über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG). Personenbezogene Daten im Rahmen Intelligenter Verkehrssysteme<sup>12</sup> im Straßenverkehr dürfen danach nur erhoben, verarbeitet oder genutzt werden, soweit dies durch eine bundesgesetzliche Regelung ausdrücklich zugelassen oder angeordnet wird. Bemerkenswert erscheint insoweit, dass die Möglichkeit der Einwilligung im Rahmen der Vorschrift keinerlei ausdrückliche Erwähnung findet. Allerdings verpflichtet Art. 10 Abs. 4 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (IVS-RL) die Mitgliedsstaaten zur Einhaltung der Bestimmungen über die Einwilligung in die Verarbeitung personenbezogener Daten. Im Geiste einer europarechtskonformen Auslegung ist § 3 S. 2 IVSG folglich dahin zu verstehen, dass eine Einwilligung des Betroffenen als Legitimation des Datenumgangs im Rahmen intelligenter Verkehrssysteme ebenfalls in Betracht kommt.<sup>13</sup> Mit Blick auf den eindeutigen Wortlaut der Vorschrift ausgeschlossen ist lediglich der Rückgriff auf landesgesetzliche Erlaubnistatbestände. Im Übrigen muss § 3 S. 2 IVSG als deklaratorischer Hinweis auf die bundesgesetzlichen Vorschriften des BDSG, TMG und TKG verstanden werden.<sup>14</sup>

Sofern geschäftsmäßige Telekommunikationsdienste erbracht oder an deren Erbringung zumindest mitgewirkt wird, finden ferner §§ 91 ff. TKG Anwendung. Möglich ist dies insbesondere im Rahmen der Signalübertragung bei intelli-

genten Verkehrssystemen. Verkehrs- und Standortdaten dürfen dann nur in eingeschränktem Umfang und unter besonderen Voraussetzungen verwendet werden.<sup>15</sup>

## II. Beteiligte

Um vernetzte Dienste anbieten zu können, werden von zahlreichen Sensoren im Auto, neben der gefahrenen Geschwindigkeit eine Vielzahl anderer Fahrinformationen, von der Achslast, über Fahrwege, bis zum Beschleunigungs- und Bremsverhalten erfasst, gespeichert und übertragen.<sup>16</sup> Je nach Ausgestaltung im Einzelfall kommen als Empfänger etwa der Hersteller des Fahrzeugs oder des Navigationssystems, der Anbieter des eigentlichen Navigationsangebots sowie der Hersteller einzelner Sensoren, sofern deren Chips eigenständig Daten übertragen, in Betracht. Beteiligt sind auch sog. Traffic Service Provider zur Staumeldung sowie viele weitere Stellen. Wirtschaftliches Interesse an den Daten haben nicht zuletzt Kfz-Versicherungen oder der Staat, wenn es um Infrastrukturplanung geht oder auch um Gefahrenabwehr durch die Polizei oder um Strafverfolgung.

## III. Personenbezug

Fahrzeuge enthalten heute Sensoren in den Sicherheitsgurten oder elektronischen Fensterhebern, Navigationssysteme, Bluetooth-Schnittstellen zu Smartphones sowie Sensoren, die das Beschleunigen und Bremsen messen. Unterstellt, diese Daten sind an die Fahrzeugidentifikationsnummer geknüpft und der Fahrer des Wagens fährt mit überhöhter Geschwindigkeit auf einer Flanierstraße nicht angeschnallt, mit offenem Fenster und lauter Musik ständig auf und ab und legt dabei mit weit überhöhter Geschwindigkeit einen Kavalierstart nach dem anderen hin – sind diese Daten personenbezogen, weil sie Informationen über das Fahrverhalten und den Charakter, als Poser, Liebhaber bestimmter Musik oder als jemand, der Verkehrsregeln verletzt, liefern? Sie können für die Kfz-Versicherung (nicht angeschnallt), die Polizei (überhöhte Geschwindigkeit, Kavalierstart), den Hersteller mit Blick auf die Garantie für die Bremsen oder

9 Allerdings finden die §§ 12 ff. TMG auf die Erhebung und Verwendung personenbezogener Daten im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken keine Anwendung (§ 11 Abs. 1 Nr. 1 TMG). In diesem Falle gelten ausschließlich die Vorschriften des BDSG, vgl. Müller-Broich, TMG, 1. Aufl. 2012, § 11 Rn. 3.

10 Als potenziell persönlichkeitsensible Nutzungsdaten können etwa Ort- und Zeitangaben genannt werden, anhand derer aussagekräftige Bewegungs-, Kontakt- oder Interessenprofile erstellt werden können, vgl. hierzu Weichert, SVR 2014, 201, 203.

11 Kinast/Kühnl, NJW 2014, 3057, 3058.

12 „Intelligente Verkehrssysteme“ im Sinne von § 2 Nr. 1 IVSG sind Systeme, bei denen Informations- und Kommunikationstechnologien im Straßenverkehr und an Schnittstellen zu anderen Verkehrsträgern eingesetzt werden. Beispielhaft sind etwa Parkleitsysteme, Navigation mit Real Time Traffic oder telematisch-basierte Versicherungen (vgl. hierzu unten unter B.III.1.) zu nennen. Näher zum Begriff Kremer, RDV 2014, 240, 241 f.

13 „Soweit angemessen“ soll im Rahmen des Betriebs von IVS-Anwendungen und -Diensten allerdings die Verwendung anonymer Daten gefördert werden, vgl. Art. 10 Abs. 3 IVS-RL.

14 Kremer, RDV 2014, 240, 246.

15 Vgl. hierzu Kremer, RDV 2014, 240, 246 f.

16 Kremer, RDV 2014, 240, 241.

für Anbieter von Musik oder Sportwagenaccessoires interessant und auch finanziell verwertbar sein. Haben diese Daten Personenbezug? Immerhin geben sie Auskunft über persönliche Dinge wie das Fahrverhalten einer bestimmten Person. Oder handelt es sich nur um bloße, einer Person nicht zuzuordnende Metadaten, die keine brauchbaren Rückschlüsse auf individuelles Verhalten zulassen? Nähme man in einem solchen Fall Personenbezug an, dann müsste die Einwilligung in die Datennutzung Vorgänge wie den geschilderten erfassen, damit sie rechtmäßig wäre. Ob diese Informationen nach § 28 Abs. 2 Nr. 2 b) BDSG, etwa mit Blick auf den nemo-tenetur-Grundsatz,<sup>17</sup> an die Polizei herausgegeben werden dürfen, wenn diese einen gefährlichen Eingriff in den Straßenverkehr prüfen will, ist eine weitere Frage.

Probleme des personenbezogenen Datenumgangs können sich allerdings nicht nur mit Blick auf Eigentümer, Halter und Fahrer eines Kfz ergeben. Darüber hinaus können auch Fußgänger oder andere Verkehrsteilnehmer betroffen sein.<sup>18</sup> Ermöglicht wird dies insbesondere durch Außenkameras, die an einem Fahrzeug angebracht sind, um etwaige Verkehrsunfälle in dessen Umfeld zu dokumentieren.<sup>19</sup>

#### IV. Verantwortliche Stelle

Ob die oben genannten Beteiligten, angefangen beim Hersteller des Fahrzeugs, verantwortliche Stellen im Sinne von § 3 Abs. 7 BDSG sind, kommt auf den Einzelfall an. Den Pflichten des Datenschutzrechts ist jede Person oder Stelle unterworfen, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 Abs. 7 BDSG). Gemäß Art. 2 d) der Datenschutzrichtlinie,<sup>20</sup> in deren Lichte die nationale Vorschrift auszulegen ist, ist „für die Verarbeitung Verantwortlicher“ jede natürliche oder juristische Person, Behörde, Einrichtung oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Erforderlich ist demnach eine tatsächliche Einflussnahme auf das „Ob“ und „Wie“ der Datenverarbeitung. Angesichts ihrer weitreichenden Gestaltungsmöglichkeiten muss die Hauptverantwortlichkeit in Bezug auf die aus Fahrzeugen gewonnenen Daten bei den Herstellern angesiedelt werden. Sie entwickeln die entsprechenden Geräte und können damit letztlich bestimmen, welche Daten im Zusammenhang mit der Nutzung des Kfz erhoben, gespeichert und verarbeitet werden. Ebenfalls datenschutzrechtlich verantwortlich können Versicherungen sein, die das Fahrverhalten der Versicherungsnehmer mittels Telematik erfassen, um hierauf basierend eine individuelle Versicherungspolice zu errechnen.<sup>21</sup> Ferner kommen als verantwortliche Stellen Vertragshändler und -werkstätten in Betracht, die die gewonnenen Kfz-Daten zur Ferndiagnostik von Fehlern oder Verschleißerscheinungen nutzen. Des Weiteren kann auch Anbietern von Online-Diensten, die innerhalb des Kfz genutzt werden, datenschutzrechtliche Verantwortlichkeit zukommen.<sup>22</sup>

Nicht zuletzt kann die Erhebung und Verarbeitung personenbezogener Daten aber auch dem Halter oder Fahrer eines

Fahrzeugs zuzurechnen sein. Dies setzt voraus, dass er die Funktionen des technischen Kfz-Systems oder jedenfalls den Zugriff hierauf steuern kann.<sup>23</sup> Soweit allerdings der Umgang des Halters bzw. Fahrers mit Daten zu seiner eigenen Person in Rede steht, ist er Betroffener und kann nicht zugleich als verantwortliche Stelle den Verpflichtungen des BDSG unterworfen sein.<sup>24</sup>

## B. Szenarien

Im welchem Kontext der Umgang mit vernetzten Fahrzeugen rechtlich relevant werden kann, zeigen die nachfolgenden Szenarien. Thematisch sind diese in die Bereiche Verkehrssteuerung, Automatisiertes Fahren, Verhaltenssteuerung und Verkehrssicherheit unterteilt, stellen aber keine abschließende rechtliche Behandlung der Materie dar.

### I. Verkehrssteuerung

#### 1. Zentrale Sammlung von Online-Verkehrsdaten (Mobilitäts-Daten-Marktplatz)

##### a) Szenario

Auf Initiative des Bundesministeriums für Verkehr und digitale Infrastruktur und der Bundesanstalt für Straßenwesen ist mit dem Projekt Mobilitäts Daten Marktplatz (MDM) eine Metadatenplattform für Verkehrsinformationen des Individualverkehrs entstanden.<sup>25</sup> Hierauf werden sämtliche bundesweit verfügbaren Online-Verkehrsdaten abrufbar gehalten. Das Angebot richtet sich an Datenanbieter, die ihre erhobenen Daten einfach und aktuell präsentieren wollen, an Datenabnehmer, die sich umfassend informieren und relevante Anbieter unkompliziert kontaktieren können, sowie an Datenveredler, die als Schnittstelle zwischen Anbieter und Abnehmer für eine einheitliche Datenqualität sorgen sollen.<sup>26</sup>

##### b) Rechtliche Bewertung

Mit Blick auf die Zielsetzung des MDM, die mobile Freiheit der Verkehrsteilnehmer zu erhalten und zu fördern sowie bei der Wahl von Verkehrsmittel und Route durch intelligente

17 Vgl. hierzu auch unten unter B.III.1.b).

18 Eingehend zur Auswahl der Betroffenen Weichert, SVR 2014, 201, 204.

19 Vgl. hierzu Lachenmann/Schwiering, NZV 2014, 291, 294 f. sowie unten unter B.IV.2.b)bb).

20 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.

21 Vgl. hierzu unten unter B.III.1.

22 Weichert, SVR 2014, 201, 205.

23 Roßnagel, SVR 2014, 281, 284. Möglich ist dies etwa im Falle von Daten, die durch die Nutzung des fahrzeugeigenen Infotainment-Systems generiert werden.

24 Roßnagel, SVR 2014, 281, 284; Dammann, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 3 Rn. 226, der darauf verweist, dass der Gesetzgeber den Betroffenen nicht vor sich selbst schützen kann und will.

25 Seit dem Jahr 2013 ist der Projektcharakter beendet. Seither arbeitet der MDM im langfristigen Regelbetrieb, vgl. hierzu unter <http://www.mdm-portal.de/ablauf.html> (letzter Abruf: 06.03.2015).

26 Vgl. hierzu unter <http://www.mdm-portal.de/projekt.html> (letzter Abruf: 06.03.2015).

Verkehrssysteme eine sinnvolle Unterstützung zu bieten,<sup>27</sup> ist davon auszugehen, dass die in Rede stehenden Daten regelmäßig keinen Personenbezug aufweisen oder jedenfalls anonymisiert angeboten werden. Für die Funktionsfähigkeit eines zentralen Verkehrsmanagementsystems ist die Angabe von Informationen zu bestimmten oder bestimmbar Personen gerade nicht erforderlich. Werden dennoch personenbezogene Daten verarbeitet, ist hiermit allerdings ein schwerwiegender Eingriff in das Persönlichkeitsrecht der Betroffenen verbunden. Angesichts der mit der Zusammenführung großer Datenmengen verbundenen Gefahren der Profilbildung,<sup>28</sup> kann der Datenumgang in diesen Fällen ausschließlich durch die Einwilligung des Betroffenen gerechtfertigt werden.<sup>29</sup> Beim Einsatz im Unternehmen ist darüber hinaus das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG zu beachten.<sup>30</sup>

## 2. Infrastrukturabgabe (Pkw-Maut)

### a) Szenario

Zur Aufrechterhaltung des deutschen Infrastrukturnetzes auf gleichbleibendem Standard soll für Halter von im Inland und im Ausland zugelassenen Pkw und Wohnmobilen ab dem Jahr 2016<sup>31</sup> eine Infrastrukturabgabe für die Nutzung von Bundesfernstraßen eingeführt werden. Die Infrastrukturabgabe soll mithilfe einer elektronischen Vignette (sog. E-Vignette) erhoben werden. Die Fahrberechtigung soll mit dem amtlichen Kraftfahrzeugkennzeichen verknüpft werden, das nach Entrichtung der Infrastrukturabgabe im System freigeschaltet wird. Zum Zweck der Erhebung der Infrastrukturabgabe führt das Kraftfahrt-Bundesamt ein Infrastrukturabgaberegister (§ 5 InfrAG-E). Die dort gesammelten Daten (u.a. Name und Wohnort des Halters, Kfz-Kennzeichen, Hubraum und Emissionsklasse, Klasse und Aufbauart, Fahrzeug-Identifizierungsnummer, Datum der Erstzulassung) dürfen ausschließlich für die Zwecke des Infrastrukturabgabengesetzes erhoben, verarbeitet und genutzt werden. Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig. Das Kraftfahrt-Bundesamt kann einem privaten Dritten die Erhebung der Infrastrukturabgabe für Kraftfahrzeuge, die nicht in der Bundesrepublik Deutschland zugelassen sind, übertragen (Betreiber). Das Bundesamt für Güterverkehr überwacht stichprobenartig die Einhaltung der Abgabepflicht nach dem Infrastrukturabgabengesetz (§ 10 InfrAG-E). Es kann sich dabei ebenfalls der Mitwirkung eines privaten Dritten bedienen. Soweit es zum Zwecke der Überwachung erforderlich ist, dürfen das Bundesamt für Güterverkehr und der private Dritte im Rahmen der Überwachung (...) folgende Daten erheben, speichern und nutzen: Bild des Kraftfahrzeugs ohne Erfassung der Fahrzeuginsassen, Name und Anschrift der Person, die das Kraftfahrzeug führt (nur im Rahmen einer Vor-Ort-Kontrolle), Ort und Zeit der Benutzung von Straßen im Sinne des § 1 Abs. 1 i.V.m. Abs. 2 und § 2 Abs. 3 InfrAG-E, Kennzeichen des Kraftfahrzeugs inklusive Nationalitätenkennzeichen, Hubraum, Emissionsklasse und Antriebsart des Kraftfahrzeugs (...) sowie Klasse und Aufbauart im Sinne des Anhangs II der Richtlinie 2007/46/EG.

Die genannten Daten dürfen ausschließlich zum Zweck der Überwachung der Einhaltung der Vorschriften des Infrastrukturabgabengesetzes verarbeitet und genutzt sowie an das Kraftfahrt-Bundesamt übermittelt werden.<sup>32</sup>

### b) Rechtliche Bewertung

Datenschutzrechtliche Probleme können sich aus der umfassenden elektronischen Erfassung der abgabepflichtigen Fahrzeuge ergeben. Das automatisierte Verfahren erleichtert nicht nur die Überprüfung der Kennzeichen, sondern bietet darüber hinaus die Möglichkeit, diese seriell in kürzester Zeit zu erfassen.<sup>33</sup>

Da im Rahmen der elektronischen Datenverarbeitung kein schlechthin belangloses personenbezogenes Datum existiert, ist der Schutzzumfang des Rechts auf informationelle Selbstbestimmung nicht lediglich auf solche Informationen beschränkt, die bereits ihrer Art nach sensibel sind. Der grundrechtliche Schutz entfällt daher nicht bereits deshalb, weil die betroffene Information – wie im Falle von Kfz-Kennzeichen – öffentlich zugänglich ist.<sup>34</sup> Zu einem Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung kommt es in den Fällen, in denen ein erfasstes Kennzeichen im Speicher festgehalten wird und somit Grundlage weiterer Maßnahmen werden kann (sog. Trefferfall).<sup>35</sup> Die Schwere des Eingriffs nimmt mit der Möglichkeit der Verknüpfung mit anderen Daten zu, die wiederum weitere Folgemaßnahmen auslösen können.<sup>36</sup>

Mit Blick auf den vorliegenden Gesetzesentwurf wird insbesondere die umfassende Datensammlung durch das Kraftfahrt-Bundesamt und das Bundesamt für Güterverkehr kritisiert.<sup>37</sup> Sofern in der Einführung einer physischen Vignette ein gleichermaßen effektives Mittel zur Kontrolle der Abgabentrachtung gesehen wird,<sup>38</sup> stellt sich die Frage nach der Verhältnismäßigkeit einer elektronisch-automatisierten

27 Vgl. hierzu unter <http://www.mdm-portal.de/index.php?id=4> (letzter Abruf: 06.03.2015).

28 Zur Problematik der Profilbildung mit Blick auf Suchmaschinen EuGH, NJW 2014, 2257, 2259, Rn. 37; zur Problematik der Profilbildung durch die Vorratsdatenspeicherung EuGH, NJW 2014, 2169, 2170, Rn. 26 f. sowie Schwartzmann/Theodorou, RDV 2014, 61, 70 ff.

29 Kremer, RDV 2014, 240, 249.

30 Vgl. hierzu auch unten unter B.III.2.b).

31 Vgl. unter [http://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/pkw-maut-infrastrukturabgabe-infopapier.pdf?\\_\\_blob=publicationFile](http://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/pkw-maut-infrastrukturabgabe-infopapier.pdf?__blob=publicationFile) (letzter Abruf: 06.03.2015).

32 Vgl. hierzu Entwurf eines Gesetzes zur Einführung einer Infrastrukturabgabe für die Benutzung von Bundesfernstraßen unter [http://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/entwurf-infrastrukturabgabengesetz-neu.pdf?\\_\\_blob=publicationFile](http://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/entwurf-infrastrukturabgabengesetz-neu.pdf?__blob=publicationFile) (letzter Abruf: 06.03.2015).

33 BVerfG, NJW 2008, 1505, 1507.

34 BVerfG, NJW 2008, 1505, 1506.

35 Unterliegt ein Fahrzeug (etwa ein Rettungswagen) nicht der Abgabepflicht (sog. Nichttrefferfall), tangiert die elektronische Kennzeichenerfassung die rechtliche Position des Betroffenen nicht, sofern der Datenabgleich unverzüglich vorgenommen wird sowie zusätzlich rechtlich und technisch gesichert ist, dass die Daten anonym bleiben und sofort spurlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden, BVerfG, NJW 2008, 1505, 1507.

36 BVerfG, NJW 2008, 1505, 1508.

37 Mitteilung des Thüringer Datenschutzbeauftragten Lutz Hasse vom 17.11.2014, FD-StrVR 2014, 363770.

38 So die Datenschutzbeauftragten des Bundes und der Länder, FD-StrVR 2014, 363770.

Überwachung. Des Weiteren ist auf mögliche Gefahren zu verweisen, die mit der teilweisen Auslagerung von Erhebungs- und Überwachungsprozessen an Private verbunden sein können.<sup>39</sup>

## II. Automatisiertes Fahren

### 1. Szenario

Vermeintlich in den Fokus der Öffentlichkeit geraten sind Kfz-Funktionen, die dem Fahrzeugführer das Fahren gänzlich abnehmen sollen. Kürzlich hat etwa der Autohersteller BMW ein Fahrzeug vorgestellt, das per Smartwatch selbstständig in einem Parkhaus ein- und ausparken kann.<sup>40</sup> Ebenso hat Mercedes einen Prototyp entwickelt, der sich ohne menschliches Zutun fortbewegt und über Gesten gesteuert werden kann.<sup>41</sup> Ein selbstfahrender Audi hat sogar knapp 900 Kilometer aus dem Silicon Valley zur Technik-Messe CES nach Las Vegas zurückgelegt.<sup>42</sup> Auch der Internet-Gigant Google arbeitet bereits seit Jahren an selbstfahrenden Autos, die sogar ohne Lenkrad, Brems- und Gaspedal konzipiert werden sollen.<sup>43</sup>

### 2. Rechtliche Bewertung

Während die Zulassung derartiger Fahrzeuge in den USA, die das Wiener Übereinkommen über den Straßenverkehr von 1968 nicht unterzeichnet haben, weniger problematisch ist, stehen der Verbreitung selbstfahrender Kfz innerhalb Deutschlands bislang wesentliche rechtliche Hindernisse entgegen. Art. 8 Abs. 1 und 5 des Wiener Übereinkommens schreiben bislang vor, dass jedes Fahrzeug einen Führer haben und dieser das Kfz dauernd beherrschen muss. Allerdings haben die Vereinten Nationen (UN) die völkerrechtliche Vereinbarung im Frühjahr 2014 um die Zulässigkeit autonom fahrender Automobile ergänzt, sofern die Assistenz-Systeme vom Fahrer übersteuert oder ausgeschaltet werden können ("when such systems can be overridden or switched off by the driver").<sup>44</sup> Die förmliche Umsetzung der Änderung steht allerdings derzeit noch aus.<sup>45</sup>

Datenschutzrechtlich wird man über § 28 Abs. 1 S. 1 Nr. 1 BDSG mangels Erforderlichkeit eine Datenerhebung und Speicherung aus autonom fahrenden Fahrzeugen ebenso wenig rechtfertigen können, wie über § 28 Abs. 1 S. 1 Nr. 2 BDSG. Schließlich würde hiermit ein völliger Entzug der Handlungsfreiheit des Betroffenen einhergehen. Zu denken wäre gegebenenfalls an eine Einwilligung des Fahrers in konkreten Einzelfällen oder möglicherweise generell in einzelne Fahrten oder Abschnitte von Fahrten. Dabei müsste jedoch geklärt werden, wer die Einwilligung zu erklären hat. In Betracht kämen der Fahrer, aber auch der Halter oder der Eigentümer des Fahrzeugs, etwa der Arbeitgeber.

Weitgehend ungeklärt sind jedoch neben datenschutzrechtlichen Problemen auch Haftungs- und Ethikfragen im Falle von Unfällen, die durch ein algorithmusgesteuertes Fahrzeug verursacht werden.<sup>46</sup> Was passiert etwa, wenn das Fahrzeug defekt ist oder gehackt wird und im Stau 200 statt 20 km/h fährt? Im Rahmen der Gefährdungshaftung nach

§ 7 Abs. 1 StVG haftet der Halter eines Kfz verschuldensunabhängig für Schäden an Menschen oder Sachen, die bei dem Betrieb eines Kraftfahrzeugs oder eines Anhängers, der dazu bestimmt ist, von einem Kraftfahrzeug mitgeführt zu werden, entstehen. Beim Betrieb eines Fahrzeugs hat sich der Unfall ereignet, wenn sich eine Gefahr realisiert, die mit dem Fahrzeug als Verkehrsmittel verbunden ist.<sup>47</sup> Da der Betriebsbegriff weit zu fassen ist,<sup>48</sup> stünde der Subsumtion von Schäden, die durch autonom fahrende Kfz verursacht worden sind, unter die Haftungsnorm des § 7 Abs. 1 StVG grundsätzlich nichts entgegen.<sup>49</sup> Weniger eindeutig stellen sich die haftungsrechtlichen Verhältnisse allerdings mit Blick auf die verschuldensabhängige Haftung des Fahrzeugführers dar, der nicht zugleich Halter des Kfz ist (§ 18 Abs. 1 StVG, §§ 823 Abs. 1, 2 BGB). Es wird daher auch weiterhin fraglich bleiben, wer für eigenmächtig handelnde Maschinen haftet. Das mag rechtlich gesehen Science Fiction sein. Technisch ist es Realität. Das Google-Auto hat schon ca. 1.125 Mio. km unfallfreie Fahrleistung absolviert. Bis 2018 soll es auf der Straße sein.

## III. Verhaltenssteuerung

### 1. Verträge auf Verhalten durch Private

#### a) Szenario

Versicherungstarife, die umsichtiges Fahren belohnen und verantwortungsloses Rasen bestrafen, tragen auf moderne Weise zur Vermeidung von Risiken bei. Sie können Fahrer, Mitfahrer, Fahrgäste und andere Verkehrsteilnehmer schützen. Sie haben einen erzieherischen Charakter, wie der „Drive like a girl“-Tarif einer britischen Versicherung zeigt.<sup>50</sup> Fahranfängerinnen fahren vorsichtiger als Fahranfänger und sind in Belangen des Straßenverkehrs Vorbilder. Da dieses Faktum statistisch belegt ist, wäre die Umerziehung vom

39 Vgl. hierzu auch FD-StrVR 2014, 363770.

40 Vgl. unter [https://www.press.bmwgroup.com/deutschland/pressDetail.html?title=bmw-innovationen-auf-der-consumer-electronics-show-ces-2015-in-las-vegas-360-grad&outputChannelId=7&id=T0198223DE&left\\_menu\\_item=node\\_\\_4098](https://www.press.bmwgroup.com/deutschland/pressDetail.html?title=bmw-innovationen-auf-der-consumer-electronics-show-ces-2015-in-las-vegas-360-grad&outputChannelId=7&id=T0198223DE&left_menu_item=node__4098) (letzter Abruf: 06.03.2015).

41 Vgl. unter <http://www.netzwelt.de/news/150575-ces-mercedes-zeigt-selbstfahrendes-auto.html> (letzter Abruf: 06.03.2015).

42 Vgl. unter <http://www.heise.de/newsticker/meldung/CES-Selbstfahrender-Audi-auf-dem-Weg-nach-Vegas-2508434.html> (letzter Abruf: 06.03.2015).

43 Vgl. unter <http://www.heise.de/newsticker/meldung/Selbstfahrende-Autos-Google-baut-ein-eigenes-Auto-2199035.html> (letzter Abruf: 06.03.2015).

44 Vgl. unter <http://www.unece.org/fileadmin/DAM/trans/doc/2014/wp1/ECE-TRANS-WP1-145e.pdf> (letzter Abruf: 06.03.2015).

45 Vgl. hierzu Lutz, NJW 2015, 119, 122 ff.

46 Dazu der Vorstandsvorsitzende der Daimler AG Zetsche, vgl. unter <http://www.heise.de/newsticker/meldung/Daimler-Chef-Zetsche-Technik-fuer-selbstfahrende-Autos-weitgehend-serienreif-2513828.html> (letzter Abruf: 06.03.2015).

47 Burmann, in: Burmann/Heß/Jahnke/Janker (Hrsg.), Straßenverkehrsrecht, 23. Aufl. 2014 Rn. 7.

48 Burmann, in: Burmann/Heß/Jahnke/Janker (Hrsg.), Straßenverkehrsrecht, 23. Aufl. 2014 Rn. 7.

49 So auch Kremer, RDV 2014, 240, 242 f.

50 Vgl. unter <http://www.drivelikeagirl.com/> (letzter Abruf: 06.03.2015).

Rowdy zum Girly verkehrspolitisch charmant und würde natürlich nicht zuletzt den Versicherungen zu Gute kommen.<sup>51</sup>

Seit Beginn des Jahres 2014 werden daher auch in Deutschland sog. Telematik<sup>52</sup>-Versicherungen angeboten.<sup>53</sup> Die Versicherungsprämie wird dabei in Abhängigkeit des konkreten Fahrverhaltens des Kfz-Halters anhand sog. Score-Werte für Geschwindigkeit, Fahrweise, Stadt- und Nachtfahrten ermittelt.<sup>54</sup> Dabei wird eine Messbox im Fahrzeug des Kfz-Halters installiert. Die gemessenen Daten werden alle 20 Sekunden an ein mit dem Versicherungsgeber kooperierendes Unternehmen gesendet, welches die Daten im Auftrag unter einer Kunden-ID in Score-Werte umrechnet. Über ein Webportal und eine Smartphone-App erhält der Versicherungsnehmer die Möglichkeit, die Daten jeder einzelnen Fahrt nachzuvollziehen. Im Falle eines guten Gesamtscores erhält er einen deutlichen Rabatt auf den zu zahlenden Jahresbeitrag.<sup>55</sup>

### b) Rechtliche Bewertung

Da sich der Versicherungsnehmer einer derartigen Vertragsgestaltung freiwillig unterwirft, ist der Datenumgang insoweit zulässig, als er für die Erfüllung des Vertragszwecks erforderlich ist (§ 28 Abs. 1 Nr. 1 BDSG). Die Grenze der Erforderlichkeit wird insbesondere dann überschritten, wenn mithilfe der übermittelten Daten die Erstellung von Bewegungsprofilen ermöglicht wird. Eine detaillierte Überwachung jeder einzelnen Fahrt ist demnach unzulässig, kann allerdings dadurch vermieden werden, dass die personenbezogenen Daten pseudonymisiert und von einem beauftragten Unternehmen ausgewertet werden, so dass sie dem Versicherungsgeber ausschließlich in Gestalt der ermittelten Score-Werte zur Kenntnis gelangen.<sup>56</sup> Solange die Versicherung kein Profil des bzw. der Fahrer, sondern nur einen Score-Wert sowie ggf. Informationen über Sonderereignisse erhält, kann ein fahrverhaltensbezogener Telematik-Tarif unter Berücksichtigung von § 28b BDSG (Scoring) also rechtskonform ausgestaltet werden. Offen ist aber die Rechtslage bei der Datenübermittlung an die Versicherung als nicht-öffentliche Stelle bei Unfällen. In Betracht käme hier eine Rechtfertigung nach § 28 Abs. 1 S. 1 Nr. 2 BDSG. Ungelöst ist allerdings, wie die Aushebelung des nemo-tenetur-Grundsatzes (z.B. bei § 142 StGB) durch automatische Unfallinformation an die Versicherung verhindert werden kann.<sup>57</sup> Darüber hinaus besteht hier die Gefahr, dass die gesetzlichen Voraussetzungen von Sicherstellungen und Beschlagnahmen (§§ 94 ff. StPO) unterlaufen werden.<sup>58</sup> Die Anordnung durch einen Richter wäre regelmäßig nicht mehr erforderlich, da ein sofortiges Einschreiten der Ermittlungsbeamten mit der Notwendigkeit der Datensicherung zu Beweis Zwecken begründet werden könnte (sog. Gefahr im Verzug, vgl. etwa § 98 Abs. 1 S. 1 StPO).<sup>59</sup> Verfahrensrechtliche Zwangsmaßnahmen zur Verwertung der Daten könnten folglich ohne Rücksicht auf die Wahrung der Verhältnismäßigkeit vorgenommen werden.<sup>60</sup>

Die Gefahr einer möglichen Überwachung geht indes nicht nur vom Versicherungsgeber aus. Eine Kontrolle des

Fahrverhaltens kommt vielmehr gerade durch den Versicherungsnehmer in Betracht, sofern dieser von dem Fahrer des telematisch versicherten Kfz personenverschieden ist. Besondere Bedeutung kommt in dieser Konstellation dem Einwilligungserfordernis zu. Eine vertragliche Vereinbarung über den Datenumgang wird regelmäßig nur im Verhältnis zwischen dem Kfz-Halter und dem Anbieter des Telematik-Versicherungstarifs vorliegen. Um auch das Fahrverhalten eines Dritten, der in die Vereinbarung nicht einbezogen ist, rechtswirksam erfassen zu können, muss folglich zunächst dessen Einwilligung eingeholt werden. Erfolgen kann dies über eine vertragliche Verpflichtung des Halters, dem Fahrer eine derartige Erklärung im Vorfeld der Kfz-Nutzung abzuverlangen.<sup>61</sup> Sofern der Fahrer aber – wie etwa im Falle der Inanspruchnahme eines Mietwagens oder Carsharing-Dienstes – gleichzeitig mit der Abgabe mehrerer Erklärungen konfrontiert ist, muss die schriftlich erteilte Einwilligung in den Einsatz von Telematik besonders hervorgehoben werden (§ 4a Abs. 1 S. 4 BDSG). Jedenfalls durch graphische Akzentuierung oder aber durch Vorlage einer separaten Einwilligungserklärung<sup>62</sup> soll dem Betroffenen verdeutlicht werden, dass im Verlauf der Kfz-Nutzung fahrtbezogene Daten erhoben und verarbeitet werden, die angesichts der Bestimmbarkeit des Fahrers Personenbezug aufweisen.

Probleme der Telematik-Versicherung können sich ferner mit Blick auf das Verbot automatisierter Einzelentscheidungen ergeben (§ 6a Abs. 1 BDSG). Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen demnach nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche

51 Vgl. hierzu auch Schwartzmann unter <http://www.marktforschung.de/nachrichten/marktforschung/researchability-verantwortung-fuer-markt-und-daten-wer-bremst-verdient/> (letzter Abruf: 06.03.2015).

52 Unter dem Begriff Telematik versteht man ein „Mittel der Informationsverknüpfung von mindestens zwei Informationssystemen mit Hilfe eines Telekommunikationssystems sowie einer speziellen Datenverarbeitung“, vgl. Nora/Minc, L'informatisation de la société: rapport à M. le Président de la République, 1978.

53 Zuvor wurde dies bereits auf dem amerikanischen und britischen Versicherungsmarkt erfolgreich praktiziert. Erster deutscher Anbieter ist die Direktversicherung der Sparkassen mit dem „Telematik-Sicherheits-Service S-Drive“, vgl. hierzu unter <https://www.sparkassen-direkt.de/telematik> (letzter Abruf: 06.03.2015).

54 Vgl. hierzu unter <https://www.sparkassen-direkt.de/popups/wie-wird-der-score-berechnet.html> (letzter Abruf: 06.03.2015).

55 Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302 f.

56 Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302, 303.

57 Würde der Betroffene zum Hergang eines bestimmten Geschehens die Aussage verweigern, könnte er dennoch anhand seiner Fahrzeugdaten eines Verkehrsverstoßes (z.B. §§ 142, 315 ff. StGB) überführt werden. Gleiches gilt mit Blick auf etwaige Zeugnisverweigerungsrechte von Angehörigen (§ 52 StPO).

58 Nach BVerfG, NJW 2005, 1917, 1920 erlaubt § 94 StPO gerade auch die Sicherstellung von Daten.

59 Vgl. hierzu auch unten unter C.

60 Mielchen, SVR 2014, 81, 85 f.

61 Kinast/Kühnl, NJW 2014, 3057, 3059.

62 Für diese Lösung Kinast/Kühnl, NJW 2014, 3057, 3059.

Bewertung und darauf beruhende Entscheidung durch eine natürliche Person stattgefunden hat. Werden demnach zur Bewertung des individuellen Fahrverhaltens ausschließlich die ermittelten Score-Werte herangezogen, liegt hierin eine automatisierte Datenverarbeitung. Eine hierauf basierende Entscheidung mit rechtlichen Folgen liegt bereits in dem möglichen Anfall einer gegenüber dem Vorjahr erhöhten Versicherungsprämie, deren Festlegung ohne menschliche Gegenprüfung und entsprechende Beurteilungsspielräume erfolgt.<sup>63</sup>

## 2. Problemfall Arbeitsverhältnis<sup>64</sup>

### a) Szenario

Ein besonderes Überwachungsrisiko ergibt sich mit Blick auf die Nutzung von Dienstfahrzeugen im Verhältnis Arbeitgeber und Arbeitnehmer. Da er den Großteil der durch sein Kfz erhobenen Daten uneingeschränkt einsehen kann, ist es dem Arbeitgeber grundsätzlich möglich, den Arbeitnehmer im Wege der Standortbestimmung oder anhand seines Fahrverhaltens umfassend zu kontrollieren. An einer vertraglichen datenschutzrechtlichen Legitimation fehlt es in dieser Konstellation bereits insoweit, als die dem Datenumgang zugrundeliegende Vereinbarung ausschließlich zwischen Arbeitgeber und Kfz-Hersteller oder Versicherungsgeber besteht.<sup>65</sup>

### b) Rechtliche Bewertung

Der Erlaubnistatbestand des § 32 Abs. 1 S. 1 BDSG<sup>66</sup> rechtfertigt zwar die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zur Durchführung des Beschäftigungsverhältnisses. Allerdings sind hiervon ausschließlich Fälle der Kosten-, Wirtschaftlichkeits- und Missbrauchskontrolle, nicht dagegen eine profilmäßige Aufzeichnung des Arbeitsverhaltens erfasst.<sup>67</sup> Eine Einwilligung des Arbeitnehmers in die datenmäßige Erfassung seines Dienstwagens ist zwar grundsätzlich möglich. Probleme können sich allerdings mit Blick auf die Freiwilligkeit ergeben. Hieran kann es etwa fehlen, wenn die Einwilligung in einer Situation wirtschaftlicher oder sozialer Schwäche oder Unterordnung erteilt wird oder der Betroffene durch übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe seiner Daten verleitet wird.<sup>68</sup>

Darüber hinaus sind im Arbeitsverhältnis die Mitbestimmungsrechte des Betriebsrats zu beachten. Gemäß § 87 Abs. 1 Nr. 6 BetrVG ist dieser insbesondere zu beteiligen, wenn es um die Einführung und Anwendung von technischen Einrichtungen geht, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.<sup>69</sup> Sofern dem Arbeitnehmer also ein Dienstwagen zur Verfügung steht, der mit entsprechenden optischen, mechanischen, akustischen oder elektronischen Geräten zur Datenerhebung oder deren alleiniger Auswertung durch den Arbeitgeber ausgestattet ist,<sup>70</sup> muss den Belangen der Arbeitnehmer durch Einschaltung des Betriebsrats Rechnung getragen werden.<sup>71</sup> Als zentrales Instrument der Mitbestimmung stellt sich angesichts ihrer unmittelbaren und zwingenden Geltung – jedenfalls in größeren Unternehmen – die

Betriebsvereinbarung dar (§ 77 Abs. 4 BetrVG).<sup>72</sup> Diese kann zugleich als den Datenumgang legitimierende Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG dienen.<sup>73</sup>

## IV. Verkehrssicherheit

### 1. eCall

#### a) Szenario

Ab Oktober 2015 wird die Vernetzung in Kraftfahrzeugen in Europa Pflicht. Neuwagen sollen ab diesem Zeitpunkt europaweit mit dem automatischen Notrufsystem eCall (emergency call) ausgestattet werden, um bei Unfällen eigenständig eine Sprachverbindung mit Notfalleinrichtungen aufbauen und Fahrzeugdaten zum Unfall übertragen zu können.<sup>74</sup> Dass diese Informationen Leben retten können, steht außer Frage. Weil vernetzte Autositze unter Umständen auch EKGs schreiben können, kann die Box im Zweifel sogar entscheiden, ob sie noch den Notarzt oder schon den Leichenwagen rufen muss. Schließlich hilft es dem Verkehrstoten nicht, wenn man ihm einen Krankenwagen schickt. Er wird gebraucht, um an anderer Stelle das Leben eines Schwerverletzten zu retten. Das ist eine harte und nüchterne, aber nicht erschreckende Erkenntnis.

#### b) Rechtliche Bewertung

Mit Blick auf die datenschutzrechtliche Legitimation des eCalls muss zwischen den Basisfunktionen des Notruf-

63 Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302, 304 f.

64 Zu rechtlichen Fragen von vernetzten Fahrzeugen und Beschäftigtendatenschutz vgl. eingehend Jaspers/Franck, RDV 2015, in diesem Heft.

65 Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302, 303 f.

66 Dreh- und Angelpunkt des Beschäftigtendatenschutzes auf europäischer Ebene ist die Regelung des Art. 82 DS-GVO-E. Danach können die Mitgliedsstaaten die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext in den Grenzen der Datenschutz-Grundverordnung regeln. Wie der Beschäftigtendatenschutz auf nationaler Ebene künftig aussehen wird, hängt allerdings maßgeblich von den endgültigen Vorgaben der Verordnung ab und kann daher erst mit deren endgültigem Inkrafttreten geklärt werden, vgl. hierzu auch Schwartzmann/Ohr, Recht der Sozialen Medien, 1. Aufl. 2015, IV. Kap. Rn. 232 sowie allgemein zur Datenschutz-Grundverordnung VIII. Kap. Rn. 287.

67 So zur sog. Telefondatenerfassung Gola/Schomerus, in: Gola/Schomerus (Hrsg.), BDSG, 11. Aufl. 2012, § 32 Rn. 17. Soweit eine derartige Beschränkung bereits für die Überwachung des Arbeitnehmers am Arbeitsplatz aufgestellt wird, muss dies erst recht für die Verhaltenskontrolle an einem externen Arbeitsplatz, etwa einem Dienstfahrzeug, gelten.

68 BGH, NJW 2008, 3055, 3056.

69 Dies ist dann der Fall, wenn die Einrichtung zur Überwachung objektiv und unmittelbar geeignet ist, ohne Rücksicht darauf, ob der Arbeitgeber dieses Ziel verfolgt und die durch die Überwachung gewonnenen Daten tatsächlich ausgewertet, vgl. BAG, AP BetrVG 1972 § 87 Überwachung Nr. 3.

70 Vgl. hierzu Kania, in: Erfurter Kommentar zum Arbeitsrecht, 15. Aufl. 2015 Rn. 48 f.

71 Fischer, Flottenmanagement 2015, 52, 54.

72 Kania, in: Erfurter Kommentar zum Arbeitsrecht, 15. Aufl. 2015 Rn. 3.

73 BAG, NJW 1987, 674, 677.

74 Rechtliche Grundlagen des eCall sind die IVS-RL (vgl. hierzu oben unter A.I.2.b), die delegierte Verordnung (EU) Nr. 305/2013 der Kommission vom 26. November 2012 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die harmonisierte Bereitstellung eines interoperablen EU-weiten eCall-Dienstes sowie der Beschluss Nr. 585/2014/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über die Einführung des interoperablen EU-weiten eCall-Dienstes.

systems und den hierauf aufbauenden Zusatzdiensten unterschieden werden. Eine Mobilfunkverbindung stellt das Basissystem ausschließlich bei Auslösen der Airbags oder bei manueller Aktivierung der Notruf Funktion her. Durch den sog. Mindestdatensatz werden nur die zur Notfallrettung erforderlichen Daten übermittelt. Von der Notrufstelle dürfen diese Daten ausschließlich für die Dauer der Rettungsmaßnahmen gespeichert und genutzt werden.<sup>75</sup> Vor diesem Hintergrund ist der Datenumgang im Rahmen des Basissystems nach deutschem Recht bereits durch § 28 Abs. 1 S. 1 Nr. 2 BDSG legitimiert.<sup>76</sup> Hieran vermag auch das Fehlen einer optionalen Abschaltung des Notrufsystems nichts zu ändern. Zum einen dürfte die Verkürzung der Reaktionszeit der Notrufdienste, die Senkung von Todesfällen und Verhinderung von Folgeunfällen<sup>77</sup> bereits im eigenen Interesse des Halters bzw. Fahrers liegen. Zum anderen ist der Schutzzweck des eCall nicht auf ihn allein beschränkt, sondern erstreckt sich zugleich auf seine Mitfahrer sowie auf die übrigen Verkehrsteilnehmer.<sup>78</sup>

Probleme des Datenschutzes können sich allerdings mit Blick auf die zusätzlichen Dienste ergeben, die auf dem Basisnotrufsystem aufsetzen. Der für den eCall bestehende gesetzliche Rahmen kann hier keine Geltung beanspruchen. Ebenso wenig sind die gesetzlichen Erlaubnistatbestände des IVSG und BDSG einschlägig.<sup>79</sup> Datenschutzrechtlich legitimiert können die Zusatzdienste demzufolge grundsätzlich nur im Wege der Einwilligung sein. Ausnahmsweise ist bei einem Monitoring von Vitalitätsfunktionen durch das Fahrzeug eine Legitimation über § 28 Abs. 6 Nr. 1 BDSG denkbar. Die gesetzliche Erlaubnis zum Umgang mit diesen Gesundheitsinformationen als besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG greift allerdings nur bei fehlender Einwilligungsfähigkeit, sprich bei bereits eingetretenem Notfall.

Ähnlich wie bei der Telematik-Versicherung ergeben sich im Falle des eCall ebenfalls Schwierigkeiten, sobald Dritte in den Datenumgang einbezogen werden. Grundsätzlich müsste jeder Mitfahrer, dessen Daten etwa durch Airbag oder Anschnallgurt erfasst werden können, im Vorfeld der Fahrt eine Einwilligung erklären, die den Voraussetzungen des § 4a BDSG hinreichend Rechnung trägt. Probleme dürften sich bereits angesichts der grundsätzlich erforderlichen Schriftform ergeben. Zwar lässt § 4a Abs. 1 S. 3 BDSG aufgrund besonderer Umstände auch andere Formen der Einwilligung zu. Allerdings muss der Betroffene auch in diesen Fällen eindeutig identifizierbar und die Höchstpersönlichkeit der Einwilligung sichergestellt sein.<sup>80</sup> Darüber hinaus muss die Einwilligung auch informiert erfolgen. Der Betroffene kann nur frei über die Einwilligung entscheiden, wenn er über die vorgesehenen Verarbeitungen in Kenntnis gesetzt wird und er weiß, was mit den Daten geschehen soll.<sup>81</sup> Fraglich ist allerdings, auf welche Weise die Informationen dem unüberschaubaren Kreis an Betroffenen zugänglich gemacht werden soll.<sup>82</sup> Weitere Schutzlücken ergeben sich mit Blick auf die Widerruflichkeit der Einwilligung. Möglich wäre ein Widerruf nur dann, wenn der entsprechende Zusatz-

dienst ohne Rücksicht auf die Funktionsfähigkeit des Basissystems deaktiviert werden kann.<sup>83</sup>

## 2. Dash-Cams

### a) Szenario

Immer größerer Beliebtheit erfreut sich der Einsatz von Videokameras im Innen- und Außenbereich von Fahrzeugen. Nachvollziehbar und durchaus legitim ist dabei das Interesse ihrer Verwender an der Sicherung von Beweismitteln bei Vandalismus oder Angriffen in Taxis und öffentlichem Nahverkehr sowie im Falle möglicher Verkehrsunfälle. Sofern aber künftig jedes Kfz standardmäßig das umliegende Verkehrsgeschehen aufzeichnet, ist hiermit eine permanente, anlasslose und flächendeckende Überwachung verbunden. Sie beträfe damit massenweise Verkehrsteilnehmer jeglicher Art (Fahrer, Beifahrer, Radfahrer, Fußgänger), die sich der filmischen Aufzeichnung ihrer Person nur schwer entziehen können. Einerseits wird der Normalbürger mit einer derartigen Überwachung schon nicht rechnen, da sie für ihn nur schwer erkennbar ist. Andererseits bestehen für denjenigen, der nicht völlig isoliert leben möchte, selbst im Kenntnisfall kaum Alternativen zur Fortbewegung im öffentlichen Straßenraum.

### b) Rechtliche Bewertung

Gemäß § 6b Abs. 1 BDSG ist die Videoüberwachung öffentlich zugänglicher Räume nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Mit Blick auf die datenschutzrechtliche Legitimation von Videoaufnahmen ist zwischen Innen- und Außenkameras zu unterscheiden. In beiden Fällen erforderlich ist eine Information über den Kamerabetrieb (z.B. „Dieser Bereich wird videoüberwacht.“) und die verantwortliche Stelle (§ 6b Abs. 2 BDSG). Sofern die erhobenen Daten einer bestimmten Person zugeordnet werden, ist diese über eine Verarbeitung oder Nutzung zu benachrichtigen (§ 6b Abs. 4 i.V.m. 19a und 33 BDSG). Für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich ist dabei derjenige, der das Kamerasystem installiert hat und/oder die hergestellten Aufnahmen auswerten kann.<sup>84</sup>

75 Lüdemann/Sengstacken, RDV 2014, 177, 179.

76 Kremer, RDV 2014, 240, 249.

77 Vgl. Erwägungsgründe 6 und 7 der Delegierten Verordnung (EU) Nr. 305/2013.

78 Lüdemann/Sengstacken, RDV 2014, 177, 179.

79 Vgl. hierzu Lüdemann/Sengstacken, RDV 2014, 177, 179 f.

80 Lüdemann/Sengstacken, RDV 2014, 177, 181.

81 Gola/Schomerus, in: Gola/Schomerus (Hrsg.), BDSG, 11. Aufl. 2012, § 4a Rn. 26.

82 Lüdemann/Sengstacken, RDV 2014, 177, 181.

83 Lüdemann/Sengstacken, RDV 2014, 177, 181.

84 Lachenmann/Schwiering, NZV 2014, 291, 292.

### aa) Innenkameras

In öffentlichen Nahverkehrsmitteln kann der Betrieb von Innenkameras sowohl präventiv als auch repressiv zur Wahrung des Hausrechts gerechtfertigt sein. Unverhältnismäßig ist die anlasslose Videoüberwachung des gesamten Fahrtgeschehens dagegen in Taxis. Dies gilt sowohl für den Fahrgast als auch für den Fahrer selbst, der insoweit den Regelungen des Beschäftigtendatenschutzes (§ 32 BDSG) unterliegt. Vorzugswürdig sind daher solche Maßnahmen, die eine geringere Intensität aufweisen und dennoch die Sicherheitsinteressen des Fahrers hinreichend wahren. In Betracht kommen etwa die bloße Fertigung einzelner Standbilder von den Fahrgästen, die manuelle Aktivierung der Videoaufnahme oder eines stillen Alarms oder ein GPS-gestützter Notruf in Bedrohungs- oder Angriffsfällen.<sup>85</sup>

### bb) Außenkameras

Ein noch deutlich höheres Potential zur Verletzung von Persönlichkeitsrechten weist der Betrieb von Kameras auf, die im Außenbereich von Fahrzeugen angebracht sind. Selbst wenn der Umstand der Videoaufzeichnung kenntlich gemacht wird, fehlt es, soweit das Kfz in Bewegung ist, regelmäßig an einer zumutbaren Wahrnehmungsmöglichkeit des entsprechenden Hinweises durch die anderen Verkehrsteilnehmer. Da sich der Überwachende im öffentlichen Straßenraum nicht auf die Wahrnehmung des Hausrechts berufen kann,<sup>86</sup> kann der Kameraeinsatz ausschließlich zur Wahrnehmung berechtigter Interessen für konkrete Zwecke legitimiert sein. Zwar mag die Sicherung von Beweismitteln im Falle möglicher Unfallszenarien in ihrer Zwecksetzung hinreichend konkret sein. Da die gezielte Überwachung öffentlicher Bereiche für die Betroffenen aber eine schwerwiegende Beeinträchtigung ihres Rechts auf informationelle Selbstbestimmung sowie des Rechts am eigenen Bild darstellt, stehen der Aufzeichnung überwiegend schutzwürdige Belange der Verkehrsteilnehmer gegenüber.<sup>87</sup> Der Bestimmung über Preisgabe und Verwendung persönlicher Daten sind die Betroffenen bereits deshalb entzogen, weil sie weder beeinflussen können, ob, noch wann und wie lange sie von einer Außenkamera erfasst werden.<sup>88</sup> Der Einzelne könnte sich demzufolge in der Öffentlichkeit nicht mehr frei und unbeschwert bewegen, ohne eine präventivbildliche Aufzeichnung seiner Person befürchten zu müssen.<sup>89</sup> Eine Außenüberwachung mit derartiger Eingriffsintensität ist weder verhältnismäßig im engeren Sinne noch erforderlich, um den Hergang möglicher Unfälle und sonstiger Zwischenfälle zu klären. Als milderer Mittel kommt insoweit die Feststellung des Unfallverlaufs durch die Polizei unter Rückgriff auf sämtliche zulässigerweise zur Verfügung stehende Beweismittel in Betracht.<sup>90</sup> Ein überwiegendes Interesse an einer Videoüberwachung durch Privatpersonen verneint die Rechtsprechung selbst bei parkenden Fahrzeugen, wenn es im Vorfeld der Kamerainstallation bereits vermehrt zu Beschädigungen innerhalb des Überwachungsbereichs gekommen ist.<sup>91</sup>

Ein Eingriff in das Recht auf informationelle Selbstbestimmung kann selbst dann gegeben sein, wenn überhaupt keine Videoaufnahmen gefertigt, sondern lediglich der Eindruck einer funktionsfähigen Kamera erweckt wird. Sofern der Betroffene befürchten muss, jederzeitiger Beobachtung durch Dritte zu unterliegen, wird bei ihm der gleiche Überwachungsdruck unabhängig davon erzeugt, ob eine Aufnahme tatsächlich erfolgt oder lediglich vorgetäuscht wird.<sup>92</sup> Der Bundesgerichtshof hält einen Unterlassungsanspruch daher bereits dann für möglich, wenn eine Überwachung objektiv ernsthaft befürchtet werden muss.<sup>93</sup>

Neben dem Recht auf informationelle Selbstbestimmung verletzt der private Betrieb von Außenkameras das allgemeine Persönlichkeitsrecht der übrigen Verkehrsteilnehmer auch in seiner Ausprägung des Rechts am eigenen Bild. Auch wenn das Beweissicherungs- und -erhebungsinteresse der Verwender mit Blick auf das generelle Unfallpotential des Straßenverkehrs dem Grunde nach schutzwürdig ist, überwiegt es die mit der permanenten, anlasslosen und vielfach ohne Kenntnis der Betroffenen erfolgenden Überwachung verbundene Beeinträchtigung des Persönlichkeitsrechts nicht. Diese Erkenntnis führt nicht nur prozessual zur Unverwertbarkeit der Aufnahmen als Beweismittel.<sup>94</sup> Auch materiell-rechtlich ist die Verbreitung oder öffentliche Schaustellung des aufgezeichneten Materials ohne Einwilligung der Betroffenen verboten (§ 22 S. 1 KUG).<sup>95</sup>

Weitere Probleme strafrechtlicher Art können sich ferner mit Blick auf den zum 27.1.2015 neu gefassten § 201a Abs. 1 Nr. 2 StGB ergeben. Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird danach bestraft, wer eine Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt, unbefugt herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt. Der räumliche Anwendungsbereich der Vorschrift ist nun nicht mehr auf Wohnungen oder gegen Einblick besonders geschützte Räume beschränkt, so dass auch Auf-

85 Lachenmann/Schwiering, NZV 2014, 291, 294.

86 Das Hausrecht am Auto umfasst nicht zugleich das Recht, öffentliche Verkehrsflächen mittels Videokamera zu erfassen, vgl. hierzu <https://www.datenschutzzentrum.de/video/20120112-videoueberwachung-taxis.html> (letzter Abruf: 06.03.2015).

87 BGH, MMR 2010, 502; NJW, 1995, 1955, 1957; AG München, RDV 2014, 345.

88 BGH, NJW 1995, 1955, 1957 zur Videoüberwachung öffentlicher Flächen zur Störungsabwehr.

89 Zu dem von Außenkameras ausgehenden Überwachungsdruck <https://www.datenschutzzentrum.de/video/20120112-videoueberwachung-taxis.html> (letzter Abruf: 06.03.2015).

90 Lachenmann/Schwiering, NZV 2014, 291, 295.

91 OLG Düsseldorf, NJW 2007, 780, 781; Lachenmann/Schwiering, NZV 2014, 291, 295 m.w.N.

92 LG Bonn, NJW-RR 2005, 1067, 1068 m.w.N.

93 BGH, MMR 2010, 502.

94 AG München, RDV 2014, 345, 347.

95 Der Ausnahmetatbestand des § 23 Abs. 1 Nr. 2 KUG, wonach solche Aufnahmen, die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit zeigen, ohne deren Einwilligung verbreitet oder zur Schau gestellt werden dürfen, greift hier nicht, da die bildliche Erfassung des einzelnen Verkehrsteilnehmers gerade Ziel des Kameraverwenders ist, AG München, RDV 2014, 345, 346.

nahmen im öffentlichen Straßenraum strafrechtlich erfasst sein können.<sup>96</sup>

### C. Herausforderung – Wem „gehören“ die Daten aus dem Fahrzeug?

Im Detail noch unbeantwortet ist die Frage nach der Hoheit über die Daten beziehungsweise nach dem Recht an einer Information aus dem Fahrzeug. Fraglich ist dies etwa mit Blick auf die Auswertung der gefahrenen Geschwindigkeit nach einem Verkehrsunfall. Die Information, ob ein Autofahrer in einer Tempo-100-Zone 150 km/h gefahren ist, ist wichtig. Sie interessiert die Versicherung so sehr wie Polizei. Letztere kann die betreffenden Daten gegebenenfalls mit Hilfe der Fahrzeug-Identifizierungsnummer (FIN) in Erfahrung bringen, die sie wiederum durch einen Abgleich mit umliegenden Intelligenten Verkehrssystemen (IVS) (z.B. Ampeln, Verkehrsanzeigen, Mautbrücken, etc.) ermitteln kann. Die Strafprozessordnung enthält zwar Erlaubnistatbestände im Sinne des § 4 Abs. 1 BDSG. So gestattet § 94 StPO die Sicherstellung und Beschlagnahme von Daten als Beweismittel.<sup>97</sup> Problematisch ist aber, ob dies beim Halter, beim Hersteller oder beim Dienstleister erfolgen muss. Zu berücksichtigen ist hier auch ein mögliches Beschlagnahmeverbot nach § 97 Abs. 1 Nr. 1 StPO i.V.m. § 52 StPO. Fragen stellen sich ferner mit Blick auf den Entfall des Richtervorbehalts bei der Beschlagnahme nach § 98 StPO. Er kann greifen, wenn man annimmt, dass bei nur flüchtig oder kurzzeitig gespeicherten Daten Gefahr im Verzug vorliegt.<sup>98</sup> Auch wenn die Rechtslage hier mit Blick auf die Befugnisse der Strafverfolgungsbehörden noch ungeklärt ist, positioniert sich der VW-Chef Winterkorn zumindest eindeutig: „Daten muss man im Auto jederzeit sperren können. Unsere Philosophie ist, dass die Daten, die Sie als Fahrer erzeugen, Ihre Daten sind. (...) Wir müssen (...) verhindern, dass alle Welt weiß, wer wo wie schnell fährt.“<sup>99</sup> Auch der 52. Deutsche Verkehrsgerichtstag hat sich für die Wahrung der Datenhoheit des Betroffenen ausgesprochen und zu deren Umsetzung folgende Punkte aufgestellt: Sicherung des informationellen Selbstbestimmungsrechts durch Transparenz und Wahlfreiheit des Betroffenen; umfassende und verständliche Information des Käufers bei Vertragsschluss, welche Daten generiert/verarbeitet und auf welchen Wegen und zu welchen Zwecken sie übermittelt werden; Sicherung des Prinzips der Datensparsamkeit (Möglichkeit zu Kontrolle und Unterbindung von freiwilliger/vertraglich vereinbarter Datenübermittlung an Dritte); verfahrensrechtliche und technische Schutzvorkehrungen bei Daten, die aufgrund gesetzlicher Regelung erhoben, gespeichert oder übermittelt werden sollen; spezifische Regelung von Zugriffsrechten der Strafverfolgungsbehörden und Gerichte.<sup>100</sup> Sofern diese Parameter in die Praxis umgesetzt werden können, dürfte es um die datenschutzrechtlichen Anforderungen nicht schlecht bestellt sein. Es werden aber mit Blick auf die vielfältigen Begehrlichkeiten Umsetzungsprobleme entstehen. Die grundsätzliche Problematik bleibt angesichts derart allgemein gehaltener Prinzipien offen.

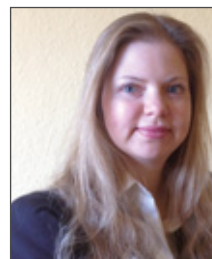
### D. Fazit

*Die Perspektiven des Einsatzes intelligenter Fahrzeuge sind weitreichend. Sie betreffen Datenschutz sowie Datensicherheit und erfassen weit mehr als die hier ausgewählten Szenarien. Der Überblick zeigt, dass das Datenschutzrecht jedenfalls in seinen Grundpfeilern den praktischen Gegebenheiten vernetzter Fahrzeuge gewachsen ist. Allerdings liegen die datenschutzrechtlichen Probleme auf der Hand. Sie beginnen bei schlecht oder nicht dokumentierter Hard- und Software und reichen über fehlendes technisches Verständnis für die Personenbeziehbarkeit der erhobenen Daten bis hin zu Schwierigkeiten bei der Ermittlung und Ansprache der Betroffenen. Zugleich wirken eine Vielzahl von nebeneinander und miteinander agierenden verantwortlichen Stellen zusammen. Auch erlaubt der Einsatz von Big-Data-Technologien Profilbildungen und wirft Probleme der Zweckbindung auf. Schließlich geht man bei Connected Cars mit personenbezogenen Daten in der Cloud um, was neben datenschutzrechtlichen Problemen auch Fragen der IT-Sicherheit berührt. Der Gesetzgeber muss hier darauf achten, dass die Wirtschaft ihre Verantwortung für datenrelevante Produkte und Dienste nicht auf den Verbraucher verlagert, sondern, etwa im Bereich der Produkthaftung, auch die Risiken zunehmend autonom handelnder Technik berücksichtigt. Die Einwilligung allein, so unverzichtbar sie ist, bietet jedenfalls in Mehrbeteiligtenbeziehungen keinen hinreichenden Schutz des Betroffenen und stößt in ihrer derzeitigen verfahrensmäßigen Umsetzung an Grenzen.*



#### Prof. Dr. Rolf Schwartzmann

Rolf Schwartzmann lehrt Medienrecht an der Fachhochschule Köln und ist Leiter der Kölner Forschungsstelle für Medienrecht ([www.medienrecht.fh-koeln.de](http://www.medienrecht.fh-koeln.de)). Er ist Mitherausgeber der RDV und Vorsitzender der GDD.



#### Sara Ohr

Ass. iur. Sara Ohr ist wissenschaftliche Mitarbeiterin an der Forschungsstelle.

<sup>96</sup> Zur Neufassung des § 201a StGB vgl. auch Schwartzmann/Ohr, *Recht der Sozialen Medien*, 1. Aufl. 2015, III. Kap. Rn. 172.

<sup>97</sup> Vgl. hierzu bereits oben unter B.III.1.b).

<sup>98</sup> Vgl. hierzu bereits oben unter B.III.1.b).

<sup>99</sup> Interview im Stern Nr. 10/2015, S. 78.

<sup>100</sup> Vgl. Empfehlung Arbeitskreis VII, 52. Deutscher Verkehrsgerichtstag, abrufbar unter [http://www.gdv.de/wp-content/uploads/2014/01/Verkehrsgerichtstag\\_2014\\_Empfehlungen\\_Arbeitskreis\\_7.pdf](http://www.gdv.de/wp-content/uploads/2014/01/Verkehrsgerichtstag_2014_Empfehlungen_Arbeitskreis_7.pdf) (letzter Abruf: 06.03.2015).

RA Andreas Jaspers/Dr. iur. Lorenz Franck

## Connected Car und Beschäftigtendatenschutz

*Hinter den schillernden Begriffen "Connected Car" oder "Car-to-X" verbergen sich unüberschaubar viele Funktionalitäten und Konnektivitäten. Der „gläserne Autofahrer“ avanciert dadurch zum Schreckgespenst. Die zunehmende Ver-*

*netzung und Automatisierung im Fahrzeug macht natürlich auch vor dem betrieblichen Flottenmanagement nicht Halt. Der folgende Beitrag erörtert die arbeitsrechtlichen Implikationen dieses Industrietrends.*

### I. Überblick

Die einstige Vorstellung von einer datenfreien Fahrt<sup>1</sup> ist überholt. Heute wirken bis zu achtzig Steuergeräte in einem modernen Kraftfahrzeug zusammen, die ihre Daten zum Teil dauerhaft in integrierten Speichern ablegen. Hinzu kommen zahlreiche Protokolle zur Kommunikation mit der Außenwelt<sup>2</sup>. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen<sup>3</sup>. Mancherorts wird sogar vom „Verrat durch den eigenen Pkw“ gesprochen<sup>4</sup>.

Der Einsatz dieser Technologien wirft an sich schon datenschutzrechtliche Fragen auf. Der Beschäftigtendatenschutz als bereichsspezifische Spezialmaterie gilt dabei im Allgemeinen als strengeres Datenschutzrecht<sup>5</sup>. Sollen also Car-to-X-Verbindungen im Unternehmensfuhrpark Verwendung finden, ist genau zu prüfen, welche Daten anfallen und was mit ihnen geschieht. Die an dieser Stelle häufig gestellte Frage, wem die Daten aus dem Fahrzeug „gehören“<sup>6</sup>, führt für hiesige Zwecke allerdings nicht weiter. Das Datenschutzrecht greift immer dann, wenn die Daten einen Personenbezug aufweisen.

### II. Datenkategorien

#### 1. Positionsdaten

Positionsdaten fallen in diversen Fahrzeugsystemen an. Zu nennen ist zunächst das Navigationssystem, welches kontinuierlich Positionsdaten verarbeitet. Die eingegebenen Zielorte und letzten Routen bleiben in aller Regel im Gerät gespeichert. Eine Außenkonnektivität ist jedoch hierbei für gewöhnlich nicht vorgesehen<sup>7</sup>.

Das Notrufsystem eCall überträgt dagegen die Position eines verunfallten Fahrzeuges automatisch an eine Leitstelle. Das System ist „schlafend“ konzipiert, sendet also erst im Ernstfall<sup>8</sup>.

Intelligente Kennzeichen ermöglichen es, Ein- und Ausfahrten in Parkhäusern und auf Werksgeländen zu protokollieren<sup>9</sup>. Zumindest mittelbar ergeben sich gefahrene Routen auch aus aggregierten Informationen öffentlicher Ladestationen für Elektroautos<sup>10</sup>. Hier werden die jeweilige Kunden-

ID und der Standort der Ladesäule zu Abrechnungszwecken erhoben.

Im Logistikbereich kann die Verfolgung ständig aktueller Positionsdaten eine Rolle spielen, ebenso wenn Fahrzeuge einer Rufbereitschaft unterliegen. Die jeweiligen Disponenten müssen ggf. Routen, Reichweiten und etwaige Verspätungen in Echtzeit verfolgen können. Infrastrukturdienste wie Stau-<sup>11</sup> oder Eiswarnungen<sup>12</sup> sind ebenfalls auf Positionsdaten angewiesen.

Elektronische Fahrtenbücher sind schließlich ein Mittel, steuerliche Vergünstigungen für privat genutzte Dienstfahrzeuge geltend zu machen. Die zurückgelegten Strecken werden automatisch aufgezeichnet und sodann vom Mitarbeiter als dienstlich oder privat veranlasst gekennzeichnet<sup>13</sup>.

#### 2. Telekommunikationsdaten

Die im fahrzeugeigenen Infotainmentsystem integrierte Freisprechanlage ist unter Umständen in der Lage, Kontakt- und Verbindungsdaten zu speichern. Das Notrufsystem eCall bringt zugleich ab Werk ein Mobilfunkmodul mit und eröffnet damit den Weg zu weiteren kommunikationsgestützten Zusatzdiensten<sup>14</sup>.

1 Vgl. Hassemer, NZV 1995, 169, 171 zum 33. Verkehrsgerichtstag 1995 in Goslar.

2 Übersicht bei Asaj, DuD 2011, 558, 559. Zu nennen sind bspw. OBD (II), GSM/UMTS, WLAN, Bluetooth, NFC, GPS u.v.m.

3 Entschließung der 88. DSK am 8./9.10.2014 („Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert“), online unter [http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK\\_DatenschutzImKfz.pdf](http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_DatenschutzImKfz.pdf).

4 Mielchen, SVR 2014, 81 ff.

5 Dies gilt, obwohl es bislang nicht zu einem eigenständigen Beschäftigtendatenschutzgesetz gekommen ist. Zu § 32g des einstigen Entwurfs Reiter/Methner, DSRITB 2014, 371, 378.

6 Grundlegend Roßnagel, SVR 2014, 281 ff.; ferner Kraus, DSRITB 2014, 381, 383 ff.; Asaj, DuD 2011, 558.

7 Treffend Rihaczek, DuD 2011, 5.

8 Grundlegend zum eCall-System Lüdemann/Sengstacken, RDV 2014, 177 ff.

9 Lüdemann/Sengstacken/Vogelpohl, ZD 2015, 55, 59.

10 Hierzu eingehend Lüdemann/Jürgens/Ortmann RDV 2014, 3 ff.

11 Asaj, DuD 2011, 558 zu sog. Floating-Car-Daten.

12 Vgl. <http://www.golem.de/news/volvo-cloud-autos-warnen-sich-genseitig-vor-glatten-strassen-1502-112332.html>.

13 Vgl. § 6 Abs. 1 Nr. 4 S. 3 EStG. Grundlegend zu elektronischen Fahrtenbüchern Rammo/Holzgräfe, DSRITB 2014, 355 ff.

14 Lüdemann/Sengstacken, RDV 2014, 177, 179.

### 3. Fahrverhalten

Unfalldatenspeicher führen bestimmte Sensordaten zusammen und halten sie für die Unfalldatenauswertung als Daten-Frame in einer Black Box fest<sup>15</sup>. Der Einbau dieser Speicher erfolgt derzeit auf freiwilliger Basis<sup>16</sup>.

Für einige Nutzfahrzeuge<sup>17</sup> sind allerdings seit 2006 digitale Tachographen vorgeschrieben, welche die Identität des Fahrers, Lenk-, Ruhe- und Arbeitszeiten, gefahrene Geschwindigkeiten nebst Geschwindigkeitsübertretungen und zurückgelegte Wegstrecken speichern. Ziel der Aufzeichnung ist der Schutz der Fahrer durch die Einhaltung von Ruhepausen und die Steigerung der Verkehrssicherheit durch Verbesserung von Kontrollmöglichkeiten der Polizei und der Gewerbeaufsicht<sup>18</sup>.

Sogenannte „Telematiktarife“ der Versicherungen gehen noch einen Schritt weiter: Überhöhte Geschwindigkeit, hastiges Bremsen oder Beschleunigen sowie Nacht- und Stadtfahrten werden an den Versicherer ausgeleitet und haben sodann unmittelbar Einfluss auf den Versicherungsbeitrag<sup>19</sup>. Nimmt der Arbeitgeber Zugriff auf diese Daten, wird hierdurch zugleich eine genaue Auswertung des Fahrverhaltens einzelner Mitarbeiter möglich.

### 4. Bild- und Videodaten

Dashcams sind kleine weitwinklige Kameras auf dem Armaturenbrett, die das Verkehrsgeschehen aufzeichnen. Die Betreiber der Kameras wollen Beweismittel für etwaige Verkehrsunfallsituationen sammeln. Im Unternehmenseinsatz würde auch hier eine Kontrolle der Beschäftigten denkbar. Der Düsseldorfer Kreis<sup>20</sup> und die Rechtsprechung<sup>21</sup> haben der Verwendung von Dashcams allerdings weitgehend eine Absage erteilt<sup>22</sup>. Innenkameras werden demgegenüber häufig in Taxen eingesetzt zum Schutz der Fahrer vor Übergriffen und Beförderungsbetrug. Die aufgezeichneten Daten lassen sich dabei genauso gegen den Fahrzeugführer einsetzen.

### 5. Fahrzeugdaten

Zu den reinen Fahrzeugdaten zählen jene Informationen, die sich zuvörderst auf die Maschine selbst beziehen. Hierzu gehören Drehzahlen, Temperaturen, Gas- und Flüssigkeitsdrücke, Wartungsintervalle und viele weitere. On-Board-Diagnose-Systeme nutzen diese Daten zur Fehlererkennung und -analyse.

## III. Personenbezug

Daten sind personenbezogen im Sinne des § 3 Abs. 1 BDSG, wenn es sich um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person handelt<sup>23</sup>. Bei Telekommunikations-, Fahrverhaltens- oder Bilddaten ist der Personenbezug mit Händen zu greifen. Schwieriger wird es bei Positionsdaten oder reinen Fahrzeugdaten. Ein Ort alleine oder physische Eigenschaften eines Fahrzeuges haben für sich

genommen noch keine direkte Beziehung zum Persönlichkeitskern eines Menschen. Der Bezug wird erst hergestellt, wenn der Arbeitgeber zuordnen kann, wer das Fahrzeug zu einem bestimmten Zeitpunkt gefahren hat. Bei hinreichender Kontrolldichte wird die betriebliche Fahrzeugnutzung nahezu lückenlos protokolliert sein. Somit werden die Bewegung im Raum, das Verhalten im Straßenverkehr, der Umgang mit Unternehmenseigentum und andere Persönlichkeitsaspekte ablesbar, und es können ggf. ganze Persönlichkeitsprofile<sup>24</sup> erstellt werden. Mithin muss davon ausgegangen werden, dass sämtliche im Fahrzeug anfallenden Daten auf die eine oder andere Weise Aussagekraft über eine zumindest bestimmbare Person besitzen<sup>25</sup>.

## IV. Erhebung, Speicherung und Übermittlung

So unterschiedlich die Datenkategorien sind, die in einem Fahrzeug anfallen können, so vielfältig sind auch die mit der Datenverarbeitung verfolgten Zwecke. Neben dem Arbeitgeber kann dadurch eine große Zahl weiterer Empfänger Begehrlichkeiten entwickeln. Fahrzeughersteller, Werkstätten, Behörden oder Versicherungsunternehmen vermögen die gewonnenen Informationen ggf. nutzbringend einzusetzen. Der Beschäftigtendatenschutz endet jedoch nicht an der Betriebspforte. Jede Erhebung und Speicherung durch den Arbeitgeber, jede Weitergabe an einen Dienstleister im Rahmen einer Auftragsdatenverarbeitung und jede Übermittlung an einen Dritten müssen sich gemäß der §§ 3a, 4 Abs. 1 BDSG rechtfertigen lassen. Wie die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zutreffend festgestellt hat, entsteht die besondere Gefährdungs-

15 Hierzu eingehend Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302 ff.; Brenner/Schmidt-Cotta, SVR 2008, 41 ff.

16 Die Frage der datenschutzrechtlichen Zulässigkeit einer Weiterleitung von Unfalldaten an den Haftpflichtversicherer wurde vom OLG Oldenburg, Urteil vom 23.12.2014, Az. 13 U 66/14 (<https://openjur.de/u/754111.html>) ausdrücklich offengelassen.

17 Lastwagen und Busse mit mehr als neun Plätzen.

18 Zum Ganzen Gola, NZA 2007, 1139, 1142 f.

19 Kinast/Kühnl, NJW 2014, 3057.

20 Beschluss vom 26./27.02.2013, „Videoüberwachung in und an Taxis“; Beschluss vom 25./26.02.2014, „Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)“.

21 VG Ansbach, Urteil vom 12.08.2014, Az. AN 4 K 13.01634; AG München Beschluss vom 13.08.2014, Az. 345 C 5551/14; LG Heilbronn, Urteil vom 17.02.2015, Az. I 3 S 19/14.

22 Andere Ansicht: Atzert/Franck, RDV 2014, 136 ff.

23 Auf die Frage, ob bestimmte Fahrassistenzsysteme zur Auswertung der Augenbewegungen oder des Atemalkoholgehalts ggf. besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG verarbeiten, soll hier nicht eingegangen werden; hierzu Kremer, RDV 2014, 240, 241.

24 Asaj, DuD 2011, 558, 560; Lüdemann/Jürgens/Ortmann, RDV 2014, 3, 4; Weichert, SVR 2014, 241, 241 f. Vgl. auch die Entschlüsselung der 88. DSK (Fn 3).

25 Kinast/Kühnl, NJW 2014, 3057, 3060; wohl auch Kremer, RDV 2014, 240, 244.

lage bereits zum Zeitpunkt des Erfassens und nicht erst mit dem Auslesen oder Übermitteln<sup>26</sup>.

## V. Datenschutzrechtliche Rechtfertigung

### 1. § 32 BDSG

In Ermangelung eines eigenständigen Beschäftigtendatenschutzgesetzes bleibt § 32 BDSG die Kernvorschrift für alle Fragen hinsichtlich Arbeitnehmerdaten. Solche dürfen grundsätzlich für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. In Connected Car-Szenarien wird des Öfteren auf § 32 BDSG rekurriert<sup>27</sup>. Die Einführung elektronischer Fahrtenbücher lässt sich dabei ohne größere Schwierigkeiten auf § 32 Abs. 1 S. 1 BDSG stützen<sup>28</sup>. Auch für die unmittelbare Optimierung des Fuhrparkeinsatzes oder (irrig) das Wiederauffinden gestohlener Fahrzeuge wird dies in der Literatur vertreten<sup>29</sup>. Allen Darstellungen ist unterdessen gemein, dass eine vollständige Überwachung oder Kontrolle der Beschäftigten als unzulässig anzusehen ist<sup>30</sup>. Hauptaugenmerk bei der Bewertung liegt insoweit bei der tatbestandlichen Erforderlichkeit. Die Datenverarbeitung ist erforderlich, soweit sie zur Erreichung eines konkret festgelegten Zweckes geboten ist. Die Erforderlichkeit ist weitgehend identisch mit der verfassungsrechtlichen Verhältnismäßigkeitsprüfung, bestehend aus legitimem Zweck, Geeignetheit zur Zweckerfüllung, mindestens gleichgeeignetem Mittel und der Verhältnismäßigkeit im engeren Sinne<sup>31</sup>. Die Zweckbestimmung wird dabei bereits durch § 32 Abs. 1 S. 1 BDSG vorgegeben.

Ergeben sich Anhaltspunkte für eine Straftat im Beschäftigungsverhältnis, die mit oder am Dienstfahrzeug begangen wurden, darf der Arbeitgeber nach Maßgabe des § 32 Abs. 1 S. 2 BDSG Daten des Connected Car erheben und verarbeiten.

### 2. § 28 BDSG

Ob neben der Spezialnorm des § 32 BDSG noch Teile des § 28 BDSG anwendbar sind, ist bis heute trefflich umstritten. Die herrschende Meinung geht davon aus, dass allein § 28 Abs. 1 S. 1 Nr. 1 BDSG völlig verdrängt werde<sup>32</sup>. Für andere Zwecke, die nicht unmittelbar Zwecke des Beschäftigungsverhältnisses sind, bleibt ein Anwendungsbereich für § 28 Abs. 1 S. 1 Nrn. 2 und 3 BDSG.

Der Abschluss von Telematiktarifen etwa und die Übermittlung der dadurch anfallenden Daten an den jeweiligen Versicherer kann nach § 28 Abs. 1 S. 1 Nr. 2 BDSG gerechtfertigt sein, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Das Gleiche gilt für den Einbau von Unfalldatenspeichern und die Ausleitung fahrzeugspezifischer Daten an Werkstätten.

### 3. Betriebsvereinbarung

Betriebsvereinbarungen gelten als Rechtsvorschriften im Sinne des § 4 Abs. 1 BDSG i.V.m. § 77 Abs. 4 S. 1 BetrVG und stellen damit vollwertige datenschutzrechtliche Erlaubnistatbestände dar. Auch eventuelle Probleme der AGB-Inhaltskontrolle werden hierdurch abgemildert (§ 310 IV BGB). Die Einführung von Connected Car-Konzepten kann folglich durch eine Betriebsvereinbarung geregelt werden<sup>33</sup>. Um einen datenschutzrechtlichen Freibrief handelt es sich gleichwohl nicht: Das Privatleben ist der Regelungsmacht der Betriebsvereinbarung entzogen. Gemäß § 75 Abs. 2 S. 1 BetrVG haben Arbeitgeber und Betriebsrat zudem die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Der gläserne Autofahrer wird also auch durch eine Betriebsvereinbarung nicht ermöglicht.

### 4. Einwilligung

Die datenschutzrechtliche Einwilligung bietet in Zweifelsfällen eine elegante Nachweismöglichkeit für die verantwortliche Stelle und lässt Datenverarbeitungen zu, die ansonsten nicht zu rechtfertigen wären. Nach zutreffender Ansicht erfasst sie zugleich Umfang und Reichweite technisch-organisatorischer Maßnahmen<sup>34</sup>.

Gemäß § 4a Abs. 1 S. 1-3 BDSG muss die Einwilligung informiert, freiwillig und grds. in schriftlicher Form erfolgen. An der Freiwilligkeit kann es indes in Fällen wirtschaftlicher Abhängigkeit, wie insbesondere in Arbeitsverhältnissen, hapern<sup>35</sup>. Daher ist genau darauf zu achten, ob eine rein einseitige Durchsetzung von Arbeitgeberinteressen be-

26 88. DSK (Fn 3).

27 Kremer, RDV 2014, 240, 251; Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 304; Rammo/Holzgräfe, DSRITB 2014, 355.

28 Rammo/Holzgräfe, DSRITB 2014, 355, 360

29 Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 304. Das Wiederauffinden gestohlener Fahrzeuge dürfte ein Zweck sein, der außerhalb des eigentlichen Beschäftigungsverhältnisses liegt, und insoweit eher § 28 Abs. 1 S. 1 Nr. 2 BDSG unterfallen, so auch Rammo/Holzgräfe, DSRITB 2014, 355, 360.

30 Kinast/Kühnl, NJW 2014, 3057, 3059 f.; Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302, 304; Rammo/Holzgräfe, DSRITB 2014, 355, 359; Wedde, in: <http://www.eurotransport.de/news/flottenmanagement-systeme-immer-im-visier-des-chefs-537682.html>. Mit identischer Stoßrichtung BGH, Urt. v. 04.06.2013, Az. 1 StR 32/13 (<https://openjur.de/u/634193.html>) zu GPS-Trackern sowie BAG, Urt. v. 19.02.2015, Az.: 8 AZR 1007/13 (<http://dejure.org/2015,2096>) zur Observation von Arbeitnehmern.

31 Wolff, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, Syst. A, Rn. 26 f.

32 Riesenhuber, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 32 BDSG Rn. 26 ff.; Gola/Jaspers, RDV 2009, 212 ff. Konkret zu Connected Car-Szenarien ebenso Kremer, RDV 2014, 240, 251; Rammo/Holzgräfe, DSRITB 2014, 355, 360.

33 Wesentliche Regelungsinhalte finden sich bei Gola/Wronka, Handbuch Arbeitnehmerdatenschutz, 6. Aufl. 2013, Rn. 1929.

34 VG Berlin, Urt. v. 24.05.2011, 1 K 133/10 (<http://openjur.de/u/284643.html>).

35 Weichert, SVR 2014, 241, 243; Simitis, in: Simitis, BDSG, 8. Aufl. 2014, § 4a Rn. 62; Kühling, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 4a Rn. 35.

absichtigt ist<sup>36</sup>, und ob dem Arbeitnehmer eine zumutbare Handlungsalternative bleibt.

Im Allgemeinen wird davon ausgegangen, dass eine wirkliche Einwilligung in Connected Car-Konzepte durchaus möglich ist<sup>37</sup>. Zweifelhaft ist jedoch, welche praktische Relevanz die Einwilligung für Connected Car-Systeme besitzt, wenn die maßgeblichen Verwendungen bereits durch gesetzliche Erlaubnistatbestände oder Betriebsvereinbarungen gedeckt sind. Die Transparenzpflichten erhalten insofern größeres Gewicht.

## VI. Transparenzpflichten

Bereits bei der Datenerhebung hat die verantwortliche Stelle gemäß § 4 Abs. 3 BDSG über den Umfang der Datenverarbeitung zu informieren. Für jene Informationspflicht kommt es darauf an, ob der Arbeitgeber selbst Daten mittels eines Connected Car erhebt. Jedenfalls wird man aus der arbeitgeberseitigen Fürsorgepflicht ableiten können, dass der Dienstwagenutzer bei Übergabe des Fahrzeugs über die Datenerhebung durch Dritte (z.B. Werkstätten oder Versicherer) und die Daten, die bei der Fahrzeugbenutzung anfallen, hinzuweisen ist.

Werden personenbezogene Daten anderweitig erstmals für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist dieser gem. § 33 Abs. 1 S. 1 BDSG zu informieren.

## VII. Betriebliche Mitbestimmung

§ 87 BetrVG regelt Mitbestimmungsrechte des Betriebsrates. Hinsichtlich Connected Car-Vorhaben fällt vor allem Abs. 1 Nr. 6 ins Auge, der die Einführung und Anwendung von technischen Einrichtungen erfasst, „die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“. Entgegen dem missverständlichen Wortlaut der Nr. 6 („dazu bestimmt“) greift das Mitbestimmungsrecht bereits dann ein, wenn die Maßnahme lediglich zur Überwachung geeignet ist. Eine gezielte Zweckbestimmung durch den Arbeitgeber ist hingegen nicht erforderlich<sup>38</sup>. Sämtliche im Fahrzeug anfallenden Daten sind schlechthin geeignet, eine Verhaltens- und ggf. auch Leistungskontrolle durchzuführen.

Bestimmungen, die den Umgang mit den Fahrzeugen selbst betreffen, können darüber hinaus Rechte nach § 87 Abs. 1 Nrn. 1 (Ordnung und Verhalten) oder 2 (Arbeitszeiten) BetrVG auslösen. Die Gewährung eines Dienstwagens unterliegt der Mitbestimmung nach § 87 Abs. 1 Nr. 10 BetrVG, gleichwohl handelt es sich hierbei im Kern nicht um eine datenschutzrechtliche Norm.

Verletzt unterdessen der Arbeitgeber die im Gesetz niedergelegten Mitbestimmungsrechte in grober Weise, kann der Betriebsrat ggf. nach § 23 Abs. 3 S. 1 BetrVG die Verwendung von Connected Car-Konzepten arbeitsgerichtlich untersagen lassen.

## VIII. Widerspruchsrecht

§ 35 Abs. 5 BDSG gewährt dem Betroffenen ein Widerspruchsrecht gegen die automatisierte Verarbeitung seiner Daten oder Verarbeitung in nicht automatisierten Dateien. Dies gilt jedoch nur, sofern das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt.

Hier fließen Aspekte ein, die der verantwortlichen Stelle im Rahmen der Erforderlichkeitsprüfung des § 32 Abs. 1 S. 1 BDSG oder der Interessenabwägung des § 28 Abs. 1 S. 1 Nr. 2 BDSG noch unbekannt waren. Den Betroffenen trifft insoweit eine Initiativverantwortung, entgegenstehende Gesichtspunkte geltend zu machen. Beispielhaft können dies etwa Fälle sein, in denen der genaue Aufenthaltsort eines Betroffenen aus Sicherheitsgründen geheimzuhalten ist<sup>39</sup>. Eine schematische Lösung, welche Beschäftigteninteressen beim Einsatz von Connected Cars höher zu gewichten sind, als diejenigen des Arbeitgebers, kann an dieser Stelle freilich nicht angeboten werden.

## IX. Praxisbeispiel 1: Auswertung von Fahrverhaltensdaten

Sowohl bei rein dienstlicher als auch bei gestatteter Privatnutzung eines Dienstfahrzeuges hat der Arbeitnehmer eine Sorgfaltspflicht beim Umgang mit Unternehmenseigentum zu beachten. Durch die Einführung eines Telematiktarifes oder die Rückmeldung durch die Werkstatt könnte der Arbeitgeber nun in den Besitz von Daten zum Fahrverhalten gelangen. Zeigt sich dabei ein unsachgemäßer Gebrauch des unternehmenseigenen Fahrzeuges, hat der Arbeitgeber ein Interesse daran, diese Daten zur Begründung etwaiger Regressforderungen heranzuziehen.

Bei rein dienstlicher Nutzung lässt sich ein solches Vorhaben ggf. auf § 32 BDSG stützen. Dies gilt jedenfalls dann, wenn die Fahrzeugnutzung eng mit dem übrigen Pflichtenkreis des Arbeitnehmers verknüpft ist, wie dies bei Berufskraftfahrern, Kurieren etc. der Fall ist. Um eine unzulässige Ausforschung des Beschäftigten handelt es sich nicht, da der Arbeitgeber nicht anlasslos handelt.

Nun ist die Überlegung gestattet, inwiefern die Grundsätze der gestuften Arbeitnehmerhaftung<sup>40</sup> bereits auf der Ebene der Tatbestandsermittlung anzuwenden sind. Richtigerweise wird man davon ausgehen müssen, dass es sich hierbei maßgeblich um eine Problemstellung auf Rechtsfol-

36 Kinast/Kühnl, NJW 2014, 3057, 3059 f.

37 Rammo/Holzgräfe, DSRITB 2014, 355, 359; Kinast/Kühnl, NJW 2014, 3057, 3060.

38 Vgl. bereits Franck, RDV 2013, 185, 188 zum Themenfeld BYOD.

39 Brink, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 35 BDSG Rn. 76 zu Gefahren für Leib und Leben.

40 Volle Haftung nur bei Vorsatz oder grober Fahrlässigkeit, ansonsten anteilige bis gar keine Haftung des Arbeitnehmers, vgl. BAG, Beschl. v. 27.09.1994, Az.: GS 1/89 (<http://dejure.org/1994,77>).

genseite handelt. Die Daten dürfen daher verarbeitet werden, bis geklärt ist, ob das Fahrverhalten tatsächlich auf Vorsatz oder grobe Fahrlässigkeit hindeutet.

Bei gestatteter Privatnutzung verlässt die Datenverarbeitung den Boden des Beschäftigtenverhältnisses. Informationsbeschaffungen über Privatfahrten sind für den Arbeitgeber grundsätzlich unzulässig. Ergeben sich jedoch Anhaltspunkte für eine sorgfaltswidrige Privatnutzung und eine damit einhergehende Beschädigung am Fahrzeug, wird der Arbeitgeber anhand eigener oder ihm übermittelter Daten über das Fahrzeug auf Grundlage des Nutzungsvertrages gemäß § 28 Abs. 1 S. 1 Nr. 1 BDSG vertragliche (Regress-)Ansprüche prüfen dürfen.

## X. Praxisbeispiel 2: GPS-Tracking

Die Ortung mobiler Beschäftigter kann wegen arbeitsvertraglicher Kontrollrechte oder einer direktionsrechtlichen Ordnungsbefugnis gerechtfertigt sein. Sämtliche Maßnahmen, die der Durchführung des Beschäftigungsverhältnisses dienen, müssen jedoch einer Erforderlichkeitsprüfung im Sinne des § 32 Abs. 1 S. 1 BDSG standhalten. Die Erforderlichkeit ist stets nur dann gegeben, wenn kein milderes, weniger in die Persönlichkeitsrechte eingreifendes Mittel zur Verfügung steht. GPS-Tracking zur reinen Arbeitszeitkontrolle dürfte unverhältnismäßig sein, wenn bspw. die Auswertung reiner Kilometerstände genügt. Die Optimierung des Personaleinsatzes insgesamt, Diebstahlschutz und die persönliche Sicherheit der Mitarbeiter sind hingegen legitime Ziele einer solchen Datenerhebung und -verarbeitung. Vorab zu prüfen bleibt, ob ein vollständiges Tracking aufgezeichnet werden muss, oder ob nur die jeweils letzte Position für die Zweckerreichung genügt. Die Überwachung muss dabei – außer in Fällen konkreten Strafverdachts – transparent gemacht werden<sup>41</sup>.

## XI. Zusammenfassung

*Die Einführung neuer Technik im Fahrzeug stellt den Datenschutz zweifelsohne vor neue Herausforderungen. Neuartig sind jedoch keineswegs die anfallenden Datenkategorien oder die betrieblichen Verarbeitungszwecke, sondern die schiere Masse an gebündelter Information, die durch Connected Car-Systeme zur Verfügung steht.*

*Die geltenden Datenschutzbestimmungen, seien es Befugnisnormen, Betroffenenrechte oder Vorschriften zur betrieblichen Mitbestimmung, werden mit diesen Herausforderungen fertig<sup>42</sup>. Den Unternehmen, die am technischen Segen partizipieren wollen, müssen jedoch die Grundsätze der Datensparsamkeit<sup>43</sup>, der Zweckbindung und der Transparenz<sup>44</sup> klar vor Augen stehen. Sowohl die betriebliche Datenschutzkontrolle als auch die Mitarbeitervertretung müssen im Vorhinein wissen, was von Seiten der Autoindustrie auf sie zukommt, um in angemessener Weise die Rechte der Beschäftigten schützen zu können.*



### RA Andreas Jaspers

RA Andreas Jaspers ist Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. und Mitherausgeber der RDV.



### Dr. iur. Lorenz Franck

Dr. iur. Lorenz Franck ist Referent für Beschäftigten-, Sozial- und Gesundheitsdatenschutz bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. sowie Lehrbeauftragter für Datenschutzrecht an der FH Köln.

<sup>41</sup> Zum Ganzen Gola, RDV 2012, 285 ff., insbesondere zur Praxis der Aufsichtsbehörden.

<sup>42</sup> A.A. Fischer, Flottenmanagement 1/2015, 52 ff.; ferner Weichert, SVR 2014, 241, 247, der jedoch ausdrücklich die Notwendigkeit eines eigenständigen „Autofahrerdatenschutzgesetzes“ verneint.

<sup>43</sup> Grundlegend Weichert, SVR 2014, 201, 205 f., insbesondere zu „privacy by design“.

<sup>44</sup> Hierzu Weichert, SVR 2014, 241, 242 f.

Prof. Klaus Gennen

## Vertragsgestaltung bei Connected Car-Lösungen

Das Vorhandensein von ConnectedCar-Lösungen ist für eine zunehmende Zahl von Kfz-Käufern ein Kaufargument. Eingeführt werden diese Lösungen von Seiten der Hersteller im Verhältnis zum Käufer des Kraftfahrzeuges auf der Basis

eines Vertrages, der i.d.R. nicht bereits Teil des Kaufvertrages ist, sondern rechtlich hiervon gesondert abgeschlossen wird. Der Beitrag beleuchtet ausgewählte Aspekte der Vertragsgestaltung.

### I. Einführung

„Connected Car-Lösungen“ (CC) haben in den letzten Jahren stetig an Bedeutung gewonnen<sup>1</sup>. Das Thema CC wird nach einer jüngst bekannt gewordenen Studie der Pierre Audoin Consultants<sup>2</sup> von Seiten der Automobilhersteller jedenfalls für den europäischen Markt als (ein) strategisches Langzeitthema für die Geschäftsentwicklung betrachtet. Wer keine mit CC ausgestatteten Kfz bzw. Komponenten hierzu anbietet, wird entscheidende Wettbewerbsnachteile erleiden. Das gilt demnach nicht nur für Automobilhersteller, sondern auch für die Automobilzulieferindustrie.

Die mit CC einher gehenden technisch-fachlichen Möglichkeiten sind vielfältig:

- (1) Das Kfz kann sich in der Form mit dem *Internet* verbinden, dass in einem Rechner im Kfz eine vom Fahrer bedienbare Benutzeroberfläche mit einem Browser installiert ist, z.B. zu Zwecken der gewillkürten Hotelbuchung durch den Fahrer oder zum Streamen von Musik. Denkbar sind Fallgestaltungen, in denen, wie beim sonstigen mobile computing außerhalb von Kfz auch, der Fahrer Location Based Services (LBS) Dritter auswählt, um z.B. von ihm selektierbare Hotels in der Nähe aufzufinden. Diese Nutzungsformen unterscheiden sich demnach vom herkömmlichen, Benutzer-getriebenen mobile computing unter Einsatz von GPS- oder vergleichbarer Standortbestimmungstechnologie nicht, allenfalls dadurch, dass Mobile Devices oft persönlich zugeordnet sind, d.h. nur von einer Person genutzt werden, Kfz aber oft von mehreren Personen (Familie, Freundeskreis, Autovermietung, Fuhrpark) genutzt werden.
- (2) Verwandt sind *Car-to-Home*-Anwendungen, bei denen der Fahrer z.B. Reiseplanungen am etwas komfortabler zu bedienenden heimischen Rechner durchführt und diese dann auf sein Navigationsgerät lädt, oder Fallgestaltungen, in denen er Musik im laufenden Betrieb von der heimischen Anlage auf den Rechner seines Kfz lädt bzw. umgekehrt.
- (3) Naheliegend ist eine (bidirektionale) Verbindung zwischen dem *Kfz-Hersteller* und dem Kfz (*Car-to-Enterprise*), insbesondere zu Zwecken des Anbietens von z.B. LBS durch den Hersteller selbst, aber auch zur Übermittlung von Fahrzeugdaten, z.B. aus technischen Gründen (Zustandsanalyse, Wartung, Sicherheit). Aus einer sog. On-board-Unit werden hierzu via Telekommunikationsanbieter

laufend Daten verschickt, z.B. über Außen- und Innentemperatur, Geschwindigkeit, Benutzung einzelner Features wie z.B. Warnblinker (Unfall?) oder Nebelschlusslicht (Wetter?). Solche Daten stehen nicht nur dem Hersteller (einschließlich Vertrieb) zur Verfügung, sondern auch dem Hersteller-gebundenen *Werkstättenetz*.

Entsprechendes gilt z.B. für *Kfz-Vermieter*, *Kfz-Leasing-unternehmen* und bei *Carsharing-Systemen*. Denkbar sind auch entsprechende Verbindungen zwischen Dienstfahrzeugen und den diese zur Verfügung stellenden *Arbeitgebern*. Bei diesen Nutzern von CC steht die Kontrolle des Ortes und des Zustandes des Kfz im Vordergrund sowie die Kontrolle der Arbeit und der Einhaltung der Arbeitszeitsvorschriften. Auch andere Unternehmen jedweder Art können CC-Dienste etablieren, die darauf beruhen oder dadurch unterstützt werden, dass Fahrzeugdaten an das Unternehmen geschickt werden, z.B. Versicherungen mit „pay-as-you-drive“- bzw. Telematik-Tarifen, bei denen bestimmte Daten über die Fahrweise zu Scoring-Ergebnissen aggregiert werden, die zu einem Rabatt berechtigen – oder auch nicht<sup>3</sup>.

- (4) Hierneben sollen *Car-to-Car*-Verbindungen (C2C), bei denen sich dementsprechend mehrere Kfz als eine Form des „Internet der Dinge“ miteinander verbinden (z.B. über bestimmte Formen von Abstandswarnern), eine Erhöhung der Verkehrssicherheit ermöglichen bzw. den Informationsfluss bei außergewöhnlichen Verkehrssituationen wie Unfällen oder Staus beschleunigen. Die Kfz melden dazu untereinander z.B. Hindernisse, starkes Abbremsen, Wetterdaten und andere Informationen, die bestimmte Verkehrssituationen beschreiben bzw.

1 Angesprochen sind damit Mobile-Computing-Lösungen, bei denen im Wege über Funk hergestellter Datenverbindungen aus Kraftfahrzeugen (Kfz) die Übermittlung bzw. der Austausch von Informationen von dem bzw. über das Kfz und/oder den Fahrer an den bzw. mit einem Dritten erfolgt – einschließlich der Speicherung sowie weitergehender Verarbeitung solcher Daten im Kfz und/oder bei dem bzw. durch den Dritten, mit dem das Kfz Daten austauscht.

2 Pierre Audoin Consultants, „Connected Car in Europe“, EU-weite Umfrage bei 200 Führungskräften in Automobilindustriunternehmen, 2014/2015, s. <https://www.pac-online.com/connected-car-europe-strategies-and-technologies-connected-driving>.

3 Vgl. das 2014 abgeschlossene (1.000 Boxen umfassende) und in der Auswertung befindliche Angebot von S-Direkt, die einen Telematik-Tarif anbietet, der zurückhaltende Fahrweise mit (geringfügigen) Rabatten belohnt; die Daten hierzu werden aus einer im Fahrzeug installierten Blackbox verschickt. Die Rabattschwankungsbreite beträgt als reine Belohnung 5%, in anderen Ländern sind deutlich höhere Rabatte möglich. Vgl. hierzu Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302 ff.

über entsprechende Algorithmen Schlüsse hierauf zu lassen.

- (5) Schließlich wird es *Car-to-Infrastructure*-Verbindungen (C2X) geben, bei denen sich (öffentliche) Verkehrsinfrastrukturkomponenten mit dem Kfz in Verbindung setzen bzw. dieses mit jenen, z.B. verkehrsgesteuerte bzw. bedarfsgesteuerte Ampelanlagen zur Erleichterung des Verkehrsflusses.

Diese Zusammenstellung ist denkwürdig unvollständig, sie berücksichtigt u.a. nur einige Anwendungsfälle, einige der möglichen Beteiligten und nimmt ferner keine Rücksicht auf die Art und Weise der Speicherung (Festspeicher, Unfalldatenspeicher, flüchtige Speicher, punktuelle Speicherung oder Speicherung von Werteverläufen). So sind naturgemäß, zumindest in technischer Hinsicht, an der Abwicklung von CC-Leistungen auch Funknetzbetreiber beteiligt. Zudem werden durch Hersteller und durch Dritte immer neue Apps für Kfz bzw. für die Verwendung im Zusammenhang mit Kfz entwickelt<sup>4</sup>. Dritthersteller liefern die Hard- und Software für CC, Softwareanbieter bzw. Lösungsanbieter für im Kfz zu verwendende Browser und Social-Media-Komponenten sowie Payment-Anbieter<sup>5</sup> sind ebenfalls beteiligt. Die weitere Entwicklung ist zudem rasant, eCall ist jüngst verpflichtend geworden<sup>6</sup> – und wegen der für andere, vom Hersteller gewünschte Zwecke nutzbaren, im Kfz zu verbauenden Technologie von vornherein in der Kritik. Das pilotierte Fahren befindet sich bei einigen Herstellern in der praktischen Erprobung. Dass CC-Lösungen bisweilen technisch unsicher sind<sup>7</sup>, steht auf einem anderen Blatt bzw. tut dem Vordringen solcher Lösungen ganz offensichtlich keinen Abbruch.

Bei einigen Herstellern wird das Kfz selbst mit einer fest verbauten SIM-Karte ausgerüstet, andere stellen entsprechende Funktionalitäten her durch Verbindung eines Smartphones mit dem Kfz oder durch Einführen einer SIM-Karte, die nicht fest verbaut ist.

Damit ist jedenfalls klar, dass der Fahrer, der vor den CC-Zeiten das von ihm benutzte Kfz als einen Teil seines persönlichen Lebensraums, gleichsam als Rückzugsgebiet und damit als seine Privatsphäre betrachtet hat, bei Einsatz von CC von dieser etwas überkommenen Vorstellung von Privatheit Abschied nehmen muss. Wer schon im Ansatz ohne jede datenschutzrechtliche bzw. Datensicherheitsherausforderung Auto fahren will, muss ein sehr altes Fahrzeug benutzen, das weder Daten an Dritte versendet noch Daten im Motorsteuerungsgerät oder anderswo intern speichert, die zumindest von einer Werkstatt mit entsprechender Ausrüstung auslesbar sind. Dieser künstliche Verzicht nutzt aber künftig jedenfalls dann nichts mehr, wenn eCall in Neuwagen Pflicht ist und alte Fahrzeuge vom Markt verschwinden.

## II. Arten anfallender Daten, personenbezogene Daten

Bei CC-Lösungen unter Benutzung von Funktechnologie fallen Daten unterschiedlicher Kategorien an, Bestands- bzw.

Stammdaten (§§ 14 TMG, 95 TKG<sup>8</sup>), Nutzungs- bzw. Verkehrsdaten (§ 96 TKG) und Inhaltsdaten (BDSG). Ob bei dieser Reihenfolge mit sozusagen aufsteigender Tendenz bei den materiellrechtlichen und verfahrensrechtlichen Eingriffsvoraussetzungen gearbeitet werden kann bzw. muss, ist bei Daten aus CC-Lösungen bisweilen zweifelhaft: Rein technische Inhaltsdaten wie z.B. der Öldruck oder der Zustand der Wasserpumpe werden für sich genommen datenschutzrechtlich keine Bedeutung haben, wohingegen Verkehrsdaten der Erstellung von (Bewegungs-) Profilen dienen können. Es werden jedoch Inhaltsdaten i.d.R. auch bei CC-Lösungen die sensibelsten Daten darstellen, insoweit denke man z.B. an die Erfassung des Alkoholisierungszustandes des Fahrers durch Sensoren oder die Abspeicherung eines zurückgelegten Fahrweges.

Datenschutzrechtlich unproblematisch wären mit CC verknüpfte Leistungen bzw. Dienste jedoch, wenn ihnen keine personenbezogenen bzw. personenbeziehbaren Daten zugrunde lägen bzw. solche gar nicht erst entstehen, erhoben bzw. verarbeitet würden. Keine personenbezogenen Daten lägen vor, wenn ausschließlich fahrzeugbezogene Daten in Rede stünden und auch mithilfe dieser Daten, ggf. in Verbindung mit anderen, auch nicht auf eine bestimmte oder bestimmbare natürliche Person geschlossen werden könnte. Dies jedoch kann man nicht nur nicht ausschließen, vielmehr muss man umgekehrt davon ausgehen, dass viele Daten personenbezogen oder zumindest personenbeziehbar sein werden, z.B. die Position des Fahrzeuges, verknüpft mit der an anderer Stelle erzeugten Erkenntnis, welche natürliche Person zu

4 So hat z.B. Accenture jüngst die Fertigstellung einer neuen Backend-Plattform für Connected Drive von BMW bekanntgegeben. Über den entsprechenden Store sollen Konsumenten sich Dienste und Apps erstmals unmittelbar über die BMW Group erwerben; Leistungen sollen in Echtzeit „over the air“ im Kfz bereitgestellt werden können.

5 Das Kreditkartenunternehmen Visa arbeitet in den USA offenbar an einer Lösung („Visa Connected Car Commerce“), mit der u.a. aus dem Kfz heraus bei einer bundesweit bekannten Pizza-Restaurantkette bestellt und mit der Visa-Karte bezahlt werden kann. Die Bestellung erfolgt über das Auto selbst. Dazu wird im Kfz ein Display benötigt, das einen Webbrowser zeigt. Die Bestellung wird in der nächstgelegenen Filiale des Pizza-Restaurants bearbeitet, während der Fahrer dorthin fährt. Vor Ort erkennen Bluetooth-Beacons das Kfz, und die Bestellung wird herausgereicht, während im Display die Bezahlung autorisiert wird. Bezahlt wird per Visa Checkout-Dienst.

6 VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden borgelegenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG, vom Rat angenommen am 17.12.2014, Beschluss Nr. 585/2014/EU des Parlamentes und des Rates.

7 Zu den (zwischenzeitlich wohl geschlossenen) Sicherheitslücken bei Connected Drive von BMW (für bis zum 08.12.2014 produzierte Fahrzeuge verschiedener Modelle) aus technischer Sicht s. Spaar, Auto, öffne dich!, c't 2015, Heft 5/2015, 86 ff.; zu evtl. technischen Einbruchsstellen bei dem o.a. Versicherungsangebot von S-Direkt vgl. den Artikel unter [www.heise.de/autos/artikel/Verwandtschaft-2044333.html](http://www.heise.de/autos/artikel/Verwandtschaft-2044333.html) v. 12.11.2013, gleichzeitig zur aus Sicht des Autors fehlenden Datensparsamkeit.

8 Die Frage, ob bestimmte mobile Angebote Telemediendienste nach § 1 Abs. 1 TMG sind oder ob ein TK-Dienst nach § 3 Nr. 24 TKG vorliegt, bleibt hier einstweilen unentschieden, wenngleich mehr dafür spricht, dass Telemediendienste vorliegen, insbesondere, wenn komplexe Leistungen über eine im Fahrzeug fest verbaute SIM-Karte erbracht werden und der Kunde den Vertrag über diese Leistungen mit dem Kfz-Hersteller schließt, ein Telekommunikationsprovider in die Gestaltung mit dem Kunden vertraglich also nicht eingebunden ist.

einem bestimmten Zeitpunkt das Fahrzeug führte<sup>9</sup>. Jedenfalls wird man solche Daten auf den Halter beziehen. Somit wird man davon ausgehen müssen, dass letztlich alle Daten zur Fahrweise und Fahrverhalten, zu Internetanwendungen sowie Geo- und Kommunikationsdaten aus mobilen Anwendungen personenbezogene bzw. personenbeziehbare Daten sind, wenn sie mit einer Information über die Identität des Fahrers als natürlicher Person verknüpft sind bzw. werden können. Keine personenbezogenen Daten sind damit Daten über z.B. Wetterverhältnisse oder Verkehrszustände als solche.

Keine nennenswerten datenschutzrechtlichen Herausforderungen bestünden wohl auch dann, wenn der Fahrer vor dem eigentlichen Start des Kfz wählen könnte, welche Daten aus dem Kfz in welcher Form an welchen Dritten übermittelt werden, er diese bzw. ggf. schon eine technische Aufnahme von Daten im Ganzen zuverlässig unterdrücken kann (was spätestens bei eCall wohl nicht mehr funktionieren wird) oder durch Wahl eines bestimmten (gern auch als Default eingestellten) Modus eine Art automatisierter Anonymisierung der Daten vornehmen kann (Datenschutz durch Selbstschutz). Umfassende privacy-by-design- bzw. privacy-by-default-Vorstellungen auf Kundenseite sind aber wohl derzeit naiv<sup>10</sup>. Oft sind bestimmte Leistungen nur insgesamt deaktivierbar, also durch Deaktivierung des Sendemoduls bzw. einer entsprechenden technischen Abkopplung. Dies wiederum stößt bei Kunden auf Bedenken, weil dann auch Funktionalitäten wie der automatische Notruf nicht mehr arbeiten. Vor die Wahl gestellt, alles oder nichts zu deaktivieren, wird der Kunde eher dazu neigen, nichts zu deaktivieren. Es werden herstellereits ungeachtet des Grundsatzes der Datensparsamkeit (§ 3a BDSG) im Zweifel so viele Daten wie technisch möglich und vernünftig verwaltbar erhoben und gespeichert, auch, weil man nicht weiß, ob es nicht zumindest später noch weitere Zwecke geben kann, zu denen die Daten genutzt werden könnten – und dies wiederum ungeachtet der Frage, wie mit späteren Zweckänderungen in Bezug auf die Erhebung bzw. Verarbeitung der erhobenen Daten umzugehen ist.

### III. Erlaubnistatbestand und Vertragsgestaltung, Erfordernis der und Anforderungen an die Einwilligung

a) Es sind Fallkonstellationen typisch, in deren Rahmen schon die Bereitstellung einer bestimmten Leistung gegenüber dem Kfz-Besitzer/-Benutzer eine Berechtigung zur Verarbeitung nach § 28 Abs. 1 BDSG zeitigt, eine gesonderte Einwilligung nach § 4 Abs. 1 BDSG also nicht notwendig ist. Wenn ein Kunde ein Angebot einer Kfz-Werkstatt in Anspruch nimmt, alle 25.000 km oder bei Verschleiß bestimmter Teile eine Inspektion durchzuführen und vereinbarungsgemäß der Kfz-Besitzer/-Benutzer diese Intervalle bzw. den Verschleiß nicht selbst feststellen soll, sondern die Werkstatt, dann muss es für die Kfz-Werkstatt vorbehaltlich der Mitteilung der Zweckbestimmung (§ 28 Abs. 1 Satz 2 BDSG) möglich sein, jedenfalls solche Daten zu erfassen, die dieses Intervall betreffen bzw. das Ausmaß des Verschleißes

einzelner Teile. Mehr an Daten wäre wegen § 28 Abs. 1 Satz 1 Nr. 1 BDSG nicht erlaubt, wobei es jedoch verwundern würde, wenn nicht tatsächlich doch mehr Daten erhoben würden. In Fällen wie dem Protokollieren eines technischen Verschleißes werden aber voraussichtlich ohnehin keine personenbezogenen Daten anfallen, sondern nur Daten über den Zustand einzelner technischer Komponenten, lösgelöst vom Fahrer und auf diesen i.d.R. auch nicht beziehbar. Beziehbar werden die Daten, wenn sie an den Hersteller bzw. an die Werkstatt gesendet werden und dieser bzw. diese den Halter des Kfz anruft, um einen Termin zu vereinbaren.

b) Die Zulässigkeit ergibt sich damit im Zweifel dem Grunde und der Reichweite nach aus der im CC-Vertrag vereinbarten Leistungsbeschreibung.

Es können auch komplexere Leistungsbilder sowie die damit einhergehende Verarbeitung personenbezogener Daten unter § 28 Abs. 1 BDSG fallen. Voraussetzung ist stets, dass im Zweifel ein Nachweis möglich ist, wonach eine entsprechende Datenverarbeitung zur Wahrung berechtigter Interessen des Herstellers erforderlich ist. Je deutlicher ein Hersteller also sein Angebot in Bezug auf Leistungen ausweitet, zu deren Erbringung die Verarbeitung personenbezogener Daten aus dem Fahrzeug erforderlich ist, und diese Leistungen auch im Vertrag bzw. in Merkblättern beschreibt, desto mehr an Verarbeitung ist durch § 28 Abs. 1 Satz 1 Nr. 1 BDSG gedeckt<sup>11</sup>.

Unklar ist, wann hier eine Grenze erreicht ist. Plausibel erscheint, dass diese auch durch § 28 Abs. 1 Satz 1 Nr. 2 BDSG gebildet wird: Wenn ein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, ist eine Verarbeitung nicht zulässig. Das schutzwürdige Interesse kann erheblich sein, wenn Daten erhoben werden, die unmittelbare bzw. deutliche Schlüsse auf das (legale) Fahrverhalten zulassen bzw. dieses Fahrverhalten unmittelbar protokollieren. Je mehr die Daten auf eine individuelle Verhaltensweise des (jeweiligen) Fahrers schließen lassen bzw. eine solche beschreiben, deren Offenbarung Dritten gegenüber der Betroffene zurückhaltend vornehmen würde, desto größer ist die Gefahr, dass die Datenverarbeitung wegen entgegenstehender schutzwürdiger Interessen des Betroffenen nicht zulässig ist. Insoweit sollte in vermute-

9 Vgl. auch Weichert, SVR 2014, 201, 204, der an komplexe Identifikatoren anknüpft, die insgesamt zu einer Personenbeziehbarkeit der Daten führen, ggf. unter Einbeziehung des Kfz-Kennzeichens und der Fahrzeug-Identifizierungsnummer; vgl. auch Reiter/Methner, Datenschutz im Fahrzeug, in: DSRITB 2014, 367, 372.

10 Vgl. hierzu die EntschlieÙung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9.10.2014 zu „Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert“ (fünfter Aufzählungspunkt).

11 Vgl. hierzu auch das Merkblatt des Verbandes der deutschen Automobilindustrie und der Datenschutzaufsichtsbehörden zur Verbesserung der Transparenz und der Datenumgänge im Zusammenhang mit Kraftfahrzeugen in Form einer „Muster-Information über Datenspeicher im Fahrzeug“. Dieses betrifft zunächst die im Motorsteuerungsgerät bzw. Kfz selbst gespeicherten Daten, verweist aber auf deren Auslesbarkeit und (lediglich) auch darauf, dass vertraglich vereinbarte Zusatzfunktionen (eben CC-Lösungen) die Übermittlung „bestimmter“ Fahrzeugdaten aus dem Fahrzeug erlauben. Das ist für sich genommen sicherlich nicht ausreichend, um CC-Lösungen für den Rahmen des § 28 Abs. 1 BDSG zu beschreiben.

ten Grenzfällen eher mit einer ausdrücklichen ergänzenden Einwilligung i.S.d. §§ 4 Abs. 1, 4a BDSG gearbeitet werden, zumal diese vorderhand nicht schwierig erlangbar erscheint.

Entsprechendes wird i.d.R. für Fallgestaltungen gelten, in denen aufgrund der permanent bestehenden Internetverbindung laufend Daten erzeugt werden, die zu Profilen aggregiert werden können. Solche Erhebungen mögen in manchen sozialen Netzwerken nachgerade das Etappenziel auf dem Weg zu einer umfassenden Auswertung sein, bei CC-Basislösungen ist eine solche Erhebung zur Profilerzeugung oft nicht notwendig, so dass eine Erhebung für eigene Zwecke nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG vielfach ausscheiden dürfte. Nun mag es aber auch CC-Dienste geben, die auf genau solche spezifizierten Leistungen abzielen<sup>12</sup>; in einem solchen Fall ist es wiederum Aufgabe einer detaillierten Leistungsbeschreibung, die Einzelheiten der erlaubten Datenverarbeitung indirekt zu bestimmen.

Je komplexer die Leistungsbeschreibung ist, desto schwieriger erscheint es indes, treffsicher und zweifelsfrei das Ausmaß der zulässigen Datenverarbeitung zu bestimmen, insbesondere in Ansehung von § 28 Abs. 1 Satz 2 BDSG, jedenfalls, wenn man diese Norm ernst nimmt.

Bedeutsam für die Berechtigung nach § 28 Abs. 1 BDSG ist nämlich die „konkrete“ Festlegung der Zwecke für die Verarbeitung bzw. Nutzung spätestens bei der Erhebung. Bisweilen wird in Vereinbarungen über die Durchführung entsprechender Leistungen jedoch gerade keine solche konkrete Festlegung vorgenommen, sondern eine allgemeine Formulierung gewählt, etwa in der Art „zur Durchführung des Wartungs- und Mobilitätsvertrages“. Soweit verschiedentlich eingewendet wird, eine solche pauschale Formulierung sei vorteilhaft<sup>13</sup>, insbesondere weil bei einer etwaigen Zweckänderung sonst zu viel Aufwand getrieben werden müsse, widerspricht eine derart allgemeine Formulierung aber der Anforderung einer konkreten Festlegung der Zwecke. So scheint es eher opportun, mehrere konkrete Zweckbestimmungen (der Plural „Zwecke“ in Satz 2 lässt dies zu) zu treffen als eine einzige vage. Während im Bereich CC zunächst Zweckbestimmungserklärungen eher unscharf waren, ist in Zeiten erhöhter Datenschutzsensibilität zumindest bei einigen deutschen Kfz-Herstellern festzustellen, dass in Leistungsbeschreibungen bzw. AGB nicht mehr verbreitet mit einer einzelnen pauschalierten Zweckbestimmung gearbeitet wird, sondern eher mit einer erhöhten Anzahl deutlich konkreterer Leistungsbeschreibungen und damit Zweckbestimmungen, teilweise gegliedert nach einzelnen Teilleistungen aus Gesamtleistungspaketen.

c) Außerhalb der Fallkonstellation des § 28 Abs. 1 BDSG muss man davon ausgehen, dass im Bereich CC eine Einwilligung des Betroffenen zur Datenverarbeitung notwendig ist (§§ 4 Abs. 1, 4a BDSG bzw. § 13 TMG). Nach § 4a BDSG muss die Einwilligung (grundsätzlich) schriftlich erfolgen, ausreichend bestimmt sein und auf der freien Entscheidung des zuvor nach Maßgabe des § 4a Abs. 1 Satz 2 BDSG ausreichend informierten Betroffenen beruhen. Wird die Einwilligung zusammen mit anderen Erklärungen erteilt, ist sie besonders (drucktechnisch) hervorzuheben (§ 4a Abs. 1 Satz 4

BDSG). Die Einwilligung muss widerruflich sein. Ist für den Anwendungsbereich des § 13 TMG eine elektronische Einwilligung nach § 13 Abs. 3 TMG eingeholt worden, muss diese Erklärung protokolliert werden und jederzeit abrufbar sein.

Eine wirksame Einwilligung setzt insbesondere voraus, dass der Betroffene über die Daten, die erhoben pp. werden sollen, informiert wird und über den Zweck der Erhebung, Verarbeitung bzw. Nutzung; pauschalierte Formulierungen werden hier nicht ausreichen. Nimmt man dies ernst, kann für die Information vor der Einholung der Zustimmung nichts wesentlich anderes gelten als für die Konkretisierung der Zweckbestimmung i.S.d. § 28 Abs. 1 Satz 2 BDSG. Hierneben gelten die Prinzipien der Bindung an den vereinbarten Zweck – die Änderung desselben bedarf einer erneuten Einwilligung – und der Erforderlichkeit mit Blick auf den vereinbarten Zweck. Eine Datenverarbeitung darf nur innerhalb des Zeitraums erfolgen, in dem sie für die Erreichung des Zwecks notwendig ist.

Schließlich muss die Einwilligungserklärung freiwillig abgegeben werden. Dazu darf sie nicht in unzulässiger Weise mit anderen Zweckbestimmungen verbunden werden, d.h. mit Werbung, und die Datennutzung, zu der eingewilligt werden soll, darf nicht von einer Seite unter Ausnutzung eines Machtgefälles gleichsam oktroyiert werden<sup>14</sup>.

#### IV. Typische Vertragsgestaltung im Verhältnis zwischen Kfz-Hersteller und Käufer

a) Der Vertrag über CC-Lösungen (CC-Vertrag) kommt zu meist ungeachtet des Kaufs des Kfz vom Händler rechtlich gesondert zwischen dem Hersteller und dem Kfz-Käufer zustande. Der Abschluss eines gesonderten CC-Vertrages neben der Bestellung des Fahrzeuges ist für den Kunden im Grundsatz derzeit noch eher ungewöhnlich, weil recht neu.

Daher wird von Seiten mancher Hersteller Wert darauf gelegt, dass für den Kunden keine besondere Hürde durch den besonders formell wirkenden Abschluss eines weiteren Vertrages aufgebaut wird. Der Kunde soll möglichst sein Kfz bestellen können wie gehabt, und es mit allen seinen Funktionen einfach in Betrieb nehmen, einschließlich der Freischaltung einer in das Kfz (fest) eingebauten SIM-Karte als eine Art Regelvorgang wie das erstmalige Betanken. Diesem Vorgehensmodell passt sich i.d.R. die Vorgehensweise zum Zustandekommen des CC-Vertrages an.

b) Zumeist fungiert ein CC-Vertrag als Rahmenvertrag in der Form, dass einzelne CC-Leistungen im Wege eines Einzelvertrages aufgebucht werden können, der jeweils eine eigene Laufzeit relativ zum Rahmenvertrag hat. Die Laufzeit ist i.d.R. (für Verbraucher) die AGB-rechtlich maximale von

<sup>12</sup> Vgl. hierzu ausführlich Schwenke, Datenschutz und Individualisierung. Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Eigen- und Fremdindividualisierung, 2006.

<sup>13</sup> Z.B. Plath/Plath, BDSG, Rz. 89 zu § 28 BDSG.

<sup>14</sup> Beispiele wären hier Arbeitsverhältnisse oder Versicherungsverhältnisse, letztere zumindest dann, wenn bestimmte Arten von Tarifen nur von wenigen Versicherern angeboten werden.

zwei Jahren Grundlaufzeit mit jährlicher Verlängerung (§ 309 Nr. 8 BGB). Dabei wird unterschieden zwischen der Laufzeit eines Rahmenvertrages, der als solches keine (entgeltlichen) Verpflichtungen des Kunden zeitigt, und den Einzelverträgen, die die o.a. maximal AGB-rechtlich zulässige Laufzeit aufweisen.

c) Besonderheiten gelten für das Zustandekommen des CC-Vertrags mit Blick darauf, dass, wie eingangs erwähnt, dem Kunden zwar gern die Leistung als solche, kaum aber in besonderer Weise der CC-Vertrag und dessen Zustandekommen vor Augen geführt werden sollen.

Der bloße Umstand, dass ein Kunde bei einem Vertrags Händler ein Fahrzeug bestellt, das CC als Serienausstattung enthält, kann nach den AGB den Antrag des Kunden an den Hersteller auf Abschluss des CC-Vertrages darstellen. Das dürfte dem Kunden i.d.R. nicht bewusst sein, es sei denn, (i) der Händler hat ihn darauf aufmerksam gemacht, dass seine Bestellung diese Bedeutung hat oder (ii) die Bestellung selbst sieht in einem Feld bzw. im Text eine entsprechende Erklärung vor. Jedenfalls dürften anlässlich der Bestellung auch die AGB des Herstellers an den Kunden übermittelt werden. Wenn diese AGB in einem Stoß von Prospektmaterial vorhanden sind, wird das dem Kunden nicht weiter auffallen, auch wenn den Formalien genügt wird (§ 305 Abs. 2 BGB). Nachdem CC-Lösungen in einem gewissen Marktsegment bereits einen hohen Durchdringungsgrad erlangt haben und sich Kunden aus einem Sicherheitsbedürfnis heraus oder aus Convenience-Gründen zumeist ganz bewusst für eine solche Lösung entscheiden, auch wenn sie Teil der Serienausstattung ist, dürfte eine solche Regelung über das Zustandekommen der Bestellung heute nicht (mehr) überraschend (§ 305c Abs. 1 BGB) sein.

Es bleibt aber fraglich, ob dem Kunden zum Zeitpunkt des Vertragsschlusses bewusst ist, wer sein Vertragspartner für den CC-Vertrag ist bzw. dass sich Vertragspartner des Kaufvertrages und Vertragspartner des CC-Vertrages unterscheiden bzw. unterscheiden können. Nur dem aufgeklärten Verbraucher wird fachlich unmittelbar einsichtig sein, dass zentral erbrachte CC-Leistungen nicht aus dem Händlernetz oder von einzelnen Händlern erbracht oder vermittelt werden (können), sondern mit einer herstellerzentralen Infrastruktur von dem Hersteller, und zwar auch in Bezug auf die Leistungen, die z.B. die Überwachung von Wartungsintervallen erleichtern sollen und daher letztlich den Händler mit Vertragswerkstatt angehen und nicht den Hersteller unmittelbar. Dass auch der Hersteller Interesse an diesen Daten über den Verschleißzustand der Fahrzeuge hat, im besten Falle, um Qualitätsverbesserungen durchzuführen, liegt jedoch nahe.

Auch ein Vertragsschluss zeitlich nach dem Erwerb des Kfz ist naturgemäß möglich, z.B. bei Weiterverkauf. Die Bedingungen der Hersteller sehen dabei i.d.R. vor, dass die Antragshandlung des Kunden darin besteht, dass dieser erstmals den Sicherheitscode (PIN) der SIM-Karte eingibt oder sein Kfz auf einer Herstellerplattform zu einem entsprechenden CC-Dienst anmeldet. Die Annahmeerklärung steckt dann, je nach Fallgestaltung, darin, dass ein Kfz auf

der Herstellerplattform als anwählbar bzw. parametrierbar erscheint oder der Kunde eine Leistung des CC-Dienstes tatsächlich erhält. Dabei besteht die Besonderheit, dass in einem solchen Fall des nachträglichen Vertragsschlusses Kunde des CC-Vertrags nicht nur der Käufer sein kann, sondern jede Person, welcher der Eigentümer des Kfz dieses berechtigt auf Dauer zur Nutzung überlässt. Das eröffnet z.B. die Möglichkeit, Arbeitnehmer für die ihnen persönlich auf Dauer zur Verfügung gestellten Dienstwagen unmittelbar einen CC-Vertrag mit dem Hersteller schließen zu lassen, mit der Folge, dass bestimmte Daten bzw. Auswertungen – jedenfalls auf der Basis des CC-Vertrages – nicht beim Arbeitgeber auflaufen, sondern beim Arbeitnehmer unmittelbar.

In beiden Fällen fehlt es, wie dargestellt, an einer gesonderten Annahmeerklärung durch den Hersteller, die Leistung wird durch ihn schlicht bereitgestellt und von dem Kunden entgegengenommen. Das ist nach § 151 BGB nur wirksam, wenn ein solches Vorgehen nach der Verkehrssitte üblich ist, wie z.B. bei der Benutzung der Straßenbahn nach Lösen eines Fahrscheines, oder der Kunde auf eine gesonderte Annahmeerklärung verzichtet. Dieser Verzicht wird ihm daher vorsorglich in den AGB abverlangt, was AGB-rechtlich als nicht unproblematisch erscheint. Die Hürde, einen solchen CC-Vertrag abzuschließen, wird von Seiten der Händler außerordentlich niedrig angesetzt. Sofern man davon ausgehen kann, dass dem Kunden vor der Bestellung bzw. vor dem Abschluss des Kaufvertrages im Autohaus die Leistungsbeschreibung und die AGB ausgehändigt werden und er einen Hinweis auf den gesonderten Vertrag erhält, den er eingeht, dürfte ein solches Vorgehen, den Vertrag durch eine Inbenutzungnahme zustande zu bringen, wohl auch nach der Verkehrssitte zu erwarten sein. Solche Hinweise mögen aber nicht immer erteilt werden. Dies alles betrifft zunächst die zivilrechtliche Seite des Zustandekommens des CC-Vertrages als solchem; sofern damit eine etwa als notwendig anzusehende datenschutzrechtliche Einwilligung verbunden sein soll, bedarf dies ggf. gesonderter Betrachtung.

In anderen Konstellationen wird ein Vertrag über die Nutzung von CC-Lösungen komplett außerhalb des Kfz-Verkaufs, über eine gesonderte Plattform, die der Hersteller bereitstellt, geschlossen. Hierzu gibt der Kunde die Fahrzeugidentifikationsnummer ein, wird zu seinen persönlichen Daten geführt, kann Dienste buchen, schickt das Formular ab und erhält eine Bestätigungsemail. In dieser sind Informationen vorhanden, mit denen der Kunde die CC-Lösung in seinem Kfz aktivieren kann. Für die Aktivierung des Kontos ist bisweilen eine Höchstfrist vorgesehen mit der Folge, dass das Konto verfällt oder neue Zugangsdaten angefordert werden müssen.

Ist in diesen Konstellationen einmal ein Konto auf der Herstellerplattform angelegt, kann auf der Plattform auch die Auswahl für weitere Leistungen getroffen werden und dergleichen mehr.

d) Gebräuchlich ist auch die Vereinbarung von (überschaubaren) Mitwirkungspflichten des Kunden, z.B. durch Gestellung einer Email-Adresse zur Kommunikation.

e) Da die Leistung des CC-Vertrages über eine SIM-Karte erbracht wird, enthält ein CC-Vertrag standardmäßige Hinweise auf technische Leistungshindernisse oder eine etwa aus technischen Gründen verminderte oder ausgeschlossene Leistung. Die Übertragungsleistung wird vielfach nicht von dem Hersteller unmittelbar erbracht, sondern von einem TK-Provider, im Verhältnis zum Kunden als Vorlieferant bzw. Subunternehmer des Herstellers. Für Mängel dieser Vorleistung kann der Hersteller sich nicht pauschal enthaften, umso weniger von einer eigenen Leistung, wenn er selbst als TK-Provider fungiert. Einerseits ist technisch klar, dass die CC-Leistung nicht erbracht werden kann, wenn das Netz nicht zur Verfügung steht. Andererseits dürften Freizeichnungsklauseln, die darauf hinauslaufen sollen, dass eine CC-Leistung ohne nähere Eingrenzung des Grundes nur in dem Rahmen zur Verfügung gestellt wird, in dem der Hersteller Leistungen von dem TK-Provider tatsächlich erhält bzw. diese technisch möglich sind, AGB-rechtlich zumindest problematisch sein.

f) Standardmäßig sind in AGB Klauseln enthalten, wonach die zur Verfügung gestellten Leistungen nicht für gesetzwidrige Zwecke benutzt werden dürfen bzw. der Kunde für jede missbräuchliche Nutzung haftbar ist; letzteres spielt für das Innenverhältnis eine Rolle, wenn der Kunde Dritte das Kfz benutzen lässt. Zumeist gibt es in Verträgen auch Einschränkungen dergestalt, dass über das zur Verfügung gestellte technische Equipment ausschließlich Leistungen nach dem CC-Vertrag erbracht bzw. bezogen werden dürfen. Ob damit auch die Verwendung von Apps ausgeschlossen werden soll, die von Drittherstellern stammen, ist unklar. Sofern es sich um Apps handelt, die von dem Hersteller erbrachte Leistungen sollen ersetzen können, soll die Regelung aber jedenfalls greifen.

g) Wie nahezu alle AGB, zumindest zu Dauerschuldverhältnissen, enthalten CC-Verträge Regelungen über einseitige Leistungsänderungen durch den Verwender nach Vertragsschluss. Diese sind in erster Linie an § 308 Nr. 4 BGB zu messen, also an der Zumutbarkeit der Änderung für den Kunden. So hat der BGH im Zusammenhang mit der Zugangsvermittlung zum Internet entschieden, dass selbst dynamische Marktverhältnisse den Verwender nicht dazu berechtigen, einseitig die Leistung bzw. Leistungsbeschreibung und die Gegenleistung bzw. den Preis anzupassen<sup>15</sup>. Sofern man grundlegend eine Zumutbarkeit der Leistungsänderung annimmt, wird man davon ausgehen müssen, dass Änderungen bei reinen Convenience-Anwendungen aus Kundensicht eher zumutbar sein werden als Änderungen im Bereich von Leistungen zur Unterstützung der Fahrsicherheit oder in prekären Situationen bzw. Notfällen. Änderungen an Leistungen, bei denen die Zumutbarkeitsgrenze überschritten ist, sind nur einvernehmlich möglich, wobei im Grundsatz mit einer Mitteilung einschließlich Zustimmungsfiktion gearbeitet werden kann. Erfolgt ein Widerspruch des Kunden, muss der Vertrag insoweit beendbar sein. Das dürfte durch Deaktivierung des Dienstes, ggf. unter Zuhilfenahme einer Werkstatt, erfolgen. Sofern verschiedene CC-Dienste

als Paket angeboten werden und nicht getrennt deaktiviert werden können, wird ein Herausschneiden nicht möglich sein, und damit nur eine einheitliche Deaktivierung zumindest des betroffenen Pakets. Ist eine paketweise Deaktivierung nicht möglich, muss der Kunde den Dienst insgesamt deaktivieren – das wird er ggf. scheuen.

h) In diesen Zusammenhang sind auch Vereinbarungen zu sehen über die mit einer Frist versehene Kündbarkeit von Diensten oder die jederzeitige Deaktivierbarkeit eines Dienstes (dies unabhängig davon, ob gleichwohl die für die Laufzeit bis zur ordentlichen Beendigung geschuldete Vergütung zu zahlen ist). Oft werden Leistungspakete so geschnürt, dass eine vorzeitige Beendbarkeit einzelner Dienste daraus nicht sinnvoll ist, so dass das gesamte Paket gemeinsam beendet wird oder gar nicht. Entsprechendes gilt für die oft herrschende technische Voraussetzung, dass bestimmte Basisdienste nur deaktivierbar sind, wenn die SIM-Karte deaktiviert wird und damit keinerlei Dienst mehr möglich ist. Das jedenfalls werden Kunden scheuen, die sich aus Sicherheitsgründen für die CC-Lösung entschieden haben. Mit der Einführung von eCall mag sich dies ändern, weil das Absetzen des Notrufs unabhängig von etwaigen anderen angebotenen Diensten gewährleistet sein muss.

i) Mit einer Verweisung auf die gesetzliche Gewährleistung scheint der Hersteller bereits recht gut aufgeschickt. Er wird davon ausgehen, dass er im Wesentlichen Dienstleistungen i.S.d. §§ 611 ff BGB erbringt, also insbesondere keinerlei Erfolgshaftung übernimmt. Immerhin vermutet § 280 Abs. 1 BGB das Verschulden des Leistungsverpflichteten. Wer Stauinformationen übermittelt, will keine Haftung dafür übernehmen, dass nicht doch Stau herrscht – hier soll die von dem Kunden hinzunehmende Grenze für Fehlinformationen allenfalls unter Unzufriedenheitsgesichtspunkten entstehen, aber keine vertragliche Haftung. Kritisch erscheint dies bei Leistungen, die im engeren Sinne mit einer gewissen Gewährleistung der Gesundheit des Kunden zusammenhängen. Insoweit gibt es aber aus dem Kaufvertrag noch die Produkthaftung und die allgemeine Mangel- und sonstige Haftung bzw. den Schadensersatzanspruch aus dem Kaufvertrag. Ungeachtet dessen bleiben Zweifel, ob alle CC-Leistungen rechtlich ausschließlich als Dienstleistungen einzuordnen sind. Das bleibt für Fälle, die einen gewissen Erfolgsbezug aus Kundensicht aufweisen, abzuwarten (vgl. auch § 631 Abs. 2, letzte Alternative, BGB, wonach auch Dienstleistungen auf die Herbeiführung eines Erfolgs gerichtet sein können).

j) In AGB zu CC-Verträgen finden sich die aus Verwendersicht üblichen Haftungsausschlüsse (jedenfalls solche bei leichter Fahrlässigkeit).

Verbreitet ist auch eine Regelung, wonach der Hersteller ganz allgemein für die Richtigkeit und die Aktualität der über die Dienste übermittelten Daten und Informationen nicht haftet. Sofern er auf Leistungen Dritter zurückgreift, mag man das in gewissen Grenzen nachvollziehen. Sofern er selbst aber Daten aus Fahrzeugen seiner Kunden aggregiert

15 BGH v. 11.07.2007, NJW-RR 2008, 136.

und diese Daten wiederum den Kunden für bestimmte Auswertungen oder Auswahlen zur Verfügung stellt, wird ein solcher pauschalierter Ausschluss wohl unwirksam sein, im Übrigen wie für lit. d) vorstehend dargestellt.

k) Naturgemäß sind die Leistungen – bisweilen: jenseits einer initialen Periode – nicht kostenfrei, dementsprechend finden sich in den Verträgen Regelungen zu Preisen. Da es um Dauerschuldverhältnisse geht, sind gängige Regelungen zur Anpassung von Preisen vorhanden.

l) Schließlich stehen Regelungen zum Datenschutz im Zentrum des Vertrages.

Liegt ein Rahmenvertrag vor, enthält dieser i.d.R. zunächst Hinweise darauf, dass der Hersteller die geltenden Datenschutzvorschriften einzuhalten beabsichtigt, dass Änderungen personenbezogener Daten (Bestandsdaten) mitzuteilen sind, und auf den Umgang mit Abrechnungsdaten.

Die spezielleren Datenschutzregelungen finden sich indirekt in den Einzelverträgen zu den einzelnen Leistungen bzw. Leistungspaketen. Zu diesen Leistungen werden Laufzeiten, ggf. Preise, geregelt, ferner wird eine Leistungsbeschreibung ausgegeben, in der i.d.R. mitgeteilt wird, welche Daten zu welchen Zwecken erhoben werden und wie sie verarbeitet werden, einschließlich der Übermittlung an in der Leistungsbeschreibung benannte Dritte wie z.B. eine Serviceeinheit, die in Notfällen eingeschaltet wird und ggf. von dem Hersteller juristisch getrennt ist, und der Nutzung durch diesen Dritten. Leistungsbeschreibungen einiger Hersteller haben sich, wie erwähnt, in den letzten Jahren deutlich verbessert und erscheinen insoweit geeignet, über § 28 Abs. 1 Satz 2 BDSG die Reichweite der zulässigen Verarbeitung von Daten vernünftig bzw. ausreichend konkret zu beschreiben. Nicht erkennen kann man jedoch anhand dieser Leistungsbeschreibungen, inwieweit der Grundsatz der Datensparsamkeit beachtet wird. Es bleibt oft unklar, welche Daten insgesamt erhoben werden.

Es sei noch einmal darauf verwiesen, wie der CC-Vertrag zustande kommen kann, gleichsam schleichend. Ist dies der Fall, scheint es ratsam, dem Kunden (auch) im Zuge der Inbetriebnahme einzelner Leistungen die notwendigen datenschutzrechtlichen Informationen stufenweise jeweils für den in Betrieb zu nehmenden Dienst zukommen und ihn den Erhalt quittieren und seine Einwilligung geben zu lassen (Layered Policy Design der Anwendung). Entsprechendes gilt, wenn man davon ausgehen muss, dass die Leistungsbeschreibung selbst nicht ausreichend konkret ist und die Gefahr besteht, dass die Vorgaben des § 28 Abs. 1 Satz 2 BDSG nicht eingehalten sind. Solche Dinge online, sozusagen während des Beginns der Fahrt bzw. der erstmaligen Inbetriebnahme vorzunehmen, ist eine Herausforderung, weil die Einwilligung auch in Ansehung der konkreten Umstände (Displaygröße, Ablenkung, Informationsumfang usw.) wirksam sein muss. Von hier aus wäre es nur noch ein kleiner Schritt zu privacy-by-default, die es dem Kunden ermöglicht, die Übermittlung bestimmter Informationen ein- oder auszuschalten, ggf. nicht nur einmalig, sondern auch nachträglich abänderbar.

m) Bei Verkauf des Fahrzeuges endet i.d.R., wie erwähnt, der Vertrag zwischen dem Kunden und dem Hersteller, oder es besteht bei Laufzeitverträgen ein Sonderkündigungsrecht. Hersteller fordern für diesen Fall von dem Kunden die (rückstandslose) Löschung von Daten, sofern sie „im Fahrzeug“ selbst gespeichert wurden. Eine derartige Forderung ist sicherlich nur dann sinnvoll möglich, wenn die CC-Lösung eine ebensolche Löschung vorsieht oder zumindest transparent ist, wo im Fahrzeug Daten abgelegt sind, die gelöscht werden sollen. Zur Vereinfachung sollten entsprechende Anwendungen die (gegen Missbrauch geschützte) Möglichkeit vorsehen, initiativ die Daten, ggf. je Anwendung gesondert, zu löschen. Dabei ist bekannt, dass in nichtflüchtigen Speichern, die nicht mit einer festen Zeitspanne das Löschen und Überschreiben selbstständig durchführen, Rückstände verbleiben, die nicht gelöscht werden, sofern die Software selbst nicht für ein Überschreiben bzw. eine technisch gesehen vollständige Löschung sorgt. Vielfach werden Kunden beim Verkauf des Kfz entweder die Aufforderung zur Löschung ignorieren oder eine Werkstatt aufsuchen, die ihnen bei der Löschung hilft.

Ferner wird der Kunde aufgefordert, bei Verkauf etwa aktive Dienste (ggf. auch die gebuchten bzw. im Kfz installierten, jedoch deaktivierten Dienste) dem Käufer mitzuteilen.

Besteht ein Kundenkonto auf einer Plattform, insbesondere ein Konto, das mit einer Fahrzeugidentifikationsnummer belegt ist, ist das Konto zu löschen bzw. unzugänglich zu machen.

## V. Einzelaspekte der Vertragsgestaltung zwischen Eigentümer (Halter) und Fahrer

a) Benutzt nicht der Kunde selbst das Kfz, sondern mit seiner Zustimmung ein Dritter, besteht zwischen dem Hersteller und dem Dritten keine vertragliche Verbindung entsprechend Ziff. 4. Zudem erfährt der Kunde, wenn er Auswertungen der über „seine“ CC-Lösungen erfassten Daten erhält, personenbezogene Daten des Dritten. Das mag im Familienumfeld unkritisch sein, außerhalb ist es das nicht, insbesondere nicht im rein beruflichen Umfeld, hier insbesondere nicht zwischen den Parteien eines Arbeitsvertrags. Nicht gemeint ist vorliegend eine Konstellation, in der der Hersteller es dem Dritten ermöglicht, einen eigenen Vertrag mit dem Hersteller abzuschließen.

Für die Nutzung des Kfz durch Dritte sehen beispielsweise die Bedingungen des Telematik-Tarifes von S-Direkt in § 9 i vor, dass der Kunde „jeden anderen Nutzer“ des Fahrzeuges darauf hinweisen muss, „dass eine Telematik-Box in Ihrem Fahrzeug verbaut ist und Sie daher Fahrtdaten auch eines anderen Kfz-Nutzers einsehen können“. Wer diesen Hinweis mit diesem Wortlaut weitergibt, hat sicherlich datenschutzrechtlich nicht unbedingt Transparenz geschaffen, insbesondere, wenn man bedenkt, dass in den Bedingungen die Datenverarbeitung im Verhältnis zwischen S-Direkt und Kunde seitenlang beschrieben wird. Ist die Datenverarbeitung nicht offensichtlich, müsste die Datenverarbeitungs-

einrichtung den Datenschutz gewährleisten oder die Freiheit bestehen, die Einrichtung vor Fahrtantritt auszubauen. Besteht diese nicht, ist zumindest durch geeignete Vorkehrungen beim Start des Fahrzeuges, wie interne Signale bzw. Merker auf Anzeigebildschirmen, darauf hinzuweisen, dass und in welchem Umfang Daten verarbeitet werden<sup>16</sup>.

b) Bekommt ein Arbeitnehmer ein Fahrzeug zur Verfügung gestellt, sind verschiedene Fallgestaltungen denkbar, insbesondere die Gestellung eines Kfz zu rein dienstlichen wie die Gestellung desselben zu dienstlichen wie privaten Zwecken. Ferner ist zu unterscheiden zwischen einer individuellen Gestellung und einer Verwaltung von Kfz in einem Fuhrpark. In einem Fuhrpark, in dem die Fahrzeuge verschiedenen Fahrern je nach Arbeitsanfall und Eignung zugewiesen werden, stehen personenbezogene Daten jedenfalls dann in Rede, wenn die verantwortliche Stelle (Fuhrparkleitung/Arbeitgeber), wie es bei einem gut organisierten Fuhrparkmanagement die Regel ist, technisch in der Lage ist, die bei CC erzeugten Daten in einer Weise zusammenzuführen, die eine Zuordnung eines Fahrzeuges in zeitlicher Hinsicht zu einer bestimmten Person ermöglicht – dann liegen auch hier personenbezogene Daten vor. Eine Verarbeitung personenbezogener Daten ist zur Durchführung des Beschäftigungsverhältnisses erlaubt, insbesondere zur Optimierung des Fuhrparkeinsatzes und zum Aufspüren verlustig gegangener Fahrzeuge. Naturgemäß ist eine lückenlose Überwachung des Arbeitsverhaltens des Arbeitnehmers im Wege einer permanenten Ortung nicht erlaubt<sup>17</sup>. Grenzen sind auch gezogen, wenn das Kfz dem Arbeitnehmer auch zu privaten Zwecken zur Verfügung gestellt wird. In den Bereich datenschutzrechtlich erlaubter Nutzung wird man also nur kommen, wenn man den Arbeitnehmer auf die Nutzung der entsprechenden Technologie hinweist, gern unter Übermittlung der von dem Hersteller stammenden Leistungsbeschreibung, und ihn eine – freiwillige – Einwilligung zum Einsatz entsprechender Geräte und die daraus resultierende Nutzung der Daten abgeben lässt<sup>18</sup>.

Die Abgabe einer solchen Einwilligungserklärung schadet mit Sicherheit nicht, wenn sie von den unter lit. a) angesprochenen Dritten im Verhältnis zum Eigentümer bzw. Kunden des Hersteller abgegeben wird.

c) Das dürfte auch gelten für den Fall der Vermietung von Kfz an Dritte, z.B. bei Carsharing-Modellen bzw. modernen Formen der Kfz-Miete.

Insoweit besteht die Besonderheit, dass der Eigentümer/Halter bei bestimmten Abrechnungsmethoden bestimmte Telematikdaten braucht, um die Abrechnung durchführen zu können. Insoweit wird für Daten, die Abrechnungszwecke decken, eine Erlaubnis nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG vorliegen. Auch hier kommt es also wieder auf die Leistungsbeschreibung an. Erhoben werden in solchen Zusammenhängen die für das Zustandekommen und die Durchführung des Mietvertrages notwendigen personenbezogenen Daten des Mieters, letztere insbesondere in Form von „kundenbezogenen Nutzungs- und Fahrzeugdaten (einschließlich Daten zur Lokalisierung des Fahrzeuges)“. Sofern die einzelnen Mietvorgänge zu Zwecken der Abrechnung in einer

Übersicht zusammengefasst werden und dabei Startort und -zeitpunkt sowie Zielort und -zeitpunkt und die Dauer der Nutzung ausreichend sind, müssten weitere Daten zu Zwecken der Abrechnung jedenfalls nicht erhoben bzw. verarbeitet werden. Damit ist es bei modernen Formen der Mietwagenbereitstellung aber nicht getan. Vielmehr werden auf den Smartphones derjenigen Mieter, die einen Rahmenvertrag haben, Apps installiert, die Fahrzeuge in der Nähe anzeigen, sobald der Rahmenvertragsmieter die App aufruft. Teil der Daten ist bei einem solchen LBS der eigene Standort des Rahmenvertragsmieters; dieses Datum sollte nur anonymisiert an denjenigen weitergegeben werden, der die Kartendaten für die App bereitstellt<sup>19</sup>.

## VI. Fazit

*Formal werden Verträge zur Einführung von CC-Lösungen i.d.R. neben dem eigentlichen Erwerbsvertrag für das Kfz geschlossen, zum einen, weil nicht alle Kunden diese Lösung wünschen, zum anderen, weil auch andere Personen als der Ersterwerber als CC-Kunden in Betracht kommen. Diese Verträge stellen Allgemeine Geschäftsbedingungen im Rechtssinne dar (§§ 305 ff BGB). Während bei den CC-Lösungen zunächst wenig spezifische Leistungsbeschreibungen erfolgten, geht die Tendenz in den letzten Jahren zu detaillierteren und verständlicheren Leistungsbeschreibungen, auch, um über die Leistungsbeschreibung zu einer geeigneten Rechtfertigung für die Datenverarbeitung nach § 28 Abs. 1 BDSG zu gelangen. Bedeutsam ist die Leistungsbeschreibung zudem für die rechtliche Einordnung des Vertrages in die Kategorien des bürgerlichen Rechts (Dienst-/Werkvertrag) und mithin für die Bewertung nach § 307 BGB im Rahmen allgemeiner Geschäftsbedingungen.*



**RA FAITR FAArb  
Prof. Klaus Gennen**

RA FAITR FAArb Prof. Klaus Gennen ist Rechtsanwalt in Köln bei LLR LegerlotzLaschet Rechtsanwälte sowie Professor an der Fachhochschule Köln im Bereich Informationstechnologie. Er befasst sich mit Vertragsgestaltung im IT-Bereich sowie mit Datenschutzfragen.

<sup>16</sup> So generell für den Bereich der Telematik im Kraftfahrzeug Weichert, SVR 2014, 241.

<sup>17</sup> Vgl. u.a. BGH v. 04.06.2013, NJW 2013, 2530.

<sup>18</sup> Die ebenfalls mögliche Regelung über eine Betriebsvereinbarung nach § 87 Abs. 1 Nr. 6 BetrVG sein, hier nur der Vollständigkeit halber erwähnt.

<sup>19</sup> Besonderheiten können gelten, wenn die Mietfahrzeuge, wie z.B. bei DriveNow (Dienst von BMW, Mini und Sixt) als mobile Verkehrsmelder eingesetzt werden. Diese Verkehrsdaten werden an einen Dritten – BMW – weitergeleitet, offensichtlich jedoch anonymisiert, d.h. ohne Beziehbareit auf den einzelnen Mieter. Allerdings lässt sich dieser Dienst deaktivieren. Hierzu sollte bei Start des Fahrzeuges aufgefordert werden; die entsprechende Datenerhebung und -verarbeitung ist für die Durchführung des Mietvertrages nicht erforderlich.

# Kurzbeiträge

## Aus den aktuellen Berichten der Aufsichtsbehörden (18): Erhebung von Daten zu Zwecken der Werbung durch Krankenkassen

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter\*

Als ersten Tätigkeitsbericht der Aufsichtsbehörden im angelaufenen Jahr hat am 20. Januar 2015 der Bayerische Landesbeauftragte für den Datenschutz seinen 26. Jahresbericht vorgelegt, der als Berichtszeitraum die Jahre 2013/2014 umfasst. Hierbei befasst er sich auch mit der Nutzung von Daten zu Werbezwecken durch die seiner Aufsicht unterliegenden öffentlich-rechtlichen Stellen.

### I. Weitergabe von Schülerdaten zu Werbezwecken

Die Übermittlung von Schülerdaten an außerschulische Stellen ist in Bayern – und auch in anderen Bundesländern – bereichsspezifisch geregelt. Nach dem Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) ist eine Datenweitergabe grundsätzlich nur zulässig, wenn sie zur Erfüllung einer den Schulen zugewiesenen Aufgabe erforderlich ist bzw. ein Rechtsanspruch auf Herausgabe besteht. Zudem sind nach Art. 84 Abs. 1 BayEUG der Vertrieb von Gegenständen aller Art, die Ankündigungen und Werbung hierzu, das Sammeln von Bestellungen sowie der Abschluss sonstiger Geschäfte in der Schule untersagt. In Zusammenhang mit dem in Art. 84 Abs. 1 BayEUG enthaltenen Verbot der kommerziellen Werbung an Schulen ist das Verbot der Übermittlung von Schülerdaten zu diesem Zweck daher eindeutig.

Gleichwohl sind Umgehungsversuche nach wie vor feststellbar. Anstatt der Weitergabe der Daten wird eine Erhebung der Daten bei den Schülern im Zusammenhang mit der Teilnahme an einem Wettbewerb, einer Geschenkauslobung bzw. einem Gewinnspiel ermöglicht oder geduldet. „Partner“ der Schule sind häufig Kreditinstitute, (Buch-)Direktvertriebsunternehmen oder Krankenkassen.

### II. Gewinnspiele von Krankenkassen

Dass auch gesetzliche Krankenkassen das Bestreben haben, neue Mitglieder zu gewinnen bzw. an die Adressen potentieller neuer Mitglieder zu gelangen, ist u.a. im Hinblick auf den Wettbewerb unter Krankenversicherern verständlich. Gleichwohl hat ihnen der Gesetzgeber in § 284 Abs. 4 SGB V insoweit enge Grenzen gezogen. Zur Gewinnung von Mitgliedern dürfen die Krankenkassen Daten nur erheben, ver-

arbeiten und nutzen, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Im Übrigen wird für die Datenerhebung, Verarbeitung und Nutzung auf die Vorschriften des Ersten und Zehnten Buches des SGB, und damit auf §§ 67a und 67b SGB X, verwiesen. Diese Bestimmungen regeln die Erhebung und Verarbeitung von Sozialdaten und erlauben eine Verarbeitung bei Einholung der Einwilligung des Betroffenen (vgl. LDSB Baden-Württemberg, 28. TB, 2007, 3. Teil, 2. Abschnitt, Ziff. 1). Ob Daten über einen an einem Abschluss mit der Krankenkasse möglicherweise Interessierten den in § 67 Abs. 1 SGB X definierten Begriff des Sozialdatums schon erfüllen, mag hier einmal dahinstehen. Ansonsten würde sich die Erlaubnis für die Erhebung und Verarbeitung infolge Einwilligung aus dem allgemeinen Datenschutzrecht ergeben

Werden also z.B. im Rahmen einer Aktion „Mit dem Rad zur Arbeit“ personenbezogene Daten der Teilnehmer abgefragt, so muss bei der Einholung der für die werbliche Nutzung der Daten benötigten Einwilligungserklärung darauf hingewiesen werden, dass die Daten des Teilnehmers nicht nur für die Auslosung der Gewinner, sondern u.a. auch zur Mitgliedergewinnung, d.h. zur Anbahnung eines Versicherungsverhältnisses erhoben werden und dass die Angabe der nicht zur Teilnahme an dem Gewinnspiel benötigten Daten freiwillig ist (BremLDSB, 36. Jahresbericht, 2013, Ziff. 7.3; vgl. auch LDSB Baden-Württemberg, 29. TB, 2009, 5. Teil, 2. Abschnitt, Ziff. 4))

### III. Erhebung der Daten bei Minderjährigen

Werden auch Minderjährige zwecks der Erhebung von Werbedaten zur Teilnahme an einem Gewinnspiel animiert, so ist nach der Rechtsprechung des BGH (Urteil vom 22.1.2014, in diesem Heft S. 89) die eingeholte Einwilligung aufgrund der in § 4 Abs. 3 UWG untersagten Ausnutzung der geschäftlichen Unerfahrenheit Minderjähriger wettbewerbswidrig, wobei das auch für Minderjährige im Alter über 15 Jahren gilt. Auch die 15-17 jährigen Teilnehmer können

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

nach Ansicht des BGH die mit der Preisgabe der Daten und mit der Einwilligungserklärung Ihnen entstehenden Nachteile sowie die wirtschaftlichen Vorteile, die sich das werbende Unternehmen davon verspricht, nur schwer erkennen. Daran ändere sich nichts durch die zunehmende Erfahrung von Jugendlichen mit Medien und auch die Tatsache, dass Minderjährige nach Vollendung des 15. Lebensjahrs ihre Krankenkasse selbst wählen dürfen.

Auch wenn der BGH als weiteres Argument erwähnt, dass Jugendliche eher als Erwachsene zu der Teilnahme an einem Gewinnspiel neigen und in diesem Zusammenhang leichter zur Datenbekanntgabe „verführt“ werden können, ist die Verbindung der Datenerhebung zu Werbezwecken bei Minderjährigen nicht nur allein wegen einer Verknüpfung mit dem Gewinnspiel unlauter. Denn die Teilnahme an einem Gewinnspiel allein ist Jugendlichen durchaus weiter möglich. Dagegen bedarf die werbliche Nutzung der Daten der Jugendlichen nunmehr generell der Einwilligung der Eltern.

#### **IV. Fallbeispiel: Datenerhebung der AOK für Werbezwecke bei einer gesponserten Sportaktion**

Unter den obigen Vorgaben wird daher die im Zusammenhang mit einer von der AOK gesponserten Sportaktion gestattete Einholung der Einwilligung bei Schülern nunmehr anders zu betrachten sein, als es 2013 durch das ULD (Häufig gestellte Fragen zum Bereich Schule, VI Ziff. 10; [www.datenschutzzentrum.de/fag/schule.htm](http://www.datenschutzzentrum.de/fag/schule.htm)) geschah. Als Gegenleistung für die Finanzierung von Preisen und den Aufwand für die Organisation der Aktion wurde der AOK gestattet, Daten der teilnehmenden Schüler zu erheben, um die Betroffenen über die Leistungen der AOK zu informieren und eben auch um neue Mitglieder zu gewinnen. Auf den Anmelde Listen konnten die Schüler bei gleichzeitiger Information über den Zweck und den Umfang der Datenverarbeitung durch Ankreuzen in die Speicherung ihrer Daten für Werbezwecke durch die AOK einwilligen oder diese Einwilligung explizit verweigern. Auch hier war einmal indirekt der Wunsch zur Teilnahme an der Aktion gegeben, und ob die umfangreichen Merkblätter – sofern sie denn gelesen wurden – die Schüler „schlauer“ gemacht hätten, bleibt fraglich. Jedoch wurden die Schüler angehalten, die Datenschutzerklärung an die Eltern weiterzuleiten. Diese hatten danach immer noch das Recht, der Verar-

beitung der Daten ihrer Kinder gegenüber der AOK zu widersprechen.

#### **V. Die Weitergabe von Bedienstetendaten an die Versicherung**

Der BayLSDB ist auch Beschwerden nachgegangen, in denen der Verdacht geäußert wurde, dass Beschäftigte von personalverwaltenden Behörden Mitarbeiterdaten an private Versicherungen oder Versicherungsvermittler weitergegeben hätten (26. JB, S. 225 f). Diese Vermutung wurde regelmäßig mit der zeitlichen Nähe der Kontaktaufnahme durch Versicherungsvertreter mit der vorangegangenen Bewerbung bei der öffentlichen Hand begründet. Die entsprechenden Recherchen des Landesbeauftragten blieben aber ohne Erfolg. Gleichwohl hat er auf eine verstärkte Sensibilisierung der Behörden bzw. ihrer Bediensteten hingewirkt, wobei deutlich gemacht wurde, dass eine Durchbrechung des Personalaktengeheimnisses zu beamten-, disziplinar-, straf- und datenschutzrechtlichen Konsequenzen führen kann.

In der Sachverhaltsaufklärung erfolgreicher war insoweit der rheinland-pfälzische Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI). Anlass seiner Untersuchungen waren Fälle sogenannter Listenkäufe, bei denen einzelne Behördenmitarbeiter weisungswidrig Datensätze von Anwärtern im öffentlichen Dienst an Mitarbeiter der Versicherung ohne Einwilligung der Betroffenen – z.T. gegen Entgeltzahlung – weitergegeben hatten.

Obwohl eine derartige Erhebung von Neukundendaten auch gegen die unternehmensinterne Vorgaben der Versicherung verstieß, wurde gegen das Unternehmen und seine Vorstandsmitglieder ein Ordnungswidrigkeitenverfahren eingeleitet, das einvernehmlich mit der Zahlung einer Geldbuße in Höhe von 1,3 Millionen Euro und der Bereitstellung von weiteren 600.000 Euro für eine Datenschutz-Stiftungsprofessur an der Johannes Gutenberg-Universität Mainz abgeschlossen wurde. Die Berechtigung hierfür wurde darin gesehen, dass nicht alle Aufsichtsmaßnahmen und Kontrollen etabliert und angewandt worden waren, die aus heutiger datenschutzrechtlicher Sicht den notwendigen Standards entsprechen. Die Höhe des Bußgeldes wurde maßgeblich durch den in § 43 Abs. 3 Satz 2 und 3 BDSG geregelten Aspekt der Gewinnabschöpfung bestimmt und wird wohl auch dazu beitragen, derartige Praktiken anderer Versicherer zu unterbinden.

# Neue Rechtsprechung: Vertragsstrafenklauseln in Adressverträgen

Stefan Wehmeyer, Stuttgart\*

Für einen gewerblichen Adresshändler sind die Adressbestände das wesentliche Wirtschaftsgut, dessen Wertbestand er absichern muss. Vertragsstrafen bilden für ihn ein Element, um sich gegenüber seinen Kunden gegen eine vertragswidrige Nutzung der überlassenen Adressen zu schützen.

## I. Vertragsbeziehungen bei Adressverträgen

Im gewerblichen Adresshandel stehen in der Praxis in der Regel zwei bzw. drei Personen miteinander in Kontakt, die sämtlich Unternehmer sind: der Adresshändler bzw. Listeigner auf der einen und der Werbende auf der anderen Seite sowie, je nach Ausgestaltung der Vertragsbeziehung, der Listbroker. Im Wesentlichen sind dabei zwei Typen von Vertragsbeziehungen zu unterscheiden, zum einen die direkte Geschäftsbeziehung zwischen dem Werbenden und dem Adresshändler und zum anderen die so genannte Listbroker-Variante. Im ersten Fall werden die vertraglichen Leistungen zwischen diesen beiden Personen ohne Einschaltung eines Dritten abgewickelt. Diese Konstellation findet sich in der Praxis vor allem dann, wenn der Werbende über eine entsprechende Marktkenntnis verfügt. Im zweiten Fall übernimmt hingegen ein Listbroker die gegebenenfalls arbeitsintensive Recherche nach den gewünschten Adressen. Er stellt den Kontakt zwischen dem Werbenden und dem Adresshändler/Eigner der Adresslisten her, wobei der Listbroker auch sämtliche Aufgaben des Adresshändlers selbst übernehmen kann<sup>1</sup>. Je nach vertraglicher Ausgestaltung werden die Adressen dabei von dem damit werbenden Kunden des Adresshändlers entweder einmalig oder beliebig häufig benutzt<sup>2</sup>.

## II. Vertragswidrige Nutzung der Adressen

In der Praxis kann es durchaus vorkommen, dass der Werbende die Daten nicht gemäß der vertraglichen Vereinbarung nutzt, z.B. indem er sie nach Ablauf der vereinbarten Dauer noch weiter verwendet. Den Nachweis eines diesbezüglichen Verstoßes führt der Adresshändler regelmäßig über die Verwendung von Kontrolladressen, die er in den Adressbestand einschleust und über die er von der vertragswidrigen Verwendung Kenntnis erlangt. Hierdurch wird dem Adresshändler praktisch eine Umkehr der Beweislast zu seinen Gunsten ermöglicht<sup>3</sup>. Die Zulässigkeit solcher Kontrolladressen ist von der Rechtsprechung – soweit diese vertraglich ausdrücklich vereinbart sind<sup>4</sup> – grundsätzlich anerkannt<sup>5</sup>.

Enthält der Adressvertrag für den Fall des Vertragsverstoßes keine spezifische Bestimmung einer Vertragsstrafe, kann der Adresshändler vom Werbenden Schadensersatz

gemäß §§ 280, 282 BGB verlangen, wobei sich die Schadenshöhe nach der fiktiven Lizenzgebühr für die tatsächlich durch den Werbenden erfolgte Adressnutzung richtet<sup>6</sup>. Aus Praktikabilitätsgründen wird in der Praxis häufig eine Vertragsstrafe vereinbart. Diese soll nicht nur dazu dienen, dass der zu leistende Schadensersatz dem realen Wert der Adressdaten entspricht, sondern zugleich auch eine abschreckende Wirkung haben, da sie neben dem Schadensersatz verlangt werden kann.

## III. Zulässigkeit von Vertragsstrafen in Adressverträgen

### 1. Grundsätzliche Zulässigkeit

Im unternehmerischen Bereich ist die rechtliche Wirksamkeit von Vertragsstrafenklauseln in Adressverträgen von der Rechtsprechung vom Grundsatz her seit längerem anerkannt<sup>7</sup>. Das Verbot in § 309 Nr. 6 BGB greift insoweit nicht<sup>8</sup> und hat auch keine Indizwirkung für die Unwirksamkeit solcher Klauseln. Zwischen Unternehmern ist für die Wirksamkeit einer Vertragsstrafenklausel § 307 BGB maßgeblich<sup>9</sup>. Gerade wenn das Ziel der Vertragsstrafe ist, eine rechtswidrige Nutzung der Adressen zu unterlassen, bringt häufig allein sie einen wirksamen Schutz<sup>10</sup>.

### 2. Höhe der Vertragsstrafe

Nicht eindeutig ist die Rechtsprechung hingegen bezüglich der zulässigen Höhe einer Vertragsstrafe. In der Praxis finden sich häufig Vertragsstrafenklauseln, die für den Fall einer vertragswidrigen Nutzung die Zahlung des Zehnfachen des vertraglich vereinbarten Entgelts vorsehen<sup>11</sup>.

\* Der Autor ist Rechtsanwalt und Chefsyndikus in einem Versandhandelskonzern.

1 Bahr, Recht des Adresshandels, Rn. 57 ff., 744 ff.

2 Bahr, Recht des Adresshandels, Rn. 760 ff.; Feldmann/Höppner, in: Moos, Datennutzungs- und Datenschutzverträge, S. 399.

3 Bahr, Recht des Adresshandels, Rn. 857.

4 Zu den Anforderungen im Einzelnen: Bahr, Recht des Adresshandels, Rn. 859 ff.

5 BGH, NJW 1970, 134; Gliss, Sicherungsmaßnahmen »Kontrolladressen«, in: DSB 7+8/2000, 24 f.

6 Bahr, Recht des Adresshandels, Rn. 835 ff.

7 BGH, NJW 1976, 1886; OLG München, NJW-RR 1993, 1334.

8 BGHZ 154, 171.

9 Hensen, in: Ulmer/Brandner/Hensen, AGB-Recht, 11. Aufl., § 309 Nr. 6 BGB, Rn.18.

10 BGH NJW 1976, Seite 1886, 1887; OLG München, NJW-RR 1993, 1334 f.

11 Brecheis, Datenschutz und Direkt-Marketing: Probleme und Lösungsansätze, 45; Gliss, Sicherungsmaßnahmen »Kontrolladressen«, in: DSB 7+8/2000, 24 f.

Der BGH hat dies in einer Entscheidung aus dem Jahre 1976 nicht beanstandet. Er hat dabei nur generell zu der Frage Stellung genommen, ob Vertragsstrafen im unternehmerischen Bereich in dieser Höhe AGB-rechtlich zulässig sind, die Klausel selbst jedoch nicht anhand der übrigen AGB-rechtlichen Vorgaben subsumiert<sup>12</sup>.

Demgegenüber lässt das OLG München offen, ob das Zehnfache zulässig ist, hält jedoch eine Vertragsstrafe in Höhe des Zwanzigfachen Entgelts für jede vertragswidrige Nutzung für unwirksam<sup>13</sup>. Das Gericht weist zur Begründung darauf hin, dass der durch die vertragswidrige Mehrfachverwendung der Adressen entstandene Schaden für den Adresshändler allein im Entgang des Entgelts für die Wiederverwendung liegt. Bei einer Vertragsstrafe in Höhe des Zwanzigfachen Betrages des Gesamtmietentgelts diene die Vertragsstrafe nicht mehr der darauf gerichteten Druckfunktion, sondern der Schaffung neuer, vom Interesse des Auftraggebers losgelöster, Geldforderungen<sup>14</sup>.

Das OLG Frankfurt a. M. lässt hingegen in einer älteren Entscheidung eine Vertragsstrafe in Höhe des zwanzigfachen Entgelts zu<sup>15</sup>. Die Literatur sieht diese Entscheidung teilweise kritisch<sup>16</sup>.

Das OLG Celle hat eine Vertragsstrafe in Höhe von 25.000 € pro Vertragsverstoß bei einem Preis jeder einzelnen Adresse von 0,15 € als unangemessene Benachteiligung gemäß §§ 307 Abs. 1 und 2, 310 Abs. 1 BGB für treuwidrig erachtet, da dies dem Klauselverwender die Möglichkeit eröffne, an den Vertragsstrafen erheblich dazu zu verdienen<sup>17</sup>.

### 3. Neuere restriktive Entscheidung des OLG Frankfurt a. M.

Allen vorgenannten Entscheidungen ist gemein, dass sie die Zulässigkeit der Vertragsstrafe allein an der Höhe messen. Für die AGB-rechtlichen Grenzen von Vertragsstrafenklauseln auch im unternehmerischen Verkehr ist neben dem Verhältnis zwischen vertraglichem Entgelt und Höhe der Vertragsstrafe aber auch ihre übrige rechtliche Struktur maßgeblich, so z.B. welche Verstöße sie abdecken sollen.

Diesen Ansatz hat in diesem Zusammenhang nunmehr richtigerweise erstmals auch das OLG Frankfurt a.M. in einer bislang nicht veröffentlichten Entscheidung aufgenommen. Dem Urteil lag eine AGB-Klausel zu Grunde, die „für jeden Verstoß [...] die Zahlung einer Vertragsstrafe des zehnfachen Entgeltes der Kosten des Nutzungsrechtes“ bzw. „bei Verletzung dieser Vereinbarung“ bzw. „für den Fall der Zuwiderhandlung“ vorsah. Das OLG hält diese Klausel nach §§ 310 Abs. 1 Satz 2, 307 Abs. 1 und 2 BGB für unangemessen und unwirksam, weil sie die die Zahlung *verschuldensunabhängig* an einen Vertragsverstoß knüpfe. Eine Vertragsstrafe setzte aber in jedem Fall – auch, wie im vorliegenden Fall, bei einem Verstoß gegen Unterlassungspflichten – voraus, dass der Schuldner schuldhaft im Sinne von § 276 BGB handelt<sup>18</sup>. Dies ist für eine Vertragsstrafe in Form einer AGB allgemein anerkannt<sup>19</sup>. Das OLG weist weiterhin darauf hin, dass von diesem Grundsatz nur im Wege einer Individu-

alabrede abgewichen werden könne. Im unternehmerischen Verkehr bestünde zwar im AGB-Bereich ein erheblich weiterer Spielraum, Vertragsstrafen zu vereinbaren, als im Verbraucherbereich. Aber auch zwischen Unternehmern sei eine verschuldensunabhängige Strafklausel als AGB nur dann ausnahmsweise zulässig, wenn gewichtige Interessen des Verwenders dies verlangten<sup>20</sup>. In dem entschiedenen Fall hat der Senat dies verneint. Unabhängig davon, dass solche Interessen im konkreten Fall nicht dargelegt wurden, sieht das Gericht eine unangemessene Bevorteilung der Klauselverwenderin allein schon darin, dass bereits die vertragswidrige Nutzung von lediglich zwei Kontrolladressen ohne Rücksicht auf ein Verschulden die hohe Vertragsstrafe verwirke. Für die werbende Adressempfängerin bedeute dies faktisch eine Beweislastumkehr, ohne dass es dabei auf ihr Vertretenmüssen ankäme<sup>21</sup>.

### IV. Fazit

Der Entscheidung des OLG Frankfurt a. M. ist zuzustimmen. Im Gegensatz zu den übrigen ergangenen Entscheidungen – insbesondere der älteren des BGH<sup>22</sup> – wird hier nicht allein auf das quantitative Verhältnis zwischen Entgelt und Höhe der Vertragsstrafe abgestellt, sondern werden richtigerweise auch qualitativ die allgemeinen zum AGB-Recht anerkannten Begleitumstände (hier das Verschulden) einbezogen. Die Berufung auf einige wenige Kontrolladressen ohne jeden Bezug zur Anzahl der insgesamt dem Werbenden überlassenen Adressen ist im Vergleich zur Höhe der verwirkten Vertragsstrafe unverhältnismäßig. Im Bereich der Werbung ist es anerkannt, dass »Ausreißer« des Werbenden ggf. rechtlich zu seinen Gunsten zu berücksichtigen sind<sup>23</sup>. Auch die Ausführungen des Gerichts zur faktischen Beweislastumkehr sind zutreffend und stehen mit der übrigen AGB-rechtlichen Rechtsprechung im Einklang. Mit der vorgeformulierten Regelung zur Vermutungswirkung eines Vertragsverstoßes gegen die Verwendung von Kontrolladressen verschafft sich der Adresshändler gegenüber dem Kunden ein Mittel, mit dem er seiner Beweislast solange genügen kann, bis der Kunde die Unrichtigkeit der Vermutung bewiesen hat. Damit verkörpert dies den typischen Fall einer Be-

12 BGH NJW 1976, 1886, 1887.

13 OLG München, NJW-RR 1993, 1334 f.

14 OLG München, NJW-RR 1993, 1334, 1335.

15 OLG Frankfurt a. M., BB 1985, 1560 f.

16 Hensen, in: Ulmer/Brandner/Hensen, AGB-Recht, 11. Aufl., § 309 Nr. 6 BGB, Rn. 20; von Westphalen, EWIR 1985, 625 f.

17 OLG Celle, NJW-RR 2013, 887.

18 OLG Frankfurt a. M., Urteil vom 10. Dezember 2013, AZ 5 U 70/13.

19 BGH NJW-RR 2007, 1505; Gottwald, in: Münchener Kommentar, BGB, 6. Auflage, § 339 Rn. 20; Palandt-Grüneberg, BGB, 74. Auflage, § 339 Rn. 15.

20 So auch: Palandt-Grüneberg, BGB, 74. Auflage, § 309, Rn. 39.

21 OLG Frankfurt a. M., Urteil vom 10. Dezember 2013, AZ 5 U 70/13.

22 BGH NJW 1976, 1886 f.

23 So ausdrücklich für Vertragsstrafen im Bereich des UWG: Köhler, in: Köhler/Bornkamm, UWG, 32. Aufl., § 7, Rn. 29.

welaständerung, die gemäß § 309 Nr. 12 b BGB – auch im unternehmerischen Verkehr<sup>24</sup> – unwirksam ist<sup>25</sup>.

## V. Ausblick

Adresshändler werden ihre Vertragsstrafenklauseln im Hinblick auf diese Entscheidung des OLG Frankfurt a. M. überprüfen und gegebenenfalls anpassen müssen.

Insbesondere ist zukünftig für Adresshändler die Verwendung solcher Klauseln riskant, die die Vertragsstrafe

zum einen verschuldensunabhängig festsetzen und/oder zum anderen der Höhe nach ohne Rücksicht auf das Verhältnis zwischen der Anzahl der vertragswidrig verwendeten und der Anzahl der vom Werbenden angemieteten Adressen auslösen.

24 Hensen, in: Ulmer/Brandner/Hensen, AGB-Recht, 11. Aufl., § 309 Nr. 12 BGB, Rn. 25 ff.

25 So jüngst BGH NJW 2014, 2857, 2859 f. unter Verweis auf BGH MDR 1986, 51, 52.

# Konzerninterner Datenaustausch in der Praxis – Ergebnisse der Online-Befragung

Andreas Leonhardt, Neckarsulm\*

Weltweit tätige Konzerne stehen vor der Herausforderung, den allgegenwärtigen Austausch personenbezogener Daten zwischen – international tätigen – Konzerngesellschaften zu erfassen und rechtskonform zu organisieren.

Bestehende Befragungen wie das GDD Privacy Panel<sup>1</sup>, die KPMG-Studie zur Auftragsdatenverarbeitung<sup>2</sup> und die 2B Advice-Studie zur Datenschutzpraxis 2012<sup>3</sup> legen bereits nahe, dass speziell der internationale Datenaustausch in vielen Unternehmen eine immer größere Rolle spielt.<sup>4</sup> Detaillierte empirische Erkenntnisse, die Konzerne zur Gewinnung von Best Practice-Ansätzen in diesem Bereich nutzen könnten, lagen jedoch bisher nicht vor.<sup>5</sup>

Im Rahmen einer Masterarbeit im Studiengang Legal Management an der German Graduate School of Management and Law, Heilbronn, wurden die in diesem Themengebiet praxisrelevanten Fragestellungen identifiziert und in einen detaillierten Fragebogen mit 64 Einzelfragen<sup>6</sup> überführt. Im Anschluss wurde zusammen mit der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) im Oktober und November 2014 eine Online-Befragung<sup>7</sup> durchgeführt. Der Gegenstand der Befragung und die wesentlichen Ergebnisse<sup>8</sup> sollen im Folgenden kurz dargestellt werden.

## I. Gegenstand der Befragung

Die Teilnehmer<sup>9</sup> wurden gebeten, Fragen zu folgenden praxisrelevanten Themen zu beantworten:

- Umsetzung der geltenden Anforderungen<sup>10</sup> zum internationalen Datenaustausch
- Umsetzung der Anforderungen der Aufsichtsbehörden an interne Kontrollen<sup>11</sup>
- Prüfungstätigkeit der Aufsichtsbehörden
- interne Organisation zur Umsetzung der Anforderungen

## II. Ergebnisse

Für die Ergebnisdarstellung konnten die Antworten aus 141 Fragebögen ausgewertet werden. Davon waren 115 (d.h.

\* Der Autor ist Informatik-Betriebswirt (VWA) und als Syndikusanwalt im Datenschutz tätig.

1 Das GDD Privacy Panel bildet eine jährlich aktualisierte Benchmark-Datenbank zu den wesentlichen Themenfeldern des Datenschutzbeauftragten, <https://www.gdd.de/privacy-panel>.

2 Die KPMG-Studie (2012) beleuchtet die Umsetzung der Anforderungen an die Auftragsdatenverarbeitung infolge der Novellierung des BDSG, <http://www.kpmg.de/Presse/29142.htm>.

3 2B Advice-Studie zur „Datenschutzpraxis 2012“, 2. Auflage 2012, <https://www.2b-advice.com/ws/GmbH-de/Studie-Datenschutzpraxis-2012>.

4 Vgl. GDD Privacy Panel (siehe Fn. 1) Auswertung Abschnitt „Konzernspezifische Fragen“ (Zugriff auf Auswertungen nur mit Registrierung).

5 Das GDD Privacy Panel (siehe Fn. 1) erfasst u.a. zur Frage „Rahmenbedingungen für den Datenaustausch im Konzern“ den quantitativen Einsatz der Gestaltungsinstrumente Standardvertragsklauseln, Safe Harbor und BCR. Die 2B Advice-Studie identifiziert zwar bei den befragten Unternehmen 85% Unzufriedenheit mit den bestehenden Gesetzen zur internationalen Datenverarbeitung, geht jedoch nicht weiter ins Detail (siehe Fn. 3, S. 63).

6 Im Fragebogen waren Filterregeln hinterlegt, so dass nicht relevante Fragen automatisch ausgeblendet wurden.

7 Die Befragungsdaten wurden anonym erhoben bzw. bei freiwilligen personenbezogenen Angaben für die Auswertung anonymisiert.

8 Die detaillierte Gesamtauswertung der Befragung kann auf der Website der GDD e.V. unter <https://www.gdd.de/aktuelles/news/ergebnisse-der-umfrage-zu-internationalen-datenermittlung> abgerufen werden.

9 81% der Teilnehmer sind selbst als Datenschutzbeauftragte (davon 17% als Konzerndatenschutzbeauftragte), 10% als Mitarbeiter des Datenschutzbeauftragten und 9% in anderer Funktion tätig.

10 Zu den Anforderungen der Aufsichtsbehörden vgl. Beschluss des Düsseldorf Kreises vom 11./12.09.2013.

11 So wird von den Aufsichtsbehörden bspw. eine Prüfung und Dokumentation der Safe Harbor-Kriterien durch das datenexportierende Unternehmen verlangt, vgl. Beschluss des Düsseldorf Kreises vom 28./29.10.2010.

82% der Teilnehmer) Konzerne oder Unternehmensgruppen<sup>12</sup> unterschiedlicher struktureller Komplexität und Unternehmensgröße.<sup>13</sup>

### 1. Spektrum der Erlaubnistatbestände wird breit genutzt

81% der Konzerne tauschen Daten auf Grundlage gesetzlicher Erlaubnistatbestände aus, wie bspw. den §§ 28, 32 BDSG. Bei den vertraglichen Regelungen dominieren Verträge zur Datenverarbeitung im Auftrag. Diese werden von 78% der befragten Unternehmen konzernintern eingesetzt. Bei 31% der Konzerne bestehen mehr als 50 Verträge, bei 2% sogar über 1.000. Von Konzernen, die Beschäftigtendaten austauschen, können 72% die Übermittlungen zudem auf entsprechende Betriebsvereinbarungen stützen. Knapp mehr als die Hälfte der Unternehmen (56%) setzt zudem auf die Einwilligung des Betroffenen. Allen Bedenken hinsichtlich der Wirksamkeit im Beschäftigungsverhältnis zum Trotz legitimieren 79% dieser Konzerne mit der Einwilligung auch die Übermittlung von Mitarbeiterdaten.

### 2. Standardvertragsklauseln sind der „Standard“

Das im internationalen Datenverkehr am häufigsten eingesetzte Instrument sind Standardvertragsklauseln der EU,<sup>14</sup> die 83% der Konzerne mit Drittstaaten transfers einsetzen. Den Antworten in den offenen Fragen zufolge werden teilweise komplexe Strukturen mit Vertragsgeflechten sowohl von Controller-Controller- als auch von Controller-Processor-Verträgen abgebildet. 48% der Konzerne vereinbaren allerdings ergänzende datenschutzrelevante Klauseln.<sup>15</sup> Gut die Hälfte der Konzerne (49%) versucht zudem, ein angemessenes Datenschutzniveau durch die Entwicklung eigener Vertragsklauseln sicherzustellen.

### 3. BCR im Aufwind

21% der Konzerne mit konzerninternem Datenaustausch mit Drittstaaten setzen bereits Binding Corporate Rules (BCR)<sup>16</sup> ein.<sup>17</sup> Die Aufsichtsbehörden verzichten offenbar weitgehend auf das Erfordernis von Einzelgenehmigungen.<sup>18</sup> Keiner der 16 Konzerne mit genehmigten BCR gibt an, dass Übermittlungen genehmigungspflichtig sind.

Von den 62% der Konzerne, die keine BCR einsetzen, wird das Genehmigungsverfahren überwiegend (77%) als zu aufwändig bzw. kostspielig angesehen. Bemerkenswert ist jedoch, dass sich BCR dennoch bereits bei weiteren 27% der Konzerne in Vorbereitung befinden.

### 4. Safe Harbor auf dem Rückzug?

Von den 73 Konzernen, die Daten mit Konzerngesellschaften in den USA austauschen, setzen 40% weiterhin auf das stark umstrittene<sup>19</sup> Abkommen. 51% dieser Konzerne haben allerdings Prüfungen<sup>20</sup> der Safe Harbor-Selbstzertifizierungen veranlasst und mit positivem Ergebnis abgeschlossen.

Die Gründe, warum Konzerne Safe Harbor nicht einsetzen, sind den Antworten in den offenen Fragen zufolge vielschichtig. Für einige Konzerne ist das Abkommen bereits aufgrund ihrer Branchenzugehörigkeit<sup>21</sup> nicht anwendbar,

andere scheuen den Aufwand der Selbstzertifizierung. Die Anzeichen für eine Abkehr der Unternehmen vom Abkommen mehren sich. Zahlreiche Teilnehmer werten das Abkommen als untaugliche Rechtsgrundlage und setzen für den Datenaustausch mit den USA auf Instrumente wie BCR oder Standardvertragsklauseln.

### 5. Interne Kontrollen überwiegend vor Ort

Über zwei Drittel (69%) der Konzerne prüfen regelmäßig die technischen und organisatorischen Maßnahmen der konzernangehörigen Gesellschaften. Die interne Prüftätigkeit der Konzerne stützt sich dabei primär auf das Instrument der Vor-Ort-Kontrolle, das von 69 % der Konzerne eingesetzt wird. An zweiter Stelle steht die Auskunft per Fragebogen (56%) und an dritter Stelle die Einsichtnahme in Zertifikate (40%).<sup>22</sup> Der Datenschutzbeauftragte kontrolliert den Antworten in den offenen Fragen zufolge jedoch nicht immer selbst, sondern bedient sich konzerninterner Mittel, wie z.B. der Revision, oder lässt externe Dienstleister prüfen.

### 6. Prüfungen durch die Aufsichtsbehörde sind die Ausnahme

Erwartet zurückhaltend ist weiterhin die Aufsichtstätigkeit der Datenschutzbehörden. Weniger als ein Zehntel der befragten Konzerne (9%) ist bislang in Bezug auf den konzerninternen Datenaustausch geprüft worden. Nur 10% der Unternehmen rechnen daher in nächster Zeit (innerhalb von ein bis drei Jahren) mit einer Überprüfung.

12 Aufgrund der vergleichbaren Interessenlage wurden in die Befragung auch Unternehmensgruppen einbezogen, die keine verbundenen Unternehmen i.S.d. §§ 15 ff. AktG sind. Der im Datenschutzrecht vereinfachend gebrauchte Begriff des „Konzerns“ soll im Folgenden auch für die Unternehmensgruppe gelten.

13 Drei Viertel der Konzerne bestehen aus bis zu 50, ein weiteres Fünftel aus bis zu 100 und in der Spitze aus 500 oder mehr Konzerngesellschaften. 17% der Konzerne beschäftigen weltweit mehr als 100.000 Mitarbeiter.

14 Bei unveränderter Übernahme sind diese genehmigungsfrei, vgl. Entscheidungen 2001/497/EG und 2004/915/EG sowie Beschluss 2010/87/EU der EU-Kommission.

15 Insbesondere bei Beschäftigtendaten, vgl. „Abgestimmte Positionen der Aufsichtsbehörden in der AG „Internationaler Datenverkehr“ am 12./13. Februar 2007 – Bezug: Protokoll der Sitzung mit Wirtschaftsverteuern am 23. Juni 2006“ vom 28.03.2007, S. 1 f.

16 Vgl. die Erläuterung der EU-Kommission unter [http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm).

17 Mit zunehmender Unternehmensgröße steigt dieser Wert an: 31% der Konzerne mit mehr als 100.000 Mitarbeitern setzen BCR ein, bei weiteren 24% sind diese in Vorbereitung. Bei kleinen Konzernen (bis 1.000 Mitarbeiter) beträgt die Implementierungsrate 9%.

18 Vgl. die offizielle Übersicht der EU-Kommission, „National filing requirements for authorisation of transfers on the basis of BCR“, [http://ec.europa.eu/justice/data-protection/document/international-transfers/files/table\\_nat\\_admin\\_req\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/international-transfers/files/table_nat_admin_req_en.pdf), S. 17.

19 So hatte u.a. das EU-Parlament bereits Anfang vergangenen Jahres die „sofortige Aussetzung“ des Abkommens gefordert, vgl. Nr. 38 der Entschließung vom 12.03.2014, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//DE>.

20 Vgl. Fn. 11.

21 Unternehmen, die nicht der Regulierung von FTC oder DoT unterliegen (u.a. Finanzinstitute, Luftverkehrs- und Telekommunikationsunternehmen), sind von der Zertifizierung ausgeschlossen, vgl. <http://www.export.gov/safeharbor/index.asp>.

22 Es waren Mehrfachnennungen möglich. An vierter und fünfter Stelle folgen externe Audits (36%) und andere Vorgehensweisen (26%).

Die Stichprobe der zehn geprüften Unternehmen lässt jedoch auf eine hohe Prüfungstiefe der Behörden schließen. Nur 30% der Unternehmen wurden ohne Beanstandungen geprüft. In mehr als der Hälfte der Fälle wurden Beanstandungen (11%) ausgesprochen oder Änderungen (44%) verlangt.

Dennoch hat nur weniger als ein Viertel (23%) der Konzerne mit Drittstaatentransfers die Instrumente zum konzerninternen Datenaustausch mit den Aufsichtsbehörden abgestimmt. Den Antworten aus den offenen Fragen zufolge bestehen bei den Konzernen teilweise Bedenken, dass die Behörden zu rigide und vor allem – für betriebliche Entscheidungsprozesse – zu langsam prüfen.

### 7. Interne Organisation – zentral oder dezentral?

Bei der überwiegenden Anzahl der Konzerne (66%) ist die Umsetzung der rechtlichen Anforderungen des konzerninternen Datenaustausches zentral organisiert.<sup>23</sup> Funktional verantworten deren Umsetzung entweder der Datenschutzbeauftragte (45%), die Fachabteilungen (27%) oder die Rechtsabteilung (23%).

Aufgrund der immensen praktischen Bedeutung der Auftragsdatenverarbeitung besteht bereits bei 89% der Konzerne ein konzernweit einheitliches Vertragsmuster.<sup>24</sup> Sofern dabei Unterauftragnehmer eingesetzt werden, verzichten 49% der Konzerne sogar auf eine ausdrückliche Zustimmung der konzerninternen Auftraggebergesellschaft.

### III. Fazit

Den Herausforderungen des konzerninternen Datenaustausches begegnen die Konzerne mit unterschiedlichen Organisationsformen und Instrumenten. Im Sinne eines Best Practice-Ansatzes treffen die folgenden Aussagen für die Mehrzahl der Konzerne zu:

- Die Umsetzung der rechtlichen Anforderungen wird überwiegend vom (Konzern-)Datenschutzbeauftragten verantwortet. Mit steigender Größe und Anzahl der Konzerngesellschaften nehmen dezentrale Organisationsmodelle zu.
- Bei der Organisation der Datenströme wenden die meisten Konzerne ein Bündel verschiedener Instrumente bestehend aus gesetzlichen Erlaubnistatbeständen, (Konzern-)Betriebsvereinbarungen, Einwilligungen und Verträgen zur Datenverarbeitung im Auftrag an.

- Interne Kontrollen technischer und organisatorischer Maßnahmen erfolgen überwiegend vor Ort, stützen sich jedoch ebenso auf Fragebogenverfahren und die Einsichtnahme in Zertifikate.

- 90% der Konzerne erwartet in den nächsten drei Jahren keine Prüfung durch die Aufsichtsbehörden.

Bei den 67% der Konzerne, die Daten mit Konzerngesellschaften in Drittstaaten austauschen, bestehen bei den Instrumenten für den internationalen Datenaustausch folgende Implementierungspräferenzen:

- Die Standardvertragsklauseln der EU werden von den meisten Konzernen bevorzugt. Fast die Hälfte der Konzerne setzt zusätzlich auf eigene Vertragsgestaltungen. Bei großen und komplexen Konzernen mit zahlreichen Konzerngesellschaften zeigt sich zudem ein starker Trend zu BCR.<sup>25</sup>
- Der schlechte Ruf der Safe Harbor Principles hält Konzerne zunehmend davon ab, diese als Grundlage für ihre Datenströme in die USA einzusetzen. Die Verbreitung ist jedoch weiterhin hoch.

Welche Organisationsformen und Instrumente für den jeweiligen Konzern in Frage kommen, bedarf einer Beurteilung des Einzelfalls. Anhaltspunkte können – aufgeschlüsselt nach Unternehmensgröße und struktureller Komplexität der Konzerne – der detaillierten Gesamtauswertung<sup>26</sup> der Befragung entnommen werden.

<sup>23</sup> Bei zunehmender Konzerngröße besteht ein Trend zur Dezentralisierung. Während 92% der kleinen Unternehmen (bis 1.000 MA weltweit) zentral organisiert sind, sind 63% der großen Unternehmen (mehr als 100.000 MA weltweit) dezentral aufgestellt.

<sup>24</sup> 45% verwenden ein eigenes Muster, 37% setzen auf das Muster der GGD e.V. und 12% auf das des BITKOM e.V. Keinen Anklang haben überraschender Weise die Muster des Hessischen Landesdatenschutzbeauftragten und des Bayerischen Landesamts für Datenschutzaufsicht gefunden.

<sup>25</sup> Weitere Erleichterungen können sich diese von der Datenschutzgrundverordnung versprechen, die mit dem verpflichtenden Kohärenzverfahren gemäß Art. 57 ff. des Kommissionsentwurfs (KOM (2012) 11 endgültig) die Aufsichtsbehörden der Mitgliedsstaaten zur Zusammenarbeit verpflichtet. Es wird erwartet, dass dies zu einer stärkeren Vereinheitlichung der Rechtsanwendung durch die Aufsichtsbehörden führen wird. Vgl. dazu Filip, ZD 2013, S. 51.

<sup>26</sup> Die Gesamtauswertung enthält auch eine Aufschlüsselung zur Größe der Datenschutzabteilungen. Zum Bezug siehe Fn. 8.

# Rechtsprechung

## Zur Reichweite „spruchrichterlicher Tätigkeit“ (Ls)

(Bundesverfassungsgericht, Beschluss vom 2. Dezember 2014 – 1 BvR 3106/09 –)

1. Die richterliche Mitteilung von Informationen an nichtverfahrensbeteiligte Dritte ist nicht allein deshalb eine der Rechtsschutzgarantie des Art. 19 Abs. 4 GG entzogene spruchrichterliche Tätigkeit, weil sie aus einem laufenden Rechtsstreit heraus erfolgt.
2. Vielmehr verlangt das Grundrecht auf effektiven Rechtsschutz, dass die Übermittlung von Aktenbestandteilen während eines zivilgerichtlichen Verfahrens an eine nicht an diesem Verfahren beteiligte Behörde (hier: an die Dienstbehörde eines Beamten) gerichtlich überprüfbar ist.

(Zu 2: Nicht amtlicher Leitsatz)

## Anspruch des Kindes auf Auskunft über die Identität des anonymen Samenspenders (Ls)

(Bundesgerichtshof, Urteil vom 28. Januar 2015 – XII ZR 201/13 –)

1. Ein Kind, das durch eine künstliche heterologe Insemination gezeugt wurde, kann grundsätzlich von der Reproduktionsklinik Auskunft über die Identität des anonymen Samenspenders verlangen. Ein bestimmtes Mindestalter des Kindes ist nicht erforderlich.
2. Machen die Eltern den Anspruch als gesetzliche Vertreter ihres Kindes geltend, setzt dies voraus, dass die Auskunft zum Zweck der Information des Kindes verlangt wird.
3. In jedem Fall muss eine Abwägung aller rechtlichen Belange – auch derjenigen des Samenspenders – das den Regelfall bildende Überwiegen der Interessen des Kindes an der Auskunft ergeben.

(Nicht amtliche Leitsätze)

## Datenerhebung bei Minderjährigen zur Mitgliederwerbung einer Krankenkasse im Rahmen eines Gewinnspiels

(Bundesgerichtshof, Urteil vom 22. Januar 2014 – I ZR 218/12 –)

**Eine gesetzliche Krankenkasse verstößt gegen das Verbot, die geschäftliche Unerfahrenheit von Jugendlichen auszunutzen (§ 4 Nr. 2 UWG), wenn sie im Zusammenhang mit der Durchführung eines Gewinnspiels von den Teilnehmern im Alter zwischen 15 und 17 Jahren umfangreiche personenbezogenen Daten erhebt, um diese (auch) zu Werbezwecken zu nutzen.**

### Sachverhalt:

Die Klägerin, die Verbraucherzentrale Nordrhein-Westfalen, nimmt die beklagte gesetzliche Krankenkasse auf Unterlassung in Anspruch, im Zusammenhang mit der Durchführung von Gewinnspielen für minderjährige Verbraucher die Daten der Teilnehmer zu Werbezwecken zu erheben.

Die Beklagte nahm im Juni 2011 an der Nordjob-Messe in Kiel teil, die sich vor allem an Schüler richtete und dazu diente, den Besuchern Ausbildungs- und Studienmöglichkeiten vorzustellen. Sie verteilte während der Messe Teilnahmekarten für ein Gewinnspiel.

Auf der Rückseite der mit „Gewinnkarte“ bezeichneten Teilnahmekarte sollten die Teilnehmer am Gewinnspiel in insgesamt neun Zeilen Angaben zum Namen, Vornamen, Geburtsdatum, zur Anschrift, zu Telefon-Nummern, zur E-Mail-Adresse und zur Krankenkasse machen. Darunter befand sich – etwas abgesetzt – folgender als „Datenschutzhinweis“ bezeichneter Hinweis:

„Die Angaben sind freiwillig. Die Daten werden nicht an Dritte weitergegeben.“

Direkt unter diesem Hinweis stand in räumlichem Zusammenhang mit dem fettgedruckten Wort „Einwilligungserklärung“ folgender Text:

„Ich bin damit einverstanden, dass die ... meine Daten (bzw. die Daten meiner Tochter/meines Sohnes) speichert und nutzt, um mich telefonisch, schriftlich, per E-Mail oder per SMS über die Vorteile einer ...-Mitgliedschaft und neue Angebote der ... zu informieren und zu beraten.“

Diese Einwilligung kann ich jederzeit mit Wirkung für die Zukunft bei der ... widerrufen. Meine Daten werden dann gelöscht.“

Unterhalb der für die Unterschrift vorgesehenen Zeile stand der kleingedruckte Hinweis:

„(Bei unter 15-Jährigen Unterschrift des Erziehungsberechtigten).“

Die Klägerin hat in der Erhebung der persönlichen Daten der Teilnehmer am Gewinnspiel einen Verstoß gegen § 4 Nr. 2 UWG gesehen. Sie hat die Beklagte mit Schreiben vom 12. September 2011 abgemahnt und zur Abgabe einer strafbewehrten Unterlassungserklärung aufgefordert. Die Beklagte hat sich daraufhin strafbewehrt verpflichtet, es zu unterlassen,

„eine an Minderjährige zwischen 15 und 18 Jahren gerichtete Werbung zur Teilnahme an einem Gewinnspiel einzusetzen, in der

die Gewinnspielteilnahme und die Einwilligungserklärung zum Erhalt von Informationen über die ... optisch derart verknüpft sind, dass die Unterscheidung zwischen beiden Angaben bzw. Erklärungen nicht hinreichend deutlich wird.“

Die Klägerin ist der Ansicht, die Unterlassungserklärung reiche nicht aus. Sie erfasse nicht die Fallkonstellation, dass die Beklagte die geschäftliche Unerfahrenheit der (minderjährigen) Verbraucher ausnutze.

Das Landgericht hat die Unterlassungsklage abgewiesen. Auf die Berufung der Klägerin hat das Berufungsgericht (OLG Hamm, WRP 2013, 375) die Beklagte unter Androhung von Ordnungsmitteln verurteilt,

„es zu unterlassen, im Rahmen geschäftlicher Handlungen im Zusammenhang mit Gewinnspielen, die die Beklagte für minderjährige Verbraucher veranstaltet, die Daten der Teilnehmer zu Werbezwecken zu erheben, wie aus der Gewinnkarte (Anlage K 1) ersichtlich geschehen“.

Mit ihrer vom Berufungsgericht zugelassenen Revision, deren Zurückweisung die Klägerin beantragt, erstrebt die Beklagte die Wiederherstellung des erstinstanzlichen Urteils.

### Aus den Gründen:

I. Das Berufungsgericht hat das auf die konkrete Verletzungsform beschränkte Unterlassungsbegehren der Klägerin gemäß § 8 Abs. 1 und 3 Nr. 3, § 3 Abs. 1, § 4 Nr. 2 UWG als begründet angesehen. Dazu hat es ausgeführt:

Die Beklagte habe mit der Aufforderung, an dem von ihr veranstalteten Gewinnspiel teilzunehmen, eine geschäftliche Handlung vorgenommen, weil es ihr um die Ermittlung von Kundendaten gegangen sei. Der Annahme eines wettbewerbswidrigen Verhaltens der Beklagten stehe nicht § 28 BDSG entgegen, da die Datenerhebung nicht für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sei. Die Beklagte nutze das Alter, die geschäftliche Unerfahrenheit und die Leichtgläubigkeit der 15 bis 17-jährigen Spielteilnehmer für ihre Zwecke aus. Es könne nicht davon ausgegangen werden, dass Minderjährige ab dem 15. Lebensjahr grundsätzlich bereits die nötige Reife hätten, die Tragweite einer Einwilligungserklärung zur Datenspeicherung und -verwendung für Werbezwecke zu erkennen.

II. Die gegen diese Beurteilung gerichteten Angriffe der Revision haben keinen Erfolg.

1. Gegenstand des Unterlassungsbegehrens der Klägerin ist nicht die Datenerhebung von Jugendlichen zwischen 15 und 17 Jahren als solche, sondern die konkrete Art und Weise, in der dies geschieht. Die Klägerin wendet sich dagegen, dass die Erhebung der Daten im Zusammenhang mit der Durchführung eines Gewinnspiels erfolgt.

2. Die Revision wendet sich ohne Erfolg gegen die Annahme des Berufungsgerichts, bei der von der Beklagten durchgeführten Erhebung von Daten der Teilnehmer an dem von ihr veranstalteten Gewinnspiel handele es sich um eine geschäftliche Handlung im Sinne von § 2 Abs. 1 Nr. 1 UWG.

a) Eine „geschäftliche Handlung“ ist nach § 2 Abs. 1 Nr. 1 UWG jedes Verhalten einer Person zugunsten des eigenen oder eines fremden Unternehmens vor, bei oder nach einem Geschäftsabschluss, das mit der Förderung des Absatzes oder des Bezugs von Waren oder Dienstleistungen oder mit dem Abschluss oder der Durchführung eines Vertrags über Waren und Dienstleistungen objektiv zusammenhängt. „Unternehmer“ im Sinne von § 2 Abs. 1 Nr. 6 UWG ist jede natürliche oder juristische Person, die geschäftliche Handlungen im Rahmen einer gewerblichen, handwerklichen oder beruflichen Tätigkeit vor-

nimmt. Die genannten Vorschriften dienen der Umsetzung von Art. 2 Buchst. b und d der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken. Sie sind daher im Lichte des Wortlauts und des Zwecks dieser Richtlinie auszulegen (vgl. EuGH, Urteil vom 5. Oktober 2004 – C-397/01 bis C-403/01, Slg. 2004, I-8835 = EuZW 2004, 691 Rn. 113 f. – Pfeiffer u.a./Deutsches Rotes Kreuz, Kreisverband Waldshut e.V.; BGH, Beschluss vom 18. Januar 2012 – I ZR 170/10, GRUR 2012, 288 Rn. 7 = WRP 2012, 309 – Betriebskrankenkasse, mwN).

b) Die Revision zieht zu Unrecht in Zweifel, dass es sich bei der von der Klägerin beanstandeten Erhebung von Daten seitens der Beklagten um eine geschäftliche Handlung eines Unternehmers im Sinne von § 2 Abs. 1 Nr. 1 und 6 UWG handelt. Entgegen der Ansicht der Revision steht eine Anwendung des § 2 Abs. 1 Nr. 1 und 6 UWG im Streitfall nicht in Widerspruch zu Art. 3 Abs. 1 in Verbindung mit Art. 2 Buchst. b und d der Richtlinie 2005/29/EG, auch wenn es sich bei der Beklagten um eine Körperschaft des öffentlichen Rechts handelt, die Aufgaben der gesetzlichen Krankenversicherung erfüllt.

Der Gerichtshof der Europäischen Union hat nach Erlass des Berufungsurteils entschieden, dass es für die Eröffnung des persönlichen Anwendungsbereichs der Richtlinie 2005/29/EG unerheblich ist, wie die Einordnung und die Rechtsstellung der fraglichen Einrichtung (hier: die Beklagte) nach nationalem Recht ausgestaltet ist. Die Richtlinie gilt nach ihrem Art. 3 Abs. 1 „für unlautere Geschäftspraktiken ... von Unternehmen gegenüber Verbrauchern vor, während und nach Abschluss eines ... Handelsgeschäfts“. Der in der Richtlinie ebenfalls verwendete Begriff „Gewerbetreibender“ stimmt in seiner Bedeutung und rechtlichen Tragweite mit dem Begriff „Unternehmen“ überein. Beide Begriffe umfassen daher gemäß Art. 2 Buchst. b der Richtlinie 2005/29/EG jede natürliche oder juristische Person, die eine entgeltliche Tätigkeit ausübt. Einrichtungen, die eine im Allgemeininteresse liegende Aufgabe erfüllen, werden davon ebenso wenig ausgenommen wie öffentlich-rechtliche Einrichtungen (EuGH, Urteil vom 3. Oktober 2013 – C-59/12, GRUR 2013, 1159 Rn. 26, 28, 32 = WRP 2013, 1454 – BKK MOBIL OIL). Auch der Zweck der Richtlinie 2005/29/EG, den Verbraucher umfassend vor unlauteren Geschäftspraktiken zu schützen, rechtfertigt es, die Beklagte als „Gewerbetreibende“ im Sinne der Richtlinie einzustufen. Nur eine solche Auslegung des Art. 3 Abs. 1 in Verbindung mit Art. 2 Buchst. b und d der Richtlinie 2005/29/EG ist geeignet, die volle Wirkung der Richtlinie zu gewährleisten, indem sie dafür sorgt, dass unlauteren Geschäftspraktiken – einschließlich der unlauteren Werbung von Gewerbetreibenden gegenüber Verbrauchern – im Einklang mit dem Erfordernis eines hohen Verbraucherschutzniveaus wirksam begegnet werden kann (EuGH, GRUR 2013, 1159 Rn. 33 f., 38 f. – BKK MOBIL OIL). Danach ist die Erhebung der personenbezogenen Daten von Teilnehmern an dem von der Beklagten veranstalteten Gewinnspiel auf der Messe in Kiel seitens der Beklagten als geschäftliche Handlung eines Unternehmers im Sinne von § 2 Abs. 1 Nr. 1 und 6 UWG einzustufen.

3. Ohne Erfolg wendet sich die Revision auch gegen die Annahme des Berufungsgerichts, die Wettbewerbswidrigkeit des beanstandeten Verhaltens der Beklagten sei nicht deshalb ausgeschlossen, weil die Datenerhebung gesetzlich zulässig sei.

a) Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben und Nutzen personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn dies für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Das Vorliegen dieser Voraussetzungen hat das

Berufungsgericht rechtsfehlerfrei verneint. Durch die Teilnahme an einem Gewinnspiel kann zwar ein rechtsgeschäftsähnliches Schuldverhältnis begründet werden (vgl. BGH, Urteil vom 25. Oktober 2012 – I ZR 169/10, GRUR 2013, 531 Rn. 20 = WRP 2013, 767 – Einwilligung in Werbeanrufe II). Im vorliegenden Fall geht die Erhebung der personenbezogenen Daten jedoch weit über den Umfang hinaus, der für die Durchführung des Gewinnspiels erforderlich ist. Zudem ist Gegenstand des Unterlassungsantrags allein die Erhebung der Daten zu Werbezwecken, also zu Zwecken, die jenseits der Teilnahme am Gewinnspiel selbst und seiner Abwicklung liegen. Das Erheben von Daten zu solchen „überschießenden“ Zwecken wird – worauf die Revisionserwiderung mit Recht hinweist – in § 28 Abs. 1 Satz 1 Nr. 1 BDSG nicht für zulässig erklärt.

b) Die Erhebung der personenbezogenen Daten ist im vorliegenden Fall auch nicht im Hinblick auf § 28 Abs. 3 BDSG zulässig. Nach dieser Vorschrift ist die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung zulässig, soweit der Betroffene eingewilligt hat. Gegenstand des vorliegenden Rechtsstreits ist indes nicht die Einwilligung des Betroffenen oder deren Wirksamkeit, sondern die Frage, ob die Beklagte bei der Erlangung von Einwilligungen die geschäftliche Unerfahrenheit von Jugendlichen ausgenutzt hat. Diese Fallgestaltung wird von § 28 Abs. 3 BDSG nicht erfasst. Auch die Vorschrift des § 4a Abs. 1 BDSG regelt allein die Frage der Wirksamkeit einer Einwilligung und nicht die Frage, ob die geschäftliche Unerfahrenheit des Einwilligenden ausgenutzt wird.

4. Ohne Erfolg bleiben schließlich auch die Angriffe der Revision gegen die Annahme des Berufungsgerichts, die Klägerin habe gegen die Beklagte gemäß § 8 Abs. 1 und 3 Nr. 3, §§ 3, 4 Nr. 2 UWG einen Anspruch auf Unterlassung, die Daten der 15 bis 17-jährigen Teilnehmer an dem in Rede stehenden Gewinnspiel zu erheben, wenn dies mittels der in Rede stehenden Gewinnkarte geschieht.

a) Nach § 4 Nr. 2 UWG sind Wettbewerbshandlungen unter anderem dann unlauter, wenn sie geeignet sind, die geschäftliche Unerfahrenheit von Kindern und Jugendlichen auszunutzen. Durch die Bestimmung sollen besonders schutzwürdige Verbraucher vor der Ausnutzung ihrer Unerfahrenheit bewahrt werden. Erfasst werden sollen auch Fälle im Vorfeld von konkreten Verkaufsförderungsmaßnahmen, beispielsweise, wenn Daten von Kindern oder Jugendlichen zu Werbezwecken erhoben werden (vgl. Begründung des Regierungsentwurfs 2004, BT-Drucks. 15/1487, S. 17). Die Vorschrift stellt eine Abweichung vom Leitbild des erwachsenen Durchschnittsverbrauchers dar, das der Gesetzgeber bei der UWG-Reform 2004 in Übereinstimmung mit der neueren Rechtsprechung zugrunde gelegt hat (vgl. Begründung des Regierungsentwurfs 2004 aaO S. 19). Damit verschiebt sich der an die Bewertung einer Wettbewerbshandlung anzulegende Maßstab zu Lasten des Unternehmers (BGH, Urteil vom 6. April 2006 – I ZR 125/03, GRUR 2006, 776 Rn. 19 = WRP 2006, 885 – Werbung für Klingeltöne, mwN). Maßgebend ist jeweils der Durchschnitt des von einer Werbemaßnahme angesprochenen Verkehrskreises. Wendet sich der Werbende gezielt an eine bestimmte Bevölkerungsgruppe wie beispielsweise Kinder und Jugendliche, so muss er sich nach § 3 Abs. 2 Satz 2 UWG an einem durchschnittlich informierten, aufmerksamen und verständigen Angehörigen dieser Gruppe orientieren (vgl. Erwägungsgrund 18 der Richtlinie 2005/29/EG; BGH, Urteil vom 2. Oktober 2003 – I ZR 150/01, BGHZ 156, 250, 252 – Marktführerschaft; BGH, GRUR 2006, 776 Rn. 19 – Werbung für Klingeltöne; Urteil vom 17. Juli 2008 – I ZR 160/05, GRUR 2009, 71 Rn. 17 = WRP 2009, 45 – Sammelaktion für Schoko-Riegel). Dementsprechend können Handlungen, die gegenüber einer

nicht besonders schutzwürdigen Zielgruppe noch zulässig sind, gegenüber geschäftlich Unerfahrenen unzulässig sein.

b) Voraussetzung für die Annahme einer Unlauterkeit im Sinne von § 4 Nr. 2 UWG ist es, dass sich die Werbung – zumindest auch – gezielt an Kinder oder Jugendliche wendet, weil sich die Vorschrift gegen ein Ausnutzen der Unerfahrenheit dieser Zielgruppe richtet. Das Erfordernis der Zielgerichtetheit trägt dem Umstand Rechnung, dass bei der Beurteilung von Wettbewerbshandlungen grundsätzlich auf den Durchschnittsverbraucher des angesprochenen Verkehrskreises abzustellen ist. In vielen Fällen wird Werbung sowohl von Erwachsenen als auch von Minderjährigen wahrgenommen. Solche Werbung ist nicht stets auch am Maßstab des § 4 Nr. 2 UWG zu messen (vgl. BGH, GRUR 2006, 776 Rn. 20 – Werbung für Klingeltöne).

Nach den unangegriffen gebliebenen Feststellungen des Berufungsgerichts wurde die Teilnahmekarte für das von der Beklagten veranstaltete Gewinnspiel während der Nordjob-Messe verteilt. Diese Messe diente der Vorstellung von Ausbildungs- und Studienmöglichkeiten und richtete sich deshalb vornehmlich an Schülerinnen und Schüler, die vor einer Berufswahl standen, und damit hauptsächlich an Jugendliche. Ausgeschlossen waren allerdings diejenigen Jugendlichen, die das 15. Lebensjahr noch nicht vollendet hatten, weil diese für die Einwilligung in die Datenerhebung die Unterschrift der Erziehungsberechtigten benötigten.

c) Allerdings ist nicht jede gezielte Beeinflussung von Minderjährigen nach § 4 Nr. 2 UWG unlauter. Die konkrete Handlung muss vielmehr geeignet sein, die Unerfahrenheit auszunutzen (vgl. BGH, Urteil vom 22. September 2005 – I ZR 28/03, GRUR 2006, 161 Rn. 21 = WRP 2006, 69 – Zeitschrift mit Sonnenbrille; BGH, GRUR 2006, 776 Rn. 22 – Werbung für Klingeltöne). Maßgeblich ist, ob sich der Umstand, dass Minderjährige typischerweise noch nicht in ausreichendem Maße in der Lage sind, Waren oder Dienstleistungsangebote kritisch zu beurteilen, auf die Entscheidung für ein unterbreitetes Angebot auswirken kann (BGH, GRUR 2006, 776 Rn. 22 – Werbung für Klingeltöne).

aa) Hiervon ausgehend hat das Berufungsgericht mit Recht angenommen, dass die Datenerhebung in der konkret durchgeführten Art und Weise geeignet ist, die geschäftliche Unerfahrenheit von Jugendlichen auszunutzen. Es hat rechtsfehlerfrei festgestellt, dass Jugendliche im Alter zwischen 15 und 17 Jahren noch nicht die nötige Reife besitzen, die Tragweite einer Einwilligungserklärung zur Datenspeicherung und Datenverwendung zu Werbezwecken abzusehen.

Entgegen der Ansicht der Revision stellt es keinen Rechtsfehler dar, dass das Berufungsgericht nicht im Einzelnen dargelegt hat, aus welchen Gründen es sich zur Beurteilung in der Lage gesehen hat, ob Jugendliche im Alter zwischen 15 und 17 Jahren die Tragweite der von ihnen abgegebenen Einwilligungserklärung hinsichtlich der Erhebung und Nutzung der personenbezogenen Daten in ausreichendem Maße erkennen können.

Die Feststellung der Wirkung einer Werbung auf die angesprochenen Verkehrskreise stützt sich auf die Anwendung von Erfahrungswissen, das gegebenenfalls mit Hilfe eines Sachverständigen zu ermitteln ist. Ermittelt der Tatrichter das Verständnis der angesprochenen Verkehrskreise ohne sachverständige Hilfe, so geht er davon aus, aufgrund eigenen Erfahrungswissens selbst über die erforderliche Sachkunde zu verfügen (vgl. BGHZ 156, 250, 254 – Marktführerschaft).

Das Berufungsgericht hat nicht im Einzelnen dargelegt, dass es über eine entsprechende Sachkunde verfügt. Das war im vorliegenden Fall allerdings ausnahmsweise auch nicht erforderlich. Die Wirkung der Werbung auf die angesprochenen Jugend-

lichen konnten die ständig mit Wettbewerbsachen befassten Mitglieder des Berufungssenats aufgrund ihrer Fachkenntnisse selbst beurteilen (vgl. BGH, Urteil vom 12. Juli 2001 – I ZR 261/98, GRUR 2002, 77, 80 = WRP 2002, 85 – Rechenzentrum; Seichter in Ullmann, jurisPK/UWG, 3. Aufl., § 4 Nr. 2 Rn. 71).

bb) Ohne Erfolg bleibt auch die Rüge der Revision, das Berufungsgericht habe bei der tatrichterlichen Feststellung der geschäftlichen Unerfahrenheit der angesprochenen Jugendlichen gesetzliche Vorschriften zur Geschäftsfähigkeit Minderjähriger und darin zum Ausdruck kommende gesetzgeberische Wertungen nicht hinreichend berücksichtigt.

(1) Das Berufungsgericht ist zutreffend davon ausgegangen, dass nach der Wertung der §§ 112, 113 BGB Minderjährige für bestimmte Geschäfte in bestimmten Situationen als uneingeschränkt geschäftsfähig angesehen werden können. Ebenso hat das Berufungsgericht die Vorschrift des § 175 Abs. 1 Satz 3 SGB V berücksichtigt, die vorsieht, dass Minderjährige nach Vollendung des 15. Lebensjahrs ihre Krankenkasse selbst wählen dürfen.

(2) Die Revision rügt, das Berufungsgericht habe übersehen, dass sowohl der selbständige Betrieb eines Erwerbsgeschäfts nach § 112 BGB als auch das Eingehen eines Dienst- oder Arbeitsverhältnisses gemäß § 113 BGB rechtlich und auch tatsächlich sehr weitreichende Konsequenzen hätten, die mit denjenigen der Angabe von Daten im Rahmen eines Gewinnspiels nicht vergleichbar seien. Anders als in den vom Gesetzgeber geregelten Fällen erscheine eine Genehmigung der gesetzlichen Vertreter und gar des Vormundschaftsgerichts bei der Datenerhebung nicht zwingend erforderlich, um den Minderjährigen vor den rechtlichen Folgen seines Handelns zu schützen. Zudem habe das Berufungsgericht außer Acht gelassen, dass die Entscheidung zur Angabe von Daten zum Zweck der Zusendung von Werbung für die Dienstleistungen einer gesetzlichen Krankenkasse nicht über die Tragweite der Wahl einer Krankenkasse hinausgehe und daher grundsätzlich nicht zu beanstanden sei.

Dieses Vorbringen verhilft der Revision nicht zum Erfolg. Die Frage, ob Jugendliche in die Nutzung ihrer Daten wirksam einwilligen können, ist nicht Gegenstand des Rechtsstreits. Die Klägerin beanstandet vielmehr, dass die Datenerhebung im Zusammenhang mit der Durchführung eines Gewinnspiels erfolgt und dadurch die Tragweite einer Preisgabe personenbezogener Daten für einen Jugendlichen zwischen 15 und 17 Jahre nicht hinreichend deutlich wird. Ebenso wenig kommt es darauf an, ob eine Werbung, die sich an die angesprochene Zielgruppe richtet, grundsätzlich zulässig ist. Entscheidend ist vielmehr, ob die Verbindung der Erteilung der Einwilligungserklärung mit der Teilnahme an einem Gewinnspiel die geschäftliche Unerfahrenheit der Minderjährigen im Alter zwischen 15 und 17 Jahren unlauter ausnutzt. Die Revisionserwiderung weist mit Recht darauf hin, dass sich ein Schluss, alle Jugendlichen ab dem Alter von 15 Jahren könnten generell absehen, welche Auswirkungen eine zu Werbezwecken erfolgende Datenerhebung habe, wenn sie im Zusammenhang mit der Auswahl einer Krankenkasse stehe, aus den Wertungen der §§ 112, 113 BGB und § 175 Abs. 1 Satz 3 SGB V nicht herleiten lässt.

cc) Das Berufungsgericht hat bei seiner Beurteilung auch nicht gegen Denkgesetze oder Erfahrungssätze verstoßen.

Das Berufungsgericht hat mit Recht angenommen, dass ein Minderjähriger im Alter zwischen 15 und 17 Jahren den Reizen eines Gewinnspiels eher erliegen wird als ein Erwachsener (vgl. Köhler in Köhler/Bornkamm, UWG, 32. Aufl., § 4 Rn. 2.34; Sosnitzer in Piper/Ohly/Sosnitzer, UWG, 6. Aufl., § 4.2 Rn. 2/10; Späth in Götting/Nordemann, UWG, 2. Aufl., § 4 Rn. 2.42, 2.44; Seichter in jurisPK-UWG aaO § 4 Nr. 2 Rn. 63) und die Folgen der Ein-

willigung in die Datenerhebung mit der Möglichkeit, ständig über mehrere Kommunikationswege erreichbar zu sein, dabei vernachlässigt (vgl. Köhler in Köhler/Bornkamm aaO § 4 Rn. 2.41; Fezer/Scherer, UWG, 2. Aufl., § 4-2 Rn. 200; Böhler, WRP 2011, 1028, 1031). Auch für Jugendliche in der hier in Rede stehenden Altersgruppe sind die mit der Preisgabe der persönlichen Daten und der Einwilligungserklärung verbundenen Nachteile nur schwer erkennbar. Das Gleiche gilt für die wirtschaftlichen Vorteile, die sich das werbende Unternehmen aus der Datenerhebung verspricht (vgl. Seichter in Ullmann, jurisPK-UWG aaO § 4 Nr. 2 Rn. 68; Böhler, WRP 2011, 1028, 1031). Mit ihrer gegenteiligen Ansicht ersetzt die Revision lediglich in unzulässiger Weise die tatrichterliche Beurteilung, ohne dabei einen erheblichen Rechtsfehler des Berufungsgerichts aufzuzeigen.

Mit Recht hat das Berufungsgericht auch angenommen, dass die Teilnahme an dem Gewinnspiel der Beklagten auf eine kurzfristige Entscheidung angelegt ist, während der Entscheidung über die Wahl der Krankenkasse häufig ein langfristig angelegter Entscheidungsprozess zugrunde liegt. Dies ergibt sich schon daraus, dass auch ein Jugendlicher die weitreichenden Folgen der Wahl einer Krankenkasse berücksichtigen wird, weil er sich – für ihn leicht erkennbar – im Allgemeinen langfristig bindet. Demgegenüber stellt die Teilnahme an einem Gewinnspiel eine spontane Entscheidung dar, deren Folgen im Zusammenhang mit der Datenerhebung ein Jugendlicher erfahrungsgemäß vernachlässigen wird.

Unter den gegebenen Umständen steht der Beurteilung des Berufungsgerichts auch nicht entgegen, dass Jugendliche durch eine verbreitete Nutzung des Internets über Computer und Handys den Umgang mit Medien und Werbung gewohnt sind und hierbei regelmäßig mit der Möglichkeit und Notwendigkeit der Eingabe personenbezogener Daten konfrontiert werden. Aus zunehmenden Erfahrungen mit solchen Medien lassen sich nicht ohne weiteres Rückschlüsse auf die Erkennbarkeit der Folgen einer Preisgabe von personenbezogenen Daten ziehen.

## Frage nach der Gewerkschaftszugehörigkeit

(Bundesarbeitsgericht, Urteil vom 18. November 2014 – 1 AZR 257/13 –)

- 1. Art. 9 Abs. 3 GG schützt eine Gewerkschaft auch darin, der Arbeitgeberseite in einer konkreten Tarifvertragsverhandlungssituation Angaben über ihren Organisationsgrad und die Verteilung ihrer Mitglieder in bestimmten Betrieben vorzuenthalten.**
- 2. Verlangt ein Arbeitgeber während laufender Tarifvertragsverhandlungen von seinen Arbeitnehmern die Offenlegung ihrer Gewerkschaftszugehörigkeit, handelt es sich um eine gegen die gewerkschaftliche Koalitionsbetätigungsfreiheit gerichtete Maßnahme.**

### Sachverhalt:

Die Parteien streiten über die Befugnis der Arbeitgeberin, betriebszugehörige Arbeitnehmer nach ihrer Mitgliedschaft in einer bestimmten Gewerkschaft zu befragen.

Die Klägerin – die Gewerkschaft Deutscher Lokomotivführer (GDL) – organisiert ua. das Fahrpersonal von Nahverkehrsunterneh-

men im Freistaat Bayern und ist Mitglied der dbb tarifunion. Die Beklagte ist als kommunales Dienstleistungsunternehmen mit Sitz in M ua. im Personennahverkehr tätig und gehört dem Kommunalen Arbeitgeberverband Bayern e.V. (KAV Bayern) an. Dieser schloss am 18. August 2006 mit der dbb tarifunion sowie mit der Vereinten Dienstleistungsgewerkschaft (ver.di) – Landesbezirk Bayern – jeweils einen gleichlautenden, am 1. Januar 2007 in Kraft getretenen „Tarifvertrag Nahverkehrsbetriebe Bayern (TV-N Bayern)“. Seitdem enthalten die Arbeitsverträge der bei der Beklagten beschäftigten Arbeitnehmer eine Bezugnahme auf den TV-N Bayern. Zuvor geschlossene „Alt“arbeitsverträge verweisen – in unterschiedlichen Formulierungen – auf die Bestimmungen des „Bundesmanteltarifvertrags für Arbeiter gemeindlicher Verwaltungen und Betriebe“.

Nach Kündigungen des jeweils mit ihnen geschlossenen TV-N Bayern (in den Fassungen des 2. Änderungstarifvertrags) zum 30. Juni 2010 verhandelten ver.di und dbb tarifunion zunächst gemeinsam mit dem KAV Bayern über einen neuen Tarifabschluss. Am 20. August 2010 erzielten ver.di und der KAV Bayern eine Einigung. Die dbb tarifunion erklärte in einem an den KAV Bayern gerichteten Schreiben vom 25. August 2010 „die Verhandlungen ... formal für gescheitert“ und teilte mit, dass „der Vorstand ... die Durchführung der Urabstimmung beschlossen“ habe. Mit Schreiben vom selben Tag wandte sich die Beklagte an „die Tarifbeschäftigten des Unternehmensbereichs Verkehr“. Das Schreiben und ein ihm beigelegtes Antwortformular lauten:

„...“

es hat nach Kündigung des Tarifvertrag Nahverkehrsbetriebe Bayern (TV-N Bayern) durch die Gewerkschaft ver.di und GDL/dbb Tarifunion mehrere Verhandlungsrunden, zuletzt am 20. August 2010, in Nürnberg gegeben.

Mit der Gewerkschaft ver.di wurde am 20. August 2010 eine Tarifeinigung erzielt.

Diese Einigung sieht unter anderem bereits zum 1. September eine Erhöhung des Tabellenentgeltes um 1,6% sowie eine Einmalzahlung von 240 EUR vor.

Ebenfalls wurde mit ver.di vereinbart, dass die Schicht- und Wechselschichtzulagen ab dem 1. September 2010 um 1,6 % erhöht werden und es zu zusätzlichen strukturellen Verbesserungen beim Zusatzurlaub für Nachtarbeit kommt.

Im Gegensatz dazu, hat die GDL / dbb tarifunion die Verhandlungen für gescheitert erklärt.

Ansprüche aus der Einigung mit der Gewerkschaft ver.di können GDL-Mitglieder daher nicht geltend machen.

Für die Mitglieder der GDL gibt es keine entsprechende Einigung über eine prozentuale Erhöhung des Tabellenentgeltes, der Erhöhung der Schicht- und Wechselschichtzulagen, der strukturellen Verbesserungen beim Zusatzurlaub für Nachtarbeit sowie über eine Einmalzahlung zum 01. September 2010.

Damit die S M GmbH ihrer arbeitsvertraglichen Verpflichtungen auf die Umsetzung des mit ver.di abgeschlossenen Tarifvertrages nachkommen kann und – wie auch in der Vergangenheit – die nichtorganisierten Mitarbeiterinnen und Mitarbeiter ebenfalls an der Umsetzung teilhaben, sind wir auf Ihre Mitwirkung angewiesen.

Dies ist in Ihrem eigenen Interesse, da wir ohne Beantwortung und Rückmeldung der als Anlage beigeführten Frage davon ausgehen müssen, dass Sie keinen Anspruch auf die Umsetzung des Tarifeinigungsabkommens aus der Einigung vom 20.08.2010 haben.

Ihre Antwort wird ausschließlich für die Prüfung eines Anspruches auf die Tarifeinigung mit der Gewerkschaft ver.di verwendet.

Bitte senden oder faxen Sie uns Ihre Antwort unterschrieben bis spätestens 10. September 2010 in beigelegtem Rückantwortkuvert an Herrn D, P-SC-S1. Sollten Sie an der zeitgerechten Rückmeldung gehindert sein, holen Sie diese schnellstmöglich nach. Solange keine Rückmeldung erfolgt, kann die Tarifeinigung für Sie in der Entgeltabrechnung nicht umgesetzt werden.

...

Rückantwort

Name: ...

Vorname: ...

Personalnummer: ...

Hiermit erkläre ich, dass ich Mitglied der Gewerkschaft Deutscher Lokomotivführer GDL bin (bitte ankreuzen).

ja

nein

M, den .....

Unterschrift“

Durch die Befragungsaktion vom 25. August 2010 sieht sich die Klägerin in ihren Rechten aus Art. 9 Abs. 3 GG beeinträchtigt. Mit ihrer am 22. September 2010 beim Arbeitsgericht eingegangenen Klage – und späteren Klageerweiterungen um Hilfsanträge – hat sie die Beklagte auf Unterlassung in Anspruch genommen.

Die Klägerin hat zuletzt beantragt, die Beklagte zu verurteilen, es zu unterlassen, die in ihrem Unternehmen beschäftigten Arbeitnehmer schriftlich aufzufordern, schriftlich zu erklären, ob sie Mitglied der Gewerkschaft Deutscher Lokomotivführer GDL sind oder nicht;

### Aus den Gründen:

II. Das hauptsächliche Unterlassungsbegehren ist in der Fassung, das es jedenfalls im zweiten Rechtszug erfahren hat, zulässig, aber unbegründet.

1. Der Antrag ist zulässig.

a) Die Klägerin verlangt die Unterlassung jeglicher schriftlicher Aufforderungen der Beklagten an die in ihrem Unternehmen beschäftigten Arbeitnehmer zu einer schriftlichen Erklärung, ob sie bei der Klägerin organisiert sind oder nicht. Dieses Begehren ist dahin zu verstehen, dass die Unterlassungspflicht der Beklagten unabhängig von der Zielrichtung und den konkreten Einzelfallumständen einer schriftlichen Aufforderung zu der beschriebenen Erklärung bestehen soll.

b) In diesem Verständnis begegnen dem in erster Linie verfolgten Antrag keine Zulässigkeitsbedenken; insbesondere ist er hinreichend bestimmt iSv. § 253 Abs. 2 Nr. 2 ZPO. Er lässt mit der erforderlichen Deutlichkeit erkennen, welche Handlung der Beklagten untersagt werden soll. Dass es sich um einen Globalantrag handelt, der eine unbestimmte Vielzahl möglicher zukünftiger Fallgestaltungen erfasst, steht seiner Bestimmtheit nicht entgegen. Er ist ausnahmslos auf alle denkbaren Fälle gerichtet. Ob das verfolgte Unterlassungsbegehren für sämtliche Fälle berechtigt ist, betrifft die Begründetheit und nicht die Zulässigkeit des Antrags (BAG 24. April 2007 – 1 AZR 252/06 – Rn. 25, BAGE 122, 134).

2. Der Antrag ist unbegründet. Die Klägerin hat gegen die Beklagte keinen Anspruch auf Unterlassung jeglicher schriftlicher Aufforderungen an die in deren Unternehmen beschäftigten Arbeitnehmer zu einer schriftlichen Erklärung, ob sie Mitglied der GDL sind oder nicht. Ein solcher Anspruch folgt nicht aus § 1004 Abs. 1, § 823 Abs. 1 BGB iVm. Art. 9 Abs. 3 GG. Zwar verletzt das Schreiben der Beklagten vom 25. August 2010 die Klägerin in ihrer von Art. 9 Abs. 3 GG geschützten kollektiven Koalitionsfreiheit. Die beanspruchte Unterlassung umfasst aber auch Fallgestaltungen, bei denen es schon an einer Wiederholungs- oder Erstbegehungsgefahr fehlt, die eine – von der Klägerin darzulegende – Anspruchsvoraussetzung ist.

a) Nach § 1004 Abs. 1 BGB kann der Eigentümer vom Störer die Beseitigung und weitere Unterlassung der Beeinträchtigung verlangen, wenn das Eigentum in anderer Weise als durch Entzie-

hung oder Vorenthaltung des Besitzes beeinträchtigt wird. Diese Ansprüche sind nicht auf Eigentumsverletzungen beschränkt, sondern bestehen darüber hinaus zur Abwehr von Eingriffen in alle nach § 823 Abs. 1 BGB geschützten Rechte, Lebensgüter und Interessen (BAG 17. Mai 2011 – 1 AZR 473/09 – Rn. 39, BAGE 138, 68). Hierzu gehört auch die durch Art. 9 Abs. 3 GG gewährleistete kollektive Koalitionsfreiheit. Gegen rechtswidrige Eingriffe in diese Freiheit kann sich eine Koalition mit auf § 1004 Abs. 1 Satz 2, § 823 Abs. 1 BGB iVm. Art. 9 Abs. 3 GG gestützten Unterlassungsklagen wehren (zum Unterlassungsanspruch einer Gewerkschaft vgl. BAG 17. Mai 2011 – 1 AZR 473/09 – Rn. 39, aaO; 20. April 1999 – 1 ABR 72/98 – zu B II 2 a der Gründe, BAGE 91, 210; zum Unterlassungsanspruch eines Arbeitgeberverbandes vgl. BAG 24. April 2007 – 1 AZR 252/06 – Rn. 54, BAGE 122, 134).

b) Für die mit dem Hauptantrag erstrebte Unterlassung liegen die Voraussetzungen eines solchen Anspruchs aber nicht vor.

aa) Allerdings hat die Beklagte mit ihrer Frageaktion die kollektive Koalitionsfreiheit der Klägerin aus Art. 9 Abs. 3 GG verletzt.

(1) Die Befragung von Arbeitnehmern nach Maßgabe des Schreibens vom 25. August 2010 beeinträchtigt die kollektive Koalitionsbetätigungsfreiheit der Klägerin.

(a) Der sich auf alle koalitionsspezifischen Betätigungsweisen erstreckende Schutz des Art. 9 Abs. 3 GG umfasst insbesondere die Tarifautonomie, die im Zentrum der den Koalitionen eingeräumten Möglichkeiten zur Verfolgung ihrer Zwecke steht (BVerfG 10. September 2004 – 1 BvR 1191/03 – zu B II 1 der Gründe mwN; BAG 22. September 2009 – 1 AZR 972/08 – Rn. 33, BAGE 132, 140). Ihre Aufgabe ist es, den von der staatlichen Rechtssetzung frei gelassenen Raum des Arbeitslebens durch Tarifverträge sinnvoll zu ordnen, insbesondere die Höhe der Arbeitsvergütung für die verschiedenen Berufstätigkeiten festzulegen, und so letztlich die Gemeinschaft sozial zu befrieden (BVerfG 6. Mai 1964 – 1 BvR 79/62 – BVerfGE 18, 18). Dazu versuchen die Koalitionen auf Arbeitgeber- und Arbeitnehmerseite in gemeinsamen Verhandlungen zu einem Interessenausgleich zu gelangen und die jeweils andere Seite zur Übernahme der selbst für richtig befundenen Position ganz oder in Teilen zu bewegen (BAG 13. Juli 1993 – 1 AZR 676/92 – zu III 1 b der Gründe, BAGE 73, 320). Die Verhandlungsstärke einer Arbeitnehmerkoalition hängt von der Zahl ihrer Mitglieder ab (BVerfG 14. November 1995 – 1 BvR 601/92 – BVerfGE 93, 352). Diese sichern nicht nur deren finanziellen Bestand, sondern sind auch Garanten ihrer Durchsetzungsfähigkeit in den Vertragsverhandlungen mit dem sozialen Gegenspieler. Der Organisationsgrad einer Gewerkschaft wie die Verteilung ihrer Mitglieder in den Betrieben des jeweiligen Tarifgebiets sind bestimmend für die Wahl der Mittel, die eine Arbeitnehmerkoalition einsetzen kann, um in Tarifverhandlungen mit der Arbeitgeberseite zum Abschluss zu gelangen. Ein solches Mittel ist auch der Arbeitskampf. Welches Arbeitskämpfungsmittel die Arbeitnehmerorganisation in welchem Umfang einsetzt und welches Kampfgebiet sie hierfür wählt, geben vor allem der Organisationsgrad und die betriebliche Zuordnung ihrer Mitglieder vor. Sind der Arbeitgeberseite diese Daten bekannt, kann sie sowohl ihre Verhandlungsposition als auch im Falle eines Arbeitskampfes ihre Arbeitskämpfungsmittel hierauf einstellen. Die Ungewissheit des sozialen Gegenspielers über die tatsächliche Durchsetzungskraft der Arbeitnehmerkoalition in einer konkreten Verhandlungssituation ist demnach grundlegend dafür, dessen Verhandlungsbereitschaft zu fördern und zu einem angemessenen Interessenausgleich zu gelangen. Im Hinblick darauf schützt Art. 9 Abs. 3 GG eine Gewerkschaft auch darin, diese Angaben der Arbeitge-

berseite in einer konkreten Verhandlungssituation vorzuenthalten, um sich nicht selbst zu schwächen.

(b) Die Befragungsaktion der Beklagten ist eine gegen die koalitionsspezifische Betätigungsfreiheit der Klägerin gerichtete Maßnahme. Die von ihren Arbeitnehmern geforderten Auskünfte verschaffen der Beklagten Kenntnis vom Umfang des Mitgliederbestandes der GDL in ihrem „Unternehmensbereich Verkehr“ sowie dessen konkreter innerbetrieblicher Verteilung. Bei wahrheitsgemäßer Beantwortung erlangte die Beklagte anhand des geforderten Namens sowie der Personalnummer Informationen über den Organisationsgrad der GDL und zum konkreten Einsatzort des einzelnen GDL-Mitglieds. Diese Informationen des gewerkschaftlichen Binnenbereichs erlauben es ihr, die Verhandlungsstärke der Gewerkschaftsseite in einer laufenden Tarifaueinandersetzung konkret einzuschätzen und damit die Verhandlungsmöglichkeiten der Arbeitgeberseite hierauf einzustellen. Darüber hinaus ist die mit der Befragungsaktion verbundene Zusage, allen Arbeitnehmern, die nicht Mitglied der GDL sind, ungeachtet einer Gewerkschaftszugehörigkeit den mit ver.di erzielten Tarifabschluss zukommen zu lassen, geeignet, durch finanzielle Anreize Nichtorganisierte von einem Beitritt zur GDL abzuhalten und damit Einfluss auf deren Mitgliederbestand zu nehmen. Diesen Druck verstärkt die weitere Ankündigung der Beklagten, bei Ausbleiben einer Antwort die Tarifeinigung in der Entgeltabrechnung nicht umzusetzen.

2) Die von der Beklagten vorgebrachten Gründe für die Befragungsaktion vermögen die Beeinträchtigung der kollektiven Koalitionsbetätigungsfreiheit der Klägerin nicht zu rechtfertigen.

(a) Untauglich ist schon die als Begründung für die Aufforderung vom 25. August 2010 angegebene Tarifeinigung zwischen ver.di und dem KAV Bayern. In ihrem Schreiben geht die Beklagte von „ihrer arbeitsvertraglichen Verpflichtung“ zur „Umsetzung des mit ver.di abgeschlossenen Tarifvertrages“ aus. Hierfür ist die Kenntnis von einer Mitgliedschaft zur GDL aber unmaßgeblich. Nach ihrem eigenen Vorbringen verwendet die Beklagte in ihren Formulararbeitsverträgen Bezugnahmeklauseln, die nicht nach einer Gewerkschaftszugehörigkeit differenzieren. Soweit diese Tarifabschlüsse mit ver.di erfassen, ist die Beklagte vertraglich allen Arbeitnehmern zur Anwendung dieser Tarifverträge verpflichtet, deren Verträge eine entsprechende Bezugnahme enthalten. Ansonsten begründen diese Tarifabschlüsse nur eine normative Verpflichtung gegenüber den Mitgliedern von ver.di (§ 3 Abs. 1, § 4 Abs. 1 Satz 1 TVG). Hierzu muss die Beklagte einzig die Tarifgebundenheit dieser Arbeitnehmer und nicht die von Anders- oder Nichtorganisierten kennen.

(b) Gleiches gilt für ihre Annahme, sie habe die Zugehörigkeit einzelner Arbeitnehmer zur GDL kennen müssen, um einem zu erwartenden Streikdruck der GDL mit einer selektiven Aussperrung von deren Mitgliedern begegnen zu können. Unabhängig davon, dass die Beklagte in dem Schreiben vom 25. August 2010 ausdrücklich angegeben hat, die Antwort der Arbeitnehmer werde „ausschließlich für die Prüfung eines Anspruchs auf die Tarifeinigung mit der Gewerkschaft ver.di verwendet“, verletzt eine selektive Aussperrung, die gezielt nur die Mitglieder der streikenden Gewerkschaft erfasst, also schon Nichtorganisierte hiervon ausnimmt, ihrerseits die positive Koalitionsbetätigungsfreiheit der kampf führenden Gewerkschaft (st. Rspr. BAG 10. Juni 1980 – 1 AZR 331/79 – BAGE 33, 195). Darüber hinaus wäre die Beklagte schon aus allgemeinen arbeitskampfrechtlichen Grundsätzen zu einer Abwehraussperrung nicht befugt gewesen. Sie befand sich in einer Auseinandersetzung um einen Verbandstarifvertrag. In einem solchen Fall liegt die Entscheidung über Kampfmaßnahmen der Arbeitgeberseite allein in der

Verantwortung des kampf führenden Arbeitgeberverbandes und nicht in der eines einzelnen Mitglieds (vgl. BAG 31. Oktober 1995 – 1 AZR 217/95 – zu I 1 der Gründe, BAGE 81, 213).

bb) Gleichwohl hat der nicht auf die Befragungsaktion vom 25. August 2010 beschränkte Unterlassungsantrag keinen Erfolg. Das zur Entscheidung gestellte Globalbegehren umfasst auch Fallgestaltungen, in denen sich der Unterlassungsanspruch bereits aus deliktsrechtlichen Gründen als unbegründet erweist.

(1) Das in die Revisionsinstanz gelangte Begehren ist nicht nur – im Sinn einer abstrakten Beschreibung der mit dem Beklagtenschreiben vom 25. August 2010 erfolgten Verletzungshandlung – auf die Untersagung von Befragungen der Arbeitnehmer im Unternehmen der Beklagten nach ihrer Zugehörigkeit zu der Klägerin im Zusammenhang mit Tarifvertragsverhandlungen oder bevorstehenden Arbeitskämpfmaßnahmen gerichtet. Es erfasst vielmehr jegliche schriftliche Aufforderungen der Beklagten an die im Unternehmen beschäftigten Arbeitnehmer, schriftlich zu erklären, ob sie Mitglied der Klägerin sind oder nicht.

(2) Ob in solch einer Aufforderung generell und ausnahmslos eine rechtswidrige Beeinträchtigung der kollektiven Koalitionsfreiheit der Klägerin liegt – oder ob und unter welchen Umständen der Arbeitgeber in einem tarifpluralen Betrieb nach der Gewerkschaftszugehörigkeit der Arbeitnehmer fragen darf –, muss nicht entschieden werden. Es fehlt bei den nicht vom Anlassfall umfassten Fallgestaltungen an der für einen Anspruch aus § 1004 Abs. 1, § 823 Abs. 1 BGB iVm. Art. 9 Abs. 3 GG notwendigen Begehungsgefahr. Die Besorgnis weiterer Beeinträchtigungen (vgl. § 1004 Abs. 1 Satz 2 BGB) ist Tatbestandsmerkmal des Unterlassungsanspruchs und damit materielle Anspruchsvoraussetzung (vgl. BAG 20. November 2012 – 1 AZR 179/11 – Rn. 82, BAGE 143, 354).

## Bewerberdaten für den örtlichen Betriebsrat bei zentralem Online-Recruitment-Center

(**Bundesarbeitsgericht**, Beschluss vom 21. Oktober 2014 – 1 ABR 10/13 –)

- 1. Schreibt der Arbeitgeber offene Stellen zentral über ein Recruitment-Center aus, ist dieses nicht befugt, ihm ungeeignet erscheinende Bewerbungen auszusortieren und dem für die Einstellung zuständigen jeweiligen Store-Leiter und damit auch dem an der Einstellung zu beteiligenden Betriebsrat vorzuenthalten.**
- 2. Der Arbeitgeber ist nach § 99 Abs. 1 S. 1 BetrVG verpflichtet, dem Betriebsrat vor der Einstellung eines Arbeitnehmers alle erforderlichen Unterlagen vorzulegen, die von Personen eingereicht werden, die sich im Onlineportal auf die zu besetzende Stelle beworben haben.**

*(Nicht amtliche Leitsätze)*

### Sachverhalt:

A. Die Beteiligten streiten über die Reichweite der Unterrichts- und Vorlagepflichten der Arbeitgeberin bei Einstellungen.

Die zu 2. beteiligte Arbeitgeberin ist ein Textilhandelsunternehmen mit bundesweit 390 Filialen. Ihr Verkaufsgebiet ist in 15 Areas

eingeteilt, für die jeweils ein Büro mit einem Recruitment-Center zuständig ist. Die Filiale Nr. 698 in Flensburg, in der 40 Arbeitnehmer beschäftigt sind und der antragstellende Betriebsrat gebildet ist, gehört mit weiteren 28 Filialen zur Area 1. Sie wird – wie andere Filialen auch – von einem Store-Manager geleitet. Dieser trifft in personellen und sozialen Angelegenheiten die Entscheidungen.

Seit Mai 2009 nimmt die Arbeitgeberin ausschließlich Online-Bewerbungen entgegen. Dazu teilen die Store-Manager die zu besetzenden Stellen einschließlich Anforderungsprofil dem für sie zuständigen Recruitment-Center mit. Von diesem werden die Positionen mit ihren Bedingungen in ein Onlineportal eingegeben und die eingehenden Bewerbungen gesichtet sowie daraufhin geprüft, ob ein Bewerber die geforderte Qualifikation aufweist. Anhand der ihm vom Recruitment-Center zugeleiteten Bewerbungsunterlagen trifft der Store-Manager eine Auswahlentscheidung und leitet das Verfahren zur Beteiligung des Betriebsrats nach § 99 BetrVG ein. In diesem Zusammenhang informiert er den Betriebsrat über die ihm vom Recruitment-Center weitergeleiteten Bewerbungen und stellt ihm die entsprechenden Unterlagen zur Verfügung.

Am 8. Oktober 2010 bewarb sich Frau E, wohnhaft in Flensburg, im Onlineportal für die Position „Mitarbeiterin im Verkauf“ in Teilzeit in der den Großraum Mannheim umfassenden „Area 10“. Am 11. Oktober 2010 erhielt sie eine schriftliche Absage. Am 9. November 2011 hörte die (damalige) Store-Managerin der Filiale Nr. 698 den Betriebsrat zur Einstellung von zwei Bewerbern an, ohne über die Bewerbung von Frau E zu informieren. Daraufhin forderte der Betriebsrat die Filialleitung mit Schreiben vom 16. November 2010 auf, künftig alle Bewerbungen vorzulegen, wobei er davon ausging, Frau E habe sich aufgrund ihres Wohnsitzes auf eine Stelle in der Flensburger Filiale beworben. Im Juli und August 2011 wurden weitere die Filiale Nr. 698 betreffende Stellen ausgeschrieben; zwei als Mitarbeiter/in im Verkauf in Voll- bzw. Teilzeit und eine als Filialassistent/-assistentin. Hierauf bewarb sich ua. Herr R. Auf seine Bewerbung als Filialassistent erhielt er mit E-Mail der „Recruitment“ vom 22. Juni 2011 eine Absage. Bei seinen Bewerbungen auf eine Verkäuferstelle ging die Arbeitgeberin davon aus, er habe diese vor Abschluss des Auswahlverfahrens zurückgezogen. Die Unterlagen seiner Bewerbungen wurden an die (damalige) Store-Managerin nicht weitergeleitet; entsprechend wurde der Betriebsrat über die Bewerbungen nicht unterrichtet. Am 1. Dezember 2011 wurde der Betriebsrat bei der Besetzung der Stelle eines Visual Merchandiser (m/w) beteiligt. Über die Online-Bewerbung von Frau V auf diese Stelle, die dem Recruitment-Center vorlag, wurde er nicht informiert.

Der Betriebsrat hat in dem von ihm eingeleiteten Beschlussverfahren geltend gemacht, ihm müssten bei seiner Beteiligung nach § 99 Abs. 1 BetrVG auch die vom Recruitment-Center „vorab aussortierten“ Bewerbungen vorgelegt werden.

### Aus den Gründen:

2. Der Antrag ist begründet. Die Arbeitgeberin ist nach § 99 Abs. 1 Satz 1 BetrVG verpflichtet, dem Betriebsrat vor der Einstellung eines Arbeitnehmers in der Filiale Flensburg (auch) diejenigen erforderlichen Bewerbungsunterlagen vorzulegen, die von Personen eingereicht wurden, die sich im Onlineportal auf eine ausgeschriebene Stelle für diese Filiale beworben (und ihre Bewerbung nicht wieder zurückgezogen) haben und die von einem Area-Büro nicht an die Filialleitung weitergegeben worden sind. Gleichfalls ist ihm Auskunft über die Person (auch) dieser Beteiligten iSv. § 99 Abs. 1 Satz 1 BetrVG zu geben.

a) Nach § 99 Abs. 1 Satz 1 BetrVG hat der Arbeitgeber in Unternehmen mit in der Regel mehr als zwanzig wahlberechtigten Arbeitnehmern den Betriebsrat ua. vor jeder Einstellung zu unterrichten, ihm die erforderlichen Bewerbungsunterlagen vorzulegen und Auskunft über die Person der Beteiligten zu geben; er

hat dem Betriebsrat unter Vorlage der erforderlichen Unterlagen Auskunft über die Auswirkungen der geplanten Maßnahme zu geben und die Zustimmung des Betriebsrats zu der geplanten Maßnahme einzuholen.

b) Hiernach besteht die beanspruchte Vorlage- und Auskunftspflicht.

aa) Bei der Arbeitgeberin handelt es sich um ein Unternehmen mit in der Regel mehr als zwanzig wahlberechtigten Arbeitnehmern.

bb) Die Vorlage- und Auskunftspflicht des § 99 Abs. 1 Satz 1 BetrVG erstreckt sich gegenüber dem Betriebsrat der Filiale Flensburg (auch) auf solche die Filiale betreffende – nicht zurückgenommene – Bewerbungen, die dem Recruitment-Center vorliegen, aber nicht an die Filialleitung weitergegeben werden. Das folgt aus Sinn und Zweck der Vorlage- und Auskunftspflicht.

(1) Die Unterrichts- und Vorlagepflicht nach § 99 Abs. 1 Satz 1 BetrVG soll zum einen dem Betriebsrat die Informationen verschaffen, die er benötigt, um sein Recht zur Stellungnahme nach § 99 Abs. 2 BetrVG sachgerecht ausüben zu können. Der Arbeitgeber hat den Betriebsrat daher so zu unterrichten, dass dieser aufgrund der mitgeteilten Tatsachen in die Lage versetzt wird zu prüfen, ob einer der in § 99 Abs. 2 BetrVG genannten Zustimmungsverweigerungsgründe vorliegt (vgl. BAG 27. Oktober 2010 – 7 ABR 86/09 – Rn. 21 mwN, BAGE 136, 123). Zum anderen soll der Betriebsrat bei seiner Beteiligung vor einer Einstellung die Möglichkeit haben, Anregungen für die Auswahl der Bewerber zu geben und Gesichtspunkte vorzubringen, die aus seiner Sicht für die Berücksichtigung eines anderen als des vom Arbeitgeber ausgewählten Stellenbewerbers sprechen. Das gilt unabhängig davon, ob hierauf eine Zustimmungsverweigerung nach § 99 Abs. 2 BetrVG gestützt werden kann (vgl. BAG 28. Juni 2005 – 1 ABR 26/04 – zu B II 2 b aa (2) der Gründe, BAGE 115, 173).

(2) Nach der Rechtsprechung des Bundesarbeitsgerichts hat der Arbeitgeber die Unterlagen bezüglich aller Stellenbewerber – auch der nicht berücksichtigten oder abgelehnten – vorzulegen (vgl. BAG 14. Dezember 2004 – 1 ABR 55/03 – zu B II 2 b aa der Gründe mwN, BAGE 113, 109; 10. November 1992 – 1 ABR 21/92 – zu B I 2 a der Gründe, BAGE 71, 337). Nur so kann der Betriebsrat seiner gesetzlichen Prüfungspflicht genügen (vgl. BAG 17. Juni 2008 – 1 ABR 20/07 – Rn. 25, BAGE 127, 51). Damit sind alle Stellenbewerber iSd. § 99 Abs. 1 Satz 1 BetrVG auch „Beteiligte“, über deren Person Auskunft zu geben ist (vgl. BAG 28. Juni 2005 – 1 ABR 26/04 – zu B II 2 b bb (1) der Gründe, BAGE 115, 173; 14. Dezember 2004 – 1 ABR 55/03 – zu B II 2 b aa der Gründe mwN, BAGE 113, 109). Die für das Mitbestimmungsrecht relevante „Beteiligten“stellung kommt all denjenigen zu, die ihr Interesse an einem konkreten zur Besetzung ausgeschriebenen Arbeitsplatz bekunden. Auch derjenige, der sich auf eine Stelle bewirbt, deren Anforderungsprofil oder Qualifikationsvoraussetzungen er nicht erfüllt und damit – ggf. sogar offensichtlich oder objektiv – für die Stelle ungeeignet ist, bringt sein Interesse an dem ausgeschriebenen Arbeitsplatz zum Ausdruck (vgl. auch BAG 6. April 1973 – 1 ABR 13/72 – zu II 1 der Gründe). Gleiches gilt für etwaige – ohnehin mit einer rechtlichen Bewertung verbundene – nicht ernsthafte Bewerbungen.

(3) Nach diesen Grundsätzen erstreckt sich das Recht des Betriebsrats der Filiale Flensburg, die erforderlichen Bewerbungsunterlagen vorgelegt und Auskunft über die Person der Beteiligten zu bekommen, auch auf diejenigen Bewerbungen um eine Stelle in der Flensburger Filiale, die vom Recruitment-Center aussortiert werden, etwa weil nach dessen Einschätzung von nicht ernsthaften Bewerbungen auszugehen ist oder der Bewerber dem geforderten Anforderungsprofil nicht entspricht. Die Unterrichtung

über die Bewerbung (vermeintlich) ungeeigneter Interessenten ist schon im Hinblick auf den weiten Zweck der Unterrichtungspflicht geboten, denn der Betriebsrat soll die Möglichkeit haben, Anregungen für die Auswahl der Bewerber zu geben und Gesichtspunkte vorzubringen, die aus seiner Sicht für die Berücksichtigung eines anderen als des ausgewählten Stellenbewerbers sprechen. Gleiches gilt für als nicht ernsthaft angesehene Bewerbungen. Im Hinblick auf die so eingeschätzten Bewerbungen stellen sich im Übrigen regelmäßig Bewertungsfragen, so dass schon zur Vermeidung von Abgrenzungsproblemen im Einzelfall und der damit einhergehenden Rechtsunsicherheit eine umfassende Vorlage- und Auskunftspflicht angezeigt ist.

cc) Der verfahrensgegenständlichen Vorlage- und Auskunftspflicht stehen die organisatorischen Vorgaben des Bewerbungsverfahrens durch die Arbeitgeberin nicht entgegen.

(1) Für das Beteiligungsverfahren nach § 99 Abs. 1 Satz 1 BetrVG ist nicht ausschlaggebend, auf welche Weise der Arbeitgeber konkrete Arbeitsplätze anbietet. Allerdings ist „Bewerber“ (oder „Beteiligter“) iSv. § 99 Abs. 1 Satz 1 BetrVG nur derjenige, der sein Interesse für einen konkreten Arbeitsplatz bekundet (vgl. BAG 1. Juni 2011 – 7 ABR 117/09 – Rn. 26). Im Rahmen des § 99 Abs. 1 Satz 1 BetrVG setzt die Eigenschaft als Bewerber voraus, dass ein Anbahnungsverhältnis zum Arbeitgeber für einen konkreten Arbeitsplatz besteht (BAG 10. November 1992 – 1 ABR 21/92 – zu B I 2 b der Gründe, BAGE 71, 337). Aus diesem Grund ist etwa im Fall der Einschaltung eines Personalberatungsunternehmens, das keine Stellenanzeige für den Arbeitgeber aufgegeben hat und allein damit beauftragt wurde, geeignete Bewerber vorzuschlagen, nur derjenige als Bewerber anzusehen, der vom Personalberater vorgeschlagen wird (vgl. BAG 18. Dezember 1990 – 1 ABR 15/90 – zu B I 3 c der Gründe, BAGE 66, 328).

(2) Danach besteht vorliegend die Vorlage- und Auskunftspflicht des § 99 Abs. 1 Satz 1 BetrVG auch hinsichtlich solcher Personen, die sich auf eine ausgeschriebene Stelle in der Filiale Flensburg bewerben und von einem Area-Büro „vorab aussortiert“ werden. Diese sind Bewerber, weil sie ihr Interesse für einen bestimmten Arbeitsplatz aufgrund einer von der Arbeitgeberin veranlassten Stellenausschreibung in einem von ihr organisierten Verfahren zum Ausdruck gebracht haben (vgl. BAG 18. Dezember 1990 – 1 ABR 15/90 – zu B I 3 c der Gründe, BAGE 66, 328).

dd) Entgegen der Ansicht der Arbeitgeberin ist sie – und nicht die Filialleitung – Verpflichtete der Vorlage- und Auskunftspflicht des § 99 Abs. 1 Satz 1 BetrVG. Die Unterrichtungspflicht des § 99 Abs. 1 Satz 1 BetrVG trifft nach dem ausdrücklichen Wortlaut der gesetzlichen Bestimmung den „Arbeitgeber“. Der Store-Manager handelt bei der Einstellungsentscheidung und bei der Erfüllung der mit der Einstellung zusammenhängenden Beteiligungsrechte des Betriebsrats nach § 99 Abs. 1 Satz 1 BetrVG für die Arbeitgeberin. Er wird dadurch nicht selbst zum (Betriebs- oder Vertrags-)Arbeitgeber. Das gilt auch dann, wenn ihm wegen seiner Befugnisse die Stellung eines leitenden Angestellten im betriebsverfassungsrechtlichen Sinn zukommen sollte.

ee) Schließlich ist es für die Unterrichtungspflicht nach § 99 Abs. 1 Satz 1 BetrVG entgegen der Ansicht der Arbeitgeberin unerheblich, ob der für die Einstellungsentscheidung zuständige Store-Manager Kenntnis von der Bewerbung hat und ob ihm die Bewerbungsunterlagen zur Verfügung gestellt werden. Es trifft zu, dass der Arbeitgeber nur das mitteilen kann und muss, was ihm selbst bekannt ist. Auch ist er grundsätzlich nicht verpflichtet, dem Betriebsrat Unterlagen zur Verfügung zu stellen, die er selbst nicht hat (vgl. BAG 18. Dezember 1990 – 1 ABR 15/90 –

zu B I 2 b der Gründe, BAGE 66, 328). Die Arbeitgeberin erkennt jedoch, dass es nicht darauf ankommt, ob die Filialleitung über die entsprechende Kenntnis oder Unterlagen verfügt, sondern darauf, ob ihr selbst die Bewerbungen vorliegen.

## Zur Einsichtnahme in das Dienstverhältnis betreffende behördeninterne E-Mails

(Oberverwaltungsgericht Nordrhein-Westfalen, Beschluss vom 7. Januar 2015 – 1 B 1260/14 –)

**Eine Beamtin hat ein Akteneinsichtsrecht in eine E-Mail ihrer Vorgesetzten an das Personalreferat, in der gravierende Auffälligkeiten in der dienstlichen Arbeitsweise der Beamtin beispielhaft dargestellt sind.**

### Aus den Gründen:

1. Der Antragstellerin steht ein Anspruch auf Einsicht in das streitgegenständliche Schreiben (E-Mail) zu. Der Senat kann offen lassen, ob dies bereits aus § 110 Abs. 1 und 2 BBG folgt, weil es sich bei dem in Rede stehenden Schreiben materiell um einen Bestandteil der für die Antragstellerin geführten Personalakte handelt, in die sie ohne weiteres Einsicht nehmen darf. Denn jedenfalls ergibt sich der Anspruch aus § 110 Abs. 4 Satz 1 BBG. Nach dieser Vorschrift hat ein Beamter ein Recht auf Einsicht auch in andere Akten (als die ihn betreffende Personalakte) (dazu a)), die personenbezogene Daten über ihn enthalten (dazu b)) und für sein Dienstverhältnis verwendet werden (dazu c)), soweit gesetzlich nichts anderes bestimmt ist (dazu d)).

a) Das in Rede stehende Schreiben ist, wenn man es nicht als Bestandteil der Personalakte einstuft, jedenfalls eine Akte im Sinne des § 110 Abs. 4 Satz 1 BBG. Der dort genannte Begriff der Akte ist im materiellen Sinne zu verstehen (dazu aa)). Der Annahme, dass es sich bei dem Schreiben um eine Akte im Sinne des § 110 Abs. 4 Satz 1 BBG handelt, steht nicht entgegen, dass es nach den Angaben der Antragsgegnerin nicht in einen Verwaltungsvorgang aufgenommen werden und vertraulich sein sollte (dazu bb)).

aa) Der Aktenbegriff im Sinne der Regelung über Akteneinsichtsrechte gemäß § 110 Abs. 4 Satz 1 BBG ist – ebenso wie der Begriff der in den §§ 110 Abs. 1, 106 Abs. 1 Satz 1 und 4 BBG genannten Personalakte – umfassend und im materiellen Sinne zu verstehen. Danach ist entscheidend, ob sich in Unterlagen oder elektronischen Dokumenten, die dem Dienstherrn zur Verfügung stehen, personenbezogene Daten über einen Beamten befinden, die für sein Dienstverhältnis verwendet werden. Es kommt nicht auf Art und Ort der Aufbewahrung und der Speicherung dieser Daten an (vgl. Kathke, in Schütz/Maiwald, Beamtenrecht des Bundes und der Länder, Stand: Nov. 2014, Teil C, § 87 LBG NRW, Rn. 86: „Das Einsichtsrecht bezieht sich auf alle personenbezogenen Daten – und nur auf diese –, nicht auf die gesamten Akten“; BVerwG, Beschluss vom 8. Mai 2006 – 1 DB 1.06 –, ZBR 2006, 309 = juris, Rn. 7, und Urteil vom 1. Juli 1983 – 2 C 42.82 –, BVerwGE 67, 300 = DVBl. 1984, 55 = juris, Rn. 20 (jeweils zu beamtenrechtlichen Personalakten); BGH, Senat für Anwaltssachen, Urteil vom 25. November 2013 – AnwZ (Brgf) 39/12 –, NJW-RR 2014, 883 = juris, Rn. 5 (zum Begriff der Personalakte i. S. d. § 58 Abs. 1 BRAO); Nds. Staatsgerichtshof,

Urteil vom 24. Oktober 2014 – StGH 7/13 –, juris, Rn. 63 (zum Begriff der Akten in Art. 24 Abs. 2 Satz 1 Nds. Verfassung)).

Andernfalls könnte der Dienstherr Einsichtsrechte des betroffenen Beamten dadurch aushebeln, dass er personenbezogene und in einem inneren Zusammenhang mit dem Dienstverhältnis stehende Daten außerhalb der üblichen Aktensammlungen vorhält. Dies widerspräche Sinn und Zweck des Rechtes auf Akteneinsicht. § 110 Abs. 4 Satz 1 BBG soll gewährleisten, dass der Beamte grundsätzlich auch solche ihn betreffenden, personenbezogenen Daten kennt, die dem Dienstherrn außerhalb der Personalakte vorliegen und die für das Dienstverhältnis relevant sind. Das Recht auf Einsicht in personenbezogene Daten ist unter Berücksichtigung der Fürsorgepflicht des Dienstherrn aus Art. 33 Abs. 5 GG und des verfahrensrechtlichen Schutzes des Rechtes auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG auszulegen (vgl. Kathke, in Schütz/Maiwald, Beamtenrecht des Bundes und der Länder, Stand: Nov. 2014, Teil C, § 87 LBG NRW, Rn. 14 ff. (zum Einsichtsrecht in Personalakten); zum Akteneinsichtsrecht aus beamtenrechtlicher Fürsorgepflicht siehe VG Frankfurt, Urteil vom 28. Mai 1986 – III/V – E 1373/83 –, NVwZ 1986, 864).

Die beamtenrechtliche Fürsorgepflicht (Art. 33 Abs. 5 GG, § 78 BBG) umfasst u.a. die Verpflichtung des Dienstherrn, den Beamten bei seiner amtlichen Tätigkeit und in seiner Stellung als Beamten zu schützen (§ 78 Satz 2 BBG). Dazu gehört es, ihn gegen unberechtigte Vorwürfe in Schutz zu nehmen. Sie gebietet es auch, dem Beamten Hilfen zu bieten, damit er sich selbst gegen Behauptungen und Anschuldigungen Dritter, die seine Amtsführung betreffen, zur Wehr setzen kann (vgl. BVerwG, 27. Februar 2003 – 2 C 10.02 –, BVerwGE 118, 10 = NJW 2003, 3217 = juris, Rn. 19).

Falls der Dienstherr aufgrund seiner nicht zu den Personalakten zu nehmenden Erkenntnisse dienstlich nachteilige Folgerungen ziehen will, muss er dem Beamten jedenfalls so viel offenbaren, dass dieser seine Rechte sachgemäß wahren kann (vgl. BVerwG, Urteil vom 26. Januar 1978 – 2 C 66.73 –, BVerwGE 55, 186 = NJW 1978, 1643 = juris, Rn. 25 (zur Einsicht in Sicherheitsakten)).

Dies gilt entsprechend für interne Äußerungen eines Vorgesetzten bezüglich der Arbeitsweise eines Beamten. Damit der betroffene Beamte prüfen kann, ob die Vorwürfe berechtigt sind, und sich ggf. dagegen wehren kann, muss er sie zunächst einmal kennen.

Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, über die Preisgabe und Verwendung seiner persönlichen Daten grundsätzlich selbst zu bestimmen. Fehlender Zugang zum Wissen Dritter über die eigene Person kann die von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte individuelle Selbstbestimmung berühren. Daher verschafft das Grundrecht auf informationelle Selbstbestimmung seinem Träger auch Rechtspositionen, die den Zugang zu den über ihn gespeicherten persönlichen Daten betreffen. Aus dem Selbstbestimmungsrecht kann ein Anspruch auf Abwägung nach Maßgabe des Grundsatzes der Verhältnismäßigkeit folgen, der sich zu einem Informationsanspruch dann verdichtet, wenn keine mindestens gleich gewichtigen Belange entgegenstehen (vgl. BVerfG, Beschlüsse vom 10. März 2008 – 1 BvR 2388/03 –, BVerfGE 120, 351 = NJW 2008, 2099 = juris, Rn. 58, und vom 9. Januar 2006 – 2 BvR 443/02 –, NJW 2006, 1116 = juris, Rn. 20 ff.).

Dieses vor dem verfassungsrechtlichen Hintergrund gebotene umfassende Verständnis des Begriffs „Akte“ im Sinne von § 110 Abs. 4 Satz 1 BBG entspricht auch dem Willen des Gesetzgebers.

Dieser wollte auf Vorschlag des Bundesbeauftragten für Datenschutz eine „Regelung über die Einsicht personenbezogener Daten außerhalb der Personalakte“ schaffen (vgl. BT-Drs. 12/2201, S. 23).

Dies macht deutlich, dass es um die Kenntniserlangung von bestimmten Daten geht, nicht um Einsicht in bestimmte, vom Dienstherrn als Akte gekennzeichnete Sammlungen von Schriftstücken. Dem steht nicht entgegen, dass der Begriff der Akte nach dem Vortrag der Antragsgegnerin häufig formell bestimmt, nämlich „gemeinhin definiert [wird] als ‚themenbezogene Sammlung von Vorgängen und Unterlagen‘“. In § 110 Abs. 4 Satz 1 BBG ist aus den genannten Gründen nicht dieser Aktenbegriff, sondern der materielle Aktenbegriff maßgeblich. Daher kommt es auch nicht darauf an, ob das in Rede stehende Schreiben ein isoliertes Schriftstück oder eine E-Mail ohne Einbindung in eine Akte im wohl üblichen Sinne ist.

Die Befürchtung der Antragsgegnerin, bei einem solchen Normverständnis wäre jegliche verschriftlichte Äußerung mit personalbezogenen Daten künftig auf Verlangen vom Betroffenen einzusehen, teilt der Senat nicht. Es sind vielmehr in jedem Einzelfall die Voraussetzungen des § 110 Abs. 4 Satz 1 BBG zu prüfen. Das Ergebnis dieser Prüfung hängt davon ab, von wem welche Äußerung in welchem Zusammenhang in welcher Weise und zu welchem Zweck verschriftlicht worden ist.

bb) Ohne Erfolg macht die Antragsgegnerin geltend, die E-Mail sei eine „nicht verfahrensbezogene[n] Äußerung[en]“ und von vornherein nicht für eine Akte vorgesehen. Sie beruft sich damit der Sache nach darauf, dass Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen, u. U. keine Daten sind, für die Einsichtsrechte bestehen können (vgl. etwa § 2 Nr. 1 Satz 2 Informationsfreiheitsgesetz – IFG –, wonach Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen, nicht zu den amtlichen Informationen im Sinne des Informationsfreiheitsgesetzes gehören).

Entwürfe und Notizen sind deswegen vom Informationszugang des Informationsfreiheitsgesetzes ausgenommen, weil ein innerbehördlicher Freiraum für die Erarbeitung von Konzepten erhalten bleiben soll. Entwürfe in diesem Sinne sind vorläufige Gedankenskizzen, die nach der Vorstellung des Verfassers noch weiter bearbeitet werden sollen und deshalb noch nicht als Beleg für seine Auffassung oder eine von ihm angestrebte Entscheidung verstanden werden können. Notizen in diesem Sinne sind zur Stützung des Gedächtnisses gefertigte Aufzeichnungen, die allein Zwecken des Verfassers dienen, etwa zur Vorbereitung später zu fertigender Vermerke, Stellungnahmen, Entscheidungen oder Berichte. Verlässt ein Schreiben ein Referat oder Dezernat, liegt eine endgültige Festlegung des Behördenwillens zumeist bereits vor. Weder um einen Entwurf noch um eine bloße Notiz handelt es sich auch bei bearbeitungsbedürftigen Eingängen von anderen Referaten (vgl. Scheel, in: Berger u. a., IFG, 2. Aufl. 2013, § 2 Rn. 31 ff.; Schoch, IFG, 2009, § 2 Rn. 45 ff., Jastrow/Schlatmann, IFG, 2006, § 2 Rn. 13 ff.).

Es kann offen bleiben, ob diese für das Informationsfreiheitsgesetz geltenden Maßstäbe in gleicher Weise auf den Begriff der Akte im Sinne des § 110 Abs. 4 Satz 1 BBG übertragbar sind. Denn das streitgegenständliche Schreiben ist weder ein bloßer Entwurf einer Stellungnahme an das Personalreferat noch eine Notiz im Sinne einer Gedankenstütze nur für die Verfasserin. In dem Schreiben hat vielmehr die Leiterin des Referates 4 C 6 für das Personalreferat die Arbeitsweise der Antragstellerin aus ihrer Sicht mit dem Ziel dargestellt, dass das Personalreferat sich um die innerdienstlichen Schwierigkeiten mit der Antragstellerin kümmert. Schon dadurch, dass das

Schreiben als Grundlage für das weitere dienstliche Handeln einer anderen Person diene und dienen sollte, verlor es einen etwaigen unverbindlichen Charakter.

Im Übrigen ist nach der allgemein geltenden Dokumentationsfunktion von Behördenakten und der Pflicht zur wahrheitsgetreuen und vollständigen Aktenführung das streitgegenständliche Schreiben zumindest in den Verwaltungsvorgang betreffend die Problempunkte zwischen der Antragstellerin und der Leiterin des Referates 4 C 6 aufzunehmen, um den Vorgang wahrheitsgetreu, vollständig und nachprüfbar zu dokumentieren (vgl. zu diesen Pflichten BVerwG, Beschluss vom 16. März 1988 – 1 B 153/87 –, NVwZ 1988, 621 = juris, Rn. 11).

Ein solches Verwaltungsverfahren hat die Antragsgegnerin nach ihren Angaben auch bereits eingeleitet, indem sie den Leiter der Abteilung 4 um Stellungnahme zu den in den Personalgesprächen benannten Problempunkten gebeten hat. Die Antragsgegnerin kann demgegenüber nicht erfolgreich geltend machen, das von ihr eingeleitete Verwaltungsverfahren beziehe sich nur auf die im Gespräch vom 14. Januar 2014 angesprochenen Probleme, und das Schreiben vom 11. November 2013 sei nicht für dieses Gespräch, sondern nur für das Gespräch vom 19. November 2013 verwendet worden. Die in diesen Personalgesprächen erörterten Schwierigkeiten sind nämlich dieselben: Es ging um „Auffälligkeiten und hieraus angeblich resultierende Spannungen zwischen der Leiterin des Referates 4 C 6 und der Antragstellerin“ (so die Antragsgegnerin in ihrem Schriftsatz vom 7. November 2014). Für die Frage, ob eine Mitteilung sich auf ein Verwaltungsverfahren bezieht, kommt es im Übrigen auf ihren Inhalt an, nicht aber auf die Art der Übermittlung. E-Mails sind daher nicht schon als solche verwaltungsverfahrensrrechtlich unverbindlich oder nicht verfahrensbezogen.

Die Antragsgegnerin kann sich auch nicht auf „Vertraulichkeit“ der E-Mail berufen. Vertraulich kann eine solche Mail sein, soweit es nur um private Belange des Verfassers und des Adressaten geht oder um Informationen, die nicht mit der amtlichen Tätigkeit zusammenhängen (vgl. Scheel, in: Berger u. a., IFG, 2. Aufl. 2013, § 2 Rn. 20, zum Begriff amtlicher Informationen im Gegensatz zu privaten Informationen).

Dies ist hier nicht der Fall. Die E-Mail betrifft die dienstliche Arbeitsweise einer dritten Person, der Antragstellerin. Daher besteht keinerlei schutzwürdiges Interesse an einer Vertraulichkeit dieser gegenüber. Sollte die E-Mail, wie die Antragstellerin vermutet, in einem Stil verfasst sein, der ein ungünstiges Licht auf die Verfasserin werfen könnte, ist das Interesse an einer Geheimhaltung erst recht nicht schutzwürdig. Wer sich in seiner Funktion als Vorgesetzter an das Personalreferat wendet, weil es Schwierigkeiten mit einem Mitarbeiter gibt, und seine negative Sicht der Arbeitsweise eines Beamten dem Personalreferat schriftlich mitteilt, muss sich überlegen, wie er dies formuliert, weil damit zu rechnen ist, dass diese Mitteilung dienstrechtliche Konsequenzen haben kann.

b) Das Schreiben der Leiterin des Referates 4 C 6 enthält personenbezogene Daten im Sinne des § 110 Abs. 4 Satz 1 BBG über die Antragstellerin.

Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person (zum Rückgriff auf die Definition im Datenschutzrecht vgl. OVG NRW, Urteil vom 8. Februar 1994 – 6 A 2704/91 –, RiA 1994, 258 = juris, Rn. 15).

Dazu zählen Meinungsäußerungen, Beurteilungen und Werturteile, die sich auf eine bestimmte Person beziehen, sowie die Darstellung des dienstlichen Verhaltens eines Beamten (so BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08 –, BGHZ 181,

328 = NJW 2009, 2888 = juris, Rn. 17 (zu Internetbewertungsforen); siehe auch Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 4 ff., 12, und Gola/Schomann, BDSG, 11. Aufl. 2012, § 3 Rn. 2 ff., 6, wonach Werturteile zu personenbezogenen Daten i. S. d. § 3 Abs. 1 BDSG gehören).

Nach den Angaben der Antragsgegnerin in ihrem Beschwerdebegründungsschriftsatz vom 7. November 2014 stellt das Schreiben „Auffälligkeiten in der Arbeitsweise der Antragstellerin beispielhaft“ dar, ist also eine bewertende Darstellung deren dienstlicher Arbeitsweise.

c) Das Schreiben vom 11. November 2013 wird im Sinne des § 110 Abs. 4 Satz 1 BBG für das Dienstverhältnis der Antragstellerin verwendet.

Indem der Gesetzgeber das in Rede stehende Tatbestandsmerkmal in der Zeitform des Präsens formuliert, verdeutlicht er, dass das Einsichtsrecht in Sachakten nach § 110 Abs. 4 Satz 1 BBG nur besteht, wenn diese Akten – noch – für das Dienstverhältnis des Betroffenen verwendet werden. Es kommt also darauf an, ob und in welchem Ausmaß der Beamte damit rechnen muss, dass die Sachakte für sein Dienstverhältnis (weiterhin) relevant sein kann. Dafür ist vor allem maßgebend, mit welcher Zweckbestimmung der Dienstherr die entsprechende Akte (fort-)führt und aufbewahrt und diese dementsprechend einem Zugriff (noch) offen steht. Wenn die fragliche Sachakte künftig auf keinen Fall mehr für das Dienstverhältnis des Beamten verwendet werden kann, besteht kein Akteneinsichtsrecht (vgl. zur Parallelvorschrift des § 107 c Abs. 4 Satz 1 HBG a. F. von Roetteken, in: von Roetteken/Rothländer, Hessisches Bedienstetenrecht, Stand: Dez. 2014, § 107 c Rn. 55, m.w.N.; siehe auch OVG NRW, Urteil vom 8. Februar 1994 – 6 A 2704/91 –, RiA 1994, 258 = juris, Rn. 15, zur Parallelvorschrift des § 102 c Abs. 4 Satz 1 LBG NRW a. F.).

In Anwendung dieser Grundsätze muss die Antragstellerin damit rechnen, dass die fragliche E-Mail noch im Rahmen ihres Dienstverhältnisses verwendet werden wird. Das ergibt sich schon daraus, dass die E-Mail bereits entsprechend genutzt worden ist (nachfolgend aa)) und der Vorgang, innerhalb dessen dies geschehen ist, noch nicht abgeschlossen ist (nachfolgend bb)); vor diesem Hintergrund sind die Behauptungen der Antragsgegnerin, sie werde von der E-Mail keinen Gebrauch (mehr) machen, nicht nachvollziehbar (nachfolgend cc)).

aa) Die fragliche E-Mail ist bereits in der Vergangenheit für das Dienstverhältnis der Antragstellerin verwendet worden, indem sie zur Vorbereitung der Leiterin des Personalreferates auf das Personalgespräch am 19. November 2013 diente. Dies ergibt sich schon aus den Angaben der Antragsgegnerin zur Entstehung des Schreibens: „Anfang November 2013 kam die Leiterin des Referates 4 C 6 auf das Personalreferat zu und teilte mit, dass in der Arbeitsweise der Antragstellerin gravierende Auffälligkeiten aufgetreten seien. Um sich ein Bild von der entstandenen Situation machen zu können, bat die – seinerzeit kommissarische – Leiterin des Personalreferats die Leiterin des Referates 4 C 6, diese Auffälligkeiten in der Arbeitsweise der Antragstellerin beispielhaft darzustellen. Eine entsprechende Darlegung wurde daraufhin am 11.11.2013 von der Leiterin des Referates 4 C 6 an die Leiterin des Personalreferats per Intranet-Mail übermittelt. Diese Darstellung, die der Leiterin des Personalreferates im Vorfeld des Gesprächs am 19.11.2013 zum Verständnis der entstandenen Situation diente, befindet sich in elektronischer Form weiterhin im Posteingang ihres dienstlichen Intranet-Mailaccounts.“ Nach der Darstellung der Antragsgegnerin diente das genannte Gespräch – ebenso wie das am 14. Januar 2014 geführte – „allein dazu, diese Auffälligkeiten und hieraus angeblich resultierende Spannungen

zwischen der Leiterin des Referates 4 C 6 und der Antragstellerin offen zu erörtern, die Sichtweise der Antragstellerin hierzu zu erfragen und die Situation nach Möglichkeit konstruktiv und konsensual zu lösen“. Der in der E-Mail dargestellte Inhalt sei der Antragstellerin dagegen nicht vorgeworfen worden.

Schon nach dieser Darstellung zeigt sich, dass die in dem Streitgegenständlichen Schreiben enthaltenen Angaben für das Dienstverhältnis der Antragstellerin verwendet worden sind: Es gab ein dienstliches Personalgespräch am 19. November 2013 zwischen der Antragstellerin und der Leiterin des Personalreferats über die Art und Weise der Aufgabenerfüllung durch die Antragstellerin.

bb) Vor dem Hintergrund des Vorstehenden und bei lebensnaher Betrachtung spricht eine ganz überwiegende Wahrscheinlichkeit dafür, dass – was entscheidend ist – die Daten auch zukünftig für das Dienstverhältnis der Antragstellerin verwendet werden. Denn das Verhältnis zwischen der Antragstellerin und ihrer Dienststelle ist nach Aktenlage unverändert schwierig. Unabhängig davon, wer dies verursacht hat, gehen beide Beteiligten der Sache nach davon aus, dass die aufgetretenen und in dem Schreiben angesprochenen Probleme bisher ungelöst sind. Dies ergibt sich neben der eben wiedergegebenen Darstellung der Antragsgegnerin zur Entstehung des Schreibens aus Folgendem:

Die Antragsgegnerin trägt zu den Ergebnissen der Gespräche mit der Antragstellerin vor: „Das Ziel einer offenen Erörterung und einer nach Möglichkeit konsensualen Lösung war jedoch aufgrund des Verhalte[n]s der Antragstellerin und ihres Bevollmächtigten nicht erreichbar. Insbesondere war der Verlauf des Gesprächs am 14.01.2014 von der Antragstellerin und ihrem Bevollmächtigten in der Sache wenig konstruktiv gestaltet, dafür aber durch eine Vielzahl von Vorwürfen und Vorhaltungen geprägt. Daher entschied die Antragsgegnerin, die im Gespräch zutage getretenen Problempunkte im Rahmen eines förmlichen Verwaltungsverfahrens aufzuarbeiten“. Für dieses förmliche Verwaltungsverfahren hat die Antragsgegnerin den Leiter der Abteilung 4 um Prüfung und Stellungnahme gebeten. Nach den Angaben von Herrn Dr. I. gegenüber der Berichterstatterin vom 9. Dezember 2014 liegt diese Stellungnahme noch nicht vor.

Die Antragstellerin wirft der Antragsgegnerin demgegenüber eine „zum Teil falsche Sachdarstellung“ vor. Die ihr gegenüber erhobenen Vorwürfe (gravierende Auffälligkeiten) hätten sie „zutiefst verletzt und in eine tiefe Lebenskrise gestürzt“, weil sie nicht gewusst habe und immer noch nicht wisse, was ihr überhaupt vorgehalten werde. Sie geht von einem „unwiderruflich zerstörten Vertrauensverhältnis“ aus und kann sich einen weiteren dienstlichen Einsatz im Zuständigkeitsbereich der Antragsgegnerin daher nicht mehr vorstellen.

Unter Berücksichtigung dieser Situation ist es lebensfremd und kann nicht mit der Antragsgegnerin angenommen werden, dass das Schreiben vom 11. November 2013 mit seiner Darstellung von „Auffälligkeiten“ zukünftig in keiner Weise mehr für das Dienstverhältnis der Antragstellerin von Bedeutung sein wird. Die „Auffälligkeiten“ waren nach Aktenlage immerhin der Anlass, überhaupt Personalgespräche mit der Klägerin zu führen. Dass keinerlei zukünftige Personalmaßnahmen beabsichtigt sind, die zumindest der Sache nach auch auf der Grundlage dieses Schreibens ergehen, ist nach Aktenlage auszuschließen. Denn die Antragsgegnerin selbst hat in ihrem Schreiben vom 28. Februar 2014 an den Prozessbevollmächtigten der Antragstellerin mitgeteilt, angesichts der Konflikte, die das Vertrauensverhältnis zwischen der Vorgesetzten und der Antragstellerin maßgeblich gestört hätten, sehe die Personalverwaltung Handlungsbedarf und prüfe, ob durch eine Umsetzung der Antragstel-

lerin in einen anderen Arbeitsbereich eine Befriedung erreicht werden könne. Da das Vertrauensverhältnis – aus welchen Gründen auch immer – offenbar beschädigt ist, erscheint es auch angezeigt, dass die Personalverwaltung prüft, auf welche Weise und durch welche Maßnahmen sich diese Störung am besten beheben lässt. Zu einer sachgerechten Prüfung dieser Art gehört es, den Sachverhalt umfassend und vollständig aufzuklären, wozu auch die Kenntnis des streitgegenständlichen Schreibens für alle Beteiligten gehört. Schon aus Gründen der Fairness muss auch die Antragstellerin dieses Schreiben und die darin erwähnten „Auffälligkeiten“ kennen, damit sie ihre Sichtweise der Lage geltend machen und diese berücksichtigt werden kann.

d) Dem Einsichtsrecht der Antragstellerin stehen keine gesetzlichen Regelungen im Sinne des § 110 Abs. 4 Satz 1 BBG entgegen. Solche sind weder geltend gemacht worden noch sonst ersichtlich. Insbesondere sind keine schützenswerten Rechte anderer Personen berührt. Es handelt sich bei dem streitgegenständlichen Schreiben auch nicht um eine Sicherheitsakte im Sinne des § 110 Abs. 4 Satz 2 BBG. Es ist schließlich weder geltend gemacht noch sonst ersichtlich, dass die im Schreiben enthaltenen Daten der Antragstellerin mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sein könnten, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich wäre (vgl. § 110 Abs. 4 Satz 3 BBG). Im Übrigen wäre in einem solchen Fall nach § 110 Abs. 4 Satz 4 BBG zumindest Auskunft zu erteilen.

e) Auf die Frage, ob aus der Anhörungspflicht nach § 109 BBG folgt, dass auch Anhörungsrechte im Sachaktenbereich bestehen, kommt es für die Frage des Akteneinsichtsrechts in Sachakten nicht an. Dieses ergibt sich hier jedenfalls aus § 110 Abs. 4 Satz 1 BBG. Das Verwaltungsgericht hat in seinem Beschluss auf diesen Rechtsgedanken nach der Subsumtion unter § 110 Abs. 4 Satz 1 BBG auch nur ergänzend hingewiesen.

## Kein einstweiliger Rechtsschutz gegen Umsetzung auf den Posten des Behördlicher Datenschutzbeauftragten (Ls)

(Oberverwaltungsgericht Nordrhein-Westfalen, Beschluss vom 7. Oktober 2014 – 6B 1021/14 –)

- 1. Wird der Leiter der EDV auf Grund von Führungsproblemen auf den Dienstposten des behördlichen Datenschutzbeauftragten umgesetzt, so kann die Rücknahme dieser Maßnahme im Wege einer einstweiligen Anordnung nur dann erfolgreich verlangt werden, wenn dem Beamten ohne Weiterbeschäftigung auf seinem bisherigen Dienstposten unzumutbare Nachteile drohen.**
- 2. Diese liegen auch dann nicht vor, wenn der Posten des Datenschutzbeauftragten bislang neben einem anderen Dienstposten ausgeübt wurde und damit eine quantitativ nicht angemessene Beschäftigung vorliegen würde, wenn der Aufgabenzuschnitt der neuen Position noch näher definiert werden soll.**

*(Nicht amtliche Leitsätze)*

## Unzulässige Drohung mit Schufa-Einmeldung – Kosten der Abmahnung

(Landgericht Darmstadt, Urteil vom 16. Oktober 2014, 27 O 133/14 –)

- 1. Wird in einem „letzten“ Mahnschreiben eine nach § 28 Abs. a Ziff. 4 d BDSG unzulässige Meldung an die Schufa zumindest irreführend in Aussicht gestellt, ist dies datenschutz- und wettbewerbswidrig.**
- 2. Dem klagenden Verbraucherschutzverband steht, nachdem der Unterlassungsanspruch im Verfahren anerkannt wurde, auch die Erstattung der durch die zuvor ergangene Abmahnung entstandenen Kosten zu.**

*(Nicht amtliche Leitsätze)*

### Sachverhalt:

Der Kläger ist der Dachverband aller 16 Verbraucherzentralen und 26 weiterer verbraucher- und sozialorientierter Organisationen in Deutschland. Gemäß § 2 seiner Satzung bezweckt der Kläger u.a. die Wahrnehmung von Verbraucherinteressen. Die Beklagte beschäftigt sich u.a. mit dem Einzug von Forderungen.

Die Beklagte verschickt an Verbraucher letzte Mahnschreiben, in denen Forderungen für vermeintliche Serviceaufträge geltend gemacht werden. Des Inhalts wegen wird auf die Anlage K1 (BI.9d.A.) verwiesen.

Ein solches Schreiben ging auch am 17.10.2013 an N.N., welche zuvor auf Mahnungen mehrfach darauf hingewiesen hatte, dass ein Vertrag nicht zustande gekommen sei und die Forderung bestritt.

Die Klägerin forderte die Beklagte mit Abmahnschreiben vom 16.04.2014 zur Abgabe einer strafbewehrten Unterlassungserklärung wie folgt auf:

„...im Rahmen geschäftlicher Handlungen wie als Anlage beigelegt, eine letzte Mahnung an Verbraucher zu senden und mitzuteilen dass unbestrittene und fällige Forderungen an die SCHUFA gemeldet werden können, wenn diese die Forderung gegenüber der Tropmi Payment GmbH zuvor bestritten haben“.

Die Beklagte ließ mit Rechtsanwaltschreiben vom 29.04.2014 das Anliegen der Klägerin zurückweisen. Sie ließ insbesondere dazu auffordern, die Anspruchsvoraussetzungen schlüssig und nachvollziehbar darzulegen.

Im Verfahren gab die Beklagte folgende Erklärung ab:

„1. Die Beklagte verpflichtet sich gegenüber dem Kläger ohne Anerkenntnis einer Rechtspflicht und ohne Präjudiz für die Sach- und Rechtslage, gleichwohl rechtsverbindlich, es ab sofort zu unterlassen, im Rahmen geschäftlicher Handlungen an Verbraucher eine „letzte Mahnung“ wie in Anlage K 1 zur Klageschrift vom 7. Mai 2014 beigelegt zu senden, in der es heißt: „Weil Sie auch keine rechtlichen erheblichen Einwendungen gegen diese Forderung geltend gemacht haben, ist der Anspruch einredfrei und fällig. Hinzu kommt, dass unbestrittene und fällige Forderungen an die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) gemeldet werden können“, wenn die angeschriebenen Verbraucher die Forderung zuvor gegenüber der Beklagten bestritten haben.“

2. Die Beklagte verpflichtet sich gegenüber dem Kläger weiter, an ihn für jeden Fall der schuldhaften Zuwiderhandlung gegen die Unterlassungsverpflichtung aus vorstehender Ziffer 1 eine in sein billiges Ermessen gestellte und im Streitfall vom sachlich und örtlich zuständigen Gericht zu überprüfende Vertragsstrafe zu zahlen.

Die Parteien haben daraufhin den Rechtsstreit wegen des geltend gemachten Unterlassungsanspruchs der Klägerin in der Hauptsache übereinstimmend für erledigt erklärt.

**Aus den Gründen:**

Die Klage ist in dem zuletzt gegebenen Umfang zulässig und begründet.

Der Anspruch des Klägers auf Aufwendungsersatz gründet sich auf § 12 Absatz 1 Satz 2 UWG. Danach kann bei einer berechtigten Abmahnung Ersatz der erforderlichen Aufwendungen verlangt werden. Hierbei kann ein Verband auch eine Pauschale verlangen (Bornkamm in: Bornkamm/Köhler, UWG, 32. Aufl. 2014, zitiert nach beck-online).

Die erfolgte Abmahnung der „Letzten Mahnung“ war berechtigt. Bei einer bereits bestrittenen Forderung ist die Inanspruchnahme einer Datenübermittlung an die Schufa unzulässig (OLG Celle, 13 U 64/13, Urteil vom 19.12.2013; zitiert nach-juris). Dies ist vor dem Wortlaut des § 28a Nr. 4d BDSG überzeugend, der eine Übermittlung personenbezogener Daten über eine Forderung an Auskunftsteilen u.a. „nur für zulässig“ erachtet, wenn der Betroffene die Forderung nicht bestritten hat. Hierbei ist es Sache der Beklagten, ein bereits erfolgtes Bestreiten zu berücksichtigen. Durch das Versenden einer „Letzten Mahnung“ wird ein solches Bestreiten jedoch komplett ignoriert. Dem Adressaten der „Letzten Mahnung“ wird kommuniziert, dass seine bereits erfolgten Einwendungen rechtlich nicht erheblich seien, weswegen der Anspruch einredefrei und fällig sei. Die Beklagte kann sich auch nicht durch die Differenzierung zwischen „einredefrei“ und „unbestritten“ in der „Letzten Mahnung“ entlasten. Die Beklagte hat bei ihrer Wortwahl auf den Empfängerhorizont abzustellen. Nachdem sich die „Letzte Mahnung“ gerade nicht an Juristen richtet, muss sie bei Verwendung anerkannter rechtlicher Termini darauf achten, dass diese nicht missverständlich sind, was hier aber erkennbar nicht der Fall ist. Für einen juristischen Laien erschließt sich der Unterschied beider Termini nicht aus sich heraus.

Bei dem Hinweis auf die SCHUFA handelt es sich nicht lediglich um einen solchen auf eine bestehende Möglichkeit. Anders als in der Entscheidung des Hanseatischen OLG (5 U 174/11, Urteil vom 30.01.2013; zitiert nach-juris), kann der Formulierung nicht entnommen werden, dass ein Dritter die Eintragung veranlasst. Dies ergibt sich bereits aus einer Zusammenschau des Hinweises mit dem Satz zuvor, in dem von einer Berechtigung der Beklagten die Rede ist. Vor diesem Hintergrund kann der Hinweis auf das „können“ in dem folgenden Satz, der auf die Meldung an die SCHUFA zielt, nicht anders verstanden werden.

## Anspruch auf förmliche Rücknahme einer Abmahnung (Ls)

(Landesarbeitsgericht Niedersachsen, Urteil vom 20. November 2014 – 5 Sa 980/14 –)

**1. Ein Klageantrag auf „Rücknahme und Entfernung“ einer Abmahnung ist regelmäßig als einheitlicher Anspruch auf Beseitigung der durch die Abmahnung erfolgten Beeinträchtigungen des Persönlichkeitsrechtes zu verstehen. Daneben kann, neben einer begehrten Entfernung, auch der Widerruf der darin enthaltenen Äußerungen gemeint sein.**

**2. Ein Arbeitnehmer hat keinen Anspruch auf Abgabe einer förmlichen Rücknahmeerklärung einer Abmahnung, wenn zuvor der Arbeitgeber erklärt hat, er werde diese Abmahnung nicht für etwaige personelle Konsequenzen gegenüber dem Arbeitnehmer verwenden. Dies gilt auch, wenn er erklärt, er halte an der sachlichen Richtigkeit der dort erhobenen Vorwürfe fest.**

(Leitsatz zu 1 nicht amtlich)

## Kein Abwehrrecht von Mietern gegen als Attrappen bekannte Videokameras im Hauseingangsbereich (Ls)

(Amtsgericht Berlin-Schönefeld, Urteil vom 30. Juli 2014 – 103 C 160/14 –)

**1. Die Mieter eines Mehrfamilienhauses haben keine Abwehrrechte aus §§ 823 Abs. 1, 1004 BGB, wenn sie darüber informiert sind, dass es sich bei den zur Vermeidung von Vandalismusschäden installierten Videokameras um Attrappen handelt.**

**2. Ein einen Unterlassungsanspruch begründender „Überwachungsdruck“ könnte hier nur dann bestehen, wenn der Umtausch der Attrappen in aktive Kameras zu befürchten wäre.**

(Nicht amtliche Leitsätze)

## Posttraumatische Belastungsstörungen als Dienstoffall nach Einsicht in Personalakte (Ls)

(Verwaltungsgericht Aachen, Urteil vom 11. Dezember 2014 – 1 K 1161/13 –)

**1. Posttraumatische Belastungsstörungen infolge Einsicht in die Personalakte sind kein Dienstoffall, wenn ein in der Akte enthaltenes Schreiben des Personalrats allgemeine Negativ-Einschätzungen ohne beleidigenden Inhalt enthält.**

**2. Die Einsichtnahme ist insbesondere nicht dazu geeignet, eine psychische Erkrankung hervorzurufen, wenn der Betroffene über Existenz und Inhalt des Schreibens bereits zuvor informiert worden ist. Ein schockartiges Erleben durch das eigene Lesen ist schon wegen dieser Vorwarnung ausgeschlossen.**

(Nicht amtliche Leitsätze)

# Berichte, Informationen, Sonstiges

## 36. Internationale Datenschutzkonferenz auf Mauritius

Im Oktober 2014 war die Datenschutzaufsichtsbehörde von Mauritius (mit Unterstützung des Premierministers) Gastgeber der 36. Internationalen Datenschutzkonferenz unter dem Motto „Eine Weltordnung zum Datenschutz: Wird unser Traum wahr?“ Zum ersten Mal in ihrer Geschichte fand die Konferenz in Afrika statt. Mauritius, bei uns vor allem als exotisches Reiseziel bekannt, hat sich, neben dem weiteren Ausbau des Tourismus, die Informationstechnologie als Entwicklungsschwerpunkt gesetzt. Im Übrigen besteht ein starkes Interesse daran, die eigene Rechtsordnung internationalen Standards anzupassen – daher wird Mauritius auch als potentielles Beitrittsland für die Konvention Nr. 108 des Europarats angesehen.

Nur 187 Personen aus aller Welt nahmen an der Datenschutzkonferenz teil. Trotz der um rund zwei Drittel im Vergleich zu anderen Konferenzen geringeren Teilnehmerzahl, gab es Vorkonferenzen mit wichtigen Themen, während parallel der nichtöffentliche Teil der Konferenz stattfand. Das Global Privacy Enforcement Network (GPEN) hat zum ersten Mal auch für Nichtmitglieder eine öffentliche Veranstaltung durchgeführt. Prof. Graham Greenleaf stellte die frei zugängliche internationale Bibliothek zum Datenschutzrecht (Privacy Law) vor. Sie ist über [www.worldlii.org/int/special/privacy/](http://www.worldlii.org/int/special/privacy/) erreichbar und enthält neben verschiedenen Dokumenten zum Datenschutz vor allem auch Fallkonstellationen zu von Aufsichtsbehörden ergriffenen Maßnahmen. Die Bibliothek wird unter anderem die Aktivitäten der GPEN-Gruppe als gemeinsames Archiv unterstützen. Weitere Anstrengungen zur Verbesserung der internationalen Zusammenarbeit im Datenschutz übernimmt das von der EU maßgeblich geförderte PHAEDRA-Projekt. Das auf

zwei Jahre angesetzte Projekt, das sich unter anderem auf die Resolution von Mexiko-City zur internationalen Zusammenarbeit als Mandat stützt, hatte den ersten Workshop auf der 35. Konferenz 2013 in Warschau und danach zwei weitere Treffen. Im Rahmen der Vorkonferenz auf Mauritius wurde der vierte Workshop durchgeführt. Mit Ergebnissen ist auf der 37. Konferenz 2015 zu rechnen. Mit dem Mandat der Konferenz im letzten Jahr in Warschau leitet die französische Datenschutzaufsicht CNIL eine internationale Arbeitsgruppe zur digitalen Erziehung, bei der weltweit unterschiedliche Konzepte im Dialog mit Aufsichtsbehörden, Wissenschaft und Wirtschaft mit dem Ziel verglichen werden, vorbildliche Lösungen herauszuarbeiten. Auch hier ist mit Ergebnissen vorerst noch nicht zu rechnen. Seitens privater Organisationen fand als Vorkonferenzbeitrag eine Podiumsdiskussion zum Thema der Accountability statt, die auf Einladung von Nymity erfolgte und auf der u.a. der ausscheidende EU-Datenschutzbeauftragte Peter Hustinx sprach. Die Kriterien zur Entwicklung eines Datenschutzprogramms im Sinne der Accountability sind weiter verfeinert worden und wirken ausgereifter, müssen aber in einzelnen Punkten noch weiter ergänzt werden, so zum Beispiel hinsichtlich der Notwendigkeit der ausreichenden Berücksichtigung von Löschkonzepten. Microsoft hielt eine Podiumsdiskussion zur Frage der Selbstverpflichtungen zum Datenschutz bei den sog. „Trusted Clouds“ ab.

In ihrem öffentlichen Teil begann die 36. Internationale Datenschutzkonferenz mit einer Zusammenfassung des Vorsitzenden des Exekutivkomitees der Konferenz, Jacob Kohnstamm. Es wurden fünf Resolutionen verabschiedet.

Resolution zur Akkreditierung: Die Gruppe der vertretenen Aufsichtsbehörden hat sich weiter vergrößert. Für Deutschland ist die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen, neben Ghana und Sene-

gal, als neues Mitglied aufgenommen worden. Mehrere Organisationen haben Beobachterstatus erhalten, u.a. die Commodity Futures Trading Commission (CFTC) der USA.

Resolution zum Datenschutz im digitalen Zeitalter: In dieser Resolution begrüßt die Internationale Datenschutzkonferenz den Bericht des Hohen Kommissars der Vereinten Nationen für Menschenrechte vom 30.06.2014 (A/HRC/27/37), mandatiert das Exekutivkomitee, am Dialog zum Datenschutz im digitalen Zeitalter teilzunehmen, und fordert die Teilnehmer der Konferenz dazu auf, sich dafür einzusetzen, dass bei jeder elektronischen Überwachung als Minimum die Datenschutzgrundsätze der Erklärung von Madrid aus dem Jahr 2009 eingehalten werden. Zudem unterstützt die Konferenz den UN-Beschluss 68/167, nach dem jedermann die gleichen Rechte offline wie online haben muss, einschließlich des Rechts auf Datenschutz. Diese wichtige Resolution ist die Positionierung der Datenschutzaufsichtsbehörden mit Blick auf die Snowden-Affäre.

Resolution zu Big Data: Nach den Resolutionen der 34. und 35. Internationalen Datenschutzkonferenz zum Profiling bringt diese Resolution Bedenken zu Big Data zum Ausdruck, nicht ausschließlich hinsichtlich des Datenschutzes, sondern auch bei Themen wie Antidiskriminierung und Wahrung der Bürgerrechte. Zentraler Kritikpunkt aus Datenschutzsicht ist die Wiederverwendung von Daten, was notwendig mit den Grundsätzen der Zweckbindung und Datenvermeidung kollidiert. Daher wird die Beachtung der Zweckbindung, der Begrenzung der Datenerhebung auf den verfolgten Zweck sowie, soweit angebracht, das Einholen einer Einwilligungserklärung bei Analysen und Profilbildungen gefordert. Transparenz, Zugang zu den erhobenen personenbezogenen Daten und insbesondere auch Information über die Schlüsselemente der Entscheidungskriterien der zugrundelie-

genden Algorithmen, Durchführung von Datenschutzfolgeabschätzungen und Nutzung von Privacy by Design kommen hinzu. Entscheidend ist zudem die Anonymisierung bereits bei der Datenanalyse. Die Verwendung pseudonymisierter Daten ist sorgfältig zu prüfen. Insgesamt müssen Entscheidungen bei Einsatz von Big Data fair, transparent und verantwortlich getroffen werden.

Resolution zum Internet der Dinge: Die Resolution betont, angesichts der unaufhaltsamen technologischen Entwicklung, das Recht auf informationelle Selbstbestimmung – die persönliche Entwicklung eines Jeden soll nicht dadurch bestimmt werden, was Unternehmen und Regierungen über die betreffenden Personen wissen. Das Internet der Dinge potenziert die Gefahren von Big Data. Daher sollen Transparenz, Privacy by Design und Default sowie eine Ende-zu-Ende-Verschlüsselung als Lösungsansätze eingesetzt sowie Verstöße durch die internationale Gemeinschaft der Datenschutzaufsichtsbehörden angemessen geahndet werden.

Resolution zur Zusammenarbeit bei Aufsichtsmaßnahmen (Enforcement Cooperation): Die Grundlage der internationalen Zusammenarbeit der Datenschutzaufsichtsbehörden als Mitglieder der internationalen Datenschutzkonferenz wird mit dem nunmehr im Rahmen dieser Resolution verabschiedeten „Global Cross Border Enforcement Cooperation Arrangement“ weiter ausgebaut. Das elfseitige Papier ist als Positionierung ohne rechtlich verbindliche Verpflichtung anzusehen, was verständlich ist, da die jeweiligen Datenschutzaufsichtsbehörden (Privacy Enforcement Authorities) jeweils ihrem eigenen nationalen Recht als Handlungsgrundlage unterworfen sind. Als gemeinsame Grundsätze werden betont: Gegenseitigkeitsprinzip, Vertraulichkeit und der gegenseitige Respekt für die unterschiedlichen Datenschutzgrundsätze. Daneben werden Verfahrensfragen geregelt, worin vor allem das Exekutivkomitee der internationalen Datenschutzkonferenz unterstützt wird, unter anderem durch eine Bewertung der in der Resolution gere-

gelten Zusammenarbeit nach drei Jahren. Durch die Resolution zur Enforcement Cooperation nimmt das seit Jahren diskutierte Thema, zu dem sich bereits die GPEN-Gruppe engagiert, deutlich an Fahrt auf.

Die Datenschutzkonferenz beschäftigte sich vor allem vor dem Hintergrund des diesjährigen Mottos „Eine Datenschutzweltordnung: Wird unser Traum wahr?“ mit bekannten Themen, so Interkonnektivität und Datenschutz ohne territoriale Grenzen, sowie mit der Tatsache, dass in Entwicklungsländern nunmehr von Jahr zu Jahr eigene Datenschutzgesetze verabschiedet werden. Für Afrika sprach die Leiterin der Datenschutzaufsicht von Burkina Faso, das in 2014 ein Datenschutzgesetz verabschiedet hat. In ihrer Rede machte sie deutlich, dass immer mehr afrikanische Staaten Datenschutzgesetze verabschieden werden. Frau Falque-Pierrotin, Chefin der CNIL und Vorsitzende der Art. 29 Gruppe, sprach sich für einen pragmatischen Ansatz bei der Weiterentwicklung des Datenschutzes aus, der auch in der Resolution zur Zusammenarbeit von Aufsichtsmaßnahmen zum Ausdruck kommt. Man sei sich trotz aller Unterschiede einig in dem, was Datenschutz leisten soll, nämlich die Betroffenen angemessen zu schützen. Der Datenschutzbeauftragte von Hongkong zeigte anhand von vier Aufsichtsfällen seiner Behörde auf, dass die bekannten Grundsätze der Zweckbindung, Verhältnismäßigkeit und Transparenz gute Grundlagen zur Durchsetzung von Datenschutzprinzipien im Einzelfall sind. Die Vertreter der FTC betonten erneut die Notwendigkeit, eine globale Interoperabilität zu schaffen. Hinsichtlich der Entwicklung im eigenen Land, der Consumer Privacy Bill of Rights zum Datenschutz von 2012, war nichts Neues zu hören. Es bleibt abzuwarten, ob die Ankündigung von Präsident Obama vom 15. Januar 2015 über die beabsichtigte Einführung eines Bundesgesetzes zum Datenschutz in Form der Consumer Privacy Bill of Rights neuen Auftrieb für die Entwicklung des Datenschutzes in den USA gibt.

Auf der Konferenz wurden ebenfalls ausführlich die EU-Reformvorhaben

vorgelegt. Als eine der grundsätzlichen Differenzen zwischen EU und USA wurden die Unterschiede im Verständnis des Verhältnismäßigkeitsprinzips genannt. Wie auch in den vergangenen Jahren fand eine Vielzahl von parallelen Diskussionen zu unterschiedlichen Datenschutzthemen statt, von denen vor allem die Diskussion um den Vergleich von APEC Cross Border Privacy Rules (CBPR) zu den EU Binding Corporate Rules hervorzuheben ist. Unter der Leitung der französischen Datenschutzaufsicht mit Teilnahme eines Vertreters des US Departments of Commerce sowie Wirtschaftsvertretern und Wissenschaftlern wurde das Thema kontrovers diskutiert. Vor allem Prof. Graham Greenleaf von der Universität von New South Wales machte deutlich, wie weit die beiden Regelungen in der Praxis noch voneinander entfernt sind. Zum Beispiel ist eine Zertifizierung nach CBPR für Endverbraucher wenig aussagekräftig, da die Zertifizierung sich nur auf die Daten erstreckt, die das Unternehmen zu exportieren beabsichtigt, nicht aber auf die tatsächlich von dem Unternehmen erhobenen und verarbeiteten Daten. Zum Abschluss wurde das komplexe Thema Ethik, Menschenrechte und Big Data diskutiert. Mit dem Big Data Ethics Projekt, das von Firmen unterstützt wird, soll versucht werden, eine weltweit einheitliche ethische Grundlage für Datenverarbeitungen zu finden. Ob es hierzu aber überhaupt einen Lösungsansatz geben kann, blieb offen.

Der langjährige Vorsitzende der Internationalen Datenschutzkonferenz, der niederländische Datenschutzbeauftragte Jakob Kohnstamm, hat seinen Vorsitz niedergelegt und an den Privacy Commissioner Neuseelands, John Edwards, übergeben. Der Dialog wird auf der 37. Internationalen Datenschutzkonferenz in Amsterdam im Oktober 2015 fortgesetzt. Die Konferenz findet voraussichtlich vom 26. bis 29.10.2015 statt.

*(Paul Gürtler, TARGOBANK, Düsseldorf)*

*Der Bericht gibt ausschließlich die persönliche Meinung des Referenten wieder.*

## Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Dezember 2014:

### Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, – zum Teil mehrfach wöchentlich – von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz – GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen

Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“ gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

### Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI):

#### Datenschutzverstoß als Wettbewerbsverstoß

Im Rahmen eines Sondergutachtens zum Wettbewerb auf digitalen Märkten gemäß § 44 GWB hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) zu Fragen der Monopolkommission im Schnittpunkt zwischen Datenschutz- und Wettbewerbsrecht Stellung genommen. Im Rahmen des Sondergutachtens regt der HmbBfDI unter anderem an, künftig darüber nachzudenken, Verstöße gegen Datenschutzregeln einem Wettbewerbsverstoß gleichzusetzen. Bezüge zwischen Datenschutz und Wettbewerbsrecht gingen wesentlich weiter, als die uneinheitliche und in sich widersprüchliche Rechtsprechung dies nahe lege.

Den Umstand, dass Datenmacht dazu tendiere, die Marktmacht von Unternehmen zu festigen, und umgekehrt die Marktmacht globaler Akteure das Entstehen von Datensammlungen über Massen von persönlichen Informationen begünstige, wird in der Stellungnahme anhand der Beispiele von

facebook und google belegt, wo teilweise Verstöße gegen Datenschutz im Zusammenhang mit der Verbesserung der eigenen Marktstellung des Unternehmens erfolgten.

In Konsequenz wird die Forderung nach einer Gesetzesinitiative formuliert, da die Linie der Gerichte in der Schnittmenge von Datenschutzverstoß und Wettbewerbsverstoß uneinheitlich sei und bislang keine Rechtssicherheit herrsche. Hier gelte es, die Bedeutung des Neben- und Miteinander beider Regelungsbereiche auch und gerade im Zuge der europäischen Rechtsentwicklung mit Blick auf die EU-Datenschutzgrundverordnung im Auge zu behalten.

Damit wären nach Ansicht des HmbBfDI in Zukunft auch alle Wettbewerber in der Lage, Datenschutzverstöße über das UWG im Wege des wettbewerblichen Unterlassungsanspruchs geltend zu machen. Eine Ausweitung der Marktmacht über Datenschutzverstöße zu verhindern, wie auch zum Vollzug der Datenschutzregelungen zugunsten der Datensouveränität des Individuums beizutragen, könne dann letztlich auch in den Händen der jeweils anderen Marktteilnehmer selbst liegen, der dazu nicht nur das eigene wirtschaftliche Interesse, sondern auch die erforderlichen finanziellen Ressourcen und den Sachverstand für eine zügige Rechtsverfolgung habe. Datenschutzrecht müsse daneben auch Anwendung finden, wenn es um die kartellrechtliche Prüfung von Firmenzusammenschlüssen gehe.

### Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein:

#### Auftraggeberhaftung für den „Mindestlohn“ aus Datenschutzsicht

In dem Informationstext des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) wird dargelegt, dass es zur Vermeidung von Haftungsrisiken nach dem „Mindestlohngesetz“ in der Regel weder erforderlich noch zulässig ist, Beschäftigtendaten von einem beauftragten Unternehmen an den Auftraggeber zu übermitteln:

Ein Unternehmer, der einen anderen Unternehmer mit der Erbringung von Werk- oder Dienstleistungen beauftragt, haftet für die Verpflichtungen dieses Unternehmers, eines Nachunternehmers oder eines von dem Unternehmer oder einem Nachunternehmer beauftragten Verleihers zur Zahlung des Mindestentgelts an Arbeitnehmerinnen oder Arbeitnehmer oder zur Zahlung von Beiträgen an eine gemeinsame Einrichtung der Tarifvertragsparteien wie ein Bürge, der auf die Einrede der Vorausklage verzichtet hat. Die entsprechende Bestimmung nach § 14 Satz 1 des Arbeitnehmerentendegesetzes (AEntG) gilt nach § 13 des Mindestlohngesetzes auch für Unternehmer, welche einen anderen Unternehmer mit der Erbringung bestimmter Werk- oder Dienstleistungen beauftragt haben. Der jeweilige Auftraggeber haftet dann dafür, dass die von ihm beauftragten Unternehmer sowie die von diesen beauftragten Subunternehmer ihren Arbeitnehmerinnen und Arbeitnehmern den gesetzlich zustehenden Mindestlohn zahlen.

Die damit verbundene verschuldensunabhängige Haftung des Auftraggebers kann durch keine noch so sorgfältige Auswahl und Überwachung der Nachunternehmer ausgeschlossen werden. Das führt jedoch nicht zur Unverhältnismäßigkeit dieser Haftungsregelung (BAG, Beschluss v. 06.11.2002, 5 AZR 617/01 = NZA 2003, 490, 496 bzgl. einer Haftung nach § 14 AEntG). Der Auftraggeber ist gehalten, sein Haftungsrisiko durch geeignete Maßnahmen zu verringern.

Dabei wird von der Auftraggeberseite nicht selten die Erhebung und Verarbeitung personenbezogener Daten der Arbeitnehmerinnen und Arbeitnehmer des beauftragten Unternehmers in Erwägung gezogen. Der Auftraggeber und auch die beauftragten Unternehmen und Subunternehmen müssen bei der Auswahl und dem Einsatz der Kontrollmittel die datenschutzrechtlichen Anforderungen einhalten. Aus Sicht des Auftraggebers ist zu prüfen, inwieweit die Erhebung und Speicherung der personenbezogenen Beschäftigtendaten als Mittel für die Erfüllung eigener Geschäftszwecke zur

Wahrung berechtigter Auftraggeberinteressen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Der beauftragte Unternehmer sowie die Subunternehmer müssen untersuchen, ob die Übermittlung personenbezogener Daten ihrer Beschäftigten für die Durchführung des Beschäftigungsverhältnisses erforderlich ist (§ 32 Abs. 1 Satz 1 BDSG). Dabei darf keine pauschale Bewertung erfolgen, es bedarf einer Prüfung im konkreten Einzelfall.

Vor diesem Hintergrund ist es datenschutzrechtlich nicht zulässig, wenn der Auftraggeber auf Basis einer vertraglichen Abrede mit dem beauftragten Unternehmer bei diesem einen pauschalen Zugriff auf bestimmte arbeitsvertragliche Unterlagen möglicherweise aller Beschäftigten oder gar auf deren Personalakten erhält. Ebenso unzulässig ist die Übermittlung nichtanonymisierter Gehaltsbescheinigungen.

Angaben z.B. zur Konfessionszugehörigkeit, zum Familienstand, zur gewählten Steuerklasse, zur Anzahl der Kinder, zum vollständigen Geburtsdatum und zur Privatanschrift des Beschäftigten stellen Angaben dar, deren Erhebung zur Verringerung des Haftungsrisikos für den Auftraggeber nicht erforderlich sind.

Regelmäßig ergeben sich schon aus einem Angebot Indizien dafür, dass keine Mindestlöhne bezahlt werden. Ein Auftraggeber muss alle Möglichkeiten ausschöpfen, um ohne zuordenbare Beschäftigtendaten sein Haftungsrisiko zu verringern. Zur Begrenzung seiner Haftung muss der Auftraggeber zunächst auf Maßnahmen zurückgreifen, bei denen eine Erhebung personenbezogener Daten entbehrlich ist. Hierzu zählt, dass sich der Auftraggeber einen Teil seines Haftungsrisikos durch eine vom beauftragten Unternehmer beizubringende Bankbürgschaft absichern lässt. Der Auftraggeber kann bezüglich der Beauftragung weiterer Subunternehmer einen vertraglichen Zustimmungsvorbehalt mit dem zu beauftragenden Unternehmer vereinbaren. Es ist möglich,

dass sich der zu beauftragende Unternehmer verpflichtet, den Auftraggeber von Forderungen der Beschäftigten weiterer Subunternehmer auf Zahlung des Mindestlohnes freizustellen (vgl. BAG, Urteil v. 12.01.2005, 5 AZR 617/01 = NZA 2005, 627, 633 bzgl. einer Haftung nach § 14 AEntG). Weiterhin kann sich der Auftraggeber von den zu beauftragenden Unternehmern vertraglich unter Aufnahme einer Vertragsstrafenregelung zusichern lassen, die Verpflichtungen nach dem Mindestlohngesetz einzuhalten. Die vertragliche Verpflichtung der zu beauftragenden Unternehmer sollte sich darauf erstrecken, die Subunternehmer einer gleichlautenden Bestimmung zu unterwerfen. Zulässig ist Schließlich die Übersendung anonymisierter Aufzeichnungen über erbrachte Arbeitsstunden und gezahlte Arbeitsentgelte der eingesetzten Mitarbeiter.

*(Pressemitteilung vom 06.02.2015; /artikel/871-Auftraggeberhaftung-fuer-den-Mindestlohn-aus-Datenschutzsicht.html)*

## **BITKOM kritisiert Verbandsklagerecht beim Datenschutz: Stellung des Datenschutzbeauftragten wird geschwächt**

Der Digitalverband BITKOM hat das vom Bundeskabinett beschlossene Verbandsklagerecht beim Datenschutz scharf kritisiert. „Ein starker Datenschutz ist wichtig, aber das Verbandsklagerecht schafft mehr Probleme, als dass es den Verbrauchern tatsächlich nützt“, sagte BITKOM-Präsident Prof. Dieter Kempf. Anders als in anderen Bereichen gebe es mit den Datenschutzbeauftragten in den einzelnen Bundesländern bereits Instanzen, die Verbraucher bei Verstößen gegen das Datenschutzrecht unterstützen. „Die Datenschutzbeauftragten ermitteln, wenn sie Hinweise oder Beschwerden von Verbrauchern erhalten, und leiten bei Bedarf weitere Schritte ein“. Mit dem Aufbau paralleler Strukturen

werde die Stellung der Datenschutzbeauftragten geschwächt. Zudem könnten die Verbraucherschützer schon jetzt gegen Unternehmen klagen, wenn diese in den Allgemeinen Geschäftsbedingungen (AGB) gegen Datenschutzvorschriften verstoßen. Für Unternehmen, die Daten von Kunden verarbeiten, werde die Rechtsunsicherheit steigen, wenn es verschiedene Rechtswege gibt.

Aus Sicht des BITKOM wird das deutsche Verbandsklagerecht weit über die geplante EU-Datenschutzgrundverordnung hinausgehen. Damit würde das neue deutsche Recht gegen die angestrebte Harmonisierung in der EU verstoßen. Die nationale Regelung werde nur so lange gelten, bis die EU-Datenschutzgrundverordnung in Kraft trete. Positiv wertet der BITKOM, dass der Anwendungsbereich des Gesetzes im Vergleich zu früheren Überlegungen eingeschränkt wurde. So soll ein Verbandsklagerecht nur möglich sein, wenn Unternehmen personenbezogene

Daten kommerziell nutzen. Klagen sind dagegen nicht erlaubt, wenn die Unternehmen zur Datenverarbeitung gesetzlich oder vertraglich verpflichtet sind.

*(Auszug aus einer BITKOM Pressemitteilung vom 04.02.2015)*

## Akzeptanz des vernetzten Autos

Nach den Ergebnissen einer repräsentativen Umfrage im Auftrag des Digitalverbands BITKOM können sich 35 Prozent der Autofahrer in Deutschland grundsätzlich vorstellen, Fahrzeugdaten an Dritte zu übermitteln. Bei den 14- bis 29-Jährigen ist es mit 54 Prozent sogar die Mehrheit. Voraussetzung ist für die meisten Befragten allerdings, dass sie dafür einen Gegenwert erhalten, zum Beispiel Rabatte bei ihrer Kfz-Ver-

sicherung (25 Prozent) oder in Form nützlicher Informationen wie Routenvorschläge oder Stauinfos (21 Prozent). 9 Prozent würden Daten auch ganz ohne Gegenleistung zur Verfügung stellen.

Die Umfrage zeigt, dass die Bürger neuen Diensten wie dem E-Call-Notruf offen gegenüber stehen, aber die Folgen für ihre Privatsphäre im Blick haben. So halten zwar 39 Prozent der befragten Autofahrer das E-Call-System für uneingeschränkt sinnvoll. 48 Prozent befürworten das System dagegen nur unter der Voraussetzung, dass die Weitergabe von Daten genau geregelt ist. 12 Prozent sehen das Projekt grundsätzlich kritisch. Zudem sind fast drei Viertel (74 Prozent) der Befragten der Ansicht, dass jeder Autofahrer selbst entscheiden sollte, ob das automatische Notrufsystem im Fahrzeug aktiviert wird.

*(Auszug aus einer BITKOM Pressemitteilung vom 18.02.2015)*

# Literaturhinweise

## Buchbesprechungen

Gregor Thüsing, **Beschäftigtendatenschutz und Compliance**, Verlag C.H. Beck, 2. Aufl., München, 2014, 424 S., kartoniert 89,00 €

Die Anforderungen an Unternehmen zur Verhinderung von Straftaten rücken von Jahr zu Jahr mehr ins Bewusstsein von Juristen und einer immer breiteren Öffentlichkeit. Werden diese Anforderungen nicht erfüllt, drohen Management und Unternehmen Haftung und Sanktionen. Viele Unternehmen haben daher detaillierte Compliance- und Betrugsbekämpfungsprogramme eingeführt. Durch das Gesetz vom 3. Juli 2009 hat der Gesetzgeber die Voraussetzungen für den zulässigen Umgang mit Arbeitnehmerdaten nochmals erhöht.

Dieses Werk soll für die Praxis Hilfestellung geben, Compliance und Datenschutz zu einem angemessenen Ausgleich zu bringen. Ein Formulierungsvorschlag für eine rechtssichere Betriebsvereinbarung sowie weitere wichtige Praxistipps machen das Werk für jedes Unternehmen sowie für Berater besonders interessant. Die Neuauflage bringt das etablierte Werk auf den neusten Stand und erweitert die Themen um

- Social Media
- BYOD
- Datenschutz im internationalen Konzern
- Whistleblowing und
- Datenverarbeitung in der Cloud

Der Band richtet sich an Vorstände und Geschäftsführer von Unternehmen, Aufsichtsgremien in Unternehmen, Compliance-Officer, Revisionsleiter sowie Juristen in Rechtsabteilungen, Rechtsanwälte als rechtliche Berater von Unternehmen und an Betriebsräte.

Beatrice Lederer, **Open Data – Informationsöffentlichkeit unter dem Grundgesetz**; Internetrecht und Digitale Gesellschaft (IDG), Band 1, Duncker & Humblot, Berlin, 2015, 566 S. Print: 89,90 €, E-Book: 79,90 €

Wissen ist seit jeher Macht. Und seit jeher ist es Grundgedanke der Demokratie, den Einzelnen an der Ausübung von Macht teilhaben zu lassen. Trotzdem ist die Teilhabe des Einzelnen am staatlichen Wissen noch immer die Ausnahme. Doch staatliche Informationen können in der Informationsgesellschaft des 21. Jahrhunderts zugänglich gemacht werden. Und sie müssen es: Das Internet hat das Verhältnis zwischen Staat und Bürger verändert. An die Stelle eines Über-/Unterordnungsverhältnisses tritt zusehends eine Interaktion auf Augenhöhe. Bei der Auslegung der Anforderungen, die das Grundgesetz an die Ausgestaltung des demokratischen Rechtsstaats stellt, ist dieser Wandel zu berücksichtigen. In einer Gesamtschau von Informationsfreiheit und demokratischem Rechtsstaat führt dies zu einer Pflicht des Staats, Informationen öffentlich zugänglich zu machen. „Transparenz“ und „Open Data“ sind mehr als Schlagworte der politischen Diskussion. Sie sind Funktionsbedingung des demokratischen Rechtsstaats im 21. Jahrhundert.

Die Arbeit wurde mit dem Wissenschaftspreis der Universität Passau 2014 und dem Wissenschaftspreis der Deutschen Stiftung für Recht und Informatik 2014 ausgezeichnet.

(Redaktion)

Marc Osken, **Die schlichte Einwilligung im Urheberrecht – Eine Untersuchung unter Berücksichtigung der Vorschau-Bilder-Rechtsprechung des BGH**, Verlag Peter Lang GmbH, Frankfurt/Main, 2014, 377 S. 71,95 €.

Mit Formulierungen wie z.B. „Verdinglichung bzw. Vergegenständlichung“,

„obligatorisch wirkender schuldvertraglicher Gestalt“, „Eigentumsplitter“, „Urheberrechtssplitter“, „Rechtssparomie“, „Wille zur Konsentierung“, „Revokationsakt“, „praktisch undenkbar“ sowie der Aufforderung an den Gesetzgeber, seine Terminologie zu übernehmen (S. 26), versucht der Autor, nicht vorhandene Wissenschaftlichkeit vorzutäuschen. Höhepunkt seiner Ausführungen ist der dumm-dreiste Satz „die Frage stellen heißt, sie zu verneinen.“

Sofern er andere Autoren oder die Entscheidungen des BGH zitiert, empfiehlt es sich daher, diese nur im Original anzusehen. Praktisch ist diese Dissertation wertlos. Für die Qualitätsmängel ist der Doktorvater Prof. Ralph Backhaus, auf dessen mangelhafte Ausführungen zu § 97 UrhG kritiklos hingewiesen wird, mit verantwortlich.

Die im Tatbestand von § 106 UrhG genannte Einwilligung erwähnt Osken nur oberflächlich. Meine Darlegung zur Einwilligung im Urheberrecht/Strafrecht, zur Einwilligung bei unbekanntem Aufenthalt, die postmortale Einwilligung im Urheberrecht, die vermutete Einwilligung und die Relevanz eines Irrtums über die Einwilligung (Mestmäcker/Schulze/Deumeland, Kommentar zum deutschen Urheberrecht, April 2005, § 106 Rn. 10-24) übergeht er. Ebenso verschweigt er die ausgezeichnete Kommentierung von § 106 UrhG durch B. Heinrich im Münchener Kommentar zum StGB (2010, Band 6/1).

Verwerflich ist die zitatlöse Übernahme der fehlerhaften Behauptung, nach § 51 UrhG dürfe nur in ein urheberrechtlich geschütztes Werk zitiert werden (S. 316; vgl. Rehbinder, UrhR, 16. Aufl. 2010, Rn. 488). Wie grob fehlerhaft eine solche Aussage ist, hatte ich bereits im Jahre 2004 dargelegt (Mestmäcker/Schulze/Deumeland, Kommentar zum deutschen Urheberrecht, Juni 2004, § 51 Rn. 6; ebenso

Cherpillod, in: Schweizerisches Immaterialgüter- und Wettbewerbsrecht, 2. Aufl. 2006, 2. Band, 1. Teilband, S. 298 Fn. 135). Meiner Ansicht hat sich der EU-Gerichtshof im Luxemburg durch Urteil v. 1.12.2011 uneingeschränkt angeschlossen (GRUR Int 2012, 167; zustimmend Dreyer/Kotthoff, UrhR, 3. Aufl. 2013, § 51 Rn. 4 und 11). Das verschweigt Osken, und daher ist seine Dissertation nicht nur lächerlich und unnützlich, sondern auch irreführend.

Das Buch ist den überhöhten Preis nicht wert.

*(Klaus Dieter Deumeland, Hochschul-lehrer für Rechtswissenschaften a.D.)*

**Wolfgang Däubler, Gläserne Beleg-schaften**, Bund-Verlag, 6. Aufl., 2015, 724 S., 59,90 €

Der „Däubler“ ist inzwischen als ein Standardwerk anzusehen, das jeder, der sich mit dem Arbeitnehmerdatenschutz zu beschäftigen hat, kennen muss. Es ist nicht nur ein tägliches Handwerkszeug für Praktiker wie Datenschutzbeauftragte, Betriebsräte, Rechtsanwälte oder Rechtsabteilungen der Unternehmen, sondern hilft gleichermaßen der dogmatischen Durchdringung und Fortbildung des wissenschaftlichen Meinungsstands eines überaus komplexen Rechtsgebiets. Dass Däubler trotz vereinzelter etwas stärker der Arbeitnehmersichtweise zugeneigten Beurteilungen eine insgesamt sehr ausgewogene Gesamtdarstellung vorlegt, unterstreicht die hohe Qualität des zu Recht als „Handbuch“ ausgewiesenen Werks.

Das Themenspektrum, das der Arbeitnehmerdatenschutz umschließt, wird vom Autor gründlich unter Berücksichtigung der wichtigsten, vor allem auch aktuellen Literatur und Rechtsprechung abgehandelt, so dass der interessierte Leser ausreichend Gelegenheit erhält, im Einzelfall

seinen weitergehenden Informationsbedarf zu decken. Das Buch ist in 17 Kapitel gegliedert, die im Wesentlichen der Struktur der Voraufgaben angepasst sind. Zu ihnen zählen

- die Diskussion der Einwilligung im Arbeitsverhältnis als Rechtfertigungstatbestand (§ 4),
- die Erörterung der Zulässigkeitsbedingungen bei der Datenerhebung, und zwar in Bezug auf Bewerber (§ 5) wie auf Arbeitnehmer (§ 6),
- die Behandlung des Zulässigkeitsrahmens bei Datenauswertungen und -übermittlungen (§§ 7-9),
- die Darstellung der Rechte der betroffenen Beschäftigten (§§ 10 und 11) sowie
- der Kontrollmechanismen (§§ 12-15).

Die beiden letzten Kapitel befassen sich mit dem staatlichen Zugriff auf Beschäftigtendaten (§ 16) sowie mit einer Auflistung eher rechtspolitisch ausgerichteter Themen, sozusagen Merkposten, die zu weitergehenden Diskussionen anregen sollen (§ 17, beispielsweise Rn. 949 ff: „Die nicht bewältigten Probleme“).

Däubler hat im Vergleich zur Voraufgabe nicht nur seine Ausführungen zu einzelnen in der Praxis besonders relevanten Fragenkomplexen „aufgebohrt“, sondern auch neue Themen aufgenommen, so dass der Umfang um 100 Seiten zunahm. Insoweit sind beispielhaft zu erwähnen die Abschnitte betr.

- die Überwachung des Arbeitsverhaltens (Rn. 297 ff.),
- Geltung/Anwendungsgrenzen der §§ 88 ff. TKG im Arbeitsverhältnis (Rn. 336 ff., 378 ff.),
- die Behandlung von Emails ausgeschiedener/wegen Krankheit länger abwesender Mitarbeiter (Rn. 354 a f.),
- Überwachung im Call Center (Rn. 378 d ff.)
- Compliance (427k ff.).

Die umfassende Themenbehandlung und die kritische, aber faire Auseinandersetzung mit divergierenden Meinungen vermitteln dem Leser ein hohes Maß an Information. Dabei werden ihm durch die klare, schnörkellose Sprache des Verfassers die Lektüre und damit das Verständnis sehr erleichtert. Kurzum: Ein überaus gelungenes, rundum empfehlenswertes Werk, das weite Verbreitung verdient.

*(Rechtsanwalt Dr. Georg Wronka, Bonn)*

**Oliver Busch (Hrsg.), Realtime Advertising – Digitales Marketing in Echtzeit: Strategien, Konzepte und Perspektiven**, Springer Gabler, Wiesbaden, 2014, 252 S., € 39,99

Dieses Grundlagenwerk zu Realtime Advertising erklärt praxisnah und fundiert, welche Rolle automatisierte Echtzeit-Werbung in einem orchestrierten Media-Mix spielt und wie sie von Grund auf funktioniert. Denn: Realtime Advertising ist für Marketingverantwortliche so neu, bedrohlich und chancenreich wie die Internetwerbung zur Jahrtausendwende und selbst für viele Marketing- und Mediaexperten erklärungsbedürftig.

28 Branchenexperten aus Unternehmen, Agenturen und Medien erläutern diese revolutionäre Art des digitalen Marketing. Aufgezeigt werden:

- die Anbieterseite: Werbeplatzvermarktung und Technik
- die Nachfragerseite: Kampagnenkonzeption und Kreativität
- die Praxis: Best Cases und Erfahrungswerte

mit klaren Handlungsempfehlungen und handfesten Praxistipps für die begonnene Transformation des Marketings.

*(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.

*Tobias Born*, **Bonitätsprüfungen im Online-Handel**, ZD 2015, S. 66 ff.

Bonitätsprüfungen sind zulässig bei Bestehen eines potenziellen Zahlungsausfallrisikos. Beim Online-Handel hängt dies von dem vom Kunden gewählten bzw. ihm anzubietenden Zahlungsmodus ab. Unproblematisch ist es, wenn die Bonitätsprüfung nach der Entscheidung des Kunden über die Zahlungsart erfolgt. Soll sie bereits zuvor erfolgen, um direkt bestimmte Zahlungsarten nicht anzubieten, bedarf sie der Einwilligung.

*Jörg Feige*, **Personaldaten(über)fluss – Konzerne als illegale Datensammler**, ZD 2015, S. 116 ff.

Aufgezeigt werden u.a. die §§ 32 Abs. 1 S. 1 und 28 Abs. 1 S. 1 Nr. 2 bzw. Abs. 2 S. 2 a BDSG als Zulässigkeitsnormen für konzerninterne Personaldatenübermittlungen.

*Christian Galetzka*, **Datenschutz und unlauterer Wettbewerb**, K&R 2015, S. 77 ff.

Der Beitrag geht der Frage nach, ob Verstöße gegen datenschutzrechtliche Vorschriften wettbewerbslich abgemahnt werden können und weist dazu Datenschutzvorschriften des BDSG zumindest dann marktverhaltensregelnde Funktionen gemäß § 4 Nr. 11 UWG zu, wenn sie die Zulässigkeit und Transparenz der kommerziellen Verwertung von Kundendaten regeln.

*Peter Gola/Christoph Klug*, **Die Entwicklung des Datenschutzrechts im zweiten Halbjahr 2014**, NJW 2015, S. 674 ff.

Aufgelistet wird in der seit über 35 Jahren stattfindenden Berichterstattung die wichtigste Entwicklung in Gesetzgebung, Rechtsprechung und Literatur mit den Schwerpunkten Telekommunikation, Beschäftigten- und Kundendatenschutz und Internationales.

*Martin Greßlin*, **Umgang mit Bewerberdaten – was geht und was geht nicht?** BB 2015, S. 117 ff.

Die Speicherung von Bewerberdaten ist bezüglich ihrer zulässigen Dauer bisher nicht hinreichend klar. Der Verfasser befürwortet eine Speicherdauer von 5 Monaten, zusammengesetzt aus der Ausschlussfrist des § 15 Abs. 4 AGG und der anschließenden Frist zur gerichtlichen Geltendmachung in § 61b Abs. 1 ArbGG. Es werden die anschließende Löschung bzw. Sperrung, das Anlegen einer Bewerberdatenbank, die Folgen unzulässiger Erhebung und Speicherung sowie Gestaltungsmittel zur Erweiterung des Handlungsspielraums dargestellt.

*Thomas Helbing*, **Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung**, K&R 2015, S. 145 ff.

Der Beitrag erläutert den Zweckbindungsgrundsatz, stellt dessen Umsetzung im deutschen Recht dar und untersucht auf dieser Grundlage typische Fallgruppen von Big Data-Anwendungen unter spezieller Betrachtung der Werbung.

*Michael Knopp*, **Dürfen juristische Personen zum betrieblichen Datenschutzbeauftragten bestellt werden?**, DuD 2015, S. 98 ff.

Der Autor argumentiert gegen die gestellte Frage negativ beantwortende Stimmen der Literatur und der Aufsichtsbehörden und sieht u.a. die Anforderungen an einen externen DSB auch durch juristische Personen – ggf. sogar besser – als erfüllbar an.

*Flemming Moos*, **Die Entwicklung des Datenschutzrechts im Jahre 2014**, K&R 2015, S. 158 ff.

Aufgezeigt werden besonders praxisrelevante Aktivitäten des Gesetzgebers und ausgewählte kommentierte Rechtsprechung im Berichtszeitraum.

*Fabian Novara*, **Bewerberauswahl nach Kundenwünschen?**, NZA 2015, S. 142 ff.

Der Beitrag geht der Frage nach, ob eine Ungleichbehandlung nach dem AGG durch subjektive Erwartungen Dritter, d.h. z.B. durch vermutete Wünsche der Kunden hinsichtlich des sie bedienenden Personals, nach § 8 Abs. 1 AGG gerechtfertigt sein kann. Letztlich sei eine Ungleichbehandlung auf Grund eines unternehmerischen Konzepts bzw. wirtschaftlicher Nachteile nur in engen Fällen zulässig.

*Tim Wybitul*, **E-Mail-Auswertung in der betrieblichen Praxis – Handlungsempfehlungen für Unternehmen**, NJW 2014, S. 3605 ff.

Der Autor greift die Problematik der Auswertung privater E-Mails im Betrieb auf. Hierbei geht er insbesondere auf mögliche Verstöße des Arbeitgebers gegen das Fernmeldegeheimnis (§ 88 TKG, § 206 StGB), ein. Um die Risiken eines solchen Rechtsverstoßes zu vermeiden, werden Hinweise gegeben.



Wie sicher sind unsere Datenvorräte?

## Zweierlei Maß bei der Vorratsdatenspeicherung

Vorratsdatenspeicherung mag niemand. Es ist keine angenehme Vorstellung, dass der Staat Zugriff auf persönliche Daten erhält und uns gegebenenfalls kontrollieren kann. Auf der anderen Seite würde die Vorratsdatenspeicherung, wenn sie einmal eingeführt würde, festen Regeln folgen. Welche Daten unter welchen Voraussetzungen erhoben und gespeichert würden, wäre gesetzlich festgelegt und der ohnehin schon an die Grundrechte gebundene Staat müsste sich kontrollieren lassen.

Auch Datendienste wie Google, Facebook & Co. speichern massenhaft Daten auf Vorrat. Sie legen die Verwendungszwecke für ihr Sammeln und Verwerten aber weder fest noch offen. Sie sind zwar auch an das Recht gebunden. Das unterscheidet sich aber

in den EU-Staaten, in den USA und sonst wo auf der Welt. Es gibt Schlupflöcher und bei der Rechtsverfolgung fällt man leicht durchs Rost. Zudem nutzen wir die Dienste obwohl sie rechtswidrig sind und beschwerten uns nicht.

Dennoch hat der Staat in Sachen Vorratsdatenspeicherung den viel übleren Leumund. Was macht private Onlinedienste in Sachen Vorratsdatenspeicherung denn harmloser und sympathischer als den Staat? Der Nutzungszweck wohl kaum. Staaten verfolgen in erster Linie Sicherheitsinteressen. Das ist in Zeiten des internationalen Terrors ein berechtigtes Anliegen. Private Unternehmen wollen Daten in erster Linie wirtschaftlich nutzen. Das adelt die private Vorratsdatenspeicherung nicht.

Vielleicht liegt der Unterschied darin, dass der Staat uns für die Überwachung nur Sicherheit anbieten kann und die – so denken viele – muss er auch ohne Vorratsdatenspeicherung gewährleisten. Die privaten Dienste bieten uns aber für unsere Daten einen spürbaren Nutzen. Wir wollen deren Segnungen nicht mehr missen und glauben nicht, dass sie uns im Zweifel etwas anhängen wollen. Dass private Vorratsdatenspeicherung wirklich harmloser ist als staatliche, muss sie aber erst beweisen.

