ISSN 0178-8930

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

4/2014

Recht der Datenverarbeitung

Herausgegeben von

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

Aufsätze

LÜDEMANN / SENGSTACKEN – Lebensretter eCall: Türöffner für neue Telematik-Dienstleistungen

BITTNER – Der Datenschutzbeauftragte gemäß EU-Datenschutz-Grundverordnungs-Entwurf

KEBER – Rechtskonformer Einsatz von Social Media im Unternehmen – ausgewählte Einzelaspekte im Lichte aktueller Rechtsprechung

Kurzbeiträge

THÜSING –Persönlichkeitsschutz durch Datenschutz

FRANZEN – Beschäftigtendatenschutz: Was wäre besser als der Status quo?

GOLA – Aus den aktuellen Berichten der Aufsichtsbehörden (14)

REIF – Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts

Rechtsprechung

Aus dem Inhalt

EUGH, Kosten für eine Auskunft über personenbezogene Daten (Ls)

EUGH, Ausnahmen von der Informationspflicht bei Verarbeitung personenbezogener Daten (Ls)

BGH, Einwilligung in die Abtretung von Zahnarztforderungen

BAG, Positive Kenntnis des Arbeitgebers von der Arbeitnehmerinsolvenz

BVERWG, Kein Anspruch des Personalrats auf personenbezogene Informationen der elektronischen Arbeitszeiterfassung

30. Jahrgang
August 2014
Seiten 175–228

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

30. Jahrgang 2014
Heft 4
Seiten 175–228

RDV
Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 175

Veranstaltungen 176

Aufsätze

Prof. Dr. Volker LÜDEMANN / Christin SENGSTACKEN, LL.M.
Lebensretter eCall: Türöffner für neue Telematik-Dienstleistungen 177

Timo BITTNER LL.M., LL.M.
Der Datenschutzbeauftragte gemäß EU-Datenschutz-Grundverordnungs-Entwurf 183

Prof. Dr. Tobias KEBER
Rechtskonformer Einsatz von Social Media im Unternehmen – ausgewählte Einzelaspekte im Lichte aktueller Rechtsprechung 190

Kurzbeiträge

Prof. Dr. Gregor THÜSING
Persönlichkeitsschutz durch Datenschutz 196

Prof. Dr. Martin FRANZEN
Beschäftigtendatenschutz: Was wäre besser als der Status quo? 200

Prof. Peter GOLA
Aus den aktuellen Berichten der Aufsichtsbehörden (14) 203

RAin Yvette REIF, LL.M.
Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts 206

Rechtsprechung

Kosten für eine Auskunft über personenbezogene Daten (Ls)
(EuGH, Urteil vom 12.12.2013) 208

Ausnahmen von der Informationspflicht bei Verarbeitung personenbezogener Daten (Ls)
(EuGH, Urteil vom 07.11.2013) 208

Einwilligung in die Abtretung von Zahnarztforderungen
(BGH, Urteil vom 10.10.2013) 208

Positive Kenntnis des Arbeitgebers von der Arbeitnehmerinsolvenz
(BAG, Urteil vom 29.01.2014) 210

Kein Anspruch des Personalrats auf personenbezogene Informationen der elektronischen Arbeitszeiterfassung
(BVerwG, Beschluss vom 19.03.2014) 212

Video eines Bordellbesuchs im Internet als „Druckmittel“
(OLG Koblenz, Urteil vom 15.01.2014) 215

Evangelische Kirche darf die Bewerbung um die Stelle eines „Antirassismus-Referenten“ wegen Konfessionslosigkeit ablehnen (Ls)
(LAG Berlin, Urteil vom 28.05.2014) 216

Umbaumaßnahmen im Betriebsratsbüro unterliegen nicht der Mitbestimmung (Ls)
(HessLAG, Beschluss vom 03.03.2014) 216

Zur Sperrung personenbezogener Daten in einer Gesundheitsakte des Sozialpsychiatrischen Dienstes (Ls)
(OVG Berlin-Brandenburg, Beschluss vom 21.01.2014) 217

Zulässigkeit eines Ärztebewertungsportals
(LG Kiel, Urteil vom 06.12.2013) 217

Datenschutzrechtliches Verbot des Scannens von Personalausweisen
(VG Hannover, Urteil vom 28.11.2013) 219

Berichte, Informationen, Sonstiges

Studie der Initiative Markt- und Sozialforschung: Vertrauen in Datenschutz hängt von der bearbeitenden Einrichtung ab. Vertrauen bei Gesundheitseinrichtungen und Staat am häufigsten – bei IT und Telekommunikation am seltensten: Soziale Medien liegen hinter NSA 222

Nutzung privater E-Mail-Postfächer für dienstliche Zwecke 223

Werbung und Adresshandel 224

Literaturhinweise

Buchbesprechungen

Kevin Marschall, Entwicklung einer Handlungsanleitung für ein unternehmensinternes Compliance-Management-System (REDAKTION) 225

Stephan Weth/Maximilian Herberger/Michael Wächter (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (WRONKA) 225

Thomas Sassenberg/Reto Mantz, WLAN und Recht. Aufbau und Betrieb von Internet-Hotspots (SCHRIFTLEITUNG) 225

Christina Schmidt-Holtmann, Der Schutz der IP-Adresse im deutschen und europäischen Datenschutzrecht. Zur Auslegung des Begriffs des personenbezogenen Datums, Beiträge zum Informationsrecht (SCHRIFTLEITUNG) 226

Neuerscheinungen

Aufsätze 227

Nachgefasst 228

Beilagenhinweis GDD-Mitteilungen 4/2014; Bundesanzeiger Verlag GmbH, Köln; DATAKONTEXT, Frechen

Manuskripte
Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an die Schriftleitung erbeten. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. 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.

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
Verlagsgruppe Hüthig Jehle Rehm GmbH
Standort 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
Verlagsgruppe Hüthig Jehle Rehm GmbH
Standort 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
Verlagsgruppe Hüthig Jehle Rehm GmbH
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
30. Jahrgang 2014 Heft 4
Seiten 175–228

RDV
Recht der Datenverarbeitung

30. Jahrgang · August 2014 · Seiten 175–228

Editorial

Beschäftigtendatenschutz – Warten auf Brüssel?

Der Koalitionsvertrag regelt, dass eine gesetzliche Regelung zum Beschäftigtendatenschutz erst dann erfolgen soll, wenn mit einem Abschluss der Verhandlungen über die EU-Datenschutz-Grundverordnung (DS-GVO) nicht in angemessener Zeit gerechnet werden könne.

Der Begriff der „Angemessenheit" ist sicherlich dehnbar. Wer jedoch die schleppenden Verhandlungen auf Seiten des Europäischen Rates verfolgt, wird konstatieren müssen, dass dort angesichts von Meinungsverschiedenheiten sogar in Grundsatzfragen mit einer Entscheidungsfindung nicht in diesem Jahr gerechnet werden kann. Erst nach einer Positionierung des Rates schließt sich der Trilog mit der noch zu besetzenden Europäischen Kommission und dem Europäischen Parlament an. Eine Verabschiedung der Grundverordnung im Jahr 2015 ist damit trotz entsprechender Prognose des Innenministers wohl nicht wahrscheinlich. Bei dieser zeitlichen Perspektive ist zu hinterfragen, ob sich ein Warten auf Brüssel überhaupt lohnt. Zugleich stellt sich die Frage, ob ein Warten auch notwendig und sachlich geboten ist.

Die DS-GVO will bereits ihrem Wortsinne nach nur Grundregeln der personenbezogenen Datenverarbeitung festlegen. Detaillierte Regelungen zum Beschäftigtendatenschutz sind nicht beabsichtigt und auch nicht zu erwarten. Eine Öffnungsklausel soll „im Rahmen der Verordnung" Spielraum für einen nationalen Beschäftigtendatenschutz geben. Wie *Franzen* in diesem Heft nachweist, wäre ein vollständig harmonisierter Beschäftigtendatenschutz auf Ebene der EU sogar kompetenzwidrig.

Vor diesem sachlichen und europarechtlichen Hintergrund besteht somit kein Hindernis, bereits jetzt mit der Erarbeitung eines nationalen Beschäftigtendatenschutzes zu beginnen. Hierfür besteht auch ein Regelungsbedarf unter zwei Aspekten: Zum einen ist mit § 32 BDSG nur eine vorläufige Regelung geschaffen worden, die in der Rechtspraxis mehr Fragen als Lösungen bietet. Zum anderen ist nach In-Kraft-Treten der DS-GVO eine gesetzliche Klarstellung dahingehend dringend geboten, wonach Tarifverträge und Betriebsvereinbarungen vorrangige Erlaubnisnormen für die Verarbeitung von Beschäftigtendaten darstellen, da in der DS-GVO einer Privilegierung kollektivarbeitsrechtlicher Regelungen fehlt.

Grundlagen für ein Beschäftigtendatenschutzgesetz könnten die Vorarbeiten in der letzten Legislaturperiode des Bundestages sein. Wie *Thüsing* in dieser Ausgabe der RDV darlegt, stellten diese einen durchaus angemessenen Ausgleich zwischen Arbeitgeber- und Arbeitnehmerinteressen dar. Ungeachtet der Frage, ob der Beschluss des Europäischen Parlaments zu Mindeststandards für den Beschäftigtendatenschutz europarechtskonform ist, deckt der Gesetzentwurf in seiner letzten Fassung auch weitestgehend die Vorgaben des Europäischen Parlaments ab. Insbesondere der Vorschlag für eine Konzernklausel ist zielführend. Es bedarf dringend spezieller Rechtsgrundlagen für die Weitergabe von Beschäftigtendaten im Konzern, um das arbeitsteilige Zusammenwirken in Konzernstrukturen zu legitimieren. Auch der Einsatz der Informations- und Kommunikationstechnik am Arbeitsplatz und deren Nutzung durch Beschäftigte bedarf vor dem Hintergrund einer uneinheitlichen Rechtsprechung einer gesetzlichen Klarstellung.

Sowohl vom Europäischen Parlament als auch im Gesetzentwurf der letzten Bundesregierung ist die Kontrollkompetenz des betrieblichen Datenschutzbeauftragten beim Betriebsrat nicht angesprochen. Um die Lücke im betrieblichen Kontrollsystem zu schließen, muss die Schweigepflicht des betrieblichen Datenschutzbeauftragten auf die Gesamtumstände der Betriebsratsarbeit erweitert werden. Damit kann das Hauptargument des BAG gegen eine solche Kontrollkompetenz entkräftet werden.

Fazit: Nicht warten – machen!

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

Termin	Thema	Ort	Kontakt
04.09.2014	ConnectedCar und Datenschutz im Flottenmanagement	Köln	GDD e.V. und DATAKONTEXT
11.09.2014	Cloud Computing: Leit- und Richtlinien	Frankfurt/M.	GDD e.V. und DATAKONTEXT
15.09.2014	Rechtssichere Personaldatenverarbeitung und Prozesse	Düsseldorf	GDD e.V. und DATAKONTEXT
22.-26.09.2014	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
25.09.2014	Data Leakage Prevention	Köln	GDD e.V. und DATAKONTEXT
29.-30.09.2014	Datenschutz Kompakt	Frankfurt/M.	GDD e.V. und DATAKONTEXT
30.09.2014	Prüfpraxis der Datenschutzaufsichtsbehörden	Stuttgart	GDD e.V. und DATAKONTEXT
30.09.2014	Rechtskonformer Einsatz von Big Data	Köln	GDD e.V. und DATAKONTEXT
01.10.2014	Kontrolle von Auftragnehmern im Rahmen der Auftragsdaten-verarbeitung	Stuttgart	GDD e.V. und DATAKONTEXT
06.10.2014	Datenschutz und Videoüberwachung – Was geht und was geht nicht?	Köln	GDD e.V. und DATAKONTEXT
06.-07.10.2014	Betriebsrat und Datenschutz	Berlin	GDD e.V. und DATAKONTEXT
13.10.2014	IT-gestützte Datenschutzpraxis	Köln	GDD e.V. und DATAKONTEXT
13.-17.10.2014	Der Auditor zur Auftragsdatenverarbeitung	Hamburg	GDD e.V. und DATAKONTEXT
15.10.2014	Die 30 häufigsten Datenschutz-Schwachstellen und deren Lösung	Düsseldorf	GDD e.V. und DATAKONTEXT
20.10.2014	Toolgestütztes Datenschutz-Management	Köln	GDD e.V. und DATAKONTEXT
21.10.2014	Grundlagen der Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
20.-22.10.2014	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Potsdam	GDD e.V. und DATAKONTEXT
22.10.2014	Kundendatenschutz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
27.10.2014	Der Teilzeit-Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
28.10.2014	Personalprozesse datenschutzkonform organisieren	Köln	GDD e.V. und DATAKONTEXT
28.10.2014	Drop Box und Iphone: dienstliche Nutzung privater IT – Bring Your Own Device-Strategie	Frankfurt/M.	GDD e.V. und DATAKONTEXT
28.10.2014	Datenschutzaudit leicht gemacht	Köln	GDD e.V. und DATAKONTEXT
30.10.2014	Das neue Melderecht	Köln	GDD e.V. und DATAKONTEXT
04.11.2014	Was der Datenschutzbeauftragte von der IT-Sicherheit wissen sollte!	Frankfurt/M.	GDD e.V. und DATAKONTEXT
05.11.2014	Die Datenpanne! Ein Albtraum jedes Unternehmens	Köln	GDD e.V. und DATAKONTEXT

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

Aufsätze

Prof. Dr. Volker Lüdemann, Christin Sengstacken, LL.M.

Lebensretter eCall: Türöffner für neue Telematik-Dienstleistungen

Die Einführung des europaweiten automatischen Notrufs steht vor der Tür. Die europäischen Verordnungsentwürfe zielen jedoch nicht allein auf die Verbesserung der Notfallrettung ab. Gleichzeitig erlangen private Wirtschaftsteilnehmer auf legitime Weise Zugang zum automobilen Datenschatz. In diesem Fall können Datenschutzregelungen unterlaufen werden – vor dem Hintergrund einer verbraucherorientierten und lebensrettenden europäischen Gesetzgebung.

I. Einleitung

Die europaweite Einführung des automatischen Notrufsystems in Kraftfahrzeugen „eCall" (Kurzform für emergency call) rückt näher. Nach dem EU-Parlament hat Ende Mai auch der Rat dem Verordnungsvorschlag der EU-Kommission im Grundsatz zugestimmt. Derzeit befindet sich der Entwurf in den interinstitutionellen Verhandlungen. Inhaltlich liegen die Positionen nicht weit auseinander. Strittig ist vor allem der Starttermin. Je nach Verhandlungsergebnis werden möglicherweise schon ab Ende 2015 neue Personenkraftwagen und leichte Nutzfahrzeuge verpflichtend mit einem bordeigenen 112-eCall-System[1] ausgestattet sein. Dieses setzt bei einem Unfall automatisch einen Notruf ab und übermittelt die für die Rettung notwendigen Daten. Die EU-Kommission geht davon aus, dass hierdurch bis zu 2500 Menschenleben jährlich gerettet und die Schwere der durch Verkehrsunfälle verursachten Verletzungen signifikant verringert werden können. Wer angesichts des Nutzens dieser Technik auf Datenschutzprobleme hinweist, läuft Gefahr, sich dem Vorwurf der Unangemessenheit auszusetzen. Das datenschutzrechtliche Interesse tritt in den Hintergrund, wenn das eigene Überleben in Rede steht. Wenn sich die Autoren des Themas dennoch unter datenschutzrechtlichen Gesichtspunkten annehmen, dann aus einem anderen Grund. Erklärtes Ziel des Gesetzgebers ist nämlich nicht nur die Verbesserung der Notfallrettung. Mit dem eCall soll zugleich in jedem Fahrzeug eine technische Plattform für Zusatzdienstleistungen etabliert werden, um die europäische Informationstechnologie auf den Weltmärkten zu stärken. Weitgehend unbemerkt von der kritischen Öffentlichkeit sieht die Verordnung vor, dass parallel oder aufbauend auf dem bordeigenen System umfangreiche Zusatzdienste angeboten werden können.[2] Das eCall-System beruht damit in Wirklichkeit auf zwei Säulen: dem gesetzlichen Notruf und einer Zusatzdienstesäule. Während der gesetzliche Notruf datenschutzrechtlich unproblematisch ist, droht die Zusatzdienstesäule zum Dreh- und Angelpunkt für alle möglichen automobilen Datensammler zu werden. Dadurch ausgelöste Gefahrenkonstellationen finden in den Verordnungsentwürfen keine Berücksichtigung. Im Gegenteil, die EU nimmt es bewusst in Kauf, dass der eCall unter dem Deckmantel der Lebensrettung zum Türöffner für weitreichende Datennutzungen wird.

Der Beitrag analysiert nach einem kurzen Überblick über das Gesetzgebungsverfahren (II.) und die Funktionsweise des eCalls (III.) die datenschutzrechtliche Einordnung des gesetzlichen Notrufs und Zusatzdiensten (IV.). Abschließend wird der Gesetzentwurf einer kritischen Wertung unterzogen (V.).

II. Stand des Gesetzgebungsverfahrens

Das europaweite Notrufsystem für Kraftfahrzeuge steht seit 2003 auf der Prioritätenliste der EU[3]. Nach umfangreichen Vorarbeiten unter Beteiligung der Industrie[4] legte die Kommission im August 2009 erstmals Maßnahmen und Zeitplan für die unionsweite Einführung eines bordeigenen Notrufsystems vor[5]. Der Versuch einer freiwilligen Einführung schlug fehl. Das EU-Parlament forderte daraufhin im Juli 2012 die Kommission auf, den Entwurf für ein gesetzlich verbindliches, öffentliches Notrufsystem auszuarbeiten[6]. Die Kommission kam dieser Forderung mit dem „Vorschlag für eine Verordnung des Europäi-

1 Im Folgenden werden die Begriffe „bordeigenes 112-eCall-System", „bordeigenes eCall-System" und „gesetzliches eCall-System" synonym verwendet.

2 Legislative Entschließung des Europäischen Parlaments vom 26. Februar 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG (COM(2013)0316 – C7 – 0174/2013 – 2013/0165 (COD)), Erwägung 7b.

3 Mitteilung der Kommission: Informations- und Kommunikationstechnologien für sichere und intelligente Fahrzeuge, KOM(2003) 542 endg. vom 15.9.2003.

4 Vgl. hierzu die Darstellung in Artikel-29-Datenschutzgruppe, Arbeitsdokument „Eingriffe in den Datenschutz und die Privatsphäre im Rahmen der Initiative eCall" (1609/06/EN – WP 125), S. 2f.

5 Mitteilung: eCall: Zeit zur Einführung COM (2009) 434 endg. vom 21.08.2009.

6 Bericht: „eCall: ein neuer Notruf 112 für die Bürger", 2012/2056 (INI) vom 22.06.2012.

schen Parlaments und des Rats über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46EG“[7] nebst einem entsprechenden Beschlussentwurf nach[8]. Das EU-Parlament legte seinen Standpunkt hierzu in erster Lesung am 26.2.2014 fest[9]. Der Rat verabschiedete am 26.5.2014[10] eine „allgemeine Ausrichtung“ zu dem Verordnungsvorschlag[11]. Die Verordnung ist nun Gegenstand der interinstitutionellen Verhandlungen. Ein wesentlicher Streitpunkt ist das Einführungsdatum. Während das EU-Parlament für eine Einführung ab Oktober 2015 plädiert, will der Rat den Autoherstellern eine 36-monatige Übergangsfrist einräumen. Nach derzeitigem Stand ist davon auszugehen, dass man die Positionen zwischen Kommission, Parlament und Rat in den kommenden Monaten ausverhandelt und der Verordnungsvorschlag dann zur endgültigen Abstimmung gestellt wird[12].

III. Funktionsweise des eCalls

Das Prinzip des eCalls ist einfach. Sobald die Airbags ausgelöst werden, wählt sich das System über eine eigene SIM-Karte automatisch in das Mobilfunknetz ein und baut eine Sprach- und Datenverbindung zur nächstgelegenen Notrufstelle auf[13]. Über die Datenverbindung werden die notwendigen Rettungsdaten übermittelt. Die Notrufstelle leitet auf dieser Grundlage die Rettungsmaßnahmen ein und nimmt über die Mobilfunkverbindung Kontakt zum Unfallfahrzeug auf.

Alle Neufahrzeuge werden mit den hierzu erforderlichen technischen Voraussetzungen verpflichtend ausgestattet. Dazu gehören u.a. ein GPS-Empfänger zur Feststellung der Fahrzeugposition, eine GSM-Antenne zum Senden des Notrufs, ein Steuergerät zur Meldung des Standorts, ein Crash-Sensor zum Erkennen der Unfallart, eine Freisprecheinrichtung, eine Notstromversorgung zur Überbrückung von Unfallschäden an der Fahrzeugbatterie, eine Taste zur manuellen Auslösung des Notrufs und eine Kontrollleuchte, welche die Funktionsfähigkeit des Systems anzeigt[14]. Der eCall-Notruf selbst besteht aus einem Mindestdatensatz (Minimum Set of Data, MSD). Festgelegt sind die zulässigen Daten in der Norm „Intelligente Transportsysteme – Elektronische Sicherheit – Minimaler Datensatz für den elektronischen Notruf eCall.“[15] Hierin vorgesehen sind Unfallort, Unfallzeitpunkt, Fahrtrichtung, Fahrzeugkennung mit Fahrzeugtyp und Treibstoffart[16] sowie die Anzahl der angelegten Sicherheitsgurte, um die Zahl der Insassen zu bestimmen[17]. Die Daten erhält das eCall-System über standardisierte Schnittstellen (SST) zur Bordelektronik.

IV. Datenschutzrechtliche Einordnung

Mit dem verpflichtenden Einbau der Notruftechnik verfügt künftig jedes Neufahrzeug in Europa über einen Mobilfunkzugang. Damit ist grundsätzlich möglich, Fahrzeugbewegungen nachzuvollziehen. Insoweit entspricht das Gefährdungspotential dem der Mobiltelefonie. Neue Herausforderungen für den Datenschutz ergeben sich hingegen daraus, dass mit dem Notrufsystem zugleich eine technische Plattform an der Schnittstelle zwischen Bordelektronik und Internet geschaffen wird. In modernen Fahrzeugen arbeiten bis zu 80 Steuergeräte, die mit Hilfe von Sensoren alle relevanten Fahr- und Fahrzeugdaten erfassen, speichern und verarbeiten[18]. Diese Daten sind wirtschaftlich höchst interessant. Mit der Netzanbindung des Notrufsystems können diese nach außen transportiert und für verschiedenste Dienste nutzbar gemacht werden. Für die Sicherung von Privatsphäre und Datenschutz ist es mithin entscheidend, wie diese Schnittstelle konzipiert und ausgestaltet ist.

1. Unbedenklichkeit des gesetzlichen Notrufsystems (Basissystem)

Das gesetzliche Notrufsystem ist unter Datenschutzgesichtspunkten im Wesentlichen bedenkenfrei. Dieses Ergebnis ist nicht zuletzt auf die kritische Begleitung des Gesetzgebungsverfahrens in der Öffentlichkeit zurückzuführen[19]. Die datenschützenden Bestimmungen wurden im Laufe des Gesetzgebungsverfahrens gegenüber dem ursprünglichen Entwurf deutlich verschärft. Die Verordnung stellt in der jetzigen Form nun eine ausreichende Rechtsgrundlage für die Erhebung und Verarbeitung der in diesem Zusammenhang benötigten Daten dar.

7 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46EG COM (2013) 316.

8 Vorschlag für einen Beschluss des Europäischen Parlamentes und des Rates über die Einführung des interoperablen EU-weiten eCall-Dienstes (Dok. 11159/13 TRANS 338 CODEC 1516) vom 13.02.2014.

9 Legislative Entschließung des Europäischen Parlaments vom 26. Februar 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG (COM(2013) 0316 – C7 – 0174/2013 – 2013/0165 (COD)) vom 26.02.2014.

10 Rat der Europäischen Union 9879/14.

11 Nimmt der Rat eine allgemeine Ausrichtung an, nachdem das EU-Parlament seinen Standpunkt in erster Lesung festgelegt hat, so stellt dies kein Handeln des Rates im Sinne des Artikels 294 Absätze 4 (Billigung) und 5 (Nichtbilligung) AEUV dar.

12 Zur besseren Unterscheidbarkeit werden die unterschiedlichen Verordnungsentwürfe wie folgt abgekürzt: Verordnungsentwurf der Europäischen Kommission = E-K, Verordnungsentwurf des Europäischen Parlaments = E-P, Verordnungsentwurf des Rates = E-R.

13 Für das Hoheitsgebiet der Bundesrepublik ergibt sich die nächstgelegene Notrufabfragestelle aus §§ 2a Nr. 2, 3 Abs. 1 NotrufV.

14 Detaillierte Informationen zum technischen Ablauf auf der Homepage des ADAC, abrufbar unter http://www.adac.de/infotestrat/unfall-schaeden-und-panne/ecall_gps_notruf/.

15 DIN EN 15722:2011.

16 Aus der Fahrzeugkennung ergibt sich u.a. die Personenbeziehbarkeit der Daten, da sich hierüber der Halter des Fahrzeugs ermitteln lässt.

17 Art. 3 Abs. -3 (E-R).

18 Weichert, Thilo, Kfz-Notfallsystem eCall – Möglichkeiten und Versuchungen, netzpolitik.org vom 03.06.2014.

19 Anstatt vieler „E-Call soll helfen, nicht horchen“, carIT vom 03.02.2014 abrufbarunterhttp://www.car-it.com/e-call-soll-helfen-nicht-horchen/id-0039128.

a) Privatsphäre und Datenschutz sind ausreichend gewährleistet

Das eCall-System ist als „schlafendes" System ausgelegt. Erst bei Auslösen der Airbags oder manueller Aktivierung wird eine Mobilfunkverbindung hergestellt. Die Hersteller müssen sicherstellen, dass die Fahrzeuge im Normalbetrieb nicht verfolgt werden können, bevor der eCall ausgelöst wird[20]. Die Gefahr der Bildung von Bewegungsprofilen, das gefürchtete „Tracking," ist damit ausgeschlossen. Mit dem Mindestdatensatz (Minimum Set of Data) werden zudem nur jene Informationen übermittelt, die für die effiziente Notfallrettung erforderlich sind[21]. Für andere Zwecke als die Notfallrettung dürfen die Daten nicht verwendet werden. Auch die Löschung ist in der Verordnung klar geregelt. Soweit es sich um Positionsdaten handelt, müssen diese kontinuierlich überschrieben werden, damit im Fall der Notrufauslösung nur die für die Positionsbestimmung und Fahrtrichtung unerlässlichen Daten vorhanden sind[22]. Die Notrufstelle darf die Daten zudem nur für die Dauer der Rettungsmaßnahmen speichern und verwenden. Im Ergebnis unterscheidet sich die Verwendung der Daten damit nicht von der bisherigen Notrufpraxis.

b) Fehlende Deaktivierungsmöglichkeit unkritisch

Teilweise wird problematisiert, dass die Verordnung dem Nutzer keine Wahlfreiheit lässt, den eCall zu nutzen oder nicht. Ein Deaktivieren des Notrufsystems ist nicht vorgesehen. Kritiker sehen hierin einen unverhältnismäßigen und unangemessenen Eingriff in das Recht auf informationelle Selbstbestimmung[23]. Im Ergebnis vermögen diese Bedenken nicht zu überzeugen. Der eCall dient nicht nur dem Schutz des Fahrers, sondern auch dem der Mitfahrer und anderer Verkehrsteilnehmer[24]. Mit einem optionalen Abschalten des Systems ist dieses Ziel nicht zu erreichen. Mit Blick auf die grundrechtlich geschützten Rechtsgüter anderer Verkehrsteilnehmer scheint es zulässig und angemessen, das Recht auf informationelle Selbstbestimmung insoweit einzuschränken. Die Einschränkung sollte allerdings im Entwurf ausdrücklich benannt werden. An dieser Stelle muss noch nachgearbeitet werden[25]. Dann ist das Fehlen der Deaktivierungsmöglichkeit bedenkenfrei.

2. Problem der Zusatzdienste

Die datenschutzrechtliche Unbedenklichkeit besteht aber nur auf den ersten Blick. Unproblematisch ist allein das gesetzliche Notrufsystem in seiner Basisfunktion. Kritisch sind die Zusatzdienste.

a) eCall als technische Plattform für Zusatzdienste

Entsprechend der gesetzgeberischen Zielrichtung, mit dem gesetzlichen Notrufsystem zugleich in jedem Fahrzeug eine technische Plattform für Zusatzdienste rund um das Automobil zu fördern, ist die Architektur des eCall-Systems als frei zugängliche, interoperable und standardisierte Plattform konzipiert[26]. Hierauf können die Zusatzdienste aufsetzen[27]. Die Grundlage bildet das im eCall-System enthaltene Mobilfunkmodul, durch das alle Neufahrzeuge künftig über eine Internetschnittstelle verfügen[28]. Die Zusatzdienste können darüber auch im Normalbetrieb – wenn dies gewünscht ist – stets mit dem Internet verbunden sein. Zwei Arten von Zusatzdiensten sind zu unterscheiden: Solche, die direkt auf dem gesetzlichen System aufsetzen, und Dienste, die auf einem zusätzlichen privaten Notrufsystem basieren. Für die erstgenannten Zusatzdienste bedarf es nur einer zweiten SIM-Karte im Mobilfunkmodul des gesetzlichen Notrufsystems. Die zusätzlichen privaten eCall-Systeme – mittlerweile von fast allen namhaften Herstellern als Bestandteil der modernen Bordsysteme angeboten[29] – sind in der Regel bereits über das Mobilfunkmodul des Bordsystems mit dem Netz verbunden. Die Möglichkeit, solche zusätzlichen privaten Notrufsysteme zu nutzen, ist in der Verordnung ausdrücklich vorgesehen[30]. Sie übernehmen dann die Funktion des gesetzlichen Notrufs. Es muss lediglich sichergestellt sein, dass im Falle eines Defekts das gesetzliche eCall-System automatisch reaktiviert wird[31]. Die derzeit noch geführte Diskussion[32], ob im Normalbetrieb ein Datenaustausch zwischen den beiden System stattfinden darf, ist eher theoretischer Natur. Sofern sich der Fahrzeughalter für ein privates System entscheidet, ist dies in der Regel ohnehin integraler Bestandteil eines umfassenden Bordsystems mit eigenem Zugriff auf die Bordelektronikdaten und eigener Mobilfunkschnittstelle.

b) Datenschutzregelungen gelten ausschließlich für das gesetzliche Basissystem

Ungeachtet dessen, dass die Zusatzdienste stets fester Bestandteil der eCall-Initiative waren, gelten die Datenschutzbestimmungen der Verordnung ausschließlich für das gesetzliche

20 Art. 6 Abs. 1 (E-P).

21 Zu den entsprechenden Empfehlungen der Artikel-29-Datenschutzgruppe vgl. Arbeitsdokument „Eingriffe in den Datenschutz und die Privatsphäre im Rahmen der Initiative eCall" (1609/06/EN – WP 125), S. 3 f.

22 Art. 6 Abs. -1 (E-R).

23 „EU-Innenpolitiker segnen Auto-Notruf eCall ab", heise news vom 31.01.2014 abrufbar unter http://www.heise.de/newsticker/meldung/EU-Innenpolitiker-segnen-Auto-Notruf-eCall-ab-2103834.html.

24 In diese Richtung Erwägung 5 (E-R).

25 So auch Artikel-29-Datenschutzgruppe Arbeitsdokument „Eingriffe in den Datenschutz und die Privatsphäre im Rahmen der Initiative eCall" (1609/06/EN – WP 125), S. 8.

26 Erwägung 9 (E-K); Erwägung 9 (E-P); Erwägung 9 (E-R); so auch der Europäische Datenschutzbeauftragte mit Hinweis auf entsprechende Risiken in der Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG vom 29.08.2013, Nr. 14.

27 Erwägung 18 (E-R), Ziel ist die Verwirklichung des Binnenmarkts durch die Festlegung einheitlicher technischer Anforderungen.

28 So auch Weichert, Thilo, Kfz-Notfallsystem eCall – Möglichkeiten und Versuchungen (s. Fn 18).

29 Vgl. nur BMW ConnectedDrive, Mercedes Benz COMAND Online und Opel OnStar.

30 Artikel 5 Abs. 2 a (E-R).

31 Artikel 5 Abs. 2 a (E-P).

32 So das Parlament in Abweichung vom Vorschlag der Kommission, vgl. Abänderung 55 (E-P).

Basissystem. Die Zusatzdienste werden hiervon nicht erfasst. Besonders deutlich wird dies in der Entwurfsfassung des Ministerrats. Gesetzlicher Notruf („bordeigenes eCall-System") und privater Notruf („bordeigenes Drittanbieter-eCall-System") sind hierin legal definiert[33]. Die in Artikel 6 enthaltenen Bestimmungen zu Privatsphäre und Datenschutz gelten nur für das gesetzliche Notrufsystem („bordeigenes eCall-System")[34]. Der private Notruf ist damit von vornherein aus der Vorschrift ausgenommen. Gleiches gilt für Zusatzdienste, die auf dem gesetzlichen Notrufsystem unmittelbar aufsetzen. Die Legaldefinition des gesetzlichen Notrufsystems umfasst nur den Notruf in seiner Basisfunktion[35]. Auch der in Art 6 verankerte Ansatz des „privacy by design" lässt die Zusatzdienste unberührt. Auch aus den Herstellerpflichten in Artikel 4 und 5 des Ratsentwurfs lässt sich keine Einbeziehung der Datenschutzbestimmungen auf Zusatzdienste ableiten. Artikel 4 verpflichtet die Hersteller lediglich nachzuweisen, dass alle neuen Fahrzeugtypen mit dem gesetzlich verpflichtenden bordeigenen eCall-System ausgerüstet sind. In Artikel 5 Nr. 2 a werden zwar die Voraussetzungen genannt, unter denen Drittanbieter-eCall-Systeme verwendet werden dürfen. Die Einhaltung der strengen Datenschutzbestimmungen ist in dem angeführten Katalog aber gerade nicht erwähnt. Die Hersteller trifft zudem die Pflicht, die Nutzer über eine vom Basissystem abweichende Datennutzung in der Betriebsanleitung zu informieren und deren Zustimmung einzuholen[36]. Diese Regelung unterstreicht ebenfalls, dass die Zusatzdienste nicht durch die datenschutzrechtlichen Bestimmungen der Verordnung abgedeckt sind.

3. Rückgriff auf andere gesetzliche Regelungen und Datenschutzgrundsätze nicht möglich

Die bestehende Lücke kann auch nicht durch den Rückgriff auf andere gesetzliche Regelungen und die allgemeinen Datenschatzgrundsätze gefüllt werden. Außerhalb der Verordnung sind bereichsspezifische Regelungen zum Schutz der Fahrzeug- und Personendaten im Zusammenhang mit Zusatzdiensten nicht ersichtlich. Insbesondere das „Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern – Intelligente Verkehrssysteme-Gesetz (IVSG)"[37] stellt kein ausreichendes Datenschutzregime zur Verfügung. Die Vorschriften verfügen nicht über die erforderliche Regelungstiefe und Normenklarheit. Im Übrigen zielt das Gesetz in erster Linie auf die grenzüberschreitende technische Harmonisierung ab, indem es die Behörden bei der Einführung intelligenter Verkehrssysteme auf die Einhaltung der europäischen Spezifikationsvorgaben verpflichtet[38]. Die allgemeinen gesetzlichen Erlaubnistatbestände sind nicht einschlägig (§ 28 Abs. 1 BDSG)[39]. Hier dürfte es in der Regel bereits am Tatbestandsmerkmal „zur Erfüllung eigener Geschäftszwecke" fehlen. Hierzu dient die Datenverwendung nur dann, wenn sie nicht selbst den Kern des geschäftlichen Interesses darstellt[40]. Dies ist bei Zusatzdiensten aber in der Regel der Fall. Man denke etwa an die Überprüfung des Fahrzeugzustandes oder die Erfassung von Ortungsdaten.

Die allgemeinen Datenverarbeitungsgrundsätze der Datensparsamkeit und Datensicherheit sind nicht ausreichend trennscharf, um Schutz vor den Gefahren zu vermitteln, die von den Zusatzdiensten ausgehen. Selbst datensparsame und datensichere Gestaltungen können nicht verhindern, dass eine Vielzahl hochsensibler Fahr- und Fahrzeugdaten ausgetauscht werden.

4. Instrument der Einwilligung nur bedingt geeignet

Insoweit verbleibt nur das Instrument der Einwilligung[41]. Das normative Schutzkonzept der Einwilligung ist im Zusatzdienstekontext aber nur bedingt geeignet.

a) Unbestimmter Kreis von Betroffenen

Dies gilt bereits mit Blick auf den Kreis der Betroffenen. Da die Einwilligung durch ihren Grundrechtsbezug höchstpersönlicher Natur ist, kann sich grundsätzlich nur der Betroffene selbst im Vorfeld mit der Verarbeitung einverstanden erklären[42]. Die Abgabe durch einen Bevollmächtigten scheidet aus[43]. Eine Einwilligung ist mithin nur in den Fällen unproblematisch, in denen der Fahrzeughalter zugleich der einzige Fahrer ist. Wird das Fahrzeug von mehreren Personen geführt, muss – in Abhängigkeit vom Umfang des Zusatzdienstes – ggf. jede dieser Personen einwilligen. Gleiches gilt für Mitfahrer. Auch ihre Daten werden über den Anschnallgurt oder den Airbag erfasst, dieses zudem oft unbemerkt durch den Betroffenen[44]. Wie die Einwilligung vor diesem Hintergrund in

33 Art. 3 Abs. 1 und Art. 3 Abs. 2 g (E-R). Das bordeigene eCall-System ist definiert als „System, das entweder automatisch von im Fahrzeug eingebauten Sensoren oder manuell ausgelöst wird und durch das über öffentliche Mobilfunknetze ein Mindestdatensatz übermittelt und eine auf die Nummer 112 gestützte Tonverbindung zwischen den Fahrzeuginsassen und einer eCall-Notrufabfragestelle hergestellt wird."

34 So auch der Europäische Datenschutzbeauftragte in seiner Stellungnahme, Nr. 20 und 22 (s. Fn 26).

35 Auch die Artikel 29-Datenschutzgruppe geht in ihrem Arbeitsdokument davon aus, dass als bordeigenes System nur das reine Notruf-Basissystem gilt, S. 7 f. (s. Fn 21).

36 Art. 6 Abs. 3 i (E-P).

37 Gesetz vom 11.6.2013, BGBl. I, S. 1536.

38 BT-Drs. 17/12371, S. 7.

39 Der Erlaubnistatbestand des Art. 7 der Richtlinie 95/46 EG bzw. § 28 Abs. 2 BDSG kommt vorliegend nicht in Betrachtung. Zum einen würde hierdurch nur die Übermittlung und Nutzung von Daten erfasst. Zum anderen dürfte es in der Regel an der Wahrnehmung berechtigter Interessen eines Dritten mangeln.

40 Gola in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 28 Rn. 4.

41 In diese Richtung auch Artikel 29-Datenschutzgruppe, Stellungnahme 13/2011, S. 15; Stellungnahme des Europäischen Datenschutzbeauftragten, Nr. 29 (s. Fn 26).

42 Gola in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4a Rn. 2.; Däubler in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 4a Rn.

43 Simitis, in: Simitis (Hrsg.), BDSG, § 4a Rn. 31; Weichert, in Däubler/Klebe/Wedde/Weichert, BDSG, § 4 Rn. 5.; a.A. insoweit Gola, in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4a Rn. 25, wonach eine Vertretung zulässig ist, wenn sich die Vollmacht ausdrücklich auf die Erteilung der Einwilligung erstreckt. Im vorliegenden Fall kommen beide Ansichten zu demselben Ergebnis.

44 Vgl. Weichert, Thilo, Datenschutz im Auto – Teil 1, SVR 6/214, 201, 204.

der Praxis realisiert werden soll, ist unklar. Die Einwilligung ist auf solche Fälle nicht zugeschnitten. Sie stößt damit bereits in einer typischen Grundkonstellation der Zusatzdienste an ihre Grenzen.

b) Formanforderungen

Auch die gesetzlich vorgeschriebenen Formanforderungen dürften kaum durchgängig eingehalten werden können. Die Einwilligung muss grundsätzlich schriftlich erfolgen[45]. Da dies grundsätzlich für jede Datenverwendung gilt[46], ist sie schon mit Blick auf den weiten Kreis potentiell Betroffener eine kaum zu bewältigende Herausforderung. Eine Schriftform ersetzende, qualifizierte elektronische Signatur kommt vor diesem Hintergrund ebenfalls nicht in Betracht[47]. Auch die Verwendung eines „Push-Button", wie ihn die Artikel 29-Datenschutzgruppe in Zusammenhang mit der intelligenten Verbrauchsmessung (Smart Metering) vorgeschlagen hat[48], dürfte das Problem nicht lösen. Die eigenhändig zu unterzeichnende schriftliche Einwilligung soll der Identifizierung und Höchstpersönlichkeit des Betroffenen dienen und wäre durch einen einfachen Druckknopf nicht gewährleistet[49].

c) Widerruflichkeit

Die Einwilligung müsste zudem widerrufen werden können[50]. Man könnte insoweit daran denken, dem Betroffenen systemseitig die Möglichkeit einzuräumen, den Verarbeitungsprozess jederzeit stoppen zu können[51]. Bei Zusatzdiensten, die auf dem privaten Notrufsystem beruhen, könnte dies über ein manuelles Deaktivieren des Systems erfolgen. Eine Sicherheitslücke wäre nicht zu befürchten, da nach den Vorgaben der Verordnung das gesetzliche Notrufsystem automatisch übernehmen würde[52]. Schwieriger ist die Situation indes bei Zusatzdiensten, die unmittelbar auf dem gesetzlichen Notruf aufsetzen. Dieser kann nach der Verordnung nicht deaktiviert werden. Insofern kommt es darauf an, ob der jeweilige Zusatzdienst gesondert abgeschaltet werden kann.

d) Informierte Einwilligung

Problematisch ist das Instrument der Einwilligung zudem unter dem Gesichtspunkt der „informierten Einwilligung". Der Betroffene muss wissen, worin er einwilligt, um die Tragweite seiner Entscheidung abzusehen[53]. Dies setzt voraus, dass er zumindest ausreichende Informationen darüber hat, welche Daten Gegenstand der Einwilligung sind, wie diese verwendet werden und durch wen die Verwendung erfolgt[54]. Die Verordnung delegiert die Informationspflicht auf die Fahrzeughersteller. Diese sind verpflichtet, klare und umfassende Informationen über die Verarbeitung von Daten durch das bordeigene System als Teil der Betriebsanleitung bereitzustellen[55]. Dies beinhaltet gemäß Art. 6 Abs. 3 i auch jegliche sonstigen Informationen hinsichtlich der Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung eines privaten Notrufsystems und von Zusatzdiensten[56]. Die Konzentration der Informationspflicht auf eine Stelle ist zwar grundsätzlich nicht zu beanstanden, wenngleich sich die Frage stellt, wie dies bei mehreren, zeitlich gestaffelten Zusatzdiensten, die nicht über einen Hersteller laufen, praktisch funktionieren soll. Eine andere Frage ist, wie mit dem absehbaren „information overload" umzugehen ist. Zu viele Informationen können dazu führen, dass diese nur unzureichend zur Kenntnis genommen werden[57]. Entscheidend ist jedoch, dass die Problematik des unbestimmten Kreises von Betroffenen auch auf die Informiertheit der Einwilligung durchschlägt. Wenn die Person des Betroffenen unklar ist, läuft die Information ins Leere. Der Gesetzgeber legt dieses Problem in der Verordnung selbst offen. Obgleich die Informationspflicht sehr umfangreich geregelt ist, fehlt jede Angabe dazu, wem gegenüber der Fahrzeughersteller die Information zu erbringen hat. Auch dieser Befund unterstreicht, dass die Einwilligung im Zusatzdienste-Kontext nur bedingt tauglich ist. Sie vermag nur zwischen Betroffenen und verantwortlicher Stelle Wirkung zu entfalten. Auf mehrpolare Konstellationen mit Kfz-Herstellern, Haltern, Fahrern, Mitfahrern, Leihstellen, Dienste- und Geräteanbietern ist sie nicht zugeschnitten. Hinzu tritt ein grundsätzliches Problem. Die Einwilligung ist in ihrer Ausgestaltung auf überschaubare Sachverhalte angelegt. In Zusammenhang mit modernen Technologien stößt dieses Schutzkonzept an seine Grenzen[58]. Bei hoher Komplexität der Datenverarbeitungsvorgänge, wie sie für moderne Technikentwicklungen typisch sind, ist der Einwilligende kaum mehr in der Lage, die Konsequenzen seiner Entscheidung abschätzen zu können[59]. Eine solche Konstellation wird auch für den Fall Zusatzdienste angenommen[60].

45 § 4 Abs. 1 S. 3 BDSG.

46 Simitis, in: Simitis (Hrsg.), BDSG, § 4a Rn. 33 und 34.

47 § 4 a Abs. 1 BDSG iVm. § 126 a BGB.

48 Artikel 29-Datenschutzgruppe, Stellungnahme 12/2011 zur intelligenten Verbrauchsmessung 00671/11/DE WP 183, S. 10.

49 Simitis, in: Simitis (Hrsg.), BDSG, Bundesdatenschutzgesetz, § 4a Rn. 30. Eine solche Lösung stünde zudem in Widerspruch zu § 21g Abs. 6 EnWG, der bei der zusätzlichen Einwilligung für das Fernmessen auf den Letztverbraucher abstellt.

50 Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 4a Rn. 35 m. w. Nachw.

51 Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006, S. 233.

52 Vgl. Art. 5 Abs. 2 a (E-R) und (E-P).

53 Gola, in: Gola/Schomerus, BDSG, § 4a Rn. 25.

54 Roßnagel/Holznagel/Sonntag, Handbuch Datenschutzrecht, Kapitel 4.8 Rn. 45.

55 Art. 6 Abs. 1 (E-R).

56 Art. 6 Abs. 3, j (E-R).

57 Brunner, Stephan, Mit rostiger Flinte unterwegs in virtuellen Welten?, Jusletter 4. April 2011, Rz. 48.

58 Mit weiteren Beispielen auch Kutscha, Martin, Mehr Datenschutz – aber wie?, ZRP 2010, 112, 113.

59 Buchner, Benedikt, S. 233 (s. Fn 51).

60 31. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg, S. 85 abrufbar unter http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/01/31.-TB-2012-2013.pdf#.

V. Fazit

Der eCall leistet einen wichtigen Beitrag, um die Zahl der Unfalltoten auf Europas Straßen zu senken. In dieser Funktion ist er uneingeschränkt zu begrüßen und auch datenschutzrechtlich bedenkenfrei.

Im Unterschied zur öffentlichen Wahrnehmung zielt die eCall-Initiative jedoch nicht allein auf die Verbesserung der Notfallrettung ab. Der europäische Gesetzgeber verfolgt hiermit zugleich industriepolitische Zwecke. Der eCall soll die technische Plattform für die weitere Informatisierung des Autos bilden. Mit dem verpflichtenden Einbau der für den Notruf erforderlichen Technik ist künftig jedes europäische Neufahrzeug internet- und telematikfähig. Damit soll die Grundlage für innovative Mehrwertdienste rund um das Automobil geschaffen und die Stellung der europäischen Automobil-, Kommunikations- und Informationsindustrie auf den Weltmärkten gestärkt werden. Die Verordnung sieht dementsprechend vor, dass rund um das bordeigene Notrufsystem umfangreiche Zusatzdienste angeboten werden können.

In diesen Zusatzdiensten liegt die eigentliche Gefahr für die informationelle Selbstbestimmung. Die strengen Datenschutzbestimmungen der Verordnung gelten ausschließlich für den Notruf in seiner Basisfunktion. Die Zusatzdienste werden hiervon nicht erfasst. Diese dürfen ständig mit dem Netz verbunden sein und können theoretisch uneingeschränkt Daten übermitteln. Insbesondere die privaten eCall-Systeme sind vor diesem Hintergrund bedenklich. Eingebettet in die modernen Bordsysteme ist bei entsprechender Gestaltung praktisch die gesamte automobile Wertschöpfungskette in der Lage, unbegrenzt Daten über das Fahrzeug und das Fahrverhalten zu gewinnen. Die wirtschaftliche Bedeutung liegt auf der Hand. Schätzungen gehen davon aus, dass das Geschäft mit dem vernetzten Auto bereits im Jahr 2020 weltweit die Schwelle von 100 Milliarden Euro übersteigt.[61]

Der Ehrgeiz des europäischen Gesetzgebers, dem Datenschutz vor diesem wirtschaftlichen Hintergrund Geltung zu verschaffen, ist offenkundig begrenzt. Die Verordnung fordert für die Zusatzdienste im Grunde nur eine entsprechende Einwilligung des Nutzers. Die Verantwortung für den Datenschutz wird damit im Wesentlichen auf den Verbraucher verlagert. Dies ist weder sachgerecht noch angemessen. Als normatives Schutzkonzept ist die Einwilligung nicht geeignet, um die aus den Zusatzdiensten resultierenden Gefahren einzudämmen. Die Einwilligung wird zudem dadurch entwertet, dass sie im Umfeld des lebensrettenden Notrufs erfolgt. Dies birgt die Gefahr, dass Notfallrettung und Umfang der zugestandenen Datenübermittlung in gedanklichen Zusammenhang gebracht werden.

Auch gesetzgebungspolitisch ist die Verordnung in hohem Maße kritikwürdig. Sie verbindet Notfallrettung mit Industrieförderung und nimmt hierdurch billigend in Kauf, dass der eCall unter dem Deckmantel der Lebensrettung zum Türöffner für weitreichende Datennutzungen wird.

Es bleibt zu hoffen, dass die datenschutzrechtliche Lücke zügig geschlossen wird. Immer mehr Autohersteller und Diensteanbieter bauen Services rund um den Notruf 112 aus. Datenschutzfreundliche Konzepte für das Zusammenwachsen von Fahrzeug und Internet existieren jedoch erst in Ansätzen. Neben der Sensibilisierung der Verbraucher sollten daher auf europäischer Ebene rasch verbindliche Rahmenbedingungen gesetzt werden. Nur mit ausreichenden bereichsspezifischen Regelungen lässt sich ein angemessenes Schutzniveau für Datenverarbeitungen rund um das Automobil sicherstellen.

61 Vgl. Pressemitteilung PwC Strategy& vom 9.9.2013, abrufbar unter http://www.strategyand.pwc.com/de/home/Presse/Pressemitteilungen/pressemitteilung-detail/connected-car-2103-de.

Prof. Dr. Lüdemann

Prof. Dr. Lüdemann ist seit 2009 Professor für Wirtschafts- und Wettbewerbsrecht an der Hochschule Osnabrück. Zuvor war er u.a. Syndikusanwalt und Geschäftsführer im Volkswagen Konzern. Volker Lüdemann forscht und lehrt im Bereich des Datenschutzes und verfügt über umfangreiche Erfahrungen als externer Datenschutzbeauftragter für öffentliche und nicht öffentliche Stellen.

Christin Sengstacken

Christin Sengstacken, LL.M. ist Wissenschaftliche Mitarbeiterin am Forschungszentrum Energiewirtschaft und Energierecht (fee). Neben der Projektleitung Recht des Binnenforschungsschwerpunkts City Grid beschäftigt sie sich schwerpunktmäßig mit aktuellen Fragen des Datenschutzrechts.

Timo Bittner LL.M., LL.M.

Der Datenschutzbeauftragte gemäß EU-Datenschutz-Grundverordnungs-Entwurf

Entwurf des LIBE-Ausschusses – ein Schritt in die richtige Richtung für den zukünftigen DSB?

Externe und interne betriebliche Datenschutzbeauftragte (DSB) sind nicht nur darüber verunsichert, welche Aufgaben ihnen zukünftig zukommen und welche Rahmenbedingungen ihnen dabei gegeben sein würden, sondern auch darüber, ob sie ihrer bisherigen Funktion überhaupt noch nachkommen dürfen. Ursprünglich sollte die Verordnung noch vor den Wahlen des Europäischen Parlamentes verabschiedet werden. Der ursprüngliche Entwurf der Europäischen Kommission für eine Datenschutzgrundverordnung[1] vom 25.01.2012 sah klare Unterschiede zu den Vorschriften des BDSG vor. Nach dem Entwurf des Berichterstatters des Europäischen Parlaments für die geplante Datenschutz-Grundverordnung[2] vom 17.12.2012 stellt nun auch der am 21.10.2013 durch den LIBE-Ausschuss bestätigte Entwurf[3] eine weitere Annäherung[4] an das BDSG dar, obwohl dieser ein Kompromiss ist. Die EU-Kommissarin Viviane Reding gab jedoch bereits im Januar 2014 bekannt, dass die Verabschiedung der Verordnung vor den Wahlen des Europäischen Parlamentes nicht mehr vorgenommen werden kann und stellte auf eine eventuelle Verabschiedung der Verordnung in der zweiten Hälfte des Jahres 2014 ab[5].

Im vorliegenden Artikel soll kritisch der Entwurf betrachtet werden, welcher nun nach der Neuordnung des Europäischen Parlamentes die Grundlage für den Trilog zwischen Europäischer Kommission, Europäischem Parlament und Europäischem Rat bilden soll. Hierzu wird aufgezeigt, welche Punkte durch den aktuellen Entwurf geändert wurden sowie welche weiteren Unterschiede zum BDSG bestehen und was diese in der Praxis für Folgen haben könnten. Dabei wird weiterer Korrekturbedarf identifiziert, worauf in Hinblick auf die Praxis des Datenschutzbeauftragten und die Ziele des Datenschutzes entsprechende Empfehlungen ausgesprochen werden.

I. Einführung – Erforderlichkeit des Datenschutzbeauftragten

Der europäische Gesetzgeber hat verspätet erkannt, dass die europäische Datenschutzrichtlinie 95/46/EG (DSRL) veraltet ist und den Entwicklungen seit 1995 nicht mehr gerecht wird. Hierbei ist nicht nur an technische Entwicklungen, z.B. das Internet und zugehörige Neuheiten namens Soziale Netzwerke und Suchmaschinen zu denken, sondern auch an den ubiquitären Einsatz von mobilen Endgeräten, wie z.B. Smartphones, sowie an den Wandel unternehmerischer Orientierung. Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist und bleibt zum einen für viele Unternehmen ein Nebenbestandteil der täglichen Praxis, zum anderen ist diese Tätigkeit zu einem eigenen Geschäftsfeld geworden und stellt für eine nicht unerhebliche Zahl von Unternehmen das Kerngeschäftsfeld dar. Unzulässige Erhebungen, Übermittlungen und Nutzungen von Daten durch öffentliche und nicht öffentliche Stellen, insbesondere das Erstellen von Bewegungs- und Verhaltensprofilen, sind die daraus resultierenden Risiken. Diese bestehen für den Bürger nicht nur in der Rolle des Verbrauchers, sondern auch in der des Beschäftigten, da all diese Risiken dem Bürger sowahl im Privat- als auch im Berufsleben drohen.

Eine entgegensteuernde und Risiken vorbeugende Funktion kann hier der betriebliche DSB einnehmen. Dieser kann Einfluss auf die internen Datenverarbeitungsvorgänge von Unternehmen nehmen und dabei dem Beschäftigtendatenschutz dienen. Ferner kann er aber auch den Verbrauchern behilflich sein, da er z.B. auf eine ausschließlich gesetzeskonforme Datenverarbeitung von Kundendaten hinwirken kann. Hierdurch erhält der DSB mehr als je zuvor seine Daseinsberechtigung, welche auch aus seinen zahlreichen Aufgaben hervorgeht.

Im Gegensatz zum Rat der Europäischen Union, welcher die Entscheidung über eine Bestellpflicht weiterhin in den Händen der europäischen Mitgliedsstaaten belassen möchte[6], und zur DSRL, welche den bestellten DSB außerhalb von Erwägungsgründen nur kurz als Bedingung für den Wegfall der Meldepflicht in Art. 18 Abs. 2 und als durchführende Person der Vorabkontrolle in Art. 20 Abs. 2 erwähnt, hat auch die Europäische Kommission diese Tatsache zu berücksichtigen gewusst und dem DSB im Entwurf vom 25.01.2012 einen angemessenen Platz in den Art. 35-37 eingeräumt. Diese regeln die Pflicht und Art der Bestellung des DSB, seine Position und seine Aufgaben. Diese ausführlicheren Regelungen könnten nun einen klareren und festeren Rahmen als die DSRL setzen, was sowohl dem DSB als auch der verantwortlichen Stelle zu Vor- und Nachteilen gereichen könnte.

1 Europäische Kommission, KOM (2012) endg. v. 25.1.2012.

2 Jan Philipp Albrecht, Entwurf eines Berichts v. 17.12.2012.

3 Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE), Entwurf v. 07.10.2013.

4 Jaspers/Reif, RDV 2012, 78, (84).

5 Beuth, Zeit Online vom 23. Januar 2014, abrufbar unter: http://www.zeit.de/digital/datenschutz/2014-01/datenschutzreform-nicht-mehr-vor-europawahl.

6 Council of the European Union, Document 10227/13 vom 31.05.2013, Nr. 24.

II. Der Datenschutzbeauftragte gemäß LIBE-Ausschuss-Entwurf

Im Folgenden wird im Detail auf die drei Regelungsthematiken eingegangen, welche den betrieblichen Datenschutzbeauftragten direkt betreffen.

1. Die Bestellung

a) Grundlegende Regelungen

Die Voraussetzungen des BDSG, unter welchen die Bestellung eines DSB zwingend ist, sind für Laien undurchsichtig und unverständlich. § 4f Abs. 1 hängt die Bestellpflicht nicht nur an der Anzahl der datenverarbeitenden Mitarbeiter innerhalb der verantwortliche Stelle auf, sondern auch daran, ob die Verarbeitungen mittels Datenverarbeitungsanlagen vorgenommen werden. Der LIBE-Ausschuss-Entwurf greift das zweite Kriterium nicht auf und unterscheidet nicht zwischen automatisierten und nicht-automatisierten Verarbeitungen. Dies zeigt auch die entsprechende Definition des Art. 4 Abs. 3 LIBE-Ausschuss-Entwurf. Dem BDSG folgend, bestimmt Art. 35 Abs. 1 lit. (a) LIBE-Ausschuss-Entwurf einheitlich, dass alle öffentlichen Stellen, welche personenbezogene Daten verarbeiten, einen DSB zu bestellen haben. Diese Vereinfachung ist zeitgemäß, wird aber wahrscheinlich kaum praktische Auswirkungen haben, da gegenwärtig kaum noch eine Behörde Daten ohne PC verarbeitet und deshalb auch bisher eine Bestellpflicht für annähernd alle Behörden bestand. Auch bei nicht öffentlichen Stellen ist kaum noch an eine vollständige Datenverarbeitung ohne Datenverarbeitungsanlagen zu denken. Datenerhebungen in Papierform, beispielsweise an Messeständen oder bei Gewinnspielen, werden später gescannt oder manuell in elektronische Systeme übertragen.

Darüber hinaus ist auffällig, dass der offizielle Entwurf keine Pflicht zur Einhaltung der Schriftform bei der Bestellung konstituiert. Dieser Mangel besteht auch im LIBE-Ausschuss-Entwurf weiter, was zu einem Nachteil für den DSB werden könnte. Das Schriftformerfordernis diente bislang einer nachhaltigen Aufgabenbestimmung, falls diese um nicht bereits gesetzlich aufgeführte Aufgaben erweitert werden sollten. Zudem erfüllt diese üblicherweise eine Warnfunktion. Sie führt auch dem weniger erfahrenen DSB noch einmal abschließend vor Augen, worauf er sich verbindlich festlegt. Zudem hat ein schriftlicher Vertrag für beide Seiten die klassische Beweisfunktion. In Anbetracht der Ermangelung dieser Vorteile bei einem fehlenden Schriftformerfordernis sollte selbige in einem finalen Entwurf aufgenommen werden.

Eine Frist, innerhalb welcher ein DSB nach Aufnahme der Tätigkeit der verantwortlichen Stelle zu bestellen ist, enthält der LIBE-Ausschuss-Entwurf weder für öffentliche noch für nicht öffentliche Stellen, wohingegen § 4f Abs. 1 Satz 2 BDSG BDSG nur nicht öffentliche Stellen hierzu innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Dass diese Frist nicht mehr bestehen soll ist begrüßenswert, denn zum einen ist nicht ersichtlich, warum nicht öffentliche Stellen hierbei einer strengeren Regelung unterliegen sollten. Zum anderen liegt ohne Gewährung einer Frist eine sofortige Bestellpflicht vor, was dem Datenschutz zuträglich sein könnte. Auch die Frage, wann die verantwortliche Stelle ihre Tätigkeit konkret aufnimmt[7], würde obsolet werden.

In Bezug auf öffentliche Stellen hält Art. 35 Abs. 3 LIBE-Ausschuss-Entwurf ferner fest, dass diese für mehrere Bereiche einen gemeinsamen DSB bestellen können. Soweit ergeben sich keine neuen Besonderheiten bezüglich der Bestellung eines DSB durch öffentliche Stellen. In Bezug auf Unternehmensgruppen hat bereits Art. 35 Abs. 2 des Entwurfs der Europäischen Kommission angeführt, dass diese einen hauptverantwortlichen DSB bestellen können. Der LIBE-Ausschuss-Entwurf hat dies jedoch an die vernünftige Bedingung geknüpft, dass der hauptverantwortliche DSB von jedem Unternehmen aus gut zu erreichen ist. Die Regelung könnte darauf abzielen, dass Unternehmensgruppen weltweit vertreten sind. Im Hinblick darauf sollte der DSB ggf. die erforderlichen Sprachkenntnisse aufweisen und erforderliches Hilfspersonal erhalten. Es ist offensichtlich, dass die Erfüllung der erforderlichen Qualifikationen aus Art. 35 Abs. 5 eine weitere Voraussetzung ist[8].

In wörtlicher Erwähnung ist dem BDSG gegenüber jedoch Art. 35 Abs. 9 LIBE-Ausschuss-Entwurf neu. Demnach muss die verantwortliche Stelle der zuständigen Aufsichtsbehörde den Namen und die Kontaktdaten des DSB mitteilen, was bei Bedarf die Aufnahme einer entsprechenden Kommunikation beschleunigen würde. Die Rechte der Betroffenen in Art. 35 Abs. 10 LIBE-Ausschuss-Entwurf, sich mit dem DSB in Kontakt zu setzen und diesem gegenüber die Wahrnehmung der Rechte aus dem Entwurf zu beantragen, entsprechen prinzipiell denen des § 4f Abs. 5 Satz 2 BDSG. Die in Art. 35 Abs. 9 Satz 2 Berichterstatter-Entwurf angedachte Pflicht, dass die verantwortliche Stelle der Aufsichtsbehörde mitteilen muss, dass sie keinen DSB bestellt, ist nicht im LIBE-Ausschuss-Entwurf implementiert worden. Diese hätte jedoch möglicherweise dafür gesorgt, dass sich Unternehmen mehr mit der Thematik auseinandersetzen und ihrer Bestellungspflicht nachkommen[9].

b) Die Schwellenwerte

Einer der strittigsten und meist diskutiertesten Punkte, neben dem Recht auf Vergessen-Werden, der Datenportabilität und den zahlreichen Ermächtigungen der Europäischen Kommission, delegierte Rechtsakte zu erlassen, stellt sicherlich der Schwellenwert von 250 Mitarbeitern dar, welcher in nicht öffentlichen Stellen die Bestellpflicht eines DSB begründet. Dieser Schwellenwert aus Art. 35 Abs. 1 des offiziellen Entwurfs, welcher besonders in Deutschland zu häufiger Kritik geführt hat[10], ist sicherlich auch für betriebliche DSB die Vorschrift mit der meisten Brisanz und bedarf deshalb einer eingehenderen Betrachtung.

7 Vgl. Simitis, in: Simitis, Kommentar zum Bundesdatenschutzgesetz, 7. Aufl. 2011, § 4f Rdnr. 54f.; Bergmann/Möhrle/Herb, Datenschutzrecht, Stand Juli 2012, § 4f Rdnr. 54.

8 So wohl auch: Klug, RDV 2014, 90 (91).

9 So auch: Klug, RDV 2013, 14 (15).

10 Nur drei von vielen Bsp.: Hornung, ZD 2012, 99 (104); Jaspers/Reif, RDV 2012, 78 (78); GDD, Meldung vom 23.10.2013, abrufbar unter: http://www.gdd.de/aktuelles/nachrichten/.

Die Bestellpflicht für nicht öffentliche Stellen, respektive der Wirtschaft, war im offiziellen Entwurf vorgesehen, wenn ein entsprechendes Unternehmen 250 oder mehr Arbeitnehmer beschäftigt. Hierbei erscheint nicht nur die willkürliche Grenze von 250 Mitarbeitern fragwürdig, sondern auch, die Bestellpflicht von der Mitarbeiterzahl abhängig zu machen. Das Kriterium der beschäftigten Personen im Unternehmen wurde bereits in der Vergangenheit des BDSG bemängelt[11]. Zutreffend wurde bereits kritisiert, dass auch ein Unternehmen mit weniger als 10 Mitarbeitern theoretisch dazu fähig sein kann, die Daten von hunderttausenden Betroffenen zu verarbeiten[12]. Ein Industrieunternehmen mit 1000 Beschäftigten kann sich hingegen darauf beschränken, die Daten von Mitarbeitern zu ausschließlich erforderlichen Zwecken, wie der Lohnabrechnung etc., und ansonsten nur die Daten von Unternehmen zu verarbeiten.

Möglicherweise hat auch der LIBE-Ausschuss diesen Widerspruch erkannt, denn die Bestellpflicht soll nun bestehen, wenn mehr Daten als von 5000 Betroffenen durch die verantwortliche Stelle verarbeitet werden. Dieser Schwellenwert kann schnell erreicht sein. Verschickt ein Unternehmen einmalig Werbeprospekte an 5000 natürliche Personen, so wäre demnach bereits ein DSB zu bestellen. Es bleibt jedoch zweifelhaft, ob diese Regelung den Zweck vollständig erfüllt, denn sollte ein Unternehmen Daten von 4900 Betroffenen verarbeiten oder schlicht 4900 Beschäftigte aufweisen, wäre kein DSB zu bestellen. Der Beschäftigtendatenschutz in Industrieunternehmen könnte dadurch ein Stück weit gefährdet sein, da dahingehend der Wert zu hoch angesetzt scheint. Der Wert von 500 Betroffenen im Entwurf des Berichterstatters[13] wurde deutlich nach oben verschoben, was nicht begrüßenswert ist.

Ferner bleibt es zweifelhaft, ob Unternehmen stets zu dem Aufwand bereit sind, eine Auflistung darüber zu erstellen, ob und wobei die Daten von wie vielen Betroffenen verarbeitet werden. Diese Prozedur könnte von manchen Unternehmen als ein lästiges Verfahren angesehen werden, was darüber hinaus aus deren Sicht auch noch zu einem vielleicht unwillkommenen Ergebnis führen könnte. Angesichts dessen bleibt es fraglich, ob die Zahl der Betroffenen ein gutes Kriterium für die Bestellpflicht ist. Grundsätzlich könnte die Arbeitnehmerzahl ein Anhaltspunkt dafür sein, wann ein Unternehmen allein aufgrund seiner Größe einen DSB bestellen sollte, sowie die Zahl der Betroffenen ein Hinweis darauf darstellen kann, dass die Bestellung eines DSB erforderlich ist.

c) Weitere Kriterien

Entscheidend für eine Bestellpflicht sollte in erster Linie der Zweck der Datenverarbeitung sowie die Sensitivität der verarbeiteten Daten sein[14]. Art. 35 Abs. 1 lit. (c) des offiziellen Entwurfs sowie der neu eingefügte lit. (d) LIBE-Ausschuss-Entwurf setzen hier an der richtigen Stelle an. Demnach müsste ein DSB bestellt werden, wenn die Kerntätigkeit des Unternehmens in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich macht oder die Kerntätigkeit darin besteht, besondere Kategorien personenbezogener Daten, Standortdaten, Daten von Kindern oder Arbeitnehmern in umfangreichen Datenmanagementsystemen zu verarbeiten. Diese Vorschrift wird dem entsprechenden Schutzzweck, welchen eine Bestellung hat, wesentlich besser gerecht, denn sie umfasst neben den bisher aus dem BDSG bereits bekannten besonderen personenbezogenen Daten auch die Verarbeitung von weiteren besonders schutzwürdigen personenbezogenen Daten, ohne dabei an die Zahl der Mitarbeiter oder der Betroffenen sowie die näheren Verarbeitungsumstände anzuknüpfen. Der Norm nach würde bereits eine Bestellpflicht bestehen, wenn regelmäßig Standortdaten von Betroffenen über ihre Smartphones erhoben werden oder fortwährend ein Kauf- oder Konsumverhalten über das Internet analysiert wird. Außerdem könnte die Verarbeitung von Beschäftigtendaten durch den Arbeitgeber sowie die Verarbeitung der Daten von Kindern durch beispielsweise Ärzte und Krankenhäuser abgedeckt sein, insofern dabei in irgendeiner Form umfangreiche Datenmanagementsysteme verwendet werden. Bisher sind solche Systeme zwar nicht näher definiert. Es ist jedoch anzunehmen, dass hierunter typischerweise sowohl elektronische Datenbanken im Sinne von eigenständigen Programmen zu verstehen sind, als auch simple Listen, wie z.B. Excel-Tabellen, vorausgesetzt, diese enthalten eine nicht unerhebliche Anzahl an personenbezogenen Daten.

Die Änderungen des Entwurfs bezogen auf die Bestellung des DSB sind somit zweckmäßig und zielführend, da ihnen nach immer eine Bestellung vorgenommen werden muss, wenn für die Betroffenen ein erhöhtes Risiko durch die Verarbeitung von besonders sensiblen Daten besteht. Nicht ganz unbedenklich erscheint jedoch die Ergänzung des Erwägungsgrundes 75. Demnach sollen archivierte Daten, welche nicht Gegenstand der normalen Datenverarbeitung und von Zugriff und Veränderung ausgeschlossen sind, nicht bei der Ermittlung berücksichtigt werden, ob ein DSB zu bestellen ist oder nicht. Sollten hiermit nur gesperrte Daten gemeint sein, welche aufgrund von Aufbewahrungsvorschriften gespeichert werden müssen[15], ergibt die Ausnahme einen Sinn. Kritisch erscheint es jedoch, wenn hierunter auch Daten fallen, welche möglicherweise einen sensiblen Inhalt haben und nur zeitweise von Zugriff, Verarbeitung und Nutzung ausgenommen sind.

d) Kündigung

Trotz dieser positiven Änderungen könnte sich bei Inkrafttreten der Vorschläge des LIBE-Ausschuss-Entwurfs der Umstand ergeben, dass für manche nicht öffentliche Stellen die bisher

11 Simitis, in: Bundesdatenschutzgesetz, 7. Aufl. 2011, § 4f Rdnr. 16; Scheja, in: Taeger/Gabel, Kommentar zum BDSG, 2010, § 4f Rdnr. 23.

12 Scheja, in: Taeger/Gabel, Kommentar zum BDSG, 2010, § 4f Rdnr. 23.

13 ENTWURF EINES BERICHTS über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 148.

14 Auch als wichtige Kriterien angeführt durch: Klug, RDV 2013, 129 (135).

15 Klug, RDV 2014, 90 (91).

bestehende Bestellpflicht entfällt. Dies wäre z.B. denkbar, wenn eine nicht öffentliche Stelle mehr als 9 Mitarbeiter mit der Verarbeitung von personenbezogenen Daten beschäftigt, hingegen aber kein Tatbestand des Art. 35 Abs. 1 LIBE-Ausschuss-Entwurf erfüllt wäre. Dies wirft jedoch die Frage auf, ob die verantwortliche Stelle in solch einem Fall das Recht hätte, den DSB abzuberufen. Bei der Beurteilung dieser Frage scheint der Zeitpunkt der angedachten Abberufung grundsätzlich eine wesentliche Rolle zu spielen. Wäre das BDSG noch in Kraft, so kann der DSB nur abberufen bzw. gekündigt werden, wenn dies mit den Bestimmungen des § 4f Abs. 3 BDSG vereinbar wäre. Der künftige Wegfall der Bestellpflicht durch Inkrafttreten der Vorschläge des LIBE-Ausschuss-Entwurfs würde jedoch keine ausreichende Begründung für eine Kündigung gemäß § 626 Abs. 1 BGB darstellen[16]. Wäre der LIBE-Ausschuss-Entwurf bereits in Kraft getreten und würde die Bestellpflicht anschließend wegfallen, weil kein Tatbestand des Art. 35 Abs. 1 LIBE-Ausschuss-Entwurf erfüllt wäre, so erschienen die Möglichkeiten, den DSB abzuberufen ebenso gering, da Art. 35 Abs. 7 Satz 3 LIBE-Ausschuss-Entwurf abschließend regelt, dass der DSB während seiner Bestellung nur abberufen werden kann, wenn er die Voraussetzungen für die Erfüllung seiner Pflichten nicht mehr erfüllt. Dass der angeführte Art. 35 Abs. 7 Satz 3 des LIBE-Ausschuss-Entwurfs eine abschließende Nennung von zulässigen Kündigungsgründen ist, untermauert auch die Empfehlung des Erwägungsgrundes 75 des LIBE-Ausschuss-Entwurfs. Dieser konstatiert, dass DSB einen besonderen Kündigungsschutz erfahren sollten.

Zwischen einer Kündigung und einer Abberufung unterscheidet der LIBE-Ausschuss-Entwurf ferner nicht.

Dies zeigt, dass eine Abberufung auf Grundlage des Wegfalls der Bestellpflicht durch die Bestimmungen des LIBE-Ausschuss-Entwurfs zu keinem Zeitpunkt zulässig wäre, insofern dieser Entwurf verabschiedet werden sollte. Dem Wortlaut nach kann der DSB nicht einmal mehr im Fall einer Fusion abbestellt werden[17]. Dies gilt auch für externe DSB.[18] Generell sind jedoch Kündigungen, welche tatsächlich auf einem Grund basieren, der eine fristlose Kündigung gemäß § 626 Abs. 1 BGB rechtfertigt, zulässig. Verantwortliche Stellen, welche nicht nur im geringen Umfang personenbezogene Daten verarbeiten, sollten im Hinblick auf die neuen Anforderungen einer möglichen europäischen Verordnung jedoch gut abwägen, ob es sinnvoller ist, einen DSB freiwillig zu bestellen oder zu versuchen, dessen Bestellung zu beenden[19]. Obwohl es nicht unbedingt erforderlich erscheint, erwähnt Art. 35 Abs. 4 LIBE-Ausschuss-Entwurf explizit, dass auch eine freiwillige Bestellung zulässig ist.

e) Dauer und Form der Bestellung

Auch Art. 35 Abs. 8 LIBE-Ausschuss-Entwurf, in dem festgehalten wird, dass der DSB Arbeitnehmer oder Dienstleister, respektive interner oder externer DSB, sein kann, erscheint überflüssig. Bereits Art. 35 Abs. 7 Satz 1 LIBE-Ausschuss-Entwurf erwähnt beiläufig, dass der DSB für mindestens 4 Jahre bestellt werden muss, wenn dieser Arbeitnehmer ist, und für nicht weniger als 2 Jahre bestellt werden darf, wenn es sich um einen externen Dienstleister handelt. Dies nimmt bereits vorweg, dass es möglich sein muss, einen internen oder externen DSB zu bestellen.

Im offiziellen Entwurf waren für interne und externe DSB 2 Jahre Mindestbestelldauer vorgesehen. Dies zumindest für interne DSB zu erhöhen, ist ein guter Vorschlag, da der Zeitraum von 4 Jahren für die Implementierung einer vollständigen Datenschutzorganisation angemessener erscheint[20], da besonders Teilzeit-DSB nicht immer genügend Zeit für die Erfüllung ihrer Aufgaben haben. Hingegen ist nicht ganz nachvollziehbar, warum für externe DSB nur 2 Jahre vorgesehen sind. Denkbar ist, dass diese als Dienstleister einen geringeren Schutzbedarf haben oder die verantwortliche Stelle im Zweifel nicht für die Dauer von 4 Jahren an einen Dienstleister gebunden sein soll. Art. 35 Abs. 7 Satz 2 LIBE-Ausschuss-Entwurf hält fest, dass der DSB nach Ablauf der Zeit erneut bestellt werden kann. Auch dies ist ohne schriftliche Fixierung offensichtlich, da der Entwurf sich nicht entgegenstehend äußert. Vielmehr hätte der Entwurf klarstellen können, dass auch eine juristische Person als externer DSB bestellt werden kann, was bisher in Deutschland strittig ist[21]. Da aber auch mittels Dienstleistungsvertrag ein DSB bestellt werden kann und der Entwurf nicht ausdrücklich die Bestellung einer juristischen Person verbietet, würde diese Frage der Vergangenheit angehören.

Gegenüber dem BDSG wird in allen Entwurfsversionen in Art. 35 Abs. 6 und in den Erwägungsgründen 75 und 75a des LIBE-Ausschuss-Entwurfs festgehalten, dass ein DSB in Teil- oder Vollzeit beschäftigt werden kann. Diese Klarstellung ermöglicht eine Beibehaltung der beiden Beschäftigungsarten, welche in der deutschen Datenschutzpraxis anzutreffen sind.

f) Anforderungen an den DSB

Die Anforderungen an die Fachkunde und Zuverlässigkeit aus § 4f Abs. 2 Satz 1 BDSG, welche an den DSB bereits vor der Bestellung gestellt werden, finden sich in Art. 35 Abs. 5 und 6 LIBE-Ausschuss-Entwurf wieder. Die Fachkunde wird im Verordnungsentwurf selbst, wie im BDSG, nicht näher definiert. Hingegen wird aber darauf hingewiesen, dass sich der Grad des erforderlichen Fachwissens nach den jeweiligen Arten der Datenverarbeitungen und dem erforderlichen Schutz der Daten bestimmt. Diese sinnvolle Differenzierung entspricht § 4f Abs. 2 Satz 2 BDSG. Grundlegend hält aber der neue Erwägungsgrund 75a des LIBE-Ausschuss-Entwurfs Mindestanforderungen fest. Demnach zählen dazu umfangreiche Kenntnisse im Datenschutzrecht und dessen Anwendung sowie der zugehörigen technischen und organisatorischen Maßnahmen und Verfahren; Wissen über technische Anforderungen zur Umsetzung

16 Explizite Ausführungen zum deutschen Kündigungsschutz für den DSB: Gola/Schomerus, Kommentar zum BDSG, 11. Aufl., 2012, § 4f Rn. 40 ff.

17 So auch: Hoeren, ZD 2012, 355 (357).

18 Gleicher Meinung: Klug, RDV 2014, 90 (92).

19 Selber Meinung: Klug, RDV 2013, 14 (17).

20 Vgl.: Hoeren, ZD 2012, 355 (357).

21 Unterschiedlicher Meinung z.B.: v. d. Bussche, in: Plath, Kommentar zum BDSG, 2013, § 4f Rdnr. 26; Däubler, in: Däubler/Klebe/Wedde/Weichert, Kommentar zum Bundesdatenschutzgesetz, 3. Aufl. 2010, § 4f Rdnr. 22.

von Privacy by Design, Privacy by Default und Datensicherheit; Kenntnisse sowohl im Zusammenhang mit der Größe und Branche der verantwortlichen Stelle als auch der Sensibilität der zu verarbeitenden Daten und die Fähigkeit, Kontrollen, Beratungen, Dokumentationen, Protokolldateianalysen und Zusammenarbeiten mit der Arbeitnehmervertretung durchzuführen. Dieser Vorschlag für einen relativ hohen Mindeststandard[22] könnte zukünftig durch genauere Ausführungen seitens der Verbände, wie z.B. den BvD e.V. und den GDD e.V., konkretisiert werden[23]. Die treffende Aufzählung, insbesondere die wörtlichen Erwähnungen von Privacy by design und Privacy by Default, welche der ubiquitären Datenverarbeitung gerecht werden[24], verdient Anerkennung.

Die Zuverlässigkeit ist hingegen nicht wörtlich erwähnt, wohingegen Art. 35 Abs. 6 LIBE-Ausschuss-Entwurf aber festhält, dass kein Interessenskonflikt bestehen darf. Diese Anforderung stellt das BDSG nicht wörtlich, wohingegen die Literatur diese Anforderung an DSB bereits seit langem einstimmig stellt[25]. Dass der DSB auch unter dem LIBE-Ausschuss-Entwurf die entsprechende Zuverlässigkeit besitzen muss, ist jedoch aufgrund seiner Position und Aufgaben evident.

2. Die Position

Bezogen auf die Position des DSB, insbesondere seine Stellung innerhalb der verantwortlichen Stelle, und seine Rechte und Pflichten, würden sich dem BDSG gegenüber keine großen Änderungen ergeben. In Anlehnung an § 4g Abs. 1 Satz 4 Nr. 1 BDSG gewährleistet Art. 36 Abs. 1 LIBE-Ausschuss-Entwurf dem DSB eine ordnungsgemäße und frühzeitige Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen, wobei dies sinnigerweise im Gegensatz zum BDSG nicht nur auf die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme bezogen ist.

Art. 36 Abs. 2 Satz 1 LIBE-Ausschuss-Entwurf sichert ferner die bisher bestehende Weisungsfreiheit und dadurch auch die bestehende Unabhängigkeit. Diese essentiellen Voraussetzungen für die Aufgabenerfüllung des DSB ermöglichen es nicht nur in der Praxis, dass der DSB sich überhaupt seinen Aufgaben widmen kann, sondern auch, dass der DSB frei in der Ergebnisfindung ist und bei Zulässigkeitsprüfungen sowie Vorabkontrollen nicht zu vorgegebenen Resultaten kommen muss. Besonders interne DSB ziehen aufgrund ihrer ausgeprägten Abhängigkeit zum Arbeitgeber hieraus einen hohen Nutzen.

Die unmittelbare Unterstellung des DSB unter die Geschäftsführung scheint sich darin wiederzufinden, dass der DSB unmittelbar der Geschäftsführung berichtet. Diese sinnvolle Festlegung des Art. 36 Abs. 2 Satz 2 LIBE-Ausschuss-Entwurf scheint im Gegensatz zum BDSG nicht ausschließlich eine Einordnung im Organigramm zu sein, sondern konstatiert auch eine Berichtspflicht, welche dem DSB gleichzeitig Gehör bei der verantwortlichen Stelle verschafft. Diese Regelung scheint den Informationsbedürfnissen der Geschäftsführung ebenso gerecht zu werden wie dem notwendigen Kontaktbedarf zur Geschäftsführung seitens des DSB. Dieser besteht darin, dass er so leichter auf die Einhaltung des Datenschutzes hinwirken kann. Die Ergänzungen des Art. 36 Abs. 2 Satz 3 LIBE-Ausschuss-Entwurf bestimmen zudem, dass die verantwortliche Stelle ein Geschäftsführungsmitglied zu bestimmen hat, welches für die Einhaltung der Bestimmungen der Verordnung verantwortlich ist. Dies könnte zu mehr Datenschutz-Compliance führen und dem DSB mehr förderliche Aufmerksamkeit zukommen lassen. Für Fälle von Missachtung der Datenschutzvorschriften werden sich aber auch Fragen zur Haftung für das entsprechende Geschäftsführungsmitglied stellen.

Die Unterstützung des DSB mittels erforderlichem Personal und materiellen Dingen wie Räume, Einrichtungen, Geräte und andere Mittel, welche bereits das BDSG sichert, ist durch Art. 36 Abs. 3 sowie Erwägungsgrund 75a des LIBE-Ausschuss-Entwurfs gewährleistet. Dabei wurde durch den vom LIBE-Ausschuss bestätigten Entwurf explizit hinzugefügt, dass dies auch die Maßnahmen einschließt, welche erforderlich sind, um das Fachwissen des DSB auf einem aktuellen Stand zu erhalten. Dies wurde dem DSB bereits ausdrücklich durch das BDSG zugestanden. Den Bedarf an steter Weiterbildung zeigt bereits allein die Aufgabe, sich fortwährend aus Datenschutzsicht mit neuer Technik zu befassen. Auf Unternehmenskosten besteht dieses Recht bislang für interne DSB, während externen DSB die Kosten angerechnet werden sollen[26]. Im Hinblick darauf, dass andere europäische Mitgliedsstaaten zum großen Teil bislang keine genauen Regelungen bezogen auf den DSB im nationalen Recht etabliert haben, scheint diese Anführung jedoch eine gute Entlehnung aus dem BDSG zu sein.

Von großer Bedeutung[27] sowohl für den DSB als auch für den Datenschutz im Allgemeinen ist der durch den LIBE-Ausschuss eingefügte Art. 35 Abs. 4. Dieser enthält die im offiziellen Entwurf fehlende Schweigepflicht des DSB bezüglich der Identität von Betroffenen und Umständen, welche zu deren Identifizierung führen können. Diese Pflicht ist im Hinblick auf den Beschäftigtendatenschutz unentbehrlich. Mitarbeiter der verantwortlichen Stelle könnten es sonst aus Angst vor einem Konflikt mit dem Arbeitgeber unterlassen, Auskünfte bezogen auf Ihre gespeicherten Daten einzuholen oder jeglichen anderen Datenumgang beim DSB zu rügen, welcher ihnen nicht im Einklang mit dem Datenschutz erscheint.

Sollte der Betroffene den DSB von seiner Schweigepflicht entbinden, so ist dieser gemäß Art. 35 Abs. 4 LIBE-Ausschuss-Entwurf nicht länger an diese gesetzliche Pflicht gebunden. Dem Betroffenen diese Option zu geben, ist sinnvoll, denn eine Schweigepflicht macht nur Sinn, wenn der Betroffene diese auch selbst wünscht. Eine Offenbarung der Identität kann auch im Interesse des Betroffenen sein, da hierdurch Auskünfte zeitnaher erteilt und Maßnahmen im Sinne des Betroffenen schneller eingeleitet werden können. Wenn auch nicht gesetzlich gefordert, sollte der DSB jedoch zwecks Be-

22 Klug, RDV 2014, 90 (92).

23 So auch: Klug, RDV 2013, 14 (17).

24 Klug, RDV 2014, 90 (92).

25 So z.B. bereits: Königshofen, in: Roßnagel, Handbuch Datenschutzrecht, 2003, 5.5 Rdnr. 116.

26 Simitis, in: Simitis, Kommentar zum Bundesdatenschutzgesetz, 7. Aufl. 2011, § 4f Rdnr. 154.

27 Jaspers/Reif, RDV 2012, 78 (83).

weissicherung solange der Schweigepflicht genügen, bis er mehr als eine ausschließlich mündliche Schweigepflichtentbindung erhalten hat. Empfehlenswert ist eine schriftliche Form, welche den Anforderungen der Einwilligung genügt[28]. Eine dahingehende Ergänzung des Entwurfs wäre wünschenswert.

Ein weiterer Mangel des Entwurfs besteht darin, dass dieser auch nach den Änderungen des LIBE-Ausschusses weder über ein Zeugnisverweigerungsrecht für den DSB noch über eine Kündigungsschonfrist für den DSB nach erfolgter Abberufung verfügt. Dies ist ein Nachteil gegenüber dem BDSG. Eine mögliche Folge für Teilzeit-DSB ist, dass diese in der Praxis dazu tendieren könnten, sich mehr an den Bedürfnissen der verantwortlichen Stelle als an den Anforderungen des Datenschutzes zu orientieren, da ansonsten nach Ablauf der Zeit, für welche sie bestellt sind, eine unmittelbare Kündigung möglich ist. Die Unabhängigkeit des DSB könnte hierdurch gefährdet sein[29].

3. Die Aufgaben

Das BDSG trifft nicht viele konkrete Aussagen bezüglich der Aufgaben des DSB. Explizit erwähnen § 4g Abs. 1 Satz 4 Nr. 1 und 2 BDSG, dass der DSB die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme zur Verarbeitung von personenbezogenen Daten zu überwachen und Mitarbeiter mit den Anforderungen des Datenschutzes vertraut zu machen hat. Obwohl der DSB laut Art. 37 Abs. 1 lit. (a) LIBE-Ausschuss-Entwurf ein Datenschutzbewusstsein innerhalb der verantwortlichen Stelle schaffen soll, wäre die Schulung der Mitarbeiter gemäß Art. 37 Abs. 1 lit. (b) LIBE-Ausschuss-Entwurf zukünftig nicht mehr Aufgabe des DSB. Deren Durchführung hätte der DSB de jure nur noch zu überwachen. Es bietet sich jedoch aufgrund der Fachkenntnis des DSB an, selbigen im Zuge der schriftlichen Bestellung auch mit der Durchführung zu betrauen. Dies erspart der verantwortlichen Stelle Kosten, welche sie ansonsten in externes fachkundiges Personal oder spezielle Schulungssoftware investieren müsste.

Die Aufgabe, „zu überwachen", spielt im LIBE-Ausschuss-Entwurf insgesamt eine große Rolle. Der DSB hätte gemäß Art. 37 Abs. 1 lit. (b) LIBE-Ausschuss-Entwurf nicht nur die Umsetzung und Anwendung der Strategien für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten zu überwachen und zu überprüfen, sondern gemäß Art. 37 Abs. 1 lit. (c) LIBE-Ausschuss-Entwurf die Überwachung der Umsetzung und Anwendung des Entwurfs innerhalb der verantwortlichen Stelle, insbesondere die Anforderungen an einen Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, an die Datensicherheit, an die Benachrichtigung der betroffenen Personen und an die Anträge der betroffenen Personen zur Wahrnehmung der ihnen nach diesem Entwurf zustehenden Rechte, vorzunehmen. Grundsätzlich lässt sich all dies auch darunter subsumieren, dass der DSB gemäß § 4g Abs. 1 Satz 1 BDSG auf den Datenschutz und auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hinzuwirken hat. Daran knüpfen auch seine Aufgaben aus Art. 37 Abs. 1 lit. (a) LIBE-Ausschuss-Entwurf, die verantwortliche Stelle über die aus dem Entwurf erwachsenden Pflichten, insbesondere im Hinblick auf die zu ergreifenden technischen und organisatorischen Maßnahmen, zu sensibilisieren, zu unterrichten und zu beraten, an. Diese Tätigkeit und die erhaltenen Antworten hat der DSB zu dokumentieren. Darüber hinaus müsste der DSB gemäß Art. 37 Abs. 1 lit. (f) des offiziellen Entwurfs die Durchführung der Datenschutz-Folgeabschätzung sowie zugehörige Genehmigungen und Konsultationen der Aufsichtsbehörde, die Durchführung von Vorabkontrollen nach Art. 34 LIBE-Ausschuss-Entwurf und Risikoanalysen im Sinne des Art. 32a LIBE-Ausschuss-Entwurf überwachen. Durch die Änderung des Art. 34 Abs. 2 LIBE-Ausschuss-Entwurf, die Einfügung des Art. 37 Abs. 1 lit. (i) sowie eine Ergänzung des Erwägungsgrundes 75 des LIBE-Ausschuss-Entwurfs wäre der DSB für entsprechende Vorabkontrollen selbst zuständig. Aufgrund seines Fachwissens gehören diese Durchführungs- und Überwachungsfunktionen korrekterweise dem DSB zugeordnet[30], was nun auch vorgesehen wäre.

Abschließend müsste der DSB gemäß Art. 37 Abs. 1 lit. (g) LIBE-Ausschuss-Entwurf die auf Anfrage der Aufsichtsbehörde ergriffenen Maßnahmen überwachen sowie innerhalb des Rahmens seiner Zuständigkeit mit der Aufsichtsbehörde kooperieren und erhält ferner das Recht, diese jederzeit zu kontaktieren. Dies würde dem DSB eine schrankenlose Möglichkeit geben, sich jederzeit an die Aufsichtsbehörde zu wenden, zumal er Art. 37 Abs. 1 lit. (h) LIBE-Ausschuss-Entwurf folgend auch im Allgemeinen deren Ansprechpartner[31] bei der verantwortlichen Stelle ist.

Weiterhin kämen dem DSB aber auch Informationspflichten zu. Der neue Art. 37 Abs. 1 lit. (j) LIBE-Ausschuss-Entwurf überträgt dem DSB die Pflicht, die Arbeitnehmervertretung über die Verarbeitung von Beschäftigtendaten aufzuklären. Trotz möglicher Konflikte mit dem Betriebsverfassungsrecht[32] erscheint diese Vorschrift grundsätzlich angebracht, da in manchen Fällen durch diese Pflicht die Arbeitnehmervertretung erst an Informationen gelangt, welche sie zur Wahrnehmung ihrer Aufgaben benötigt. Die schriftliche Aufnahme dieser Pflicht im Entwurf hat jedoch darüber hinaus noch eine andere Bedeutung. Diese begünstigt den DSB gegenüber der verantwortlichen Stelle, denn er muss diesen Informationspflichten eindeutig aufgrund einer gesetzlichen Pflicht nachkommen. Aufgrund dieser Tatsache kann der DSB sein Handeln der verantwortlichen Stelle gegenüber rechtfertigen, falls diese ein solches Handeln rügt. Dies ist ein bemerkenswertes Novum gegenüber dem BDSG. Dagegen soll die Meldepflicht gemäß § 42a Satz 1 BDSG weiterhin der verantwortlichen Stelle obliegen. Der DSB hätte, Art. 37 Abs. 1 lit. (e) LIBE-Ausschuss-Entwurf folgend, die Dokumentation über eine meldepflichtige Datenschutzpanne sowie die zugehörige Benachrichtigung an

28 Däubler, in: Däubler/Klebe/Wedde/Weichert, Kommentar zum Bundesdatenschutzgesetz, 3. Aufl. 2010, § 4f Rdnr. 53; Simitis, in: Simitis, Kommentar zum Bundesdatenschutzgesetz, 7. Aufl. 2011, § 4f Rdnr. 171.

29 Klug, RDV 2013, 14 (16).

30 Selber Ansicht: Jaspers/Reif, RDV 2012, 78 (82).

31 Siehe hierzu: Jaspers/Reif, RDV 2012, 78 (83).

32 Klug, RDV 2014, 90 (92 f.).

die Aufsichtsbehörde und die zugehörige Kommunikation nur zu überwachen.

Fragwürdig ist zunächst, ob der DSB in Zukunft die Verarbeitungen von personenbezogenen Daten selbst zu dokumentieren oder die verantwortliche Stelle dies vorzunehmen hat. Gemäß Art. 37 Abs. 1 lit. (d) LIBE-Ausschuss-Entwurf hat der DSB die Vornahme der Dokumentation sicherzustellen. Die eigentliche Vornahme scheint demnach nicht dem DSB zu obliegen[33], da der europäische Gesetzgeber dies andernfalls sicherlich eindeutiger formuliert hätte. Dem DSB obliegt es dem Entwurf nach vielmehr, auf die verantwortliche Stelle in dem Maß einzuwirken, dass diese der Vornahme der Dokumentation tatsächlich nachkommt. Da dem DSB jedoch keine eigenen Sanktionsmittel zur Verfügung stehen, er aber die Vornahme der Dokumentation sicherzustellen hat, scheint es zu seiner eigenen Entlastung erforderlich[34], entsprechend Art. 37 Abs. 1 lit. (g) LIBE-Ausschuss-Entwurf die Aufsichtsbehörde auf eigene Initiative zu Rate zu ziehen, falls die verantwortliche Stelle sich nachhaltig nicht zur Erfüllung dieser Aufgabe bewegen lässt. Ganz anders stellt sich die Situation jedoch dar, wenn dem DSB durch Vertrag die Aufgabe der Durchführung der Dokumentation übertragen wurde.

III. Fazit

Der LIBE-Ausschuss-Entwurf würde bei Inkrafttreten gute Rahmenbedingungen für den DSB schaffen, was auch dem Datenschutz im Allgemeinen zuträglich ist. Der ursprüngliche Entwurf wurde durch die Änderungen des LIBE-Ausschusses auf positive Art modifiziert. Dennoch enthält der Entwurf weitere Mängel. Das Fehlen des Schriftformerfordernisses bezogen auf die Bestellung des DSB sowie einer Kündigungsschonfrist nach erfolgter Abberufung und Zeugnisverweigerungsrechts sind hier zu nennen. Auch der neue Schwellenwert für die Bestellpflicht des DSB ist zu hoch angesetzt, was auch nicht der Intention des Bundesministeriums des Inneren entsprechen dürfte, den deutschen Datenschutzstandard nicht senken zu wollen[35]. Dennoch sind die Regelungen, welche den DSB betreffen, nach den Änderungen durch den LIBE-Ausschuss grundlegend gelungen und stellen im Vergleich zum offiziellen Entwurf eine Verbesserung dar.

Die Aufgaben des DSB aus dem LIBE-Ausschuss-Entwurf wären im Grundsatz mit denen aus dem BDSG identisch. Bei genauerem Hinsehen lässt sich erkennen, dass Durchführung und Implementierung von Maßnahmen gemäß dem Wortlaut des LIBE-Ausschuss-Entwurfs fast vollständig der verantwortlichen Stelle obliegen würden und der DSB nur eine Überwachungs- und Beratungsfunktion einnehmen soll. Trotzdem scheint seine bisher überwiegende Funktion, auf den Datenschutz hinzuwirken, etwas ausgebaut zu werden. Dies zeigt sich in der Wortwahl „Überwachung". Durch die Entwurfsänderungen des LIBE-Ausschusses wäre die Vorabkontrolle, wie dem BDSG entsprechend, eine Aufgabe des DSB, was zu begrüßen ist. In der Praxis ist jedoch zu erwarten, dass der DSB mit weiteren praktischen Aufgaben und der Unterstützung bei der Erfüllung solcher, wie z.B. bereits bisher bei der Durchführung der Verfahrensdokumentation[36], betraut wird. Von daher ist es zu empfehlen, eine Aufgabenliste direkt in die schriftliche Bestellung aufzunehmen. Die neue Pflicht, die Arbeitnehmervertretung als auch die entsprechende Aufsichtsbehörde zu informieren, ist dem DSB vielmehr eine Hilfe statt eine Last. Im Übrigen sind auch die bisher in Art. 35 und 37 LIBE-Ausschuss-Entwurf enthaltenen Möglichkeiten zum Erlass von delegierten Rechtsakten durch die Europäische Kommission, welche theoretisch nahezu alle Bestimmungen dem Inhalt nach hätte verändern können, gestrichen worden. Dies sorgt für mehr Rechtssicherheit.

Bezogen auf die Bestimmungen zum DSB ist der Entwurf des LIBE-Ausschusses somit ein Schritt in die richtige Richtung. Trotzdem wäre es wünschenswert, dass unter Beibehaltung der Richtung ein weiterer Schritt erfolgt, bevor der Entwurf endgültig verabschiedet würde. Dieser zweite Schritt würde dazu führen, dass DSB den Unternehmen und Behörden effizienter dabei zur Seite stehen könnten, den Anforderungen des Datenschutzes gerecht zu werden, und somit mehr zur informationellen Selbstbestimmung der Bürger beitragen könnten. Ob, wann und mit welchem Inhalt die Novellierung des europäischen Datenschutzrechts beschlossen wird, bleibt jedoch weiterhin abzuwarten. Die zwischen der Europäischen Kommission, den beiden Berichterstattern des Europäischen Parlaments und dem ehemaligen sowie künftigen Ratspräsidenten erarbeitete Road Map zur Verabschiedung der Verordnung[37] lässt jedoch hoffen, dass eine Konkretisierung noch dieses Jahr erfolgt.

Timo Bittner LL.M., LL.M.
studierte IT-Recht & Recht des geistigen Eigentums an der Leibniz Universität Hannover und der University of Oslo und erhielt von beiden Universitäten den Master of Laws. Seit dem Studium, in welchem er sich bereits mehrfach mit den Auswirkungen der geplanten DSG-VO auf den deutschen Datenschutz befasste, ist er als Berater für Datenschutz bei der s-con Datenschutz & ITK tätig. Nebenbei hat er seine Dissertation im Datenschutzrecht begonnen, welche sich mit dem Datenschutzaudit bei Auftragsdatenverarbeitern befasst.

33 Selber Ansicht: Jaspers/Reif, RDV 2012, 78, (82); anderer Ansicht: Hoeren, ZD 2012, 355 (357).

34 Jaspers/Reif, RDV 2012, 78 (82).

35 Klug, RDV 2013, 143 (145).

36 Jaspers/Reif, RDV 2012, 78 (82).

37 Hofmann, CRonline Verfahrensstand-Anzeiger, abrufbar unter: http://www.computerundrecht.de/26378.htm.

Prof. Dr. Tobias Keber

Rechtskonformer Einsatz von Social Media im Unternehmen – ausgewählte Einzelaspekte im Lichte aktueller Rechtsprechung

Knapp die Hälfte der deutschen Unternehmen (47 Prozent) nutzte 2012 Social Media, weitere 15 Prozent planten den Einsatz[1]. Zwar ist der erste Hype um Social Media vorbei und die Nutzerzahlen der marktführenden Anbieter steigen nicht mehr so stark an[2]. Gleichwohl bleiben soziale Medien für Unternehmen, wenn auch branchenspezifisch und je nach Unternehmensgröße[3] in unterschiedlicher Dimension, ein wichtiger und zukunftsträchtiger Kommunikationskanal. Auch der Wettbewerb gebietet es, dass sich Unternehmen und Mitarbeiter mit dem rechtskonformen Einsatz von Social Media im Unternehmen auseinandersetzen. Zu zahlreichen in der täglichen Praxis auftretenden Fragestellungen hat es in jüngster Zeit gerichtliche Entscheidungen gegeben, die nachfolgend im Kontext dargestellt werden.

I. Ausgangssituation

Social Media versteht sich als Sammelbegriff für digitale Medien, Dienste und Technologien, mittels deren Nutzer untereinander kommunizieren und Inhalte gestalten (user generated content) sowie austauschen können. Es geht demnach grundsätzlich nicht nur um soziale Netzwerke wie Facebook oder LinkedIn. Gerade im unternehmerischen Kontext sind auch Plattformen zur Zusammenarbeit (collaboration) und Wissensmanagement (wisdom of the crowd: Wikis) sowie Blogs/Mikroblogs (z.B. Twitter) relevant. Die einzelnen Dienste unterscheiden sich erheblich in Funktionsumfang, Nutzer- und Adressatenkreis (b2c, b2b oder beides), Richtung der Kommunikation (one-to-many oder one-to-one), Reichweite und „medialem" Zuschnitt (bspw. vornehmlich Text bei twitter, Bewegtbilder auf Youtube), was auch bei der Einschätzung der rechtlichen Risiken der Dienste zu berücksichtigen ist[4].

Der Einsatz von Social Media im Unternehmen wirft eine Vielzahl juristischer Fragen in ganz unterschiedlichem Kontext auf. Aus der Unternehmer- bzw. Arbeitgeberperspektive ist etwa klärungsbedürftig, wie weit bei der Personalsuche auf die potentiell durchaus erkenntnisversprechende Informationsbeschaffung aus sozialen Netzwerken zurückgegriffen werden darf. Auch sieht sich das Unternehmen gegebenenfalls veranlasst, „privat" kommunizierten, diskreditierenden Aussagen des Beschäftigten über Betrieb oder Kunden mit einer Kündigung zu begegnen. An dieser Stelle tritt das Kernproblem unserer von Informations- und Kommunikationstechnologie (ICT) gänzlich durchdrungenen Gesellschaft offen zu Tage. Wann Kommunikation privat und wann beruflich ist, lässt sich heute nur noch sehr schwer bestimmen. Gleichwohl haben sowohl der Unternehmer als auch die Beschäftigten ein Bedürfnis nach Rechtssicherheit. Die Beschäftigten müssen wissen, wie weit Social Media als Arbeitsmittel zu verstehen ist (darf oder gar soll für das Unternehmen „getwittert" werden?) und unter welchen Umständen die private Nutzung der Dienste am Arbeitsplatz zulässig ist. Aus ihrer Perspektive ist ferner u.a. klärungsbedürftig, welche Inhalte als Geschäftsgeheimnisse nicht über Social Media Kanäle kommuniziert werden dürfen.

II. Regulierungsrahmen

Der rechtliche Rahmen, der den Einsatz von Social Media im Unternehmen steuert, betrifft verschiedene Ebenen. Neben die gesetzlichen Bestimmungen können Betriebs- (nichtöffentlicher Bereich) bzw. Dienstvereinbarungen[5] (öffentlicher Bereich) oder Unternehmensrichtlinien treten[6], die jeweils individuelle Vorgaben enthalten. Die übergreifenden gesetzlichen Vorgaben sind keinem einheitlichen „Social Media Gesetz" zu entnehmen, sondern speisen sich u.a. aus dem Urheber-, Wettbewerbs- und Werbe-, Telemedien- und Äußerungsrecht sowie dem Persönlichkeits- und Datenschutzrecht[7]. Wegen der grenzüberschreitenden Dimension der Dienste sind überdies europarechtliche Vorgaben zu berücksichtigen. Eine weitere und ebenso wichtige Ebene von Bestimmungen stellen die Nutzungsbedingungen (Allgemeine Geschäftsbedingungen) der

1 BITKOM (Hrsg.) Studie Social Media in deutschen Unternehmen, 2012, S. 6.

2 In Westeuropa verzeichnete beispielsweise das soziale Netzwerk Facebook zwischen 2010 auf 2011 eine Zunahme von 8,6 Prozent. Von 2013 auf 2014 wird dagegen nur noch ein Anstieg von 2,2 Prozent erwartet. Zahlen von eMarketer, zit. nach Bundesverband Digitale Wirtschaft (BVDW) e.V., Social Media Kompass 2013/2014, S. 69.

3 In kleinen und mittelständischen Unternehmen des Baugewerbes spielt Social Media nach wie vor keine Rolle. Wichtig sind die neuen Kommunikationswege dagegen u.a. im Bereich freiberuflicher Dienstleistungen und im Handel. Vgl. die Zahlen unter https://www.destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/UnternehmenHandwerk/IKTUnternehmen/Tabellen/03_NutzungSocialMedia_IKT_Unternehmen.html

4 Einführend Schwartmann/Keber, Merkblatt Social Media im Unternehmen, Datakontext 2014.

5 Vgl. beispielsweise die Dienstvereinbarung soziale Medien des ULD Schleswig-Holstein, abrufbar unter https://www.datenschutzzentrum.de/ldsh/dv-social-media.html.

6 Vgl. beispielsweise die Grundsätze zu sozialen Medien der Coca Cola Company, abrufbar unter http://assets.coca-colacompany.com/9a/9c/f358166143c5a72a6879ba25f078/german-social-media-principles-2013-de.pdf.

7 Guter Überblick bei Schwartmann/Ohr, in: Schwartmann (Hrsg.), Praxishandbuch Medien-, IT- und Urheberrecht, Rechtsfragen beim Einsatz sozialer Medien, 3. Aufl. im Erscheinen.

Social Media Dienste dar. Diese sind dienstespezifisch sehr unterschiedlich, wobei sich bestimmte Kernelemente bei nahezu allen Anbietern finden[8]. Verstöße gegen diese Nutzungsbedingungen können zum Ausschluss von dem Dienst führen, so dass der Zugriff auf das Konto versperrt wird. Damit kann ein zentraler Kommunikationskanal des Unternehmens versperrt werden. In diesem Kontext klarmachen muss man sich auch, dass der nicht dem deutschen Recht entsprechende modus operandi eines Social Media Dienstes eine (Mit-)Verantwortlichkeit des sich seiner Dienste bedienenden Unternehmens begründen kann[9].

III. Blickwinkel Unternehmen

Anwendungsszenarien für Social Media im Unternehmen gibt es viele. Die Portale lassen sich ebenso für die Personalgewinnung wie für die (externe) Unternehmenskommunikation einsetzen. Je nach Einsatzgebiet und Grad der Einbindung der Mitarbeiter stehen unterschiedliche Rechtsfragen im Vordergrund.

1. Social Media Recruiting und Pre-Employment Screening

Unter dem Begriff Social Media-Recruiting versteht man die gezielte Erhebung personenbezogener Daten aus sozialen Medien durch Arbeitgeber mit dem Ziel, geeignete Bewerber aufzufinden. Strukturell kann sich eine solche Suche durch den Arbeitgeber auf berufsorientierte Netzwerke (Xing, LinkedIn) beschränken, kann aber auch darüber hinausgehen und sich auf privat genutzte Dienste (Facebook) erstrecken. Begrifflich lässt sich in diesen Fällen besser von „Pre-Employment-Screenings", „Background-Investigations" bzw. „Background-Checks" sprechen. In den USA sind Pre-Employment-Screenings längst gängige Praxis, und auch hierzulande werden sie zunehmend mit der „Risikominimierung bei der Personalauswahl" begründet. Soziale Netzwerke mit ihrer Fülle von Informationen bieten zweifellos eine dankbare und vor allem kostengünstige Quelle, um Angaben eines Bewerbers im Bewerbungsverfahren zu verifizieren und weitergehende Informationen einzuholen. Für Arbeitgeber erscheint die Art und Weise der Präsentation des privaten digitalen Alter Egos der Bewerber oftmals sogar interessanter als das zu beruflichen Zwecken erstellte Profil[10]. Eine Studie einer US-amerikanischen Universität kam zu dem Ergebnis, dass eine fünf- bis zehnminütige Konsultation des Facebook-Profils eines Bewerbers aussagekräftiger ist als ein Einstellungsgespräch[11].

Durchsucht ein Arbeitgeber die Social Media Profile (bspw. Xing oder Facebook) nach geeigneten Bewerbern, werden personenbezogene Daten erhoben. Die Zulässigkeit dieser Art einer Recruiting Maßnahme hängt datenschutzrechtlich davon ab, ob ein gesetzlicher Erlaubnistatbestand greift oder der Bewerber eingewilligt hat. Ausgehend davon, dass eine nicht öffentliche Stelle handelt und keine bereichsspezifischen Regeln vorgehen, bestimmt sich dies auf Grundlage des BDSG[12]. Nach § 3 Abs. 11 Nr. 7 BDSG sind Bewerber ausdrücklich Teil des durch das BDSG geschützten Personenkreises.

a) Einwilligung der Bewerber?

Eine Einwilligung nach §§ 4 Abs. 1, 4 a BDSG wird in der Regel nicht erteilt worden sein. Das gilt namentlich für Informationen in privat orientierten Netzwerken, denn mit der Veröffentlichung der Daten auf Facebook geht nicht die hinreichend konkrete Erklärung einher, dass diese auch vom zukünftigen Arbeitgeber genutzt werden dürfen. In Ansehung eines berufsorientierten Netzwerks wie Xing lässt sich dagegen über eine Einwilligung nachdenken. Nach § 4 a Abs. 1 Satz 1 ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Wie weit man bei der Anbahnung eines Beschäftigungsverhältnisses von Freiwilligkeit sprechen kann, ist allerdings hochproblematisch[13]. Nach § 4 a Abs. 2 Satz 2 wäre der Bewerber überdies auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Denkbar ist, dass der Arbeitgeber in einer Stellenausschreibung darauf hinweist, dass er in sozialen Netzwerken recherchieren wird. Im gleichen Zuge wäre aber über die Folgen einer Verweigerung der Einwilligung hinzuweisen[14].

b) § 28 Abs. 1 S. 1 Nr. 3 BDSG

Liegt keine Einwilligung vor, sind die gesetzlichen Erlaubnistatbestände durchzuprüfen. In Betracht kommt § 28 Abs. 1 S. 1 Nr. 3 BDSG. Voraussetzung für eine auf dieser Grundlage zulässige

8 Dies sind unter anderem Bestimmungen zu Rechtswahl und Gerichtsstand, die Bestimmung des Angebots „provided as is", bzw. das Fehlen einer Pflicht des Anbieters, das Angebot aufrecht zu erhalten, das Recht des Portalanbieters, Konten und Inhalte zu löschen, die Einräumung von Lizenzen an usergenerierten Inhalten zu Gunsten des Portals, Bestimmungen zur Haftungsbeschränkung des Portals sowie Bestimmungen zur Haftung der User und zum Umgang mit Daten (Privacy Policy). Zu Reichweite und Wirksamkeit einzelner Bestimmungen in Nutzungsbedingungen vgl. Solmecke/Dam Wirksamkeit der Nutzungsbedingungen sozialer Netzwerke, MMR 2012, 71; Schwenke Nutzungsbedingungen sozialer Netzwerke und Onlineplattformen, WRP 2013, 37.

9 Vor diesem Hintergrund steht etwa die Entscheidung des Verwaltungsgerichts Schleswig-Holstein zum Analysedienst Facebook-Insights, der standardmäßig auf Facebook-Unternehmensseiten (Fanpages) läuft. VG Schleswig, Urteil v. 9.10.2013, 8 A 37/12, 8 A 14/ 12 und 8 A 218/11 (nicht rechtskräftig).

10 So jedenfalls das Ergebnis einer Befragung in den USA, wonach 2 von 5 Unternehmen Pre-Employment-Screening durchführen und von diesen dann 76% angaben, Informationen von Facebook auszuwerten. 53% gaben an, Twitter auszuwerten und lediglich 48% analysierten das berufsorientierte Netzwerk LinkedIn. Die Statistik ist abrufbar unter: http://www.go-gulf.ae/blog/social-media-pre-employment-screening/.

11 Vgl. Lobe, Software scannt Facebook-Profile von Bewerbern, Die Welt online v. 1.3.2014, abrufbar unter: http://www.welt.de/wirtschaft/karriere/article125314665/Software-scannt-Facebook-Profile-von-Bewerbern.html. An der Universität Cambridge wurde ein Werkzeug entwickelt, das auf Grundlage eines Facebook-Profils ein Psychogramm des Nutzers entwirft und damit bei Personalmanagern auf Interesse stoßen könnte. Das Tool „youarewhatyoulike" ist abrufbar unter: http://youarewhatyoulike.com/.

12 Zu den landesdatenschutzrechtlichen Vorgaben für die Erhebung personenbezogener Daten aus sozialen Netzwerken im Rahmen der Bewerbungsverfahren kommunaler Stellen: Ziltkens/Cavin, Soziale Netzwerke im Umfeld kommunaler Aufgabenerfüllung, ZD 12/2013, 603 ff.

13 Dazu Kania/Sansone, NZA 2012, 360, 363. In den USA werden Bewerber im Rahmen des Bewerbungsgesprächs „gebeten", die Zugangsdaten zu ihren Social-Media Accounts zu offenbaren. Dazu Heermann, ZD-Aktuell 2012, 02891.

14 Vgl. hierzu auch Solmecke, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 37. EL, 2014, Teil 21.1 Rn. 43.

Datenverarbeitung ist, dass die Daten "allgemein zugänglich sind". Das besagte Tatbestandsmerkmal begründet einen partiellen Dispens vom Grundsatz der Direkterhebung wobei als „allgemein zugänglich" solche Informationsquellen gelten, „die sich sowohl ihrer technischen Ausgestaltung als auch ihrer Zielsetzung nach dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln"[15]. In der Kommentarliteratur werden beispielhaft Suchmaschinen genannt, was u.a. mit einer Entscheidung des OLG Frankfurt/M. begründet wird[16]. Jene erging allerdings in urheberrechtlichem Kontext, und die urheberrechtliche Terminologie lässt sich nicht unbesehen auf das Datenschutzrecht übertragen. Als „allgemein zugänglich" im Sinne des § 28 Abs. 1 S. 1 Nr. 3 BDSG wird man die Präsenz in einem privaten Netzwerk dann ansehen müssen, wenn der Nutzer keine Zugangsbeschränkung gesetzt hat und die Informationen auch von außen aus mittels einer Suchmaschine auffindbar sind. Hat der Nutzer eine Zugangsbeschränkung gesetzt, kann man die Frage stellen, wie es sich auf das Tatbestandsmerkmal der allgemeinen Zugänglichkeit auswirkt, dass sich ein Recruiter zuerst in dem Portal anmelden muss, um an die Daten potentieller Bewerber zu gelangen.

Liegen „allgemein zugängliche" Daten i.S.d. § 28 Abs. 1 S. 1 Nr. 3 BDSG vor, schließt sich eine Interessensabwägung an. Das schutzwürdige Interesse des Betroffenen am Ausschluss der Datenverarbeitung darf die berechtigten Interessen der verantwortlichen Stelle nicht offensichtlich überwiegen. Für diese Abwägung soll es nach der herrschenden Auffassung eine Rolle spielen, ob es sich um ein berufsorientiertes („Xing") oder um ein privates („Facebook") Netzwerk handelt. Bei freizeitorientierten Netzwerken geht die Abwägung danach in der Regel zu Gunsten des von der Datenerhebung Betroffenen aus, bei berufsorientierten Netzwerken dagegen sollen grundsätzlich die Interessen des Arbeitgebers überwiegen. Im gescheiterten Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes[17] war eine Feinsteuerung der Datenerhebung vor Begründung eines Beschäftigungsverhältnisses vorgesehen, die diesem Ergebnis nahe kommt[18].

c) § 32 BDSG

Ein weiterer Erlaubnistatbestand ist § 32 BDSG. Danach dürfen personenbezogene Daten eines Beschäftigten „für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden", wenn dies „für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses […] erforderlich ist". Das Verhältnis der Vorschrift zu § 28 Abs. 1 S. 1 Nr. 3 BDSG ist umstritten. Nach teilweise vertretener Auffassung wird die allgemeine Bestimmung des § 28 Abs. 1 S. 1 Nr. 3 BDSG von der spezielleren Vorschrift in § 32 BDSG verdrängt. Diese Ansicht findet in der Gesetzesbegründung allerdings keine Stütze[19].

Im Kriterium der Erforderlichkeit klingt die auch im Rahmen des § 28 Abs. 1 S. 1 Nr. 3 anzustellende Interessenabwägung an, wobei § 32 BDSG eine spezifisch arbeitsrechtliche Schnittstelle darstellt. Demnach kann der Zugriff auf Daten in sozialen Netzwerken für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses jedenfalls dann nicht als erforderlich gelten, wenn dadurch die in der arbeitsgerichtlichen Rechtsprechung definierten Grenzen des Fragerechts des Arbeitgebers unterlaufen würden. In ständiger Rechtsprechung hat das Bundearbeitsgericht unterstrichen, dass der Arbeitgeber ein berechtigtes, billigenswertes und schutzwürdiges Interesse an der Beantwortung seiner Frage für das Arbeitsverhältnis haben muss, das objektiv so stark ist, dass dahinter das Interesse des Arbeitnehmers am Schutz seines Persönlichkeitsrechtes und an der Unverletzbarkeit seiner Individualsphäre zurücktreten muss.[20] In der Regel unzulässig sind daher Fragen nach der Schwangerschaft, nach einer Behinderung und nach der Schwerbehinderteneigenschaft, nach Religion, Weltanschauung und sexueller Identität, nach Vorerkrankungen sowie nach der Gewerkschaftszugehörigkeit.[21] Auf Informationen im besagten Kontext wird man vornehmlich in privaten Netzwerken stoßen, so dass sich der Zugriff auf Daten aus privat orientierten Netzwerken auch auf dieser Grundlage verbietet.

Einfach gesprochen bedeutet das Gesagte, dass Recruiter künftig Informationen aus Facebook nicht, aus Portalen wie Xing oder LinkedIn aber sehr wohl erheben dürfen, soweit sie in der Stellenausschreibung darauf hingewiesen haben. Dass es sich hierbei um eine sachgerechte Lösung (wie soll der Bewerber die illegale Erhebung aus seinem Facebook-Profil beweisen?) handelt, darf bezweifelt werden.

d) Grenzen des „Active Sourcing"

Grenzen der rechtlich zulässigen Bewerbersuche ergeben sich auch aus dem Wettbewerbsrecht[22]. So ist das telefonische Kontaktieren potentieller Kandidaten an ihrem (bisherigen) Arbeitsplatz unter Angabe einer falschen Identität (um zu dem Kandidaten durchgestellt zu werden) von der Rechtsprechung ebenso als wettbewerbswidrig eingestuft worden (§§ 3, 7 UWG)[23] wie die direkte Ansprache potentieller neuer Mitarbeiter über das berufsorientierte Netzwerk Xing, wenn anlässlich dessen der bisherige Arbeitgeber diskreditiert wird (§§ 4 Nr. 7 und Nr. 10 UWG). Das ist nach einer Entscheidung des LG Heidelberg etwa der Fall, wenn es in der Kontaktaufnahme ausschnittsweise heißt: „Sie wissen ja hoffentlich, was Sie sich da

15 Simitis, in: Simitis (Hrsg.), BDSG § 28 Rn. 151.

16 OLG Frankfurt, Beschluss vom 12.11.2009, 11 W 41/09.

17 BT- Drucksache 17/4230.

18 In § 32 Abs. 6 BDSG-E hieß es „Beschäftigtendaten sind unmittelbar bei dem Beschäftigten zu erheben. Wenn der Arbeitgeber den Beschäftigten vor der Erhebung hierauf hingewiesen hat, darf der Arbeitgeber allgemein zugängliche Daten ohne Mitwirkung des Beschäftigten erheben, es sei denn, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung das berechtigte Interesse des Arbeitgebers überwiegt. Bei Daten aus sozialen Netzwerken, die der elektronischen Kommunikation dienen, überwiegt das schutzwürdige Interesse des Beschäftigten; dies gilt nicht für soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind…"

19 Vgl. hierzu Gola/Schomerus, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 32, Rn 1-3a.

20 BAG, 2 AZR 923/94, Urteil vom 05.10.95.

21 Vgl. dazu Riesenhuber: Kein Fragerecht des Arbeitgebers NZA 2012, 771 ff m.w.N.

22 Vgl. hierzu Bissels/Ziegelmayer/Kiehn, Gesucht, gefunden, angesprochen: Rechtliche Tücken des „Active Sourcing" BB 2013, 2869-2875 (2874).

23 LG Bonn, Urteil vom 03.01.2013, 14 O 165/12.

angetan haben? [...] Sie wissen ja hoffentlich, in was für einem Unternehmen Sie da gelandet sind?“[24].

2. Impressumspflicht sowie wettbewerbs- und werberechtliche Vorgaben

Werden Social Media Portale im Unternehmen nicht nur für die interne Kommunikation, sondern auch extern eingesetzt, muss telemedien- sowie wettbewerbs- und werberechtlichen Vorgaben entsprochen werden. Unternehmenspräsenzen in sozialen Medien (Facebook-Fanpage, Corporate-Twitter-Account) sind nach Maßgabe des § 5 TMG (unabhängig von der gegebenenfalls parallel bestehenden Pflicht des Portals) impressumspflichtig[25] und müssen, soweit es sich um journalistisch-redaktionell gestaltete Inhalte[26] handelt, auch die zusätzlichen Angaben des § 55 RStV vorhalten (redaktionell Verantwortlicher). Technisch kann die Erfüllung der Pflichten schwierig sein, weil die Anbieter entsprechende Bereiche erst gar nicht vorsehen (Twitter) und gewährleistet sein muss, dass die Pflichtangaben der Unternehmenspräsenz auch von mobilen Endgeräten aus einsehbar sind[27].

Äußerst praxisrelevant sind wettbewerbs- und werberechtliche Vorgaben, die bestimmte geschäftsfördernde Maßnahmen verbieten. Nach § 4 Nr. 3 UWG handelt unlauter, wer den werblichen Charakter einer geschäftlichen Handlung verschleiert. Ob das dem Gebot der Trennung von Werbung und redaktioneller Berichterstattung korrespondierende Verbot verletzt ist, richtet sich nach den Umständen des Einzelfalls, wobei insbesondere Inhalt, Anlass und Aufmachung des Beitrags sowie Gestaltung und Zielsetzung der Publikation zu berücksichtigen sind[28]. Der werbliche Charakter des Beitrags muss für den durchschnittlich informierten, verständigen und situationsadäquat aufmerksamen Verbraucher eindeutig, unmissverständlich und auf den ersten Blick als solcher hervortreten[29]. In diesem Kontext gilt es zu berücksichtigen, dass geschäftsfördernde Maßnahmen von Mitarbeitern dem Unternehmen auch ohne Kenntnis der Geschäftsführung[30] über die Wertung des § 8 Abs. 2 UWG zugerechnet werden können. Ein solcher Fall des so genannten „Astroturfings“ soll beispielsweise vorliegen, wenn ein Arbeitnehmer von seinem Arbeitsplatz aus (was sich über die IP feststellen ließ) einen Blogbeitrag verfasst, der die Tätigkeit des Arbeitgebers über die Maßen positiv darstellt. Dass es sich in einem solchen Fall um eine rein private Äußerung des Beschäftigten handelt, hielt das Gericht für unwahrscheinlich[31].

3. Umfang des Direktionsrechts und Mitarbeiterdaten auf der Präsenz

Fraglich ist, ob ein Arbeitgeber im Rahmen seines Direktionsrechts einen Arbeitnehmer anweisen kann, in einem sozialen Netzwerk aktiv zu sein. In der Literatur wird zu Recht differenziert[32]. Eine Anordnungsbefugnis bezogen auf Aktivitäten in freizeitorientierten Netzwerken wird wegen der Implikationen des Allgemeinen Persönlichkeitsrechts des Arbeitnehmers abgelehnt. Zulässig soll allerdings eine Anordnung sein, die sich auf berufsorientierte Netzwerke bezieht, und, wenn die konkrete Arbeitsaufgabe des Arbeitnehmers die Teilnahme an diesem Netzwerk gebietet oder nahelegt, also etwa bei Mitarbeitern im Bereich der Öffentlichkeitsarbeit oder Human Resources[33]. Auch in diesem Fall muss allerdings weiter differenziert werden, etwa wenn es um das Profilbild des Arbeitnehmers geht, dessen Veröffentlichung sich nach § 22 KUG richtet und damit einer gesonderten Einwilligung bedarf[34]. Diese kann grundsätzlich auch konkludent erteilt werden und erlischt nicht ohne weiteres automatisch im Zeitpunkt der Beendigung des Arbeitsverhältnisses, sofern der Arbeitnehmer nicht ausdrücklich Gegenteiliges erklärt[35]. Anlässlich von Löschbegehren ist im Einzelfall eine umfassende Interessenabwägung vorzunehmen, die sowohl den arbeitsrechtlich begründeten nachvertraglichen Rücksichtnahmepflichten Rechnung trägt, als auch das allgemeine Persönlichkeitsrecht des Betroffenen hinreichend berücksichtigt. Geboten ist die Löschung eines Profilfotos jedenfalls dann, wenn der ehemalige Arbeitgeber weiterhin mit dem Profil des zwischenzeitlich bei einem Wettbewerber tätigen Arbeitnehmers wirbt[36].

IV. Blickwinkel Beschäftige

Überaus praxisrelevante Fragen des betrieblichen Alltags sind weiter, ob den Arbeitnehmern die private Nutzung von Social Media während der Arbeitszeit gestattet wird und wie sich gegebenenfalls verhängte Verbote bzw. Einschränkungen kontrollieren lassen. Im Kontext der Beendigung von Beschäftigungsverhältnissen entstehen komplexe Schnittstellen zwischen Wettbewerbsrecht, Datenschutzrecht und Arbeitsrecht, die interessengerecht aufgelöst werden müssen.

24 LG Heidelberg, Urteil vom 23.05.2012, 1 S 58/11.

25 LG Aschaffenburg, Urteil vom 19. August 2011, 2 HK O 54/11; OLG Düsseldorf, Urt. v. 13.08.2013, 1-20 U 75/13, jeweils zu „Facebook“. Zu Xing jüngst: LG München, 3.6.2014, 33 O 4149/14; zur Problematik ferner LG Stuttgart 24.4.2014 (11 O 72/14) sowie Pießkalla, Zur Reichweite der Impressumspflicht in sozialen Netzwerken ZUM 2014, 368.

26 Kennzeichnende Merkmale solcher Angebote sind nach der Rechtsprechung „eine gewisse Selektivität und Strukturierung, das Treffen einer Auswahl nach ihrer angenommenen gesellschaftlichen Relevanz mit dem Ziel des Anbieters, zur öffentlichen Kommunikation beizutragen, die Ausrichtung an Tatsachen (sog. Faktizität), ein hohes Maß an Aktualität, nicht notwendig Periodizität, ein hoher Grad an Professionalisierung der Arbeitsweise und ein gewisser Grad an organisierter Verfestigung, der eine gewisse Kontinuität gewährleistet“. OLG Bremen, Urteil vom 14. Januar 2011, 2 U 115/10.

27 Vgl. dazu OLG Hamm, Urteil v. 20.05.2010, I-4 U 225/09.

28 BGH, Urteil vom 31.10.2012, I ZR 205/11.

29 BGH, a.a.O., vgl. zur Problematik jüngst OLG Köln, Urteil vom 9.8. 2013, 6 U 3/13.

30 Vgl. dazu LG Freiburg, Urteil vom 4.11.2013, 12 O 83/13.

31 LG Hamburg, Urteil vom 24.4.2012, 312 O 715/11.

32 Eingehend dazu Thüsing, in Thüsing/Traut, Beschäftigtendatenschutz und Compliance, 2014, § 14. Social Media in Betrieb und Unternehmen, Rn. 52 ff.

33 Kort, Soziale Netzwerke und Beschäftigtendatenschutz, DuD 2012, 722 ff (726).

34 Oberwetter, Soziale Netzwerke im Fadenkreuz des Arbeitsrechts, NJW 2011, 417 ff. (419).

35 LAG Köln, Beschluss v. 10.7.2009, 7 Ta 126/09 (Foto einer Telefonistin auf Homepage einer Bank); LAG Schleswig-Holstein, Urteil v. 20.06.2010, 3 Sa 72/10.

36 Hessisches LAG, Urteil v. 24.01.2012, 19 SaGa 1480/11 (Darstellung einer Anwältin in einem Anwaltsblog).

1. Social Media Monitoring

Rechtlich laufen Verbote der privaten E-Mail-, Internet-, und Social Media Nutzung am Arbeitsplatz grundsätzlich weitgehend parallel. Der Arbeitgeber kann die private Nutzung verbieten und dies mit seinem Direktionsrecht (§§ 315 Abs. 1 BGB, 106 GewO) begründen. Tut er dies, tritt er seinem Arbeitnehmer gegenüber nicht als Anbieter eines Telekommunikationsdienstes auf, und auch die Vorgaben des TMG finden keine Anwendung. In der Praxis hat das zur Folge, dass die Überwachung (Monitoring) der Internetnutzung (aufgerufene URL´s und angewählte IP´s) des Arbeitnehmers durch den Arbeitgeber weitgehend zulässig ist. Mit der in § 32 Abs. 1 S. 1 BDSG vorgesehenen Interessenabwägung („erforderlich") wird zwar keine totale, unbegrenzte Überwachung einhergehen können, sehr wohl aber sind Stichproben zur Überprüfung der unerlaubten Privatnutzung zulässig[37].

Wird die private Nutzung dagegen ausdrücklich gestattet oder geduldet (betriebliche Übung), wird die Rechtslage ungleich komplizierter, und die Einzelheiten sind umstritten. Hält man die datenschutzrechtlichen Vorgaben des TKG (§ 88) und des TMG (§§ 11 ff.) für abschließende Sonderregelungen gegenüber dem BDSG, ist die Überwachung der Abreitnehmer (um eine von der Gestattung nicht mehr erfasste, d.h. übermäßige Privatnutzung zu kontrollieren) unzulässig, wenn der Arbeitnehmer nicht eingewilligt hat[38]. Die wohl noch herrschende Ansicht[39] begründet in den besagten Fällen die Anwendbarkeit des Fernmeldegeheimnisses mit dem Wortlaut der §§ 88 Abs. 2 und 3 TKG. Dort wird ohne weitere Differenzierung von „Dienstanbieter" gesprochen. Das ist nach § 3 Nr. 6 TKG jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt. Ein „geschäftsmäßiges Erbringen von Telekommunikationsdiensten" ist legaldefiniert als das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht, § 3 Nr. 10 TKG. Maßgeblich ist damit „nur" Nachhaltigkeit i.S. eines auf Dauer angelegten Angebots und nicht Entgeltlichkeit oder gar Gewinnerzielungsabsicht. Dritter in diesem Sinne kann auch der Beschäftigte sein. Die zur Anwendbarkeit des § 88 TKG im Arbeitsverhältnis bis dato ergangene ablehnende Rechtsprechung[40] verzichtet auf eine nähere Begründung. In der Literatur wird die angeblich fehlende Dienstanbietereigenschaft mit teleologischen und systematischen Erwägungen begründet[41]. Überzeugend ist dies nicht[42], und das Ergebnis steht auch dem klar kommunizierten Willen des Gesetzgebers[43] sowie der aufsichtsbehördlichen Praxis[44] entgegen. Für die Anwendbarkeit des § 88 TKG im Arbeitsverhältnis spricht schließlich auch die Rechtsprechung des EGMR, der einen Fall der Überwachung von privater E-Mail- und Internetnutzung am Arbeitsplatz im Lichte des Artikel 8 EMRK und dort vor allem im Lichte des Rechts auf Achtung der Korrespondenz beurteilte[45].

2. Fragestellungen im Zusammenhang mit der Beendigung von Arbeitsverhältnissen

a) Verrat von Geschäftsgeheimnissen und anderweitige Preisgabe sensibler Informationen

Der vorsätzliche Verrat von Geschäftsgeheimnissen eines Unternehmens an einen Konkurrenten kann nach der Rechtsprechung eine fristlose Kündigung rechtfertigen[46]. Auch insoweit bergen soziale Netzwerke durch ihre einfache Nutzbarkeit und virale Reichweite besondere Risiken. Ein Geschäftsgeheimnis im Sinne von § 17 UWG ist nach der Rechtsprechung des Bundesgerichtshofs „jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem bekundeten, auf wirtschaftlichen Interessen beruhenden Willen des Betriebsinhabers geheim gehalten werden soll"[47]. Vor diesem Hintergrund kommen auch Kundendaten eines Unternehmens als Geschäftsgeheimnisse in Betracht. Nach einer aktuellen Entscheidung des ArbG Hamburg[48] können auch auf XING-Profilen gespeicherte Kundendaten Geschäftsgeheimnisse eines Arbeitgebers sein[49]. Allerdings muss der Arbeitgeber im Zweifel beweisen, dass die Kontaktaufnahmen über XING, die zur Speicherung dieser Daten geführt haben, im Rahmen einer

37 Zum Ganzen Greening/Weigl, Überwachung der Internetnutzung von Arbeitnehmern – von Webtracking- und Webfiltering-Tools, CR 2012, S. 787 ff (791).

38 Greening/Weigl, a.a.O., S. 792.

39 Zum Meinungsstand Schumacher, in: Besgen/Prinz, Handbuch Internet. Arbeitsrecht, 2013, S. 53.

40 Hess. VGH, 19.5.2009, 6 A 2672/08.Z; LAG Niedersachsen, 31.5.2010, 12 Sa 875/09; LAG Berlin-Brandenburg, 16.12.2011, 4 Sa 2132/10; LAG Hamm, 10.7.2012, 14 Sa 1711/10; VG Karlsruhe, 27.5.2013, 2 K 3249/12.

41 Vgl. jüngst Diercks, Social Media im Unternehmen, K&R 1/2014, 1 ff (4 f).

42 Namentlich das mit § 1 TKG begründete Argument, das TKG bezwecke nicht, eine Beziehung zwischen Arbeitgeber und Arbeitnehmer zu regeln, sondern betreffe vielmehr das Verhältnis zum Staat und vor allem von im Wettbewerb stehenden Unternehmen, greift nicht. Wie den Regulierungszielen in § 2 TKG entnommen werden kann, geht es im TKG neben dem sektorspezifischen Kartellrecht eben auch um spezifisches Verbraucherschutzrecht sowie datenschutzrechtliche Vorgaben (§§ 91 ff. TKG), welche mit Wettbewerbsförderung offensichtlich nichts zu tun haben.

43 In der Gesetzesbegründung zum TKG heißt es: „Verpflichtet ist jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. Hier wird bewußt vom „geschäftsmäßigen" (und nicht vom „gewerblichen") Erbringen von Telekommunikationsdiensten gesprochen, um deutlich zu machen, daß es hier nicht auf eine Gewinnerzielungsabsicht ankommt […]. Auch ein ohne Gewinnerzielungsabsicht erfolgendes, auf Dauer angelegtes Angebot von Telekommunikationsdiensten verpflichtet zur Wahrung des Fernmeldegeheimnisses. Dem Fernmeldegeheimnis unterliegen damit z.B. Corporate Networks, Nebenstellenanlagen in Hotels und Krankenhäusern, Clubtelefone und Nebenstellenanlagen in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind." BT-Drucks 13/3609 S. 53. Bekräftigt wird dies noch einmal im Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes: „Nach geltender Rechtslage wird ein Arbeitgeber, der seinen Beschäftigten die private Nutzung von dienstlich zur Verfügung gestellten Telekommunikationsdiensten erlaubt, als Diensteanbieter im Sinne von § 3 Nummer 6 TKG angesehen. Für ihn gelten deshalb das Fernmeldegeheimnis und die Vorschriften des § 88 ff. TKG, die gemäß § 1 Abs. 3 BDSG den Regelungen des BDSG vorgehen." BT-Drucks. 17/4230 S. 43.

44 Vgl. dazu das ULD Papier „Private sowie dienstliche Internet- und E-Mail-Nutzung" vom 1.4.2014, online abrufbar unter: https://www.datenschutzzentrum.de/internet/private-und-dienstliche-internetnutzung.pdf.

45 Europäischer Gerichtshof für Menschenrechte (EGMR), Urteil v. 03.04.2007, 62617/00 – Lynette Copland gegen Vereinigtes Königreich.

46 LAG Berlin Urteil vom 10.07.2003; 16 Sa 545/03.

47 BGH vom 26.02.2009, I ZR 28/06, Rn. 13.

48 ArbG Hamburg, Urteil vom 24.01.2013, 29 Ga 2/13.

49 Zur Problematik auch Frik/Klühe Nutzung von Kontakten aus sozialen Netzwerken während und bei Beendigung des Arbeitsverhältnisses, DB 2013, 1174.

geschäftlichen Tätigkeit erfolgt ist, was einen Zusammenhang zur arbeitsvertraglich geschuldeten Tätigkeit voraussetzt. Weiter müssen auch die Kontaktpartner bei der Kontaktaufnahme für ihren jeweiligen Arbeitgeber gehandelt haben[50].

Die Preisgabe sensibler Informationen geschieht bisweilen nicht einmal in böser Absicht: In einem aktuellen Fall vor dem LAG Berlin-Brandenburg ging es um die Frage, ob die von einer Kinderkrankenpflegerin auf ihrer persönlichen Facebookseite ohne Zustimmung veröffentlichten Patientenbilder (eines Kindes!) eine außerordentliche Kündigung rechtfertigen. Auf Grundlage der Umstände im konkreten Fall verneinte das Gericht das Bestehen eines außerordentlichen Kündigungsrechts, wies aber sehr deutlich darauf hin, dass die Veröffentlichung der Patientenbilder einen erheblichen Verstoß gegen die arbeitsvertraglich und über §§ 5 BDSG und 203 StGB begründete Schweigepflicht darstellte und die Persönlichkeitsrechte des betroffenen Patienten verletzte. Dies gelte vor allem in Ansehung der Veröffentlichung in einem sozialen Netzwerk, weil eine weitere Verbreitung der Bilder nicht kontrolliert werden könne[51].

b) Äußerungsrecht und Grenzen im Arbeitsverhältnis

Ob eine (gegebenenfalls sogar fristlose, § 626 BGB) Kündigung des AN wegen kritischer Äußerungen über den Arbeitgeber in sozialen Medien gerechtfertigt ist, lässt sich nicht pauschal sagen. Grobe Beleidigungen des Arbeitgebers und/oder seiner Vertreter bzw. Repräsentanten stellen einen Verstoß gegen die Pflicht zur Rücksichtnahme auf die berechtigten Interessen des Arbeitgebers dar (§ 241 Abs. 2 BGB) und sind von der verfassungsrechtlich garantierten Meinungsfreiheit (Artikel 5 Abs. 1 GG) in der Regel nicht (mehr) gedeckt[52]. Mittlerweile liegt eine Reihe von Urteilen vor, wobei die Gerichte im Rahmen der anzustellenden Interessenabwägung u.a. berücksichtigten, ob es sich bei der Äußerung um ein Werturteil oder um eine (wahre) Tatsachenbehauptung handelte, ob zugleich Äußerungen über Geschäftskunden vorlagen, ob die Äußerung während oder außerhalb der Arbeitszeit getätigt wurde und ob die Äußerung allgemein, beschränkt oder für Außenstehende gar nicht zugänglich war[53].

Auch der Umstand, dass Einträge auf Social Media Seiten im Gegensatz zur flüchtigen wörtlichen Äußerung permanent auffindbar bleiben, spielte bei der Urteilsbegründung eine Rolle. Während dies nach wohl überzeugenderer Ansicht des ArbG Duisburg eine nachhaltigere Rechtsverletzung darstellt, die zudem die Gefahr negativer Folgeeinträge (Shitstorm) begründet[54], zeichnen sich entsprechende Diskussionsbeiträge nach Auffassung des Hess. LAG durch eine besondere Schnelllebigkeit aus, so dass die einzelne Äußerung schnell wieder an Bedeutung verliert[55].

V. Rechtssicherheit durch Social Media Guidelines

Social Media Guidelines sind unternehmensinterne Vorgaben für Arbeitnehmer, die als verbindliche Leitlinien auf Grundlage des Weisungsrechts (§§ 315 Abs. 1 BGB, 106 GewO) oder als unverbindliche Handlungsempfehlungen konzipiert sein können. Die Einführung von Social Media Guidelines auf Grundlage von Betriebsvereinbarungen kann die zwingende Mitbestimmung des Betriebsrats auslösen[56]. Inhaltlich sollten Social Media Guidelines die in diesem Beitrag angesprochenen Fragestellungen adressieren und dabei der Branchenspezifik sowie dem organisatorischen Umfeld des Unternehmens Rechnung tragen. Ein „one size fits all" gibt es bei Social Media Guidelines nicht[57]. Empfehlenswert ist, die mit dem Einsatz von Social Media im Unternehmen verbundenen Aspekte innerhalb der Guidelines auf verschiedenen Ebenen anzusprechen und dies auch sprachlich klarzustellen. So kann ein erster Abschnitt mit verbindlichen Vorgaben („Was wir von Ihnen verlangen") den Rechtscharakter der Guidelines determinieren, die Privatnutzung sozialer Medien am Arbeitsplatz und die Abgrenzung zur dienstlichen Nutzung regeln sowie gegebenenfalls (gestufte) Kontrollbefugnisse zur Durchsetzung eingeschränkter Nutzung vorsehen. An diese Stelle gehören auch die klare Regelung betriebsinterner Zuständigkeiten, die Nennung der betrieblich eingesetzten Social Media Kanäle, zulässige Inhalte unternehmensbezogener Kommunikation sowie das Berechtigungskonzept und der Umgang mit betrieblichen Social Media Accounts nach Beendigung des Beschäftigungsverhältnisses. Ein zweiter Abschnitt („Was das Gesetz von Ihnen verlangt") der Guidelines fasst dann wichtige gesetzliche Vorgaben (Persönlichkeitsrechte Dritter, datenschutzrechtliche Vorgaben, Wett-

50 ArbG Hamburg, Urteil vom 24.01.2013, 29 Ga 2/13.

51 LAG Berlin-Brandenburg, Urteil v. 11.04.2014, 17 Sa 2200/13.

52 Die Meinungsfreiheit schützt weder Formalbeleidigungen und Schmähungen noch bewusst unwahre Tatsachenbehauptungen (st. Rspr., statt vieler: BVerfG, Beschluss vom 07.12.2011, 1 BvR 2678/10.

53 ArbG Dessau-Roßlau v. 21.03.2012, 1 Ca 148/11, ArbG Hagen, Urteil vom 16.05.2012, 3 Ca 2597/11, ArbG Bochum v. 29.03.2012, 3 Ca 1283/11/ und hierauf LAG Hamm v. 10.10.2012, 3 Sa 644/12. Zur Fragestellung auch Zintl, Daniel/Naumann, Daniel, Verhalten von Arbeitnehmern im Bereich Social Media, NJW-Spezial 2013, 306.

54 ArbG Duisburg, 26.9.2012, 5 Ca 949/12.

55 „Da Diskussionen in Foren laufend fortgeführt werden, folgt ein Eintrag auf den anderen – dieses geschieht auf Grund der technischen Möglichkeiten oftmals mit einer sehr viel höheren Geschwindigkeit als in einem persönlichen Gespräch oder in einem Print-Medium. Die Vielzahl und Geschwindigkeit der Einträge führt in ihrer Gesamtheit dazu, dass die einzelne Äußerung schnell wieder an Bedeutung verliert, weil sich die Diskussion bereits fortbewegt oder in eine andere Richtung entwickelt hat." Hess. LAG 28.1.2013, 21 Sa 715/12.

56 Dies ist der Fall, wenn Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb betroffen sind (§ 87 Abs. 1 Nr. 1 BetrVG) oder es um die Einführung oder Anwendung technischer Einrichtungen geht, die zur Überwachung des Verhaltens oder der Leistung der Arbeitnehmer objektiv geeignet sind (§ 87 Abs. 1 Nr. 6 BetrVG). Zu den möglichen Implikationen des § 75 Abs. 2 BetrVG Diercks, Social Media im Unternehmen, K&R 1/2014, S. 6.

57 Formulierungsvorschläge bei Schwartmann/Keber/Silberkuhl, Social Media im Unternehmen, 2014. Eine kommentierte Mustervereinbarung findet sich bei Leist/Koschker, Social Media Guidelines, BB 2013, 2229-2235 (2230). Für die Konzeption unternehmensspezifischer Richtlinien hilfreich ist gegebenenfalls auch die seit 2011 nicht mehr aktualisierte Sammlung von Social Media Guidelines deutscher Unternehmen. Die Sammlung ist online abrufbar unter http://buggisch.wordpress.com/2011/10/12/deutsche-social-media-guidelines. Für die Praxis hilfreich sind schließlich die Informationen des Social Media Institutes, abrufbar unter http://socialmedia-institute.com/social-media-guideline-entwicklung-studie-strategie-best-practice/. Vgl. insgesamt auch Byers/Mößner, Die Nutzung des Web 2.0 am Arbeitsplatz, BB 2012, 2012, 1665-1671 (1669 ff); Dettermann, Soziale Netzwerke in der Arbeitswelt, BB 2013, 181-189 (183).

bewerbs- und Werberecht, Veröffentlichungsverbot von Geschäftsgeheimnissen bzw. Kundendaten) zusammen. An diese Stelle gehört auch ein Hinweis auf die Loyalitätspflicht zum Arbeitgeber auch bei Äußerungen über den privaten Account. Abschließend empfehlen sich noch unverbindliche Hinweise und Empfehlungen, die den „richtigen Ton" bei der Kommunikation im Netz betreffen und auf die Nutzungsbedingungen der Social Media Portale hinweisen.

VI. Fazit

Der Einsatz von Social Media im Unternehmen birgt rechtlich zahlreiche Risiken, die eine Querschnittsmaterie betreffen, die sich aus sehr unterschiedlichen Rechtsgebieten speist. Zudem ist das Hausrecht (Nutzungsbedingungen) der Portale zu beachten. Die gesetzlichen Regelungen halten mit dem technisch-sozialen Wandel, der auch und gerade durch Social Media reflektiert wird, nur sehr bedingt Schritt. Daher kommt der Auslegung der Normen durch die Gerichte und die Kenntnis dieser Entscheidungen in der Praxis entscheidende Bedeutung zu. Einigen, wenn auch nicht allen Unsicherheiten lässt sich durch die Erstellung individuell zugeschnittener Social Media Guidelines begegnen. Die praktische Wirksamkeit solcher unternehmensinternen Regelungen hängt maßgeblich davon ab, ob sie effizient kommuniziert werden und regelmäßig an technische Veränderungen der betrieblichen IT-Infrastruktur angepasst werden.

Prof. Dr. iur. Tobias Keber
Professur für Medienrecht und Medienpolitik in der digitalen Gesellschaft, Hochschule der Medien (HdM) Stuttgart, daneben Lehrbeauftragter für Internet- und Multimediarecht am Mainzer Medieninstitut sowie an der Universität Koblenz-Landau. Mitglied des wissenschaftlichen Beirats der Gesellschaft für Datenschutz und Datensicherheit (GDD). Prof. Dr. iur. Tobias Keber war vor seiner akademischen Laufbahn als Rechtsanwalt tätig. Er ist Autor zahlreicher Fachpublikationen zum nationalen und internationalen Medien-, IT- und Datenschutzrecht.

Kurzbeiträge

Persönlichkeitsschutz durch Datenschutz*

Prof. Dr. Gregor Thüsing**

Die GroKo weiß nicht so recht, ob sie handeln soll oder nicht. Im Koalitionsvertrag heißt es recht deutungsoffen: „Beschäftigtendatenschutz gesetzlich regeln: Die Verhandlungen zur Europäischen Datenschutzgrundverordnung verfolgen wir mit dem Ziel, unser nationales Datenschutzniveau – auch bei der grenzüberschreitenden Datenverarbeitung – zu erhalten und über das Europäische Niveau hinausgehende Standards zu ermöglichen. Sollte mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden können, wollen wir hiernach eine nationale Regelung zum Beschäftigtendatenschutz schaffen". Bei aller Unsicherheit künftiger Entwicklung ist es gut und richtig, dass das Thema gesetzgeberisch wieder auf der Tagungsordnung ist. Datenschutz ist Persönlichkeitsschutz, und als solcher ist er ernst zu nehmen.

I. Datenschutz als Forderung unserer Verfassung

Es hat einige Zeit gedauert, bis der Datenschutz verfassungsrechtliche Verankerung gefunden hat. Das ursprünglich durch die zivilrechtliche Rechtsprechung entwickelte allgemeine Persönlichkeitsrecht ist mittlerweile auch im Verfassungsrecht lex regia zur Abwehr von diversen Formen der Beeinträchtigung der Privatsphäre, die sich keinem anderen spezifischen Frei-

* Impulsreferat gehalten auf dem von der Gesellschaft für Europäische Sozialpolitik und der Gesellschaft für Datenschutz und Datensicherheit veranstalteten Diskussionsforum „Datenschutz – Was tun? Aktuelle Herausforderungen aus Europa – Vorhaben des Koalitionsvertrags" am 04.06.2014 in Berlin. Die Vortragsform wurde beibehalten.

** Der Autor ist Institutsdirektor und Hochschulprofessor am Institut für Arbeitsrecht und Recht der Sozialen Sicherheit der Universität Bonn.

heitsrecht zuordnen lassen. Es ergänzt – in den Worten des Bundesverfassungsgerichts – „als unbenanntes Freiheitsrecht die speziellen (‚benannten') Freiheitsrechte" und schützt allgemein die „engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen […], die sich durch die traditionellen konkreten Freiheitsgarantien nicht abschließend erfassen lassen"[1]. Die für das Datenschutzrecht wichtigste Ausprägung des allgemeinen Persönlichkeitsrechts ist das Recht auf informationelle Selbstbestimmung. Dieses Recht, durch das grundlegende Volkszählungsurteil des Bundesverfassungsgerichts entdeckt, entspricht – wiederum in den Worten des Gerichts – am ehesten einem „Grundrecht auf Datenschutz", denn es schützt ganz allgemein „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"[2]. Die freie Entfaltung der Persönlichkeit setzt daher den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Jeder Bürger müsse grundsätzlich darüber verfügen können, „wer was wann und bei welcher Gelegenheit" über ihn weiß.

II. Status quo und aktuelle Herausforderungen

Dieser verfassungsrechtliche Rahmen braucht, um wirksam zu werden, gesetzliche Konkretisierung. Wichtigstes Instrument ist seit 1977 das Bundesdatenschutzgesetz. Dessen Ziel bestimmt sein § 1:

„Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird."

Daran hat sich bis heute nichts geändert. Doch sind die Anwendungsfälle andere und ungleich mehr geworden als ehedem. Die Welt hat sich verändert. Big Data, Facebook, Google und andere Datengefahren 2.0 waren damals unbekannt. Datenskandale bei Lidl und Co beunruhigten noch nicht den Verbraucher, Vorratsdatenspeicherung stellte noch keine Verunsicherung breiter Bevölkerungskreise dar, Prism und Tempora zeigten noch nicht, wie sehr die Gefährdung heute international verstanden – und bewältigt – werden muss. Zu Recht ist die öffentliche Aufmerksamkeit größer geworden, die Sensibilisierung durch die Medien intensiver. Denn die Konfliktfelder des Datenschutzes sind weiter denn je; der letzte (24.) Zweijahresbericht des Bundesdatenschutzbeauftragten umfasste 264 Seiten (gegenüber 71 Seiten im Jahr 1979)[3].

Um diese neuen Herausforderungen zu meistern, um wirksamer Schutz gegen informationelle Fremdbestimmung zu sein, muss der rechtliche Rahmen immer wieder an die sich wandelnde Wirklichkeit angepasst werden. Ein Aggiornamento ist kontinuierlich erforderlich, damit sich das Recht nicht den Zeiten entfremdet, in seiner Starrheit geeignetes Instrument nur für Probleme ist, die zwischenzeitlich längst gelöst, aber unwirksames Schild gegen Gefahren, die neu entstanden sind. Diese Aufgabe liegt nicht nur in der Hand der Gesetzgebung, die allein den allgemeinen Rahmen vorgeben kann, sondern auch der Gerichte und Aufsichtsbehörden, welche die allgemeinen Vorgaben zu praktischen Leitlinien für den Einzelfall verdichten. Sie liegt nicht nur in der Hand der nationalen Instanzen, sondern auch und gerade der europäischen.

In diesem Prozess müssen sich die Akteure an Leitlinien orientieren, die Ziele vorgeben und Wege dahin beschreiben. Sie sind namentlich aus der verfassungsrechtlichen Notwendigkeit des Datenschutzes heraus zu entwickeln. Hierdurch wird er gerechtfertigt, hieran ist er zu messen.

Da ist zunächst die Notwendigkeit regulativer Transparenz. Datenschutz braucht klare Regeln. Die Ge- und Verbote des Datenschutzrechts müssen klar gefasst sein, damit sich Bürger und Unternehmen danach richten können. Was nicht verstanden wird oder dunkel spricht wie der Mund der Pythia, kann keine verhaltenssteuernde Wirkung entfalten. Hierzu steht es im strukturellen Widerspruch, dass die Grundnormen des Datenschutzrechts ausfüllungsbedürfige Generalklauseln sind, die ohne Ansehung leer sind. Das Gesetz spricht von „Verhältnismäßigkeit", „angemessenen Zwecken" und „erforderlichen Mitteln". Wann aber eine Datenverarbeitung erforderlich ist, wann den Interessen der verantwortlichen Stelle angemessen Rechnung getragen wird und wann umgekehrt die Interessen des Betroffenen im hinreichenden Verhältnis berücksichtigt werden – all dies kann im einzelnen Anwendungsfall oftmals nur schwer gesagt werden. Letztlich sind es inkommensurable Größen, die sich gegenüberstehen: Das Persönlichkeitsinteresse des Betroffenen auf der einen, die wirtschaftlichen Interessen der datenverarbeitenden Stelle auf der anderen Seite. Hier ist es gut, wenn der Gesetzgeber selber typisierend den Interessenausgleich in Fallgruppen vorzeichnet, gesondert nach problematischen und weniger problematischen Fällen.

In diesen Versuchen sind zuletzt Fortschritte ausgeblieben. Doch der Entwurf einer europäischen Datenschutz-Grundverordnung, durch die Kommission bereits 2012 auf den Weg gebracht, scheint nun doch noch voranzugehen[4]. Der ursprüngliche Entwurf wurde – nicht ohne intensive Bearbeitung der Lobbyisten, aber auch aufgrund der unterschiedlichen Grundkonzeption datenschutzrechtlicher Vorstellungen in den verschiedenen Mitgliedsstaaten – mit Änderungsanträgen überhäuft, so dass zum Schluss deren Zahl unüberschaubar war: Mehrere hundert waren es ohne Zweifel, ob es mehr als die zwischenzeitlich festgestellten 3000 Anträge sind, vermag letztlich wohl niemand zu sagen. Dass nun der gordische Knoten gelöst worden zu sein scheint und das Dickicht gelichtet, ist ermutigend. Nicht nur die Bürger und Verbraucher, sondern

1 Bundesverfassungsgericht v. 3.6.1980 – 1 BvR 185/77, BVerfGE 54, 148 (153).

2 Bundesverfassungsgericht v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 –, BVerfGE 65, 1-71.

3 Für das Jahr 1979 siehe http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/02TB_79.pdf?__blob=publicationFile, für die Jahre 2011 und 2012 siehe http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/24TB_2011_2012.pdf?__ blob=publicationFile.

4 Vgl. Mitteilung des Datenschutzbeauftragten v. 22.10.2013, abrufbar unterhttp://www.datenschutzbeauftragter-info.de/libe-ausschuss-bestaetigt-gesetzentwurf-zur-eu-datenschutz-grundverordnung/;ausführlich hierzu Wybitul/Fladung, EU-Datenschutz-Grundverordnung – Überblick und arbeitsrechtliche Betrachtung des Entwurfs, Betriebs-Berater 2012, 509.

auch die datenverarbeitenden Unternehmen und verantwortlichen Stellen sind auf ein deutungssicheres Datenschutzrecht angewiesen. Grauzonen zu verkleinern dient der Effizienz und Effektivität nicht nur des Persönlichkeitsschutzes, sondern auch wirtschaftlichen Handelns. So ist denn auch der Ansatz einer Verordnung, die anders als das europäische Richtlinienrecht nicht umgesetzt werden muss, sondern direkt im Verhältnis unter den Bürgern wirkt, zu begrüßen. Landesspezifische Besonderheiten etwa zum Schutz der Presse oder im Arbeits- und Sozialrecht können durch Öffnungsklauseln aufgefangen werden. Durch das einheitliche europäische Recht würde das Handeln der Aufsichtsbehörden vereinheitlicht – auch dies gibt Rechtssicherheit.

Gestrandet waren demgegenüber nationale Gesetzesinitiativen. Der Entwurf eines novellierten Beschäftigtendatenschutzes wurde in der letzten Legislaturperiode so oft überarbeitet, bis er zum Schluss von niemandem befürwortet wurde. Das war ärgerlich, denn diese letzten Regelungen waren zukunftsweisend und ein angemessener Ausgleich zwischen Arbeitgeber- und Arbeitnehmerinteressen[5]. Es sprach für die Ausgewogenheit der Regelung, dass sowohl Arbeitgeberverbände als auch Gewerkschaften in ihrer Ablehnung einmütig waren, freilich aus ganz unterschiedlicher Perspektive. Die einen sahen hierin eine unerträgliche Verschlechterung des Beschäftigtendatenschutzes, die anderen einen unangemessen weiten Ausbau. Die Regelungen jedoch waren kein weniger oder kein mehr im Datenschutz, sondern nur klarer und damit besser. Die geheime Videoüberwachung von Arbeitnehmern wurde gänzlich verboten, der Datenaustausch im Konzern auf eine rechtssichere Grundlage gestellt. Die Trennlinie zwischen Telekommunikationsgesetz und Bundesdatenschutzgesetz, das die Kontrolle von E-Mails und Internet bei Verdacht auf Straftaten regelt, wäre für die Praxis verlässlich gezogen worden. Aus dem zur Zeit einen Paragraphen des Beschäftigtendatenschutzes wurden 14. Mag hier auch einiges redundant gewesen sein, so führten die verschiedenen Einzelnormen doch sehr viel klarer als bislang vor Augen, was der Gesetzgeber als zulässig oder unzulässig wertet. Fehler des damaligen Entwurfs können nun vermieden werden: Handwerklich kann er sauberer gemacht werden, den Betriebspartnern kann mehr Souveränität in der Ausgestaltung zugebilligt werden.

In einem neuen Anlauf wird der Gesetzgeber an einen zweiten Punkt denken müssen: Effektives Datenschutzrecht braucht effektive Sanktionen. Ein Recht, das nur höflich an den guten Willen der Normunterworfenen appelliert, bleibt ein stumpfes Schwert. Nun sind Sanktionen über die Ordnungswidrigkeit bis zur Strafbarkeit bereits im Gesetz vorhanden, doch fehlt oftmals die praktische Durchsetzbarkeit. Der Schadensersatzanspruch scheitert daran, dass unsicher ist, inwieweit und unter welchen Voraussetzungen Schäden, die keine Vermögensschäden darstellen, durch Geld ersetzbar sind. Dies aber sind die typischen Schäden bei Datenpannen. Auf Entblößung lässt sich kein Preisschild kleben, und der Richter, der es doch tun muss, schreitet im Nebel bloßer Intuition. Die Sanktionen der Ordnungswidrigkeit und der Strafbarkeit aber, die unabhängig von der Klage des Betroffenen greifen können, bedürfen der Durchsetzung durch staatliche Organe. Hier fehlen oft die personellen Ressourcen. So bleibt das Datenschutzrecht ein Recht, das solche Unternehmen bindet, die wegen ihrer Größe unter öffentlicher Beobachtung stehen, und das reichlich Raum bietet für kleinere Unternehmen, unter der hehren Schwelle hindurch zu schlüpfen.

Aber richtig ist auch: In dieser Weiterentwicklung des Datenschutzrechts sind seine bewährten Grundstrukturen beizubehalten. Datenverarbeitung ist unzulässig, wo sie durch das Gesetz nicht ausdrücklich zugelassen ist. Bestandteil dieses Grundsystems eines Verbotes mit Erlaubnisvorbehalt ist auch die Möglichkeit, eine Datenverarbeitung durch die Einwilligung des Betroffenen zu rechtfertigen. Das ist ganz und gar richtig, besinnt man sich der Grundlage des Datenschutzrechts: Es kann gerade Ausdruck des Persönlichkeitsrechts sein, wenn der Betroffene seine Daten freigibt – sei es aus mangelndem Interesse, sei es aus der Überzeugung, dass die Datenverarbeitung nützt oder zumindest doch nicht schadet. Diese Souveränität muss er behalten können. Dies liegt nicht allein daran, dass solche Einwilligungen etablierter Bestandteil der datenschutzrechtlichen Praxis sind. Vielmehr darf der Datenschutz nicht gegen den geschützt werden, der durch den Datenschutz geschützt wird. Diesen Ansatz verfolgen jetzt aber der Koalitionsvertrag – und ebenso der Kommissions-Entwurf für eine Datenschutz-Grundverordnung, die dem Arbeitnehmer diese Mündigkeit über seine Daten absprechen[6]. Das kann nicht richtig sein. Schon heute lässt das Datenschutzrecht als Einwilligung nicht jedes eilig dahergeredete Meinetwegen genügen, sondern verlangt die schriftliche, nach Information gegebene und jederzeit widerrufbare Erklärung des Arbeitnehmers, die freiwillig in ihrer Erteilung und in ihrem Widerruf sein muss. Diese Freiwilligkeit ist zukünftig stärker zu schützen. Es sind prozedurale Sicherungsinstrumente hilfreich, dem Arbeitnehmer und jedem sonstigen Betroffenen den Umfang seiner Datenpreisgabe zu offenbaren. Hilfreich kann es sein, dass der Betroffene schriftlich belehrt werden muss über den Umfang und den spezifischen Zweck des erbetenen Einverständnisses; hilfreich wäre es, wenn dieses erst nach einer bestimmten Frist der Überlegung wirksam würde; hilfreich wäre es, wenn eine Einverständniserklärung zwingend einer separaten Unterschrift gegenüber anderen vertraglichen Erklärungen bedürfte. Dies ist bisher weder durch das Gesetz, noch durch Rechtsprechung, noch durch Aufsichtsbehörden hinreichend deutlich festgeschrieben. Dem Gesetzgeber würde eine systemstimmige Weiterentwicklung gut zu Gesichte stehen. Eine Einwilligung wäre dann tatsächlich Grundrechtsausübung durch Grundrechtsverzicht, die nach allgemeiner Dogmatik stets zulässig ist, sobald sie tatsächlich freiwillig und selbstbestimmt erfolgt und nicht in den Kernbereich privater Lebensgestaltung eingreift. Auch letzteres wäre als Schranke der Einwilligung zu beachten, doch dürfte es in den wenigsten Fällen des Datenschutzes praktisch werden. Ansonsten aber gilt: Der Datenschutz ist nicht zu

5 Hierzu Thüsing, Neue Zeitschrift für Arbeitsrecht 2009, 865.

6 KOM (2012) 11 endgültig.

schützen gegen den, der durch den Datenschutz geschützt werden soll[7].

Weil nun Datenschutz die Selbstbestimmung ernst nehmen muss, weil er aus ihrem Schutz heraus zu begründen ist, sind weitergehend ganz generell bestehende Regelungen daraufhin zu hinterfragen, ob sie den Betroffenen mündig genug machen, zum einen über seine Daten zu verfügen, zum anderen Datenverstöße wirksam geltend machen zu können. Hierzu sind Informationspflichten geeignete Instrumente. Auch diese sind bereits im Gesetz vorhanden, doch können sie erweitert, klarer gefasst und effektiviert werden. Oftmals vollzieht sich der Datenmissbrauch im Verborgenen (Prism), und die bereits aktuell gegebene Offenbarungspflicht der Datenpanne wird oftmals nicht befolgt. Vorschläge zur Weiterentwicklung liegen auf dem Tisch. Die Politik braucht sie nur aufzugreifen.

Zuletzt das wohl wichtigste Petitum: Datenschutz braucht gesellschaftliche Verankerung und Akzeptanz. Voraussetzung dieser Akzeptanz ist auf der einen Seite das Bewusstsein, dass jede gesetzgeberische Regelung im Datenschutz eine zwar freiheitssichernde im Hinblick auf den Betroffenen, jedoch zugleich freiheitsbeschränkende Maßnahme im Hinblick auf den Datenverarbeitenden ist. Sie bedarf daher einer Rechtfertigung – rechtlich wie politisch. Erforderlich ist daher ein Datenschutz mit Augenmaß, dem stets bewusst ist, dass jedes Mehr an Regelung mit einem hinreichenden Schutzziel aufgewogen werden muss. Dies mag auch mutige Entscheidungen gegen den Strom erfordern. Dies gilt im Großen wie im Kleinen. Vorratsdatenspeicherung dient der Verhinderung und Verfolgung schwerer Straftaten. Dafür soll sie genutzt werden, und nur dafür muss sie genutzt werden können. Dass dabei europarechtliche Regelungen durch eine handlungsunfähige Regierungskoalition nicht nachvollzogen werden, ist beschämend. Wer hier national den einmal gefundenen europäischen Konsens aufkündigen will, der kann dies nur durch Überzeugung der europäischen Partner, nicht aber durch europarechtswidrige Untätigkeit tun. Nachdem der Europäische Gerichtshof nun Schweden am 30. Mai vergangenen Jahres wegen Untätigkeit zu einer Strafe von 3 Millionen € verurteilt hat[8], sollte dies genug Anlass für den deutschen Gesetzgeber sein, zu handeln.

Neben diesen Konflikten im Staat/Bürger-Verhältnis muss der Datenschutz auch im privaten Bereich Augenmaß bewahren: Für die Wirtschaft ist Datenschutz mit Bürokratiekosten verbunden, nicht umsonst ist der Lobbyistenansturm bei der Reform des EU-Datenschutzes so intensiv. Eine „lex google" kann nicht in gleichem Maße für den Handwerksbetrieb von nebenan gelten. Auch ist das Bedürfnis einer vereinfachten Regelung des Datenaustauschs im Konzern ernst zu nehmen. Die Politik hat – auch außerhalb des Beschäftigtendatenschutzes – die Aufgabe, praxisnahe und gleichzeitig den Betroffenen effektiv schützende Regelungen zu finden, wie der Datentransfer innerhalb einer Unternehmensgruppe rechtmäßig gestaltet werden kann. Momentan lavieren – auch große – Unternehmen oftmals getarnt in der Vagheit einer Grauzone, die rechtliche Unsicherheiten ausnutzt und hofft, dass dort kein Richter, wo kein Kläger ist.

III. Ein Schritt weiter: Datenbewusstsein als Voraussetzung des Datenschutzes

Auf der anderen Seite – nicht weniger wichtig – ist, Datenschutz in das Bewusstsein der Betroffenen zu bringen. Eine Generation, die in digitaler Entblößung auf Facebook und Co. aufwächst, wird oftmals das intuitive Gefühl dafür verloren haben, dass allzu viel Offenherzigkeit mit Freiheitseinschränkungen und Verlust an Privatsphäre einhergeht. Viele Schulen gehen beispielhaft voran und vermitteln Nutzerkompetenz im Internet in datenschutzrechtlicher Hinsicht. Solche Initiativen sind zu fördern und zu verbindlichen Bestandteilen der Curricula zu machen. In gleicher Verantwortung stehen die Unternehmen, die eine Kultur der Datenvermeidung und Datensparsamkeit in ihrem Betrieb fördern können. Einige haben dabei aus vergangenen Pannen und Skandalen gelernt. Wenn Datenschutzbeiräte errichtet werden, die Konzerndatenbeauftragte bei der Überwachung von Standards in den Unternehmen unterstützen, dann dient das langfristig nicht nur den betroffenen Arbeitnehmern, sondern auch dem Unternehmen und seiner Reputation. Denn Datenschutz durchsetzen kann auch der Kunde und Konsument; ihm steht es frei, bei Unternehmen mit allzu laschem Datenschutz nicht mehr zu kaufen. Datenschutz muss nicht nur als Begrenzung von Compliance verstanden werden, sondern auch als ihr Gegenstand. Unternehmen müssen nicht nur darauf achten, dass Gesetz und selbstgesetzte Regeln eingehalten werden, sondern auch darauf, dass bei Überwachung der Gesetzeseinhaltung der Datenschutz eingehalten werden muss. Ergänzend können sie durch den Gesetzgeber zur Datensparsamkeit und Datenvermeidung gezwungen werden, indem sinnvolle Instrumente wie Pseudonymisierung und Anonymisierung gestärkt werden.

All dies gibt die Richtung vor, wie die Person künftig effektiver geschützt und Freiheit gesichert werden kann. Das Bedürfnis nach Persönlichkeitsschutz ist gesellschaftlich wach wie ehedem. Es ernst zu nehmen, dient nicht nur dem Einzelnen, sondern der Gesellschaft als Ganzes. Das Ziel ist klar, jeder Schritt auf dem Weg dorthin ist verdienstvoll.

7 Ausführlich Thüsing, Neue Zeitschrift für Arbeitsrecht 2009, 865.

8 Europäischer Gerichtshof v. 30.5.2013 – Rs.-C 270/11.

Beschäftigtendatenschutz: Was wäre besser als der Status quo?*

Prof. Dr. Martin Franzen, Universität München**

Die 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 27.3.2014 eine Entschließung verabschiedet mit der Überschrift „Beschäftigtendatenschutz jetzt!" Die Datenschutzbeauftragten verlangen, dass ein Beschäftigtendatenschutzgesetz alsbald geschaffen wird. Sie verweisen auf eine Vielzahl von Fragestellungen, für die es bislang noch keine klaren rechtlichen Vorgaben gebe. Die Datenschutzbeauftragten führen eine ganze Reihe solcher angeblich ungeklärter Fragen auf: „die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy oder Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielsweise aus sozialen Netzwerken."

All diese genannten Fragestellungen sind wichtig, sie sind aber nur zum Teil ungeklärt. Schaut man sich diese Problembereiche näher an, erkennt man, dass hier Grundfragen der Rechtsbeziehung zwischen Arbeitgeber und Arbeitnehmer, Grundfragen des Arbeitsverhältnisses, betroffen sind – insbesondere die Reichweite und Zulässigkeit von Informationserhebungen im Arbeitsverhältnis. Dies zu regeln ist zunächst Aufgabe des Arbeitsvertragsrechts. In Deutschland gibt es nun kein kodifiziertes Arbeitsvertragsgesetz – die Gründe hierfür sind vielfältig. Deshalb sind hier zunächst die Arbeitsgerichte gefragt, welche selbstverständlich Rechtsgrundsätze zu einigen der aufgeworfenen Fragen entwickelt haben. Die Arbeitsgerichtsbarkeit kann dies natürlich nur tun, soweit Fallgestaltungen überhaupt an sie herangetragen werden, soweit also geklagt wird. Wenn man also fehlende gesetzliche Regelungen auf diesen Feldern beklagt, müsste man zunächst einmal das Arbeitsvertragsrecht kodifizieren und nebenbei bemerkt den Regelungsauftrag aus dem Einigungsvertrag erfüllen. Dies zu schaffen wäre der erste Schritt, bevor man sich an die Kodifikation eines Beschäftigtendatenschutzgesetz macht, das all diese Fragestellungen aus seiner Perspektive lösen möchte – und das ist letztlich die Perspektive des Polizeirechts mit der Regelungstechnik Verbot mit Erlaubnisvorbehalt. Das passt nur bedingt ins Arbeitsverhältnis als ein Rechtsverhältnis zwischen Privatrechtssubjekten. Was die Datenschutzbeauftragten ebenfalls nicht vollständig in den Blick nehmen: Wir haben es im Arbeitsverhältnis mit weiteren Akteuren zu tun – neben den Arbeitsvertragsparteien, die natürlich auch Regelungen in diesen Bereichen vereinbaren können – insbesondere die Tarifvertragsparteien und in unserem Kontext besonders wichtig der Betriebsrat.

Aus meiner Sicht ist neben anderem an dieser Überambitioniertheit das Projekt der Bundesregierung mit ihrem Entwurf eines Beschäftigtendatenschutzgesetzes in der letzten Legislaturperiode gescheitert[1]. Er enthielt zu viele Regelungen einzelner genuin arbeitsvertragsrechtlicher Fragestellungen, die nur wegen der fortgeschrittenen Digitalisierung auch datenschutzrechtlich eingekleidet waren, und war verbunden mit einer aus dem Datenschutzrecht bekannten Regelungstechnik: weite, generalklauselartige Erlaubnistatbestände mit am Verhältnismäßigkeitsgrundsatz orientierten Abwägungsprogrammen. Bei solcher Regelungstechnik besteht die Gefahr, dass man als Rechtsunterworfener beides bekommt: sowohl Überregulierung und als auch Rechtsunsicherheit.

Damit bin ich bei der EU-Datenschutzgrundverordnung[2]. Angesichts des derzeitigen Stands der Diskussion besteht dieselbe Gefahr. Speziell zum Arbeitnehmerdatenschutz haben wir folgende Lage, sofern der Beschluss des Europäischen Parlaments Gesetz wird: Die Mitgliedstaaten können nun in den Grenzen der Verordnung den Beschäftigtendatenschutz eigenständig regeln – und zwar auch durch Kollektivverträge. Gleichzeitig enthält der Verordnungsvorschlag in der Fassung des Parlamentsbeschlusses aber Mindeststandards[3]. Diese stellen nicht unerhebliche Vorgaben auf und sind zum Teil aus dem Gesetzentwurf der Bundesregierung zum Beschäftigtendatenschutz aus der letzten Legislaturperiode entnommen – wie etwa das vollkommene Verbot heimlicher Videoüberwachung, das wiederum nach Auffassung des Bundesarbeitsgerichts die Grundrechte des Arbeitgebers aus Art. 12 und 14 GG unzumut-

* Impulsreferat gehalten auf dem von der Gesellschaft für Europäische Sozialpolitik und der Gesellschaft für Datenschutz und Datensicherheit veranstalteten Diskussionsforum „Datenschutz – Was tun? Aktuelle Herausforderungen aus Europa – Vorhaben des Koalitionsvertrags" am 04.06.2014 in Berlin. Die Vortragsform wurde beibehalten.

** Der Autor ist Inhaber des Lehrstuhls für deutsches, europäisches, internationales Arbeitsrecht und Bürgerliches Recht an der Juristischen Fakultät der LMU München.

1 Entwurf der Bundesregierung eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drucksache 17/4230.

2 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr KOM (2012) 11/4 vom 25.1.2012.

3 Vgl. Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Plenarsitzungsdokument A7-0402/2013 vom 21.11.2013.

4 BAG 21.6.2012 NZA 2012, 1025 Rn. 41; BAG 21.11.2013 NZA 2014, 810 Rn. 51; der EGMR 5.10.2010 – 420/07 – Kröpke – hält diese Rechtsprechung für vereinbar mit der EMRK.

bar verletzen soll[4]. Dieses Verbot der heimlichen Videoüberwachung wäre also eher eine Art „Höchststandard". Wie dem auch sei: Wenn dieses Regelungsgeflecht so Gesetz wird, werden wir eine Vielzahl zu beachtender Regulierungsstandards auf den unterschiedlichen Regelungsebenen bekommen: Mindeststandards mit einer gewissen Regulierungstiefe auf europäischer Ebene; diese können von den Regelungen der Mitgliedstaaten zugunsten der Arbeitnehmer überboten werden; daneben kommen noch Betriebsvereinbarungen und Tarifverträge als Regelungsinstrumente in Betracht. Was wir nicht bekommen, sind einheitliche Regeln zum Arbeitnehmerdatenschutz in der gesamten EU, wie dies wohl Teile der Wirtschaft gewünscht haben. Und mit der Klarheit und Vorhersehbarkeit des Rechts dürfte es angesichts dieses Regelungsgeflechts im Mehrebenensystem der EU ebenfalls nicht zum Besten bestellt sein. Mutmaßlich bekommen wir also auch hier: Überregulierung und Rechtsunsicherheit.

Noch kurz ein Wort zur Kompetenz der EU für die arbeitsrechtlichen Regelungen der EU-Datenschutz-Grundverordnung[5]. Die Kommission nennt als Kompetenzgrundlage für die VO Art. 16 Abs. 2 AEUV und Art. 114 Abs. 1 AEUV. Art. 16 Abs. 2 AEUV trägt für arbeitsrechtliche Regelungen allerdings nichts bei, weil diese Vorschrift zum einen eine Rechtsgrundlage für die Schaffung datenschutzrechtlicher Regelungen hinsichtlich der Datenverarbeitung durch die Organe der Union und durch die Mitgliedstaaten statuiert; es geht also gerade nicht um die Datenverarbeitung durch Privatrechtssubjekte. Zum anderen erlaubt Art. 16 Abs. 2 AEUV den Erlass von Rechtsvorschriften über den freien Datenverkehr. Dies betrifft ebenfalls nicht Regelungen zum Arbeitnehmerdatenschutz, weil insoweit die Sicherung der ungehinderten Datenübertragung zwischen den Mitgliedstaaten in aller Regel nicht berührt ist. Bei Art. 114 Abs. 1 AEUV – die andere im Kommissionsvorschlag genannte Kompetenzgrundlage – handelt es sich um die allgemeine Kompetenzgrundlage für die Verwirklichung des Binnenmarkts. Diese Rechtsgrundlage gilt aber nach Art. 114 Abs. 2 AEUV nicht für „die Bestimmungen über die Rechte und Interessen der Arbeitnehmer". Der Vorschlag der EU-Kommission für eine Datenschutzgrundverordnung enthält nicht mehr nur Regelungen wie die geltende EU-Datenschutzrichtlinie 95/46/EG, welche sich als Annex auf das Arbeitsrecht auswirken können, sondern er enthält genuine Bestimmungen über „Rechte und Interessen der Arbeitnehmer". Daher kann eine derartige Regulierung wegen Art. 114 Abs. 2 AEUV nicht mehr auf Art. 114 AEUV gestützt werden, sondern nur auf die sozialpolitischen Vorschriften des AEUV, insbesondere Art. 153 AEUV. Diese begrenzen aber nach Form und Inhalt die Rechtssetzungskompetenz der Union wesentlich stärker: Es dürfen nur EU-Richtlinien mit mindestharmonisierenden Regelungen erlassen werden (Art. 153 Abs. 2 AEUV). In der Form einer vollständig harmonisierenden Verordnung sind also Regelungen zum Arbeitnehmerdatenschutz auf der Ebene der EU kompetenzwidrig.

Nun zurück zur Ausgangsfrage: Was sollte man auf der Ebene der Gesetzgebung stattdessen tun?

Ich plädiere für eine Stärkung der Selbstregulierung und die Stärkung prozeduraler Lösungen[6]. Die zuständige Arbeitnehmervertretung und der betriebliche Datenschutzbeauftragte könnten präventiv wesentlich stärker eingebunden werden, als dies bislang auf der Ebene gesetzlicher Regulierungen der Fall ist. Beide Institutionen haben eine starke Stellung: Der Betriebsrat hat ein zwingendes Mitbestimmungsrecht bei der Einführung von technischen Einrichtungen, die zur Überwachung der Arbeitnehmer geeignet sind (§ 87 Abs. 1 Nr. 6 BetrVG). Außerdem gehört es zu seinen Aufgaben, darüber zu wachen, ob die für die Arbeitnehmer geltenden Gesetze eingehalten werden (§ 80 Abs. 1 Nr. 1 BetrVG). Dazu gehören ebenso die jeweiligen datenschutzrechtlichen Regelungen, also auch das BDSG oder eine künftige EU-Datenschutzverordnung. Der Betriebsrat hat also eine starke Stellung im Bereich des Arbeitnehmerdatenschutzes. Für den betrieblichen Datenschutzbeauftragten gilt Vergleichbares: Seine Unabhängigkeit wurde früher bezweifelt. Das Bundesarbeitsgericht meinte sogar im Jahr 1997, der betriebliche Datenschutzbeauftragte habe keine „neutrale Stellung" inne und sei „verlängerter Arm" des Arbeitgebers, weshalb der betriebliche Datenschutzbeauftragte die Datenverarbeitung des Betriebsrats nicht kontrollieren dürfe[7]. Dies kann man heute jedenfalls nicht mehr mit Grund so sehen. Seit 2009 ist der betriebliche Datenschutzbeauftragte nur noch außerordentlich kündbar. Dies hat seine Unabhängigkeit erheblich gestärkt. Das BAG scheint dies nun ähnlich zu sehen, wenn es die Ämter betrieblicher Datenschutzbeauftragter und Betriebsrat für kompatibel hält[8].

Man könnte nun diesen beiden Institutionen – betrieblicher Datenschutzbeauftragter und Betriebsrat – Kompetenzen im Hinblick auf die Konkretisierung der im Datenschutzrecht enthaltenen unbestimmten Rechtsbegriffe und des Abwägungsprogramms zubilligen – etwa in der Art: Wenn Arbeitnehmervertretung und betrieblicher Datenschutzbeauftragter einer bestimmten Datenerhebung, -verarbeitung oder –nutzung ausdrücklich zustimmen, wird der entsprechende Datenumgang datenschutzrechtlich privilegiert und ist nur unzulässig, wenn er offensichtlich von den durch das Datenschutzrecht aufgestellten Datenschutzstandards abweicht[9]. Unter den genannten Voraussetzungen – Zustimmung dieser beiden mit dem betrieblichen Datenschutz befassten Institutionen – könnte also die Kontrolldichte vor

5 Näher dazu Franzen, DuD 2012, 322 ff.

6 Vgl. schon Franzen, RdA 2010, 257 ff.

7 BAG 11.11.1997 AP Nr. 1 zu § 36 BDSG.

8 BAG 23.3.2011 NZA 2011, 1036.

9 Siehe dazu ausführlicher Franzen, RdA 2010, 257, 261 ff.

10 Arbeitsgerichtliche Auseinandersetzungen zwischen Arbeitnehmer und Arbeitgeber um datenschutzrechtliche Probleme sind selten. Zumeist spielen diese Themen im Rahmen von Kündigungsschutzklagen bei der Frage eine Rolle, ob der Arbeitgeber eine gegebenenfalls (datenschutz-) rechtswidrig erlangte Information im Prozess verwerten darf, siehe dazu etwa Lunk, NZA 2009, 457; Morgenroth, NZA 2014, 408; aus der Rechtsprechung etwa BAG 21.11.2013 NJW 2014, 810.

allem durch die Aufsichtsbehörde, aber auch durch Gerichte[10] reduziert werden.

Eine Stärkung der Selbstregulierung kann ferner darin liegen, das Anerkennungsverfahren nach § 38a BDSG auf unternehmens- und/oder konzerninterne Regelungen auszudehnen[11]. Nach dieser Vorschrift können bislang bereits Berufsverbände und andere Vereinigungen, welche bestimmte Gruppen von verantwortlichen Stellen repräsentieren, also etwa auch Arbeitgeberverbände, Verhaltensregeln erarbeiten und diese sich in einer Art Vorabrechtmäßigkeitskontrolle von der zuständigen Aufsichtsbehörde bewilligen lassen. Diese Vorschrift geht auf Art. 27 Abs. 2 RL 95/46/EG und letztlich auf niederländische und irische Erfahrungen zurück[12]. Sie hat in der Praxis bislang kaum eine Rolle gespielt[13]. Diese Möglichkeiten könnten erweitert und auf einzelne speichernde Stellen ausgedehnt werden. Auch für Arbeitgeberverbände läge hier noch ein zu beackerndes, derzeit noch brachliegendes Feld – vor allem für Verbände aus Branchen mit in aller Regel nur kleinen Betrieben, in denen es nur selten Betriebsräte gibt.

Ich möchte schließen mit drei konkreten Vorschlägen im Sinne der Frage, was ist besser als der jetzige Zustand?

1. Klarstellung, dass Tarifverträge und Betriebsvereinbarungen Erlaubnisnormen im Sinne von § 4 Abs. 1 BDSG sind.

Das entspricht zwar bereits bislang der Rechtsprechung des BAG. Allerdings stammen die einschlägigen Entscheidungen bereits aus den 1980er Jahren. In der Zwischenzeit wurde diese Rechtsprechung in der datenschutzrechtlichen Literatur zunehmend angegriffen. Zusätzliche Unsicherheit erzeugte der Regierungsentwurf zum Beschäftigtendatenschutz aus der letzten Legislaturperiode. Danach wurde dies zwar ebenfalls klargestellt, allerdings um ein Günstigkeitsprinzip erweitert: Die Betriebsvereinbarung oder der Tarifvertrag durften danach nicht von den datenschutzrechtlichen Regelungsstandards des BDSG zum Nachteil der Arbeitnehmer abweichen. Dies führt zu Rechtsunsicherheit und hat in der Literatur die Diskussion um die Erlaubnisnormqualität von Betriebsvereinbarung und Tarifvertrag negativ befeuert. In zwei neueren Entscheidungen aus 2013 hat das BAG seine bisherige Sichtweise allerdings bekräftigt[14].

2. Klarstellung, dass der Arbeitgeber kein Diensteanbieter im Sinne des TKG und TMG ist, wenn er private E-Mail- und Internetnutzung erlaubt.

Dieses Problem ist in der Literatur und der instanzgerichtlichen Rechtsprechung sehr umstritten. Inzwischen geht eine gewisse Tendenz dahin, den Arbeitgeber insoweit nicht als Diensteanbieter anzusehen[15]. Eine Klarstellung würde dazu führen, dass auf solche Fragen das allgemeine Datenschutzrecht anwendbar ist. In Verbindung mit der Klarstellung, dass auch Betriebsvereinbarungen Erlaubnisnormen im Sinne des § 4 Abs. 1 BDSG sein können, erlangten Arbeitgeber und Arbeitnehmer damit ein zusätzliches Maß an Rechtssicherheit. Dann könnten nämlich durch Betriebsvereinbarung Nutzungs- und Überwachungsstandards für die private Nutzung von E-Mails und Internet am Arbeitsplatz im Einklang mit dem Datenschutzrecht gesetzt werden.

3. Ein offenes Regelungsproblem stellt immer noch die Übermittlung von Personaldaten in Konzernen dar.

Das Datenschutzrecht knüpft seine Verantwortlichkeiten bekanntlich an den jeweiligen Rechtsträger, die sogenannte verantwortliche Stelle, an. Konzernunternehmen sind also im Verhältnis zueinander eigenständige speichernde Stellen. Die Übermittlung von Personaldaten im Konzern muss daher datenschutzrechtlich im Prinzip genauso gerechtfertigt werden wie die Übermittlung an eine andere speichernde Stelle außerhalb von Konzernverbindungen. Eine sachgerechte Regelung könnte etwa an den Gedanken anknüpfen, den wir aus der Problematik der Übermittlung von Daten in Drittländer her kennen. Dort fragen wir: Werden im Drittland angemessene Datenschutzstandards eingehalten? Dieser Gedanke erscheint mir auf die Problematik der Datenübermittlung im Konzern übertragbar zu sein. Im Beschluss des Europäischen Parlaments über den Vorschlag der EU-Kommission für eine Datenschutzgrundverordnung ist dieses Problem angesprochen. Dort lautet die entsprechende Passage in Art. 82 Abs. 1d Vorschlag Datenschutzgrundverordnung: „Die Übermittlung und Verarbeitung von personenbezogenen Beschäftigtendaten zwischen rechtlich selbständigen Unternehmen innerhalb einer Unternehmensgruppe und mit rechts- und steuerberatenden Berufsangehörigen ist zulässig, soweit sie für den Geschäftsbetrieb relevant ist und der Abwicklung von zweckgebundenen Arbeits- oder Verwaltungsvorgängen dient und sie den schutzwürdigen Interessen und Grundrechten des Betroffenen nicht entgegensteht“. Ich würde hier noch ergänzen: Letzteres ist dann der Fall, wenn das Zielunternehmen Gewähr dafür bietet, dass die geltenden datenschutzrechtlichen Standards eingehalten werden.

Zusammenfassend: Was ist besser als der jetzige Zustand? Drei Dinge: 1. Klarstellung, dass Tarifverträge und Betriebsvereinbarungen Erlaubnisnormen im Sinne von § 4 Abs. 1 BDSG sind. 2. Klarstellung, dass der Arbeitgeber kein Diensteanbieter im Sinne des TKG und TMG ist, wenn er private E-Mail- und Internetnutzung der Arbeitnehmer am Arbeitsplatz erlaubt. 3. Sachgerechte Regelung der Problematik „Übermittlung von Personaldaten im Konzern“.

11 In dieser Richtung rechtspolitisch auch Arbeitskreis „Datenschutz in Recht und Praxis“ im BvD, DuD 2010, 254, 256; Weichert, DuD 2010, 7, 12.

12 Siehe näher Bizer, in Simitis (Hrsg.), BDSG, 6. Aufl. 2006, § 38a Rn. 14.

13 Vgl. Weichert, DuD 2010, 7, 12.

14 BAG 9.7.2013 NZA 2013, 1433 Rn. 31; BAG 25.9.2013 NZA 2014, 41 Rn. 32.

15 Siehe zur Problematik etwa Walther/Zimmer, BB 2013, 2933; Schuster, CR 2014, 21; Sander, CR 2014, 176.

Aus den aktuellen Berichten der Aufsichtsbehörden (14)

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter*

Videoüberwachung – ein unerschöpfliches Thema

Dass die Mehrzahl der in dem ersten Halbjahr des Jahres 2014 erschienenen Tätigkeitsberichte (Baden-Württemberg, Berlin, Brandenburg, Bremen Mecklenburg-Vorpommern, Hessen, Rheinland-Pfalz, Thüringen) das bereits in den vergangenen Jahren regelmäßige Berichtsthema Videoüberwachung nicht aussparte, zeigt dessen fortdauernde Aktualität. Der hessische Landesdatenschutzbeauftragte beschreibt es so: *„Auf den ersten Blick scheinen Schultoiletten, Bäckereien, Friseursalons, Sauna- und Umkleidebereiche in Schwimmbädern, Gästebereiche in Restaurants, Spielzeughubschrauber, eine Stadthalle und sogar der hessische Wald keine Gemeinsamkeiten zu haben. Eine Gemeinsamkeit gibt es dennoch: Der „Wildwuchs“* an *Videoüberwachungsanlagen nimmt kontinuierlich zu“* (42. TB, 2013, Ziff. 4.2.2). Der 10. TB Thüringen für den öffentlichen Bereich listet 11 Fälle von „Videogaga“ auf. Da eine offenbar zunehmende Zahl von Bürgern nicht mehr bereit ist, die in nahezu allen Lebensbereichen stattfindende Videoüberwachung ohne weiteres hinzunehmen, komme das Problem auch laufend auf den Tisch der Aufsichtsbehörde (vgl. auch LfD Rh.-Pf. 24. TB, 2012/2013, III, Ziff. 3.1). Der LfD Rheinland-Pfalz sieht die Problematik auch darin, „dass die technische Qualität der Überwachungskameras (gemessen etwa an der Auflösung/Pixelzahl oder der Zoomfähigkeit) und der Überwachungstechnik insgesamt (etwa mit dem Blick auf die nahezu unbegrenzte Verfügbarkeit von Speicherkapazität und die Zugriffsmöglichkeiten auf Überwachungsmaterial via Internet) einen Quantensprung vollzogen hat“. Entsprechende Software trage dazu bei, die entstehenden Datenmengen zielgerichtet auswertbar zu machen und ungefährliche Normalsituationen von Gefahrenlagen zu unterscheiden. Dem Überwachungspersonal werden nur noch relevante Bilder präsentiert, bzw. das System löst unmittelbar den Alarm aus. Die gängige Videokamera wird beweglich durch Drohnen oder portable Kameras in Mobiltelefonen oder als Dash-Camera an Automobilen, wobei die Kameras häufig durch die Mediatisierung der Technik nicht mehr als solche erkennbar sind.

Die nachfolgend aufgegriffenen Beispiele sollen dies beleuchten, wobei einige Tatbestände in mehreren Berichten angesprochen wurden bzw. auf Beschlüssen des Düsseldorfer Kreises beruhen.

Videoüberwachung als Türspion

Den klassische Türspion, der einen noch zwang, zur Tür zu laufen, um den gebetenen oder ungebetenen Gast durch einen verborgenen Blick durch das „Guckloch“ zu erkennen, hat inzwischen die Videokamera ersetzt, die das Bild des Besuchers auf den Computer oder Fernseher liefert, so dass vom Wohnzimmersessel aus über den Einlass entschieden werden kann. Diese in Ausübung des Hausrechts stattfindende Beobachtung ist – jedenfalls in gewissen Grenzen – von dem Besucher hinzunehmen. Der HessLDSB (42. TB, 2013, Ziff. 4.2.2.3) verweist auf eine Entscheidung des BGH (vom 8.4.2011 – V ZR 210/10), die zu einer schon vor Inkrafttreten des § 6b BDSG erfolgten Überwachung erging. Danach ist die Videoüberwachung in dem Klingeltableau einer Wohnanlage zulässig, wenn

- die Kamera ausschließlich durch Betätigung der Klingel aktiviert wird,
- eine Bildübertragung allein in die Wohnung erfolgt, bei der geklingelt wurde,
- die Bildübertragung spätestens nach einer Minute beendet wird

und

- die Anlage das dauerhafte Aufzeichnen von Bildern nicht ermöglicht.

§ 6b Abs. 2 BDSG verlangt zudem den Hinweis auf die Beobachtung.

Dem folgend handelt es sich bei dem Einsatz einer eine Rundumaufzeichnung ermöglichenden Dome-Kamera um ein unzulässiges Verfahren.

Wildkameras

Von der Klingel- zur Klüngelkamera könnte man ironisch formulieren, wenn man die Diskussion in den Medien um sog. Wildkameras verfolgte. Nicht nur die Tiere des Waldes, sondern u.a. auch die Einsamkeit des Waldes aufsuchende Liebespaare wurden Gegenstand ihrer Aufzeichnungen. Nach Feststellungen des LfD Rh-Pf. (TB 2012/2013, III Ziff. 2.3.3) hat jeder Jäger zwischen zwei bis drei solcher Kameras in seinem Jagdrevier installiert, mit dem Ergebnis von etwa 30000 Kameras in rheinland-pfälzischen Wäldern. Grundsätzlich ist nach einschlägigem Landesrecht jeder zum Betreten des Waldes berechtigt, so dass Wald ein öffentlich zugänglicher Bereich ist (§ 6b Abs. 1 BDSG). Das gilt unabhängig davon, ob es sich um Privat- oder Staatswald handelt. Ein berechtigtes Interesse des Waldbesitzers bzw. des insoweit relevanten Jagdausübungsberechtigten zur Registrierung von Waldbesuchern, auch wenn diese sich abseits der Wege bewegen, besteht nicht. Auch eine durch den Einsatz der Videotechnik erleichterte Jagdausübung, d.h. die Ermittlung von konkreten Angaben zum Wildbestand ohne langwieriges Ansitzen, geht dem Schutzinteresse der Betroffenen nicht vor. Jedenfalls regelmäßig hat das Recht der

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

Spaziergänger, Pilzsammler, Jogger etc., als Waldbesucher in der freien Natur unbeobachtet zu sein, Vorrang. Ausnahmen bestätigen jedoch auch hier die Regel: Soweit nach dem Landesrecht Jagdeinrichtungen wie Wildfütterungsstellen oder Ansitze oder Wildtierbrücken nicht zu dem öffentlich zugänglich Bereich gehören, können diese von dem Jagdausübungsberechtigten beobachtet werden, wobei auch hier – auch ohne Vorgabe des § 6b Abs. 2 BDSG – der überwachte Bereich mit Benennung der verantwortlichen Stelle deutlich erkennbar gemacht sein muss (HessLDSB, 42. TB, 2013, Ziff. 4.2.2.7). Zulässig sind auch Kameras, die eindeutig nur auf die Beobachtung von Tieren ausgerichtet sind, wie z.B. bei einer Dachsbaubeobachtung.

Auto-Cockpit-Kameras

Ein verhältnismäßig neues Verfahren ist die Ausstattung von Kraftfahrzeugen mit Außenkameras. Vorrangiges Ziel ist die Gewinnung von Beweismitteln im Falle eines Unfalls. Da diese Aufzeichnungen nicht – wie Videoaufnahmen während eines Urlaubs – ausschließlich zu privaten Zwecken und damit außerhalb des Anwendungsbereichs des BDSG (§ 1 Abs. 2 Nr. 3) stattfinden, setzt nach Meinung der Aufsichtsbehörden § 6b den Zulässigkeitsmaßstab. Die Zweckbestimmung „Wahrnehmung des Hausrechts“ entfällt, so dass ein konkretes, den Schutzinteressen der unbemerkt aufgezeichneten Verkehrsteilnehmer vorrangiges berechtigtes Überwachungsinteresse festzustellen wäre. Dieses Interesse wird von den Aufsichtsbehörden verneint. Selbst wenn dann im Ereignisfall Straftaten dokumentiert würden, ist die dem vorausgehende Dauerüberwachung unbeteiligter Dritter nicht gerechtfertigt (vgl. auch BrandbLDA, 17. TB 2012/2013, Ziff. 15,4; HessLfD, 42. TB, 2013, Ziff. 4.2.2.6). Auf die hierzu mit gegenteiligem Ergebnis ergangene Bewertung des Sachverhalts durch Atzert/Franck (RDV 2014, S. 136) ist jedoch hinzuweisen.

Videoüberwachung in Taxis

Vor ihrer Stellungnahme zu „Unfallkameras“ haben die Aufsichtsbehörden sich zu innerhalb eines Taxis zum Schutz von Taxifahrern stattfindenden Videoaufzeichnungen angesichts der konkreten Risikolage positiver geäußert. Zu Recht wurde anerkannt, dass die körperliche Unversehrtheit oder das Eigentum von Taxifahrern den Einsatz von Videokameras rechtfertigen kann, wenn dieser zum Schutz der Persönlichkeitsrechte der Fahrgäste auf das erforderliche Mindestmaß beschränkt bleibt (vgl. Beschluss des Düsseldorfer Kreises vom 26./27.2.2013 = RDV 2013, 267). Demgemäß darf die Kamera nicht permanent betrieben werden, und die maximale Speicherungsfrist soll 48 Stunden betragen, wobei jedoch wohl eine Löschung erfolgen müsste, wenn eine Fahrt ohne Zwischenfälle verlaufen ist. Die Fahrgäste sind vor dem Einstieg auf die Aufzeichnung hinzuweisen (LDA Brandenburg, TB 2012/2013, Ziff. 15.5). Fraglich erscheint es jedoch, diese sicherlich zutreffenden Feststellungen aus § 6b BDSG ableiten zu wollen, da das Taxi, wenn es einen Beförderungsvertrag erfüllt, kein „öffentlich zugänglicher Raum“ ist. Anderen Fahrgästen steht es nicht mehr zur Verfügung. Der Fall ist nicht anders, als wenn ein ansonsten öffentlich zugängliches Museum eine geschlossene Veranstaltung durchführt.

Drohnen

Zur Zeit sollen sich in Deutschland mit rasant zunehmender Tendenz rund 300.000 Drohnen, die als Träger von Kameras geeignet sind, in privatem Besitz befinden. Ihr Einsatz zu Sport- und Freizeitzwecken ist – sofern eine bestimmte Größe nicht überschritten wird – genehmigungs- und anzeigefrei (§ 16 Abs. 1 Nr. 1c LuftVO). Ansonsten bedarf der Betreiber einer Aufstiegserlaubnis. Soweit Drohnen mit Überwachungstechnik ausgerüstet sind, ist ihr Einsatz – sofern nicht eine ausschließlich persönlichen Zwecken dienende Verwendung stattfindet – unter datenschutzrechtlicher Sicht an § 6b BDSG zu messen. Je nach dem Zweck findet aber auch das BDSG keine Anwendung, wenn – wie in einem dem HessLfD (42. TB, 2013, Ziff. 4.2.2.5) vorgelegten Fall –, ein Journalist unter das Medienprivileg fallende Aufnahmen anfertigen wollte.

Fraglich ist, wann der Einsatzzweck die schutzwürdigen Interessen überwiegt und wie eine nach § 6b Abs. 2 BDSG erforderliche Kennzeichnung der Beobachtung bzw. der verantwortlichen Stelle erfolgen könnte. Demgemäß sind Videobeobachtungen bzw. -aufzeichnungen per Drohnen – insbesondere auch im Hinblick auf das Recht am eigenen Bild von – ggf. in ihrem geschützten Privatbereich (§ 211a StGB) aufgezeichneter Personen – als rechtswidrig zu bewerten.

Prüfungskontrolle

Einer nicht offengelegten Beobachtung waren an einer Hochschule in Mecklenburg-Vorpommern an einer Klausur teilnehmende Studierende ausgesetzt. Eigentliche Zweckbestimmung der Videoanlage war, mittels eines Beamers zur Präsentationen der Sprechenden während der Lehrveranstaltung zu dienen. Während der Klausur wurde die Technik von der Klausuraufsicht insofern „zweckentfremdet“, als sie auf die Studierenden gerichtet war, die sich auf die schlechter einsehbaren hinteren Plätzen des Hörsaales „zurückgezogen“ hatten. Die Bildübertragung erfolgte auf einen Kontroll-Bildschirm am Rednerpult.

Da eine spezielle Ermächtigungsgrundlage für derartige Kontrollen fehlte, war die die Videoüberwachungen regelnde Bestimmung des Landesdatenschutzgesetzes maßgebend. § 37 Abs. 1 LDSG M.-V. lässt eine Videoüberwachung nur zur Wahrnehmung des Hausrechtes zu, und dieses nach einer Interessenabwägung und vorheriger Kenntlichmachung. Nicht ableiten konnte der LDSB M-V (TB 2012/2013, Ziff. 5.2.1) die Zweckbestimmung der Vermeidung/Aufdeckung von Betrugshandlungen bei einer Prüfung aus dem Hausrecht der Hochschule. Ob das in jedem Falle zutrifft, erscheint – einmal abgesehen von der Verhältnismäßigkeit der Maßnahme – zumindest für den Fall fraglich, dass festgestellt werden soll, ob nicht verbotenerweise Hilfsmittel mitgebracht wurden bzw. nicht an der Klausur Teilnahmeberechtigte anwesend waren.

Videoüberwachung am Arbeitsplatz

Aus der Reihe von Beispielen zur unzulässigen Überwachung am Arbeitsplatz seien drei herausgegriffen. So stellt der LDA Brandenburg (17. TB, 2012/2013 S. 128) eine Berechtigung, ein Firmengelände mit dem Ziel, Straftaten aufzudecken, zu überwachen als zulässig fest, wenn es je nach der Risikoanalyse genügen kann, die Überwachung auf die Zeit nach Geschäftsschluss zu beschränken. Produktionsstätten mit Video zu überwachen, um jeden Mitarbeiter schnellstmöglich aufzufinden, rechtfertigt den erzeugten Überwachungsdruck nicht, wobei vorliegend der zu überwachenden Geschäftsführer die Aufnahmen zu Hause und auch auf seinem Mobiltelefon ansehen konnte.

Als eine unzulässige, weil unverhältnismäßige Überwachung bewertete der LfD M-V (TB 2012/2013, Ziff. 5.2.2) die Überwachung einer Großbaustelle durch zwei auf den Baukränen angebrachte Kameras. Begründet wurde die Überwachung mit der Notwendigkeit der Kontrolle des reibungslosen Bauablaufs, des Einsatzes großer Geräte und schließlich mit dem Schutz des Eigentumes. Keine dieser Zweckbestimmungen wurde nach § 6b bzw. § 32 BDSG anerkannt, da für den jeweiligen Zweck, sofern er legitim war, andere effektivere und weniger eingreifende Maßnahmen zur Verfügung standen.

Gegenstand mehrerer Berichte waren teilweise flächendeckende Videoüberwachungen in Bäckereien. Begründet wurde die Überwachung mit dem Schutz des Personals und des Eigentums vor Überfällen. Offensichtlich sind Bäckereien für Raubüberfälle prädestiniert, da früh morgens oft nur eine Person in dem Geschäft anwesend ist. Der HessLDSB (42. TB, 2013, Ziff. 4.2.2.4) hält, um der Gefahrensituation vorzubeugen, eine Videokamera, die von hinten über den Kopf des Personals auf den Eingangsbereich gerichtet ist, für zulässig. Anders zu bewerten war ein ebenfalls mit der Abwehr von Überfällen begründetes komplexes Überwachungssystem, mit dem die Zentrale des Unternehmens über 90 Bäckereifilialen rund um die Uhr überwachte. Betroffenen waren Kunden und die Beschäftigten. Längere Verhandlungen mit dem Unternehmen führten dazu, dass die Überwachung reduziert und nur im Black-Box-Verfahren betrieben wird, d.h. dass der Zugriff auf die Bilder nur bei konkreten Vorfällen, unter Wahrung des Vier-Augen-Prinzips und unter Einbeziehung des betrieblichen Datenschutzbeauftragten stattfindet (LDSB M.-V. TB 2012/2013, Ziff. 5.2.8).

Zum Schluss: Verhaltenssteuerung durch Attrappen von Videokameras

Wenngleich die Installation von Kameraattrappen keine Datenverarbeitung bewirkt und damit von den Normen des BDSG nicht tangiert wird, handelt es sich um einen Eingriff in das informationelle Selbstbestimmungsrecht der vermeintlich Beobachteten. Der Überwachungsdruck bleibt für den Betroffenen der gleiche. Daher müssen für die Installationen von Kameraattrappen die gleichen Maßstäbe gelten wie für aktive Kameras (HessLDSB, 42. TB, 2013, Ziff. 4.2.3; vgl. auch die diesbezügliche Regelung in § 34 Abs. 6 LDSG Rheinland-Pfalz).

Fraglich ist, ob auch eine Kenntlichmachungspflicht entsprechend § 6b Abs. 2 BDSG besteht. Natürlich kann es sich nicht um den Hinweis auf eine Attrappe handeln, sondern um eine die Vortäuschung der Überwachung verstärkende Fehlinformation. Die Aufsichtsbehörden bejahen diese Hinweispflicht, die zudem hier im Interesse einer effektiven Abschreckung liegt.

Fazit

Dem Abschluss des Berichts kann die nachstehend wiedergegebene Gesamtbewertung des LfD Rh-Pf. (24. TB, 2012/2013, III Ziff. 2.3) bilden,. Sie lautet wie folgt:

„Insgesamt lässt sich die Videoüberwachung daher datenschutzrechtlich wie folgt bewerten:

- Jede Videoüberwachung ist ein Eingriff in das Persönlichkeitsrecht, denn alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.
- Die Videoüberwachung erfasst unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen.
- Daher ist Videoüberwachung immer begründungsbedürftig und darf immer nur offen erfolgen, sie ist stets auf das notwendige Maß zu beschränken und bedarf in zeitlicher Hinsicht der regelmäßigen Überprüfung (jährliche Evaluationspflichten).
- Vor der Einrichtung einer Videoüberwachung müssen alle Alternativen hierzu geprüft und bewertet werden. Videoüberwachung kann nur die ultima ratio sein.
- Jede Einrichtung einer Videoüberwachung muss der datenschutzrechtlichen Vorabkontrolle unterzogen werden (§ 4d Abs. 5 BDSG), gleichzeitig ist die Berufung eines behördlichen bzw. betrieblichen Datenschutzbeauftragten vor Installation der Videoüberwachung verpflichtend.
- Der Zweck der Videoüberwachung muss konkret vor Beginn der Überwachung schriftlich festgelegt werden.
- Während der Videoüberwachung müssen die Zweckbindung, die differenzierte Abstufung zwischen Aufnahmearten, die deutliche Erkennbarkeit der Videoüberwachung sowie die Löschung der Daten binnen kurzer Fristen (48 Stunden) strikt und dauerhaft sichergestellt werden.
- Rechtskonforme Videoüberwachung ist planungsintensiv, kostspielig, aufwändig und nur begrenzt effektiv. Videoüberwachung ist nur bei optimaler technischer und personeller Ausführung erfolgversprechend und nur dann verhältnismäßig.
- Die Beweislast für die Zulässigkeit der Videoüberwachung liegt bei den Betreiberinnen und Betreibern.
- Die flächendeckende Videoüberwachung muss verhindert werden, da die Gefahr besteht, dass diese Entwicklung zu einer Überwachungsinfrastruktur führt.
- Mögliche Rechtsverletzungen werden als Ordnungswidrigkeit mit hohen Bußgeldern verfolgt, können aus personellen Gründen jedoch nur unzureichend staatlich geahndet werden (Vollzugsdefizit).“

Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts

RAin Yvette Reif, LL.M., Bonn

Im Koalitionsvertrag haben sich CDU, CSU und SPD verständigt, Rechtsgrundlagen dafür schaffen, dass die Verbraucherverbände datenschutzrechtliche Verstöße abmahnen und Unterlassungsklage erheben können. Anfang Juni hat nunmehr das zuständige Bundesministerium der Justiz und für Verbraucherschutz einen entsprechenden Referentenentwurf vorgelegt.

In einer Zeit, in der Unternehmer aufgrund der Fortschritte der Informationstechnik immer mehr Daten von Verbrauchern für ihre geschäftlichen Zwecke erheben, verarbeiten und nutzen, werde wirksamer Verbraucherdatenschutz immer wichtiger, so die Gesetzesbegründung. Auch die besten datenschutzrechtlichen Regelungen nützten jedoch wenig, wenn sie nicht wirksam durchgesetzt werden könnten. Die Datenschutzaufsichtsbehörden könnten zwar Verstöße bei der Erhebung und Verwendung von personenbezogenen Daten mit aufsichtsrechtlichen Maßnahmen nach § 38 Abs. 5 BDSG beenden und bei bestimmten Verstößen auch Bußgelder verhängen. Eine flächendeckende Kontrolle durch die Aufsichtsbehörden scheide aber schon aufgrund der Zahl der Unternehmer und des stetig zunehmenden Umfangs ihres Datenumgangs aus. Häufig würden die Datenschutzaufsichtsbehörden deshalb erst tätig, wenn ihnen Verstöße gegen Datenschutzgesetze mitgeteilt würden. Die Verbraucher selbst scheuten häufig die Kosten und Mühen, die notwendig seien, um Ansprüche auf Löschung, Berichtigung oder Sperrung (§ 35 BDSG) oder ggf. auch Unterlassung (§ 1004 BGB analog) und Schadensersatz (§ 7 BDSG, § 823 Abs. 1 BGB) durchzusetzen. Dies gelte insbesondere dann, wenn die einzelnen Verbraucher nur in geringem Umfang betroffen sind. Zum besseren Schutz der Verbraucherrechte sollen deswegen neben den betroffenen Verbrauchern und den Datenschutzaufsichtsbehörden auch Verbände und Kammern gegen die unzulässige Erhebung, Verarbeitung oder Nutzung von Verbraucherdaten durch Unternehmer vorgehen können, so die Begründung des Referentenentwurfs.

Kern der vorgesehenen Neuregelung ist die Erweiterung des Unterlassungsklagengesetzes (UKlaG). Nach diesem Gesetz können näher spezifizierte Stellen, zu denen insbesondere registrierte Verbraucherschutzverbände, aber auch Verbände zur Förderung gewerblicher Interessen (z.B. Rechtsanwalts- oder Ärztekammern oder Innungen) und die Industrie- und Handels- bzw. Handwerkskammern zählen, Unternehmen im Wege der sog. Verbandsklage in Anspruch nehmen.

Ein Klagerecht auf Unterlassung beziehungsweise Widerruf besteht aktuell vor allem bei:

- Verwendung oder Empfehlung von Allgemeinen Geschäftsbedingungen (AGB), die nach der Inhaltskontrolle (§§ 307-309 BGB) unwirksam sind (§ 1 UKlaG)
- Zuwiderhandlungen gegen Verbraucherschutzgesetze (z.B. Vorschriften zu Verbrauchsgüterkauf, Haustürgeschäften, Reiseverträgen, Fernabsatzverträgen) (§ 2 UKlaG)

Durch Anfügen einer neuen Ziffer 11 in den Katalog der Verbraucherschutzgesetze nach § 2 Abs. 2 UKlaG sollen sämtliche „Vorschriften, die für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines Verbrauchers durch einen Unternehmer gelten“, künftig bei Verstoß in gleichem Maße abmahnfähig sein wie die anderen Verbraucherschutzgesetze im Sinne der Vorschrift.

Hintergrund der vorgesehenen Neuregelung ist, dass Datenschutzverstöße nach heutigem Recht nur dann nach dem UKlaG abmahnfähig sind, sofern die verletzten datenschutzrechtlichen Vorschriften, welche im Katalog der Verbraucherschutzgesetze in § 2 Abs. 2 UKlaG bislang nicht ausdrücklich aufgeführt sind, als sonstige Verbraucherschutzgesetze im Sinne der Vorschrift eingeordnet werden. Die zuständigen Zivilgerichte haben datenschutzrechtliche Vorschriften aber bislang überwiegend nicht als Verbraucherschutzgesetze angesehen. Nur ausnahmsweise, etwa wenn eine Allgemeine Geschäftsbedingung auch den Datenschutz regelte, konnten Verbraucherschutzorganisationen eine zu beanstandende Klausel abmahnen und gerichtlich prüfen lassen, so z.B. im Fall vzbv gegen Google, als der vzbv zahlreiche Klauseln aus den Datenschutzbestimmungen beanstandet hatte, in denen sich das Unternehmen sehr weitgehende Nutzungsrechte im Hinblick auf die Daten der Verbraucher einräumte. Die vorgeschlagene Regelung in § 2 Abs. 2 Nr. 11 UKlaG-E hätte hier klarstellende Funktion, indem sie den Datenschutzgesetzen ganz allgemein Verbraucherschutzcharakter zuspricht und so die Klagebefugnis der Verbraucherschutzorganisationen verbindlich festlegt. Vorgegangen werden kann dann durch die klageberechtigten Stellen nicht mehr nur gegen den Verbraucher unangemessen benachteiligende Datenschutzklauseln, sondern auch gegen Datenschutzverstöße in Form reiner

* Die Autorin ist stellvertretende Geschäftsführerin der Gesallschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn.

Realakte, wie z.B. eine unzulässige Verwendung personenbezogener Daten zu Werbezwecken.

Die Gesetzesbegründung betont allerdings explizit, dass auch bei einem Verstoß gegen datenschutzrechtliche Vorschriften, die Verbraucherschutzgesetze nach § 2 Abs. 2 Nr. 11 UKlaG-E sind, sich Ansprüche nach § 2 Abs. 1 UKlaG nur dann ergeben können, wenn der jeweilige Verstoß die Kollektivinteressen von Verbrauchern berührt (vgl. § 2 Abs. 1 UKlaG: „im Interesse des Verbraucherschutzes"). Dies sei nur der Fall, wenn die Datenschutzverletzung ihrem Gewicht und ihrer Bedeutung nach über den Einzelfall hinausreiche und eine generelle Klärung geboten erscheinen lasse. Letzteres sei vor allem dann gegeben, wenn Unternehmer die Daten vieler Verbraucher zu kommerziellen Zwecken in gleicher Weise erheben, verarbeiten oder nutzen.

Ein Unterlassungsanspruch kann darüber hinaus nicht geltend gemacht werden, wenn die Geltendmachung unter Berücksichtigung der gesamten Umstände missbräuchlich ist, insbesondere wenn sie vorwiegend dazu dient, gegen den Zuwiderhandelnden einen Anspruch auf Ersatz von Aufwendungen oder Kosten der Rechtsverfolgung entstehen zu lassen (§ 2 Abs. 3 UKlaG). Um einem Missbrauch der Ansprüche nach dem UKlaG besser vorzubeugen, soll der Anwendungsbereich dieser Missbrauchsregelung erweitert werden. Hierzu soll sie in einen neuen § 2b UKlaG-E („Missbräuchliche Geltendmachung von Ansprüchen") überführt werden, welcher anders als bisher § 2 Abs. 3 UKlaG auch für die Ansprüche nach § 1 UKlaG gilt. Der Inhalt der Missbrauchsregelung soll zudem an den der Missbrauchsregelung in § 8 Abs. 4 UWG angepasst werden. Wie in § 8 Abs. 4 Satz 2 UWG soll ein besonderer Anspruch auf Ersatz von Rechtsverfolgungskosten vorgesehen werden. Dieser Anspruch soll jedem zustehen, gegen den rechtsmissbräuchlich nach dem Unterlassungsklagengesetz vorgegangen wird.

Um wirksamen Rechtsschutz gegen datenschutzrechtliche Verstöße gewährleisten zu können, ist zudem vorgesehen, den Anspruch nach § 2 UKlaG um einen Anspruch auf Beseitigung zu ergänzen. Datenschutzverstößen könne allein durch einen Unterlassungsanspruch nicht immer wirksam begegnet werden, so die Entwurfsbegründung. Sofern ein Unternehmer Daten unzulässig gespeichert hat, reiche es nicht aus, dass er das Speichern künftig unterlasse. Er müsse auch verpflichtet werden können, die betreffenden Informationen zu löschen bzw. zu sperren.

Weitere Regelungen des Gesetzentwurfs betreffen die Anpassung der Anspruchsberechtigung der Verbraucherverbände und Kammern nach dem UKlaG und dem Gesetz gegen den unlauteren Wettbewerb (UWG). Auch sollen die Voraussetzungen, die Verbände für die Eintragung in die Liste der qualifizierten Einrichtungen erfüllen müssen (§ 4 Abs. 2 UKlaG), präzisiert werden. Durch Änderung des § 4 Abs. 1 UKlaG soll das Bundesamt für Justiz außerdem gesetzlich verpflichtet werden, die Liste der qualifizierten Einrichtungen auf seiner Internetseite zu veröffentlichen. Damit soll gewährleistet werden, dass auf der Internetseite des Bundesamtes für Justiz immer die aktuelle Liste der qualifizierten Einrichtungen zu finden ist.

Neben dem UKlaG kommt als Rechtsgrundlage für ein Klagerecht der Verbraucherschutzverbände etc. bei Datenschutzverstößen auch das UWG in Betracht (§ 8 Abs. 3). Dies setzt allerdings voraus, dass sich die Datenschutz- zugleich auch als eine Wettbewerbsverletzung darstellt. Nach § 4 Nr. 11 UWG liegt unlauteres Handeln u.a. dann vor, wenn einer gesetzlichen Vorschrift zuwidergehandelt wird, „die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln" (sog. Vorsprung durch Rechtsbruch). Die Rechtsprechung zu der Frage, inwiefern Datenschutzbestimmungen als Marktverhaltensregeln anzusehen sind, ist aber ebenfalls uneinheitlich.

Zusätzlich zu den auf das Verbandsklagerecht bezogenen Änderungen soll schließlich mit dem geplanten Gesetz eine Änderung des AGB-Rechts herbeigeführt werden. § 309 Nr. 13 BGB soll dergestalt geändert werden, dass durch AGB-Bestimmungen künftig keine strengere Form als die Textform (bisher: Schriftform) für Erklärungen und Anzeigen, die gegenüber dem Verwender der AGB oder einem Dritten abzugeben sind, vereinbart werden kann. Auf diese Weise soll sichergestellt werden, dass insbesondere auch die Be-endigung von Verträgen für Verbraucher nicht unnötig erschwert wird und diese immer einfach feststellen können, wie die vereinbarte Form zu erfüllen ist. Klargestellt werden sollen darüber hinaus die sFormanforderungen im Zusammenhang mit Informationspflichten zu Standardgeschäften (§ 675a BGB). Auch hier soll eine Information in Textform ausreichen.

Rechtsprechung

Kosten für eine Auskunft über personenbezogene Daten (Ls)

(**Europäischer Gerichtshof**, Urteil vom 12. Dezember 2013 – C-486/12 –)

1. **Art. 12 lit. A der RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass er einer Erhebung von Kosten für die Mitteilung von personenbezogenen Daten durch eine Behörde nicht entgegensteht.**
2. **Art. 12 lit. A der RL 95/46 ist dahin auszulegen, dass die für die Ausübung des Rechts auf Auskunft über personenbezogenen Daten erhobenen Kosten die Kosten der Mitteilung dieser Daten nicht übersteigen dürfen, um zu gewährleisten, dass sie nicht übermäßig im Sinne dieser Bestimmung sind. Es ist Sache des vorlegenden Gerichts, im Hinblick auf die Umstände des Ausgangsverfahrens die erforderlichen Nachprüfungen vorzunehmen.**

Ausnahmen von der Informationspflicht bei Verarbeitung personenbezogener Daten (Ls)

(**Europäischer Gerichtshof**, Urteil vom 7. November 2013 – C 473/12 – IPI –)

1. **Art. 13 Abs. 1 der RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass die Mitgliedstaaten nicht die Pflicht, wohl aber die Möglichkeit haben, eine oder mehrere der in dieser Bestimmung vorgesehenen Ausnahmen von der Pflicht, die betroffene Person über die Verarbeitung ihrer personenbezogenen Daten zu informieren, in ihr nationales Recht umzusetzen.**
2. **Die Tätigkeit eines Privatdetektives, der für einen Berufsverband handelt, um Verstöße gegen die berufsständischen Regeln eines reglementierten Berufs, im vorliegenden Fall des Berufs des Immobilienmaklers, aufzuspüren, fällt unter die in Art. 13 Abs. 1 lit. D der RL 95/46 vorgesehene Ausnahme.**

Einwilligung in die Abtretung von Zahnarztforderungen

(**Bundesgerichtshof**, Urteil vom 10. Oktober 2013 – II ZR 325/12 –)

Die von einem Zahnarzt formularmäßig verwendete Einverständniserklärung, die vorsieht, dass der Patient der Abtretung der zahnärztlichen Honorarforderung an eine gewerbliche Abrechnungsgesellschaft und gegebenenfalls der weiteren Abtretung an ein Kreditinstitut zum Zwecke der Refinanzierung zustimmt, enthält inhaltlich voneinander trennbare, einzeln aus sich heraus verständliche Regelungen, die Gegenstand einer gesonderten Wirksamkeitsprüfung sein können.

Sachverhalt:

1. Die Klägerin zu 2 (im Folgenden: Klägerin) übernimmt geschäftsmäßig die Erstellung und den Einzug zahnärztlicher Honorarrechnungen. Sie verlangt von der Beklagten aus abgetretenem Recht das Honorar für eine zahnärztliche Behandlung, die der vormalige Kläger zu 1 (im Folgenden: Zedent) durchgeführt hat.

2. Die Beklagte befand sich vom 30. Januar 2004 bis Mai 2005 in zahnärztlicher Behandlung in der Praxis des Zedenten. Dabei wurden unter anderem mehrere Implantate eingesetzt und ein Langzeitprovisorium eingegliedert. Zu Behandlungsbeginn unterzeichnete die Beklagte am 30. Januar 2004 eine von dem Zedenten formularmäßig verwendete „Einverständniserklärung" mit folgendem Inhalt:

„Einwilligung zur Abtretung

- Ich erkläre mich damit einverstanden, dass der umseitig genannte Zahnarzt zum Zweck der Erstellung der Rechnung sowie zur Einziehung und der ggf. gerichtlichen Durchsetzung der Forderung alle hierzu notwendigen Unterlagen, insbesondere meinen Namen, Anschrift, Geburtsdatum, Leistungsziffern, Rechnungsbetrag, Behandlungsdokumentation, Laborrechnungen, Formulare etc. an die ZA Zahnärztliche Abrechnungsgesellschaft D ... (im Folgenden: ZAAG) weitergibt.
- Insoweit entbinde ich den Zahnarzt ausdrücklich von seiner ärztlichen Schweigepflicht und stimme ausdrücklich zu, dass der Zahnarzt die sich aus der Behandlung ergebende Forderung an die ZAAG und diese ggf. an das refinanzierende Institut – D. bank e.G., D. – abtritt.
- Ich bin mir bewusst, dass nach der Abtretung der Honorarforderung mir gegenüber die ZAAG als Forderungsinhaberin auftritt und deshalb Einwände gegen die Forderung – auch soweit sie sich aus der Behandlung und der Krankengeschichte ergeben – im Streitfall gegenüber der ZAAG zu erheben und geltend zu machen sind und der mich behandelnde Zahnarzt als Zeuge vernommen werden kann.

Einwilligung nach Datenschutzgesetz

Ich bin gleichfalls damit einverstanden, dass meine persönlichen Daten und meine Behandlungsdaten von dem Zahnarzt und der ZAAG – ggf. elektronisch – erhoben, gespeichert, verarbeitet, genutzt und übermittelt werden zum Zweck der Erstellung der Honorarrechnung sowie der Einziehung und ggf. gerichtlichen Durchsetzung der Forderung."

Für eine am 17. März 2004 durchgeführte Behandlung stellte der Zedent unter dem 11. Juni 2004 einen Betrag von 10.272,52 € in Rechnung. Die weiteren von ihm erbrachten Behandlungsmaßnahmen machte die Klägerin nach Abtretung der entsprechenden Honorarforderungen mit Rechnung vom 14. Juni 2004 in Höhe von 23.541,41 € geltend. Die Beklagte leistete keine Zahlungen. Im nachfolgenden Rechtsstreit über die Berechtigung der in Rechnung gestellten Honoraransprüche hat die Beklagte erstinstanzlich die Forderungshöhe bestritten und insbesondere eingewandt, über die Gesamtkosten nur unzureichend aufgeklärt worden und bei Abschluss der zugrunde liegenden Vergütungsvereinbarungen geschäftsunfähig gewesen zu sein.

Das Landgericht hat die Beklagte unter teilweiser Klageabweisung zur Zahlung von 9.691,81 € an den Zedenten und von weiteren 21.048,26 € an die Klägerin (jeweils nebst Zinsen und vorgerichtlichen Mahnkosten) verurteilt. Mit ihrer Berufung hat die Beklagte erstmals geltend gemacht, die Abtretung der Honorarforderungen an die Klägerin sei gemäß § 134 BGB in Verbindung § 203 Abs. 1 Nr. 1 StGB nichtig. Das Oberlandesgericht hat die Abtretung der Honoraranspruchs an die Klägerin für unwirksam gehalten und die Klage insoweit abgewiesen. Mit ihrer vom Berufungsgericht zugelassenen Revision erstrebt die Klägerin die Wiederherstellung des landgerichtlichen Urteils.

Aus den Gründen:

Die Revision ist begründet. Sie führt zur Aufhebung des Berufungsurteils und zur Wiederherstellung des erstinstanzlichen Urteils, soweit das Berufungsgericht zum Nachteil der Klägerin erkannt hat.

I.

Das Berufungsgericht hat zur Begründung seiner Entscheidung im Wesentlichen ausgeführt:

Die Klägerin sei für den geltend gemachten Honoraranspruch nicht aktivlegitimiert. Die Abtretung des Honoraranspruchs an die Klägerin sei gemäß § 134 BGB wegen Verstoßes gegen § 203 Abs. 1 StGB nichtig, da die Einverständniserklärung der Beklagten vom 30. Januar 2004 unwirksam sei. Zwar genüge die Zustimmungserklärung bezüglich der Klägerin den Anforderungen an eine wirksame Entbindung von der ärztlichen Schweigepflicht und den datenschutzrechtlichen Vorgaben; dagegen werde die vertraglich vorgesehene Möglichkeit der Weiterabtretung durch die Klägerin an die D. bank e.G. zum Zwecke der Refinanzierung nicht deutlich gemacht. Es werde vielmehr der Anschein erweckt, dass sensible, patientenbezogene Daten lediglich an die Klägerin weitergegeben würden. Eine geltungserhaltende Reduktion beziehungsweise lediglich eine Teilnichtigkeit der Abtretung komme nicht in Betracht. Die Erklärungen hinsichtlich der Abtretung und der Einwilligung stünden in einem rechtlich und inhaltlich untrennbaren Zusammenhang, weshalb der Verstoß gegen § 134 BGB in Verbindung mit § 203 Abs. 1 Nr. 1 StGB zur Unwirksamkeit der in der Urkunde insgesamt enthaltenen Erklärungen nach § 139 BGB führe.

II.

Diese Ausführungen halten rechtlicher Überprüfung nicht stand. Die streitgegenständliche Abtretung der Honorarforderung verstößt nicht gegen § 203 Abs. 1 Nr. 1 StGB, da die Beklagte jedenfalls in die Weitergabe der Abrechnungsunterlagen an die Klägerin wirksam eingewilligt hat. Diese ist somit Inhaberin der Forderung geworden. Darauf, ob (auch) im Verhältnis zur D. bank e.G. eine rechtswirksame Einwilligung vorliegt, kommt es entgegen der Rechtsauffassung des Berufungsgerichts nicht an.

1. Zutreffend und von der Revision nicht beanstandet geht das Berufungsgericht davon aus, dass die Abtretung einer ärztlichen oder zahnärztlichen Honorarforderung an eine gewerbliche Verrechnungsstelle, die zum Zwecke der Rechnungserstellung und Einziehung erfolgt, die ärztliche Schweigepflicht verletzt und deshalb wegen Verstoßes gegen ein gesetzliches Verbot (§ 203 Abs. 1 Nr. 1 StGB) gemäß § 134 BGB nichtig ist, wenn der Patient der damit verbundenen Weitergabe seiner Abrechnungsunterlagen nicht zugestimmt hat (grundlegend BGH, Urteil vom 10. Juli 1991 – VIII ZR 296/90, BGHZ 115, 123, 124 ff). Denn den Zedenten trifft, sofern keine abweichende Vereinbarung getroffen worden ist, nach § 402 BGB die Pflicht, dem neuen Gläubiger die zur Geltendmachung der Forderung nötige Auskunft zu erteilen und ihm die zum Beweis der Forderung dienenden Urkunden, soweit sie sich in seinem Besitz befinden, auszuliefern; dies ist ohne Verstoß gegen die ärztliche Schweigepflicht (§ 203 Abs. 1 Nr. 1 StGB) nicht möglich (st. Rspr., vgl. BGH, Urteile vom 10. Juli 1991 aaO; vom 8. Juli 1993 – IX ZR 12/93, NJW 1993, 2795 f; vom 5. Dezember 1995 – X ZR 121/93, NJW 1996, 775; Beschluss vom 17. Februar 2005 – IX ZB 62/04, NJW 2005, 1505, 1506; Urteile vom 10. Februar 2010 – VIII ZR 53/09, NJW 2010, 2509 Rn. 11; vom 21. Januar 2010 – IX ZR 65/09, BeckRS 2010, 07630 Rn. 11).

Eine wirksame Einwilligung im Sinne von § 203 Abs. 1 Nr. 1 StGB setzt voraus, dass der Erklärende eine im Wesentlichen zutreffende Vorstellung davon hat, worin er einwilligt, und die Bedeutung und Tragweite seiner Entscheidung zu überblicken vermag. Er muss deshalb wissen, aus welchem Anlass und mit welcher Zielsetzung er welche Personen von ihrer Schweigepflicht entbindet; auch muss er über Art und Umfang der Einschaltung Dritter unterrichtet sein (BGH, Urteil vom 20. Mai 1992 – VIII ZR 240/91, NJW 1992, 2348, 2350; MüKoStGB/Cierniak/Pohlit, 2. Aufl., § 203 Rn. 59; Schönke/Schröder/Lenckner/ Eisele, StGB, 28. Aufl., § 203 Rn. 24).

2. Nach diesen Grundsätzen liegt eine wirksame Zustimmung der Beklagten zur Weitergabe der Abrechnungsunterlagen an die Klägerin vor. Denn die von dem Zedenten formularmäßig verwendete und von der Beklagten unterzeichnete Einverständniserklärung vom 30. Januar 2004 informierte umfassend und detailliert über die mit der Abtretung an die Klägerin verbundenen Rechtsfolgen. Für die Beklagte war eindeutig und zweifelsfrei zu erkennen, dass die Klägerin Forderungsinhaberin werden sollte und die Weitergabe der Behandlungsdaten zum Zwecke der Forderungseinziehung und gegebenenfalls zur klageweisen Geltendmachung erfolgte. Die Beklagte wurde weiterhin darauf hingewiesen, dass sie auf Grund der Abtretung in einem späteren Prozess gezwungen sein könnte, gegenüber einem außerhalb des Arzt-Patienten-Verhältnisses stehenden Dritten Einwände gegen die Honorarforderung vorzubringen und dazu unter Umständen Einzelheiten aus der Krankengeschichte und der Behandlung zu offenbaren.

3. Auf die vom Berufungsgericht bejahte Frage, ob die Einverständniserklärung der Beklagten, soweit sie sich auf eine mögliche (jedoch nicht erfolgte) Weiterabtretung an die D. bank e.G. zum Zwecke der Refinanzierung bezieht, wegen Verstoßes gegen das Transparenzgebot unwirksam ist (§ 307 Abs. 1 BGB), kommt es nicht an. Denn die Wirksamkeit der Zustimmung zur Weitergabe der Behandlungsdaten an die Klägerin bleibt davon unberührt.

a) Zutreffend hat das Berufungsgericht die in Form eines Formularvordrucks verwendete Einverständniserklärung als von dem Zedenten gestellte Allgemeine Geschäftsbedingung im Sinne der §§ 305 ff BGB gewertet. Damit beurteilen sich die Rechtsfolgen im Falle der (teilweisen) Unwirksamkeit der Klausel nach § 306 BGB. Abweichend von § 139 BGB, wonach die Teilnichtigkeit eines Rechtsgeschäfts regelmäßig seine Gesamtnichtigkeit zur Folge hat, bleibt der Vertrag nach § 306 Abs. 1 BGB im Übrigen grundsätzlich wirksam, wenn es sich bei den unwirksamen Teilen des Rechtsgeschäfts um AGB-Klauseln handelt.

b) Nach der Rechtsprechung des Bundesgerichtshofs können inhaltlich voneinander trennbare, einzeln aus sich heraus verständliche Regelungen in Allgemeinen Geschäftsbedingungen auch dann Gegenstand einer gesonderten Wirksamkeitsprüfung sein, wenn sie in einem äußeren sprachlichen Zusammenhang mit anderen – unwirksamen – Regelungen stehen. Nur wenn der als wirksam anzusehende Teil im Gesamtgefüge des Vertrags nicht mehr sinnvoll, insbesondere der als unwirksam beanstandete Klauselteil von so einschneidender Bedeutung ist, dass von einer gänzlich neuen, von der bisherigen völlig abweichenden Vertragsgestaltung gesprochen werden muss, ergreift die Unwirksamkeit der Teilklausel die Gesamtklausel (BGH, Urteile vom 10. Oktober 1996 – VII ZR

224/95, NJW 1997, 394, 395 mwN und vom 12. Februar 2009 – VII ZR 39/08, NJW 2009, 1664 Rn. 15). Die inhaltliche Trennbarkeit einer Klausel und damit ihre Zerlegung in einen inhaltlich zulässigen und einen inhaltlich unzulässigen Teil ist immer dann gegeben, wenn der unwirksame Teil der Klausel gestrichen werden kann, ohne dass der Sinn des anderen Teils darunter leidet (sog. bluepenciltest); ob beide Bestimmungen den gleichen Regelungsgegenstand betreffen, ist dabei unerheblich (MüKoBGB/Basedow, 6. Aufl., § 306 Rn. 18; Palandt/Grüneberg, BGB, 72. Aufl., § 306 Rn. 7, jeweils mwN).

c) Nach diesem Maßstab hat die Einwilligung der Beklagten in die Weitergabe der Abrechnungsunterlagen an die Klägerin auch dann Bestand, wenn ihre Zustimmung zur Weiterabtretung an das refinanzierende Kreditinstitut unwirksam sein sollte.

aa) Das Einverständnis im Sinne von § 203 Abs. 1 StGB ist teilbar. Es kann sowohl in persönlicher als auch in zeitlicher und sachlicher Hinsicht beschränkt werden, indem zum Beispiel nur bestimmte Geheimnisse mitgeteilt oder geheimhaltungsbedürftige Umstände nur an bestimmte Personen weitergegeben werden (MüKoStGB/Cierniak/Pohlit aaO Rn. 64; Schönke/Schröder/Lenckner/Eisele aaO Rn. 24d). Eine Beschränkung des Einverständnisses der Beklagten auf die Abtretung an die Klägerin ist deshalb ohne weiteres zulässig.

bb) Die Abtretung an die Klägerin und die etwaige Folgeabtretung an das zum Zwecke der Refinanzierung eingeschaltete Kreditinstitut sind auch nicht untrennbar miteinander verknüpft. Die Abtretung an die zahnärztliche Abrechnungsgesellschaft verliert ihre wirtschaftliche Bedeutung für die Vertragsparteien nicht dadurch, dass eine Weiterabtretung durch den Zessionar ausgeschlossen ist. Die Folgeabtretung zur Kreditsicherung sollte nur „ggf." erfolgen. Es handelte sich nicht um einen „Automatismus". Dementsprechend ist im Streitfall die Abtretung an die D.bank auch unterblieben. Die Klägerin ist nicht gehindert, die abgetretenen Forderungen im eigenen Namen einzuziehen und erforderlichenfalls gerichtlich durchzusetzen. Zu Recht führt die Revision in diesem Zusammenhang an, dass bei der streitgegenständlichen Klausel der Satzteil bezüglich der Folgeabtretung an die finanzierende Bank unproblematisch gestrichen werden kann, ohne dass dadurch der Sinn der verbleibenden Regelung in Frage gestellt wird. Der Fortfall der Möglichkeit zur Weiterabtretung ist nach alledem nicht von so einschneidender Bedeutung, dass von einer gänzlich neuen, von der bisherigen völlig abweichenden Vertragsgestaltung gesprochen werden muss (vgl. auch BGH, Urteile vom 12. Februar 2009 – VII ZR 39/08, NJW 2009, 1664 Rn. 17 ff; vom 16. Juni 2009 – XI ZR 145/08, NJW 2009, 3422 Rn. 32 ff; vom 28. Juli 2011 – VII ZR 207/09, NJW-RR 2011, 1526 Rn. 14, 20).

III.

Das Berufungsurteil ist demnach aufzuheben, soweit zum Nachteil der Klägerin erkannt worden ist (§ 562 Abs. 1 ZPO).

Die Sache ist zur Endentscheidung reif, so dass der Senat die Berufung der Beklagten gegen das landgerichtliche Urteil zurückweisen kann (§ 563 Abs. 3 ZPO).

Positive Kenntnis des Arbeitgebers von der Arbeitnehmerinsolvenz

(**Bundesarbeitsgericht**, Urteil vom 29. Januar 2014 – 6 AZR 642/12 –)

1. Zahlt der Arbeitgeber das Arbeitsentgelt an den im Verbraucherinsolvenzverfahren befindlichen Arbeitnehmer, hat das keine befreiende Wirkung gegenüber dem Insolvenzverwalter, wenn der Arbeitgeber positive Kenntnis von der Eröffnung des Insolvenzverfahrens hatte (§ 82 S. 1 InsO.). Grob fahrlässige Unkenntnis schließt den Gutglaubensschutz nicht aus.

2. Bezüglich der Unkenntnis trifft den Arbeitgeber die Darlegungs- und Beweislast. Dies gilt insbesondere für die organisatorischen Vorkehrungen, die dafür getroffen sind, dass eine Information über die Insolvenzeröffnung verkehrsgerecht an die zuständigen Stellen im Unternehmen weitergegeben wird.

3. Einer juristischen Person ist das Wissen ihrer Arbeitnehmer zuzurechnen, das bei ordnungsgemäßer Organisation in den Fakten festzuhalten, weiterzugeben und abzufragen ist.

(*Nicht amtliche Leitsätze*)

Sachverhalt:

Der klagende Treuhänder verlangt die Zahlung der pfändbaren Arbeitsvergütung des Schuldners T zur Insolvenzmasse. Die Parteien streiten darüber, ob die beklagte Arbeitgeberin des Schuldners die Eröffnung des Verbraucherinsolvenzverfahrens bei der Auszahlung an den Schuldner nicht kannte iSv. § 82 Satz 1 InsO.

Am 6. September 2006 wurde über das Vermögen des Schuldners das Insolvenzverfahren eröffnet und der Kläger zum Treuhänder bestellt. Zwischen dem Schuldner und der Beklagten bestand von August 2007 bis 31. März 2009 ein erstes Arbeitsverhältnis. Der Kläger forderte die beklagte GmbH mit an die Lohnbuchhaltung gerichtetem Schreiben vom 9. Juni 2009 auf, den pfändbaren Teil des Arbeitsentgelts des Schuldners ab sofort ausschließlich an ihn als Treuhänder im Insolvenzverfahren zu leisten. Daraufhin teilte die Beklagte dem Kläger mit, der Schuldner sei bereits seit Ende März 2009 nicht mehr ihr Arbeitnehmer. Ende März 2010 vernichtete die Beklagte die Personalakte des Schuldners. Seit 1. Juli 2010 besteht zwischen dem Schuldner und der Beklagten wieder ein Arbeitsverhältnis. Von Juli 2010 bis Mai 2011 erzielte der Schuldner pfändbares Arbeitseinkommen iHv. insgesamt 4.118,40 Euro netto, das die Beklagte an ihn leistete. Der Kläger forderte die Beklagte unter dem 10. Juni 2011 erneut auf, den pfändbaren Teil des Arbeitsentgelts des Schuldners an ihn zu leisten. Dem kam die Beklagte seit Juni 2011 nach.

3. Der Kläger hat die Auffassung vertreten, für die Frage der positiven Kenntnis von der Insolvenzeröffnung sei nicht auf den Geschäftsführer der beklagten GmbH als natürliche Person abzustellen. Der juristischen Person sei auch die Kenntnis von Arbeitnehmern zuzurechnen, wenn deren Wissen bei ordnungsgemäßer Organisation des Geschäftsbetriebs aktenkundig festzuhalten und vor Vertragsschluss abzufragen gewesen sei. Bei ordnungsgemäßer Betriebsorganisation seien Personalakten mindestens bis zum Ende der dreijährigen Verjährungsfrist für Vergütungsansprüche aufzubewahren. Die Beklagte sei gehalten gewesen zu prüfen, ob das Insolvenzverfahren beendet sei, zumal das online unkompliziert möglich sei.

Aus den Gründen:

A. Die Revision ist unbegründet. Die Vorinstanzen haben der Klage zu Recht stattgegeben.

I. Mit Eröffnung des Insolvenzverfahrens geht die Empfangszuständigkeit für alle Leistungen, die auf zur Insolvenzmasse gehörende Forderungen erbracht werden, auf den Insolvenzverwalter über (§ 80 Abs. 1 InsO). Nach § 82 Satz 1 InsO wird der Leistende jedoch von seiner Schuld befreit, wenn er die Eröffnung des Ver-

fahrens zur Zeit der Leistung an den Schuldner nicht kannte (vgl. BGH 16. Juli 2009 - IX ZR 118/08 - Rn. 7, BGHZ 182, 85). In diesem Fall wird der Leistende in seinem Vertrauen auf die Empfangszuständigkeit seines Gläubigers – des Insolvenzschuldners – geschützt, wenn ihm die Eröffnung des Insolvenzverfahrens unbekannt geblieben ist, solange er den Leistungserfolg noch verhindern kann (vgl. BGH 12. Juli 2012 - IX ZR 210/11 – Rn. 6; 16. Juli 2009 - IX ZR 118/08 - Rn. 9, aaO). Der aus Billigkeitsgründen eingeräumte Gutglaubensschutz ist eine besondere Vergünstigung im Sinn einer Ausnahme. Wird die Leistungshandlung – wie hier – nach der öffentlichen Bekanntmachung der Verfahrenseröffnung iSv. § 9 Abs. 1 InsO vorgenommen, trifft den Leistenden die Darlegungs- und Beweislast dafür, dass er die Eröffnung des Insolvenzverfahrens nicht kannte (vgl. BGH 16. Juli 2009 - IX ZR 118/08 - Rn. 8, 13, aaO). Nur positive Kenntnis von der Eröffnung des Insolvenzverfahrens schließt den Gutglaubensschutz des § 82 Satz 1 InsO aus. Grob fahrlässige Unkenntnis genügt nicht (vgl. BFH 12. Juli 2011 - VII R 69/10 - Rn. 12, BFHE 234, 114; VG Düsseldorf 24. September 2012 - 23 K 7855/11 - zu 2 der Gründe).

II. Die Ansprüche des Klägers auf die der Höhe nach unstreitigen pfändbaren Teile des Arbeitsentgelts für Juli 2010 bis Mai 2011 sind nach diesen Grundsätzen vom Insolvenzbeschlag erfasst. Sie beruhen auf § 611 Abs. 1 BGB iVm. § 35 Abs. 1, § 80 Abs. 1, § 304 Abs. 1 InsO. Die Beklagte konnte die pfändbaren Teile der Arbeitsvergütung für die Monate Juli 2010 bis Mai 2011 von insgesamt 4.118,40 Euro nicht mit schuldbefreiender Wirkung (§ 362 Abs. 1 BGB) an den Schuldner leisten. Ihr kommt der Gutglaubensschutz des § 82 Satz 1 InsO nicht zugute, weil sie wusste, dass über das Vermögen des Schuldners die Verbraucherinsolvenz eröffnet war. Die durch das Schreiben des Klägers vom 9. Juni 2009 vermittelte Kenntnis einer Arbeitnehmerin in der Lohnbuchhaltung von der Insolvenzeröffnung ist der juristischen Person der als GmbH organisierten Beklagten zuzurechnen. Die Beklagte reagierte auch auf das Schreiben des Klägers vom 9. Juni 2009. Ihre Kenntnis dauerte fort, obwohl der Schuldner bei Zugang des Schreibens nicht in einem Arbeitsverhältnis mit ihr stand und seine Personalakte Ende März 2010 vernichtet wurde.

1. Die organisatorische Aufspaltung von Zuständigkeiten der Arbeitnehmer einer juristischen Person und ihrer Organe kann dazu führen, dass der Vertragspartner einer juristischen Person schlechter als der Vertragspartner einer natürlichen Person gestellt ist. Dieser Nachteil wird dadurch ausgeglichen, dass der juristischen Person das Wissen auch der Arbeitnehmer zuzurechnen ist, das bei ordnungsgemäßer Organisation in den Akten festzuhalten, weiterzugeben und abzufragen ist (vgl. BGH 13. Oktober 2000 - V ZR 349/99 - zu II 3 b der Gründe). Jede am Rechtsverkehr teilnehmende Organisation ist verpflichtet, Informationen verkehrsgerecht zu verwalten. Ordnungsgemäß zugegangene Informationen sind innerhalb der Organisation weiterzugeben (vgl. BGH 15. April 2010 - IX ZR 62/09 - Rn. 11). Die einer solchen Organisation ordnungsgemäß zugegangenen rechtserheblichen Informationen müssen von ihren Entscheidungsträgern zur Kenntnis genommen werden können. Die Organisation muss es deswegen so einrichten, dass ihre Repräsentanten, die dazu berufen sind, im Rechtsverkehr bestimmte Aufgaben in eigener Verantwortung wahrzunehmen, die erkennbar erheblichen Informationen tatsächlich an die entscheidenden Personen weiterleiten. Erkenntnisse, die von einzelnen Arbeitnehmern gewonnen werden, aber auch für andere Arbeitnehmer oder Entscheidungsträger und spätere Geschäftsvorgänge erheblich sind, müssen die erforderliche Breitenwirkung erzielen. Dazu kann ein Informationsfluss von unten nach oben notwendig sein. Die Organisation hat entsprechende organisatorische Maßnahmen zu treffen. Jedenfalls dann, wenn derartige organisatorische Maßnahmen fehlen, muss sich die juristische Person das Wissen einzelner Arbeitnehmer unabhängig davon zurechnen lassen, auf welcher Ebene sie angesiedelt sind. Die juristische Person hat darzulegen, welche Organisationsstrukturen sie geschaffen hat, um rechtserhebliche Informationen aufzunehmen und intern weiterzugeben (vgl. BGH 15. Dezember 2005 - IX ZR 227/04 - Rn. 13 f.; s. auch OLG Hamm 25. November 2009 - 31 U 15/04, I-31 U 15/04 - zu B 4.5 der Gründe).

2. Nach diesen Grundsätzen ist das im Juni 2009 erlangte Wissen der Arbeitnehmerin in der Lohnbuchhaltung um die Insolvenz des Schuldners der Beklagten zuzurechnen. Die Beklagte kannte die Insolvenzeröffnung iSv. § 82 Satz 1 InsO, als sie die Vergütungen für Juli 2010 bis Mai 2011 an den Schuldner leistete.

a) Die Beklagte hat bereits nicht vorgetragen, welche Organisationsstrukturen bei ihr bestehen, um den ordnungsgemäßen Informationsfluss sicherzustellen. Sie hat lediglich ausgeführt, der Umstand der Insolvenzeröffnung sei nicht in der damals noch vorhandenen Personalakte festgehalten worden. Die Information wurde nach ihrem Vorbringen auch nicht an die im Unternehmen zuständigen Entscheidungsträger weitergeleitet. An diesen Versäumnissen wird deutlich, dass die Information nicht verkehrsgerecht verwaltet wurde. Das Wissen der Arbeitnehmerin in der Lohnbuchhaltung ist der Beklagten deshalb zuzurechnen. Die Beklagte wusste damit um die Insolvenzeröffnung. Das schließt den nur ausnahmsweise gegebenen Gutglaubensschutz des § 82 Satz 1 InsO aus.

b) Dem steht nicht entgegen, dass der Schuldner bei Zugang des Schreibens vom 9. Juni 2009 seit etwas mehr als zwei Monaten nicht mehr für die Beklagte arbeitete und die Beklagte seine Personalakte Ende März 2010 vernichtete.

aa) Die Beklagte war trotz des beendeten Arbeitsverhältnisses gehalten, die Information der Insolvenzeröffnung ordnungsgemäß zu verwalten. Zu dem innerhalb der dreijährigen Verjährungsfrist des § 195 BGB gelegenen Zeitpunkt der erlangten Kenntnis im Juni 2009 war nicht auszuschließen, dass der Schuldner noch Ansprüche aus dem ersten Arbeitsverhältnis gegen sie erheben und durchsetzen würde. Für diese zusätzlichen Beträge wären Steuern und Sozialversicherungsbeiträge abzuführen gewesen. Die Beklagte konnte im Juni 2009 auch nicht sicher davon ausgehen, dass es nicht zu Prüfungen der Finanzverwaltung oder der Sozialversicherungsträger kommen würde, die den Zeitraum des ersten Arbeitsverhältnisses zwischen ihr und dem Schuldner umfassten.

bb) Die Kenntnis der Beklagten endete auch nicht, bevor sie das Entgelt für Juli 2010 bis Mai 2011 an den Schuldner leistete.

(1) Vergisst der Dritte die Insolvenzeröffnung, ist das unerheblich (vgl. Niedersächsisches FG 29. September 2010 - 2 K 222/08 - zu 3 b aa der Gründe). Die einmal erlangte positive Kenntnis über die Eröffnung des Insolvenzverfahrens dauert fort, solange der Dritte nicht zuverlässig davon erfährt, dass das Insolvenzverfahren abgeschlossen ist (vgl. LG Dresden 2. November 2007 - 10 O 929/07 - zu I 2 der Gründe). Dafür ist der Dritte wegen des Ausnahmecharakters des § 82 Satz 1 InsO ebenso darlegungsbelastet wie für die organisatorischen Vorkehrungen, die er dafür getroffen hat, dass die Information über die Insolvenzeröffnung verkehrsgerecht an die zuständigen Entscheidungsträger im Unternehmen weitergegeben wird. Der Dritte muss damit rechnen, dass ein Insolvenzverfahren geraume Zeit dauert. Der Abschluss des Verfahrens ist ohne weiteres durch eine Internetrecherche festzustellen (vgl. BGH 15. April 2010 - IX ZR 62/09 - Rn. 14). Zu entsprechenden Bemühungen ist der Dritte schon im eigenen Interesse gehalten, weil er nach erlangter Kenntnis iSv. § 82 Satz 1 InsO nur nach Abschluss des Insolvenzverfahrens schuldbefreiend an den frühe-

ren Schuldner leisten kann (vgl. LG Dresden 2. November 2007 - 10 O 929/07 - aaO).

(2) Die Beklagte hat sich hier - aus ihrer Sicht konsequent - nicht darauf berufen, dass sie den Abschluss des Insolvenzverfahrens festgestellt habe. Sie nimmt vielmehr in einem logisch früheren Schritt an, die im Juni 2009 erlangte Kenntnis der Arbeitnehmerin in der Lohnbuchhaltung sei ihr nicht zuzurechnen. Das ist, wie schon dargelegt, unzutreffend.

Kein Anspruch des Personalrats auf personenbezogene Informationen der elektronischen Arbeitszeiterfassung

(**Bundesverwaltungsgericht**, Beschluss vom 19. März 2014 – 6 P 1.13)

Der Personalrat kann nicht verlangen, dass ihm die in der elektronischen Arbeitszeiterfassung gespeicherten Daten unter Namensnennung der Beschäftigten zur Verfügung gestellt werden; seine Überwachungsaufgabe kann er bereits effektiv wahrnehmen, wenn er zunächst nur die anonymisierten Arbeitszeitlisten der Dienststelle erhält.

Sachverhalt:

1. In der Agentur für Arbeit Duisburg findet elektronische Arbeitszeiterfassung statt. Dazu gilt die Dienstvereinbarung über Beginn und Ende der Arbeitszeit und der Pausen für die Mitarbeiterinnen und Mitarbeiter der Agentur für Arbeit Duisburg sowie zur elektronischen Zeiterfassung vom 18. Oktober 2006. Der Beteiligte gewährte den freigestellten Mitgliedern des Antragstellers lesenden Zugriff auf die erfassten Arbeitszeitdaten. Diese Berechtigung entzog der Beteiligte dem Antragsteller unter dem 8. März 2010 unter Hinweis auf datenschutzrechtliche Bestimmungen. Er erklärte sich lediglich bereit, dem Antragsteller halbjährlich anonymisierte Listen mit für die Beschäftigen festen Kennziffern teamscharf zur Verfügung zu stellen.

Das auf weitere Gewährung des lesenden Zugriffs gerichtete Begehren des Antragstellers hat das Verwaltungsgericht abgelehnt. Die Beschwerde des Antragstellers hat das Oberverwaltungsgericht aus folgenden Gründen zurückgewiesen: Der Überwachungsaufgabe des Antragstellers könne bereits durch die periodische Vorlage von Listen über den Stand der Arbeitszeitkonten der einzelnen Beschäftigten entsprochen werden, in denen diese mit Kennziffern bezeichnet seien. Derartige Listen ermöglichten eine beschäftigtenscharfe und zugleich periodenübergreifende Langzeitkontrolle etwaiger arbeitszeitrechtlicher Verstöße bzw. Unregelmäßigkeiten. Auch bei Anonymisierung sei der Antragsteller in der Lage, Maßnahmen zu ergreifen, die auf ein Abstellen der Verstöße zielten. Zudem stehe dem Antragsteller offen, bei einem entsprechenden Erfordernis durch eine gezielte Nachfrage beim Beteiligten den jeweiligen Namen des Beschäftigten in Erfahrung zu bringen. Aus diesem Grunde habe der Antragsteller auch nicht – wie zweitinstanzlich hilfsweise begehrt – Anspruch darauf, dass der Beteiligte ihm jeweils bis zum 15. des Folgemonats für jeden Beschäftigten unter Namensnennung Auskunft über Beginn und Ende der täglichen Arbeitszeit an jedem Arbeitstag des Vormonats einschließlich der Pausen erteile.

Der Antragsteller trägt zur Begründung seiner vom Senat zugelassenen Rechtsbeschwerde vor: Es genüge nicht, dem Personalrat anonymisierte Listen zu überlassen, da lediglich bei Kenntnis der jeweiligen Namen ein effektiver Einsatz für die Beschäftigten möglich sei. Nur dann könne sich der Personalrat durch Rückfrage bei den betroffenen Mitarbeitern vergewissern, ob die einschlägigen Vorschriften eingehalten seien. Eine effektive Überwachung der Vorgaben des Arbeitszeitgesetzes und der Dienstvereinbarung setze die konkrete, kurzfristig zu verschaffende Kenntnis der Arbeitszeitdaten und der Namen der Beschäftigten voraus. Datenschutzgesichtspunkte kämen im Verhältnis zwischen Dienststelle und Personalrat nicht zum Zuge.

Aus den Gründen:

Die zulässige Rechtsbeschwerde des Antragstellers ist nicht begründet. Der Beschluss des Oberverwaltungsgerichts beruht nicht auf der Nichtanwendung oder der unrichtigen Anwendung einer Rechtsnorm (§ 83 Abs. 2 BPersVG i.V.m. § 93 Abs. 1 Satz 1 ArbGG). Der Antragsteller ist weder berechtigt, lesenden Zugriff auf die in der Zeiterfassung gespeicherten Daten der Beschäftigten zu nehmen (Hauptantrag), noch kann er verlangen, ihm monatlich für jeden Beschäftigten unter Namensnennung Auskunft über Beginn und Ende der täglichen Arbeitszeit zu erteilen (Hilfsantrag).

1. Rechtsgrundlage für das streitige, mit Haupt- und Hilfsantrag verfolgte Begehren ist § 68 Abs. 2 Satz 1 und 2 BPersVG. Danach ist der Personalrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten (Satz 1). Ihm sind die hierfür erforderlichen Unterlagen vorzulegen (Satz 2). Die Pflicht des Dienststellenleiters zur Vorlage von Unterlagen ist somit Bestandteil seiner Informationspflicht gegenüber dem Personalrat. Sie besteht nur in dem Umfang, in welchem der Personalrat zur Durchführung seiner Aufgaben die Kenntnis der Unterlagen benötigt (vgl. Beschlüsse vom 23. Juni 2010 – BVerwG 6 P 8.09 – BVerwGE 137, 148 = Buchholz 251.2 § 73 BlnPersVG Nr. 1 Rn. 13 und vom 4. September 2012 – BVerwG 6 P 5.11 – BVerwGE 144, 156 = Buchholz 251.7 § 65 NWPersVG Nr. 3 Rn. 9). Der Verpflichtung des Dienststellenleiters korrespondiert ein entsprechender Anspruch des Personalrats. Der Informationsanspruch als solcher wie auch der darauf bezogene Anspruch auf Vorlage von Unterlagen sind strikt aufgabengebunden und in ihrer Reichweite durch das Erforderlichkeitsprinzip begrenzt (vgl. Beschlüsse vom 24. Februar 2006 – BVerwG 6 P 4.05 – Buchholz 251.91 § 77 SächsPersVG Nr. 1 Rn. 17 und vom 4. September 2012 a.a.O. Rn. 27 f.; zum Betriebsverfassungsrecht: BAG, Beschlüsse vom 6. Mai 2003 – 1 ABR 13/02 – BAGE 106, 111 <118>, vom 30. September 2008 – 1 ABR 54/07 – BAGE 128, 92 Rn. 28 sowie vom 7. Februar 2012 – 1 ABR 46/10 – BAGE 140, 350 Rn. 7).

a) Maßgebliche Aufgabe, auf welche der Antragsteller sein Informationsbegehren stützen kann, ist diejenige nach § 68 Abs. 1 Nr. 2 BPersVG. Danach hat der Personalrat darüber zu wachen, dass die zu Gunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge und Dienstvereinbarungen durchgeführt werden. Die Wahrnehmung der Überwachungsaufgabe ist von der Darlegung eines besonderen Anlasses, namentlich einer zu besorgenden Rechtsverletzung unabhängig. Eine Überwachung verlangt ein von einem bestimmten Anlass gerade unabhängiges, vorbeugendes Tätigwerden. Dementsprechend soll der Personalrat in die Lage versetzt werden, etwaigen Rechtsverstößen bereits im Vorfeld effektiv entgegenwirken zu können (vgl. Beschlüsse vom 16. Februar 2010 – BVerwG 6 P 5.09 – Buchholz 251.0 § 68 BaWüPersVG Nr. 4 Rn. 23, vom 23. Juni 2010 a.a.O. Rn. 44 sowie vom 4. September 2012 a.a.O. Rn. 18; ebenso zum Betriebsverfassungsrecht: BAG, Beschlüsse vom 13. Februar 2007 – 1 ABR 14/06 – BAGE 121, 139 Rn. 23, vom 19. Februar 2008 – 1 ABR 84/06 – AP Nr. 69 zu § 80 BetrVG 1972 Rn. 25 sowie vom 7. Februar 2012 a.a.O. Rn. 7).

b) Die verschiedenen Varianten der Auskunftserteilung beurteilen sich nach dem Maßstab der Erforderlichkeit, welcher in § 68 Abs. 2 Satz 1 und 2 BPersVG vorgegeben ist. Danach entscheidet sich, ob nach § 68 Abs. 2 Satz 1 BPersVG mündlich oder schriftlich

zu unterrichten ist. Bei umfangreichen und komplexen Angaben ist die Dienststelle regelmäßig gehalten, die Auskunft schriftlich zu erteilen (vgl. BAG, Beschlüsse vom 30. September 2008 a.a.O. Rn. 29 sowie vom 7. Februar 2012 a.a.O. Rn. 14). Die Pflicht zur Vorlage von Unterlagen nach § 68 Abs. 2 Satz 2 BPersVG, welche auf die bei der Dienststelle vorhandenen Unterlagen begrenzt ist (vgl. BAG, Beschlüsse vom 6. Mai 2003 a.a.O. S. 120 f. sowie vom 30. September 2008 a.a.O. Rn. 30), reicht von der Einblickgewährung bis zur zeitweisen oder dauerhaften Überlassung (vgl. Beschluss vom 23. Januar 2002 – BVerwG 6 P 5.01 – Buchholz 250 § 68 BPersVG Nr. 17 S. 1 ff.). Nach dem Erforderlichkeitsprinzip bestimmt sich ferner, ob Auskünfte fortlaufend oder in größeren Abständen zu erteilen sind.

Schließlich kommt dem Maßstab der Erforderlichkeit besondere Bedeutung zu, wenn es um die Frage geht, ob Auskünfte unter Namensnennung der betroffenen Beschäftigten oder anonym zu erteilen sind. Da Informationen unter Namensnennung stets mit einem Eingriff in das Persönlichkeitsrecht der betroffenen Beschäftigten verbunden sind, ist anonymisiert zu unterrichten, wenn dies für eine effiziente Wahrnehmung der Überwachungsaufgabe durch den Personalrat ausreicht (vgl. in diesem Zusammenhang: Beschlüsse vom 16. Februar 2010 a.a.O. Rn. 12 ff. und 18 ff., vom 23. Juni 2010 a.a.O. Rn. 43 und vom 4. September 2012 a.a.O. Rn. 14 ff.; BAG, Beschluss vom 7. Februar 2012 a.a.O. Rn. 12). Gibt die anonymisierte Information dem Personalrat bereits Aufschluss darüber, dass die Dienststelle die im fraglichen Sachzusammenhang in Betracht zu ziehenden Regelwerke durchweg einhält, so beschränkt sich eine ergänzende Unterrichtung unter Namensnennung der betroffenen Beschäftigten auf diejenigen Einzelfälle, in denen ausnahmsweise eine Rechtsverletzung zu besorgen ist. Ein derartiges zweistufiges Verfahren reduziert die Zahl der personenbezogenen Daten erheblich, ohne dass die effiziente Kontrolle des Personalrats Schaden nimmt.

2. Im vorliegenden Fall bezieht sich die Überwachungsaufgabe des Antragstellers auf die Einhaltung der arbeitszeitrechtlichen Bestimmungen bei der elektronischen Arbeitszeiterfassung in der Agentur für Arbeit Duisburg.

Die in den maßgebenden Regelwerken enthaltenen arbeitszeitrechtlichen Bestimmungen sind normative Regelungen zu Gunsten der Beschäftigten, auf welche sich die Überwachungsaufgabe des Antragstellers nach § 68 Abs. 1 Nr. 2 BPersVG bezieht. Sie dienen durchweg der Sicherheit und dem Gesundheitsschutz der Beschäftigten (vgl. Art. 1 Abs. 1 der Richtlinie 2003/88/EG und § 1 Nr. 1 ArbZG). Auch die Festlegung der regelmäßigen Arbeitszeit auf 39 Stunden wöchentlich in § 6 Abs. 1 Satz 1 TV-BA wirkt zu Gunsten der Arbeitnehmer. Damit wird die Arbeitsleistung begrenzt, welche der Arbeitnehmer erbringen muss, um dass Festgehalt nach § 17 TV-BA zu erzielen (vgl. Breier/Dassau/Kiefer/Lang/Langenbrinck, TVöD, § 6 Rn. 4 und 27; Fieberg, in: GKÖD Bd. IV, E § 6 Rn. 9). Wie die folgenden Ausführungen zeigen, reichen die beim Beteiligten geführten Arbeitszeitlisten bereits in ihrer anonymisierten Fassung aus, um dem Antragsteller Aufschluss über etwaige Rechtsverstöße zu vermitteln:

a) Dies gilt zunächst für die Tageshöchstarbeitszeit. Diese beläuft sich in der Agentur für Arbeit Duisburg auf zehn Stunden, und zwar sowohl für Arbeitnehmer und Auszubildende (Nr. 3.1 Abs. 3 DV i.V.m. § 2 Abs. 2, § 3 Satz 2 ArbZG) als auch für Beamte (Nr. 3.1 Abs. 4 DV i.V.m. § 4 Satz 2 AZV). Hinsichtlich der jugendlichen Beschäftigten sind die strengeren Regelungen des Jugendarbeitsschutzgesetzes zu beachten (Nr. 2.1.2 DV i.V.m. § 8 Abs. 1 bis 2a, § 21a Abs. 1 Nr. 1 JArbSchG). Der Antragsteller kann bereits anhand der anonymisierten Arbeitszeitlisten ersehen, ob die Tageshöchstarbeitszeit eingehalten wird.

Soll von der Ausnahmeregelung in § 14 ArbZG Gebrauch gemacht werden, so ist die Angelegenheit vorab dem Antragsteller zur Mitbestimmung vorzulegen (Nr. 3.1 Abs. 5 DV). Über die Identität der betroffenen Mitarbeiter ist der Antragsteller daher ohnehin unterrichtet. Dies muss ebenso für Beamte gelten, denen in besonderen Ausnahmefällen eine tägliche Arbeitszeit von mehr als zehn Stunden abverlangt wird (Nr. 3.1 Abs. 4 Satz 2 DV). Ergibt sich in sonstigen Fällen aus den Arbeitszeitlisten eine Abweichung von der Tageshöchstarbeitszeit von zehn Stunden, so kann der Antragsteller vom Beteiligten nähere Erläuterungen verlangen. Ist eine Abklärung auf andere Weise nicht möglich, ist die Identität des betroffenen Beschäftigten offenzulegen, auch damit der Antragsteller bei diesem Rückfrage nehmen kann (vgl. Beschluss vom 4. September 2012 a.a.O. Rn. 15; BAG, Beschluss vom 7. Februar 2012 a.a.O. Rn. 12).

b) Die Überwachungsaufgabe des Antragstellers erstreckt sich ferner auf die Ruhepausen, welche selbst nicht zur Arbeitszeit zählen (§ 2 Abs. 1 Satz 1 Halbs. 1 ArbZG, § 5 Abs. 1 AZV, § 6 Abs. 1 Satz 1 TV-BA). Für die Arbeitnehmer bestimmt § 4 Satz 1 ArbZG, dass die Arbeit durch im Voraus feststehende Ruhepausen von mindestens 30 Minuten bei einer Arbeitszeit von mehr als sechs bis zu neun Stunden und 45 Minuten bei einer Arbeitszeit von mehr als neun Stunden insgesamt zu unterbrechen ist. Für die Beamten trifft § 5 Abs. 2 AZV eine vergleichbare Regelung.

Nr. 3.8 Abs. 2 DV bestätigt, dass die Regelungen zur Ruhepause im Arbeitszeitgesetz für die Agentur für Arbeit Duisburg verbindlich sind. Nr. 4.5 Abs. 2 DV trifft Regelungen zum pauschalen Abzug der gesetzlichen Pausenzeit von der Zeit der Anwesenheit in der Dienststelle. Der Pauschalabzug wirkt auf die tatsächliche Einhaltung der genannten gesetzlichen Regelungen hin. Er vereinfacht das Abrechnungsverfahren auf Seiten der Dienststelle und enthält zugleich einen Vertrauensvorschuss für die Beschäftigten. Zu deren Gunsten wird angenommen, dass sie Pausenzeiten anzeigen, welche von dem Pauschalabzug nicht gedeckt sind. Es entsprach dem ausdrücklichen Willen des Antragstellers als eines der beiden Partner der Dienstvereinbarung, eine solche Regelung vorzusehen, welche die Selbstverantwortung der Beschäftigten betont. Dies hat freilich zur Konsequenz, dass die tatsächlichen Pausenzeiten verschwinden; der Beteiligte kann dem Antragsteller darüber keine Auskunft geben. Die Überwachungsaufgabe des Antragstellers verlagert sich demnach darauf, ob der Pausenabzug im Einklang mit den Bestimmungen der Dienstvereinbarung und des Arbeitszeitgesetzes vorgenommen wurde. Dies kann der Antragsteller leisten, weil aus den Arbeitszeitlisten die Anwesenheitszeit und die angerechnete Arbeitszeit zu ersehen ist.

Gemäß § 11 Abs. 1 Satz 2 JArbSchG gelten für Jugendliche strengere Pausenregelungen. Da in der Agentur für Arbeit Duisburg Jugendliche an der flexiblen Arbeitszeit teilnehmen (Nr. 2.1.2 DV), ist die Regelung in Nr. 4.5 Abs. 2 DV in ihrem Fall unter Beachtung der strengeren gesetzlichen Pausenregelungen analog anzuwenden. Ob dies korrekt geschieht, kann der Antragsteller anhand der Arbeitszeitlisten überprüfen.

c) Zur Überwachungsaufgabe des Antragstellers gehört weiterhin die Einhaltung der Ruhezeit. § 5 Abs. 1 ArbZG bestimmt, dass die Arbeitnehmer nach Beendigung der täglichen Arbeitszeit eine ununterbrochene Ruhezeit von mindestens elf Stunden haben müssen. Eine vergleichbare Regelung für die Beamten trifft § 5 Abs. 3 Satz 1 AZV. § 13 JArbSchG bestimmt, dass nach Beendigung der täglichen Arbeitszeit Jugendliche nicht vor Ablauf einer ununterbrochenen Freizeit von mindestens zwölf Stunden beschäftigt werden dürfen. Über die Einhaltung der vorbezeichneten Schutzbestimmungen geben die anonymisierten Listen dem Antragsteller ebenfalls Aufschluss.

d) Schließlich bezieht sich die Überwachungsaufgabe des Antragstellers auf die Wochenarbeitszeit.

§ 6 Abs. 1 Satz 1 TV-BA bestimmt, dass die regelmäßige Arbeitszeit der Arbeitnehmer ausschließlich der Pausen durchschnittlich 39 Stunden wöchentlich beträgt. Gemäß § 6 Abs. 2 Satz 1 TV-BA ist für die Berechnung des Durchschnitts der regelmäßigen wöchentlichen Arbeitszeit ein Zeitraum von bis zu einem Jahr zu Grunde zu legen. Diese Regelungen gelten nach Maßgabe von § 6 Abs. 1 TVN-BA auch für Auszubildende.

Für die Beamten schreibt § 87 Abs. 1 BBG vor, dass die regelmäßige Arbeitszeit wöchentlich im Durchschnitt 44 Stunden nicht überschreiten darf. Diesen gesetzlichen Rahmen schöpft § 3 Abs. 1 Satz 1 AZV nicht aus, indem dort die regelmäßige wöchentliche Arbeitszeit auf 41 Stunden festgelegt wird. Der Bezugszeitraum beträgt gemäß § 2 Nr. 1 AZV zwölf Monate. Für den Fall der Gleitzeit bestimmt § 2 Nr. 8 AZV das Kalenderjahr oder einen ähnlich bestimmten Zeitraum von zwölf Monaten zum Abrechnungszeitraum, in welchem ein Überschreiten der regelmäßigen wöchentlichen Arbeitszeit auszugleichen ist (vgl. ferner § 7 Abs. 4 Satz 2 AZV).

Im Einklang mit den zitierten tarifvertraglichen und beamtenrechtlichen Bestimmungen regelt Nr. 3.6 Satz 1 DV, dass Über- oder Unterschreitungen der regelmäßigen wöchentlichen Arbeitszeit innerhalb eines Abrechnungszeitraums (1. Juli bis 30. Juni des Folgejahres) auszugleichen sind. In dieser Hinsicht besteht die Überwachungsaufgabe des Antragstellers in der Überprüfung, ob die Arbeitszeit der Beschäftigten korrekt erfasst worden ist. Er hat darauf zu achten, dass alle als Arbeitszeit zu wertenden Zeiten den Beschäftigten tatsächlich gutgeschrieben werden. Mit der Wahrnehmung der Überwachungsaufgabe soll der Antragsteller zu verhindern helfen, dass Beschäftigte ihren Anspruch auf Freizeitausgleich verlieren oder zu Unrecht Arbeit im Folgezeitraum nachleisten müssen.

Als Arbeitszeit versteht Nr. 3.4 Satz 1 DV die Zeit der Arbeitsleistung in der Dienststelle und die Zeit der dienstlichen Inanspruchnahme bei Dienstreisen. Der Antragsteller hat darauf zu achten, dass Dienstreisen im Einklang mit Nr. 3.4.1 bis 3.4.3 DV i.V.m. § 11 TV-BA und § 11 AZV angerechnet, dass Ausfallzeiten insbesondere wegen Urlaub und Krankheit zutreffend gutgeschrieben (Nr. 3.5 DV), dass Gleittage zum Ausgleich von Arbeitszeitüberschreitungen in zutreffendem Umfang vom Saldo abgezogen (Nr. 3.7 DV), dass Pausen im Einklang mit dem bereits erwähnten Modell nach Nr. 3.8 und 4.5 Abs. 2 DV bei der Anrechnung der Arbeitszeit berücksichtigt und dass Unterrichtszeiten korrekt auf die Ausbildungszeit angerechnet werden (Nr. 3.5 Satz 2 DV i.V.m. § 18 Abs. 2 TVN-BA und § 9 Abs. 2 JArbSchG). Allerdings gilt der Grundsatz der Selbstverantwortung. Die Beschäftigten geben nicht nur selbst Arbeitsbeginn und -ende in das System ein, sie nehmen auch die Buchungen wegen Urlaub, Gleittagen und Dienstreisen selbst vor. Sie haben über ihren Bildschirmarbeitsplatz Zugang zum eigenen Arbeitszeitkonto, in welchem sie Korrekturen vornehmen können (Nr. 4.4 Abs. 3 Satz 1, Nr. 4.6.1 und 4.6.3 DV; vgl. für Jugendliche ferner Nr. 2.1.2 DV). Lediglich Buchungen wegen Erkrankung, Sonderurlaub oder anderer Sonderfälle sind Aufgabe des Teams Personal (Nr. 4.6.1 Satz 4 und 4.6.2 DV). Auch in dieser Hinsicht genügt zur effektiven Wahrnehmung der Überwachungsaufgabe die Vorlage anonymisierter Fassungen der Arbeitszeitlisten. Es ergibt für den Antragsteller keinen Sinn, bei den jeweiligen Beschäftigten nachzufragen, ob dieser selbst seine Arbeitszeit richtig eingegeben hat. Die Überprüfung des Antragstellers konzentriert sich auf diejenigen Fallgestaltungen, in welchen die arbeitszeitrechtliche Bewertung normativ vorgegeben ist (Dienstreisen, Ausfallzeiten, Gleittage, Pausen). Ob in dieser Hinsicht die maßgeblichen Regelwerke eingehalten sind, vermag der Antragsteller ohne Namensnennung anhand der Arbeitszeitlisten nachzuvollziehen. Dessen ungeachtet ist er berechtigt, bei Unstimmigkeiten bei der Dienststelle nachzufragen und notfalls Namensmitteilung zu verlangen, wenn auf andere Weise der rechtserhebliche Sachverhalt nicht geklärt werden kann.

e) Nach Nr. 3.6 Satz 2 DV dürfen in den Fällen, in denen bei Überschreitung der regelmäßigen wöchentlichen Arbeitszeit der Ausgleich bis zum Ende des Abrechnungszeitraums nicht möglich ist, bis zu 40 Plusstunden in den folgenden Abrechnungszeitraum übertragen werden (vgl. für Beamte ferner § 7 Abs. 4 Satz 3 AZV). In diesem Zusammenhang regelt Nr. 4.7 Abs. 2 Satz 2 DV, dass Beschäftigte, die am 1. März die Grenze von plus 40 Stunden überschritten haben, über die Teamleitung schriftlich benachrichtigt werden. Der Sinn und Zweck dieser Regelung ergibt sich mit Blick auf Nr. 4.5 Abs. 1 Satz 2 DV. Danach ist bei einer Überschreitung der im Abrechnungszeitraum festgelegten 40 Stunden das Zeitguthaben auf diese Grenze zu beschränken. Im Klartext bedeutet dies: Am Ende des Abrechnungszeitraums verfällt das Arbeitszeitguthaben, soweit es über 40 Stunden hinausgeht. In diesem Umfang erhält der betroffene Beschäftigte für tatsächlich geleistete Arbeitsstunden weder ein Entgelt noch einen Freizeitausgleich. Daraus ergibt sich unter Fürsorgegesichtspunkten die Mitteilungspflicht nach Nr. 4.7 Abs. 2 Satz 1 DV. Es handelt sich dabei somit um eine Regelung zugunsten der Beschäftigten. Deren Einhaltung hat der Antragsteller zu überwachen.

Daraus folgt freilich nicht, dass er die Arbeitszeitlisten mit den Namen der Beschäftigten jedenfalls für den Monat Februar erhalten müsste. Eine Überschreitung der maßgeblichen 40-Stunden-Grenze ist aus den anonymisierten Listen zu ersehen. Eine Namensnennung ist nur in den Fällen der Grenzüberschreitung erforderlich. In diesen Fällen muss der Antragsteller sich durch Nachfrage bei den betroffenen Beschäftigten vergewissern können, ob diese die Mitteilung tatsächlich erhalten haben (vgl. Beschluss vom 4. September 2012 a.a.O. Rn. 15; BAG, Beschluss vom 7. Februar 2012 a.a.O. Rn. 12).

Diese Grundsätze gelten auch für Teilzeitbeschäftigte. Für diese schreiben Nr. 3.6 Satz 2 und Nr. 4.5 Abs. 1 Satz 2 DV allerdings vor, dass die übertragbare Arbeitszeitmenge von 40 Stunden entsprechend dem Anteil an der regelmäßigen wöchentlichen Arbeitszeit reduziert wird. Doch braucht deswegen der Grundsatz der Anonymisierung nicht durchbrochen zu werden. Der Antragsteller kann aus den Arbeitszeitlisten das Maß der Teilzeitbeschäftigung erkennen. Da die Wochenarbeitszeit bei Arbeitnehmern (39 Stunden) und bei Beamten (41 Stunden) unterschiedlich ist, fällt die übertragbare Arbeitszeitmenge bei gleicher Wochenstundenzahl in beiden Gruppen ebenfalls unterschiedlich aus. Aus den dem Antragsteller vorzulegenden Arbeitszeitlisten muss daher erkennbar sein, ob es sich bei den Teilzeitbeschäftigten um Arbeitnehmer oder Beamte handelt.

f) Im Zusammenhang mit der flexiblen Arbeitszeit als solcher bezieht sich die Überwachungsaufgabe des Antragstellers für gewöhnlich nicht auf Überstunden.

Gemäß § 7 Abs. 8 TV-BA sind Überstunden die auf Anordnung des Dienststellenleiters geleisteten Arbeitsstunden, die über die im Rahmen der regelmäßigen Arbeitszeit von Vollbeschäftigten gemäß § 6 Abs. 1 Satz 1 TV-BA für die Woche dienstplanmäßig festgesetzten Arbeitsstunden hinausgehen und nicht bis zum Ende der folgenden Kalenderwoche ausgeglichen werden. Arbeitsstunden, die innerhalb des Gleitzeitrahmens (vgl. Nr. 3.1 und Nr. 3.2 DV) geleistet werden, sind dienstplanmäßig und deswegen keine Überstunden. Wächst daher im Rahmen der Gleitzeitregelung ein Zeitguthaben an, so handelt es sich generell auch dann nicht um

angeordnete oder gebilligte Überstunden, wenn das Guthaben nicht bis zum Ende der folgenden Kalenderwoche ausgeglichen wird (vgl. Breier u.a., § 6 Rn. 153, § 7 Rn. 81; Clemens/Scheuring/Steingen/Wiese, TVöD, § 6 Rn. 204; Fieberg, a.a.O. E § 6 Rn. 39). Arbeitsstunden innerhalb des Gleitzeitrahmens können nur Überstunden sein, wenn sie als solche ausdrücklich angeordnet werden. Erfährt der Antragsteller aus der vorgelegten Arbeitszeitliste, dass Arbeit außerhalb des Gleitzeitrahmens geleistet wurde, ist er berechtigt, darüber unter Nennung des betroffenen Beschäftigten näher unterrichtet zu werden. Die Anordnung von Überstunden ist nämlich grundsätzlich mitbestimmungspflichtig (vgl. für den Geschäftsbereich der Bundesagentur für Arbeit: Beschluss vom 30. Juni 2005 – BVerwG 6 P 9.04 – BVerwGE 124, 34 <36 ff.> = Buchholz 250 § 75 BPersVG Nr. 106 S. 40 ff.). Dass der Antragsteller in Überstundenfällen zu informieren ist, erkennt der Beteiligte ausdrücklich an (vgl. Rechtsbeschwerdeerwiderung S. 4 unter c)).

Die vorstehenden Aussagen gelten für die Mehrarbeit von Teilzeitbeschäftigten gemäß § 7 Abs. 7 TV-BA und für die Mehrarbeit von Beamten gemäß § 88 BBG entsprechend.

g) Den vorstehenden Ausführungen ist zu entnehmen, dass der Auskunftsanspruch des Antragstellers zunächst auf die Überlassung der Arbeitszeitlisten ohne Namensnennung beschränkt ist. Dies entspricht dem Grundsatz der Erforderlichkeit nach § 68 Abs. 2 Satz 1 und 2 BPersVG. Damit wird zugleich dem Grundrecht der Beschäftigten auf informationelle Selbstbestimmung Rechnung getragen (vgl. Beschluss vom 4. September 2012 a.a.O. Rn. 28). Zwar sind die Angaben über die Arbeitszeiten der Beschäftigten sowie die dabei zu bewertenden Fallgestaltungen (Dienstreisen, Urlaub, Gleittage) grundsätzlich nicht als sensibel einzustufen. Doch verbietet es der Grundsatz der Verhältnismäßigkeit, dass der Personalrat diese Angaben einer bestimmten Person zuordnen kann, ohne dass dies für die Wahrnehmung seiner Kontrollaufgabe erforderlich ist. Hinzu kommt, dass aus den Arbeitszeitlisten auch die Fehlzeiten wegen Erkrankung ersichtlich sind (vgl. Nr. 3.5 Satz 1 und Nr. 4.6.1 Satz 4 DV). Diese Angaben sind in besonderer Weise schützenswert (vgl. § 3 Abs. 9 BDSG).

Aus alledem ergibt sich, dass die Überwachungsaufgabe des Antragstellers wegen der Einhaltung arbeitszeitrechtlicher Bestimmungen in einem zweistufigen Verfahren stattfindet. Auf der ersten Stufe muss sich der Antragsteller mit der Vorlage anonymisierter Arbeitszeitlisten begnügen. Soweit die Überprüfung der Listen Unstimmigkeiten zu erkennen gibt, hat der Antragsteller auf einer zweiten Stufe Anspruch auf Erläuterungen, welcher auch zur Aufdeckung der Identität des betroffenen Beschäftigten führen kann, wenn anders eine Klärung der Angelegenheit nicht möglich ist. Entsprechendes gilt, wenn die Listen Hinweise auf besondere Fallgestaltungen enthalten, welche ein Tätigwerden des Antragstellers zum Schutz des betroffenen Beschäftigten gebieten.

Bei dieser Verfahrensweise wird der Antragsteller entgegen seiner Annahme nicht gehindert, seine Kontrollaufgabe zeitnah wahrzunehmen. Erhält er die anonymisierten Arbeitszeitlisten regelmäßig – nach Ermessen des Beteiligten – zeitgleich oder jedenfalls in angemessen kurzem Abstand nach Ende des Kalendermonats, so wird er in die Lage versetzt, Rechtsverstöße umgehend festzustellen, beim Beteiligten auf weitere Information und Abhilfe zu dringen und sich durch Nachfrage bei einem betroffenen Mitarbeiter von der erfolgten Korrektur zu vergewissern.

3. In Ansehung der vorstehenden Grundsätze beurteilt sich nunmehr das Begehren des Antragstellers:

a) Dessen Hauptantrag ist auf lesenden Zugriff auf die in der Zeiterfassung gespeicherten Daten der Beschäftigten gerichtet. Dieser Antrag ist unbegründet.

Dies folgt allerdings nicht bereits daraus, dass ein derartiges Begehren in § 68 Abs. 2 Satz 1 und 2 BPersVG von vornherein keine Grundlage findet. Vielmehr kann der Dienststellenleiter seiner Pflicht zur Vorlage von Unterlagen durch Einräumen einer Leseberechtigung genügen (vgl. BAG, Beschluss vom 16. August 2011 – 1 ABR 22/10 – BAGE 139, 25 Rn. 36).

Der Hauptantrag scheitert jedoch daran, dass der Antragsteller mit ihm Zugriff auf die Dateien mit den Namen der Beschäftigten erstrebt. Dies ist zur Wahrnehmung der effektiven Überwachungsaufgabe des Personalrats grundsätzlich nicht erforderlich, wie aufgezeigt wurde. Soweit anlassbezogen auf der zweiten Stufe des Kontrollverfahrens eine Namensnennung geboten ist, handelt es sich um nachgelagerte Einzelfälle, die vom Streitgegenstand nicht erfasst sind.

b) Der auf Auskunft über Beginn und Ende der täglichen Arbeitszeit gerichtete Hilfsantrag ist ebenfalls unbegründet, weil er ausdrücklich ebenfalls die Namensnennung zum Inhalt hat. Da der Antragsteller auf diesen Aspekt von Anfang an und auch noch im Anhörungstermin des Senats durchgehend besonderen Wert gelegt hat, verbietet sich eine Auslegung des Inhalts, dass eine Auskunftserteilung in anonymisierter Form als „Weniger“ im Hilfsantrag enthalten ist.

4. Soweit der Senat dem Personalrat einen Auskunftsanspruch unter Namensnennung der Beschäftigten abspricht, weicht er nicht von der Rechtsprechung des Bundesarbeitsgerichts ab.

Zwar hat dieses im Beschluss vom 6. Mai 2003 – 1 ABR 13/02 – (a.a.O. S. 117 ff.) dem Betriebsrat einen uneingeschränkten Anspruch auf Auskunft über Beginn und Ende der täglichen Arbeitszeit zuerkannt. Dass dabei eine Auskunftserteilung in anonymisierter Form erwogen worden ist, lässt sich der Entscheidung jedoch nicht entnehmen. Dagegen hat das Bundesarbeitsgericht in seinem Beschluss zum betrieblichen Eingliederungsmanagement vom 7. Februar 2012 – 1 ABR 46/10 – (a.a.O. Rn. 12) diesen Gesichtspunkt ausdrücklich in seine Prüfung einbezogen. Die Möglichkeit einer anonymisierten Auskunftserteilung hinsichtlich der Einhaltung der Arbeitszeit kann daher anhand der aktuellen Rechtsprechung des Bundesarbeitsgerichts nicht mehr als ausgeschlossen betrachtet werden.

Dessen ungeachtet liegt eine Abweichung auch deswegen nicht vor, weil für die Auskunftserteilung der Dienststelle an den Personalrat andere, strengere Grundsätze gelten als für die Auskunftserteilung des Arbeitgebers an den Betriebsrat. Im zitierten Beschluss vom 7. Februar 2012 (a.a.O. Rn. 50) hat das Bundesarbeitsgericht die Auffassung vertreten, der Arbeitgeber sei nicht befugt, sich gegenüber dem Überwachungsrecht des Betriebsrats auf Grundrechte von Arbeitnehmern zu berufen. Dieser Aussage kann für den Bereich des Personalvertretungsrechts nicht gefolgt werden. Die unmittelbar grundrechtsgebundene Dienststelle darf dem Personalrat keine Auskünfte erteilen, wenn damit zugleich das Persönlichkeitsrecht der Beschäftigten verletzt wird.

Video eines Bordellbesuchs im Internet als „Druckmittel“

(**Oberlandesgericht Koblenz**, Urteil vom 15. Januar 2014 – 5 U 1243/13 –)

1. **Bringt ein Gast den weiteren Betrieb eines Bordells durch Werfen von Stinkbomben zum Erliegen, was den Bordellbetreiber veranlasst, zur Identitätsklärung die Videoauf-**

zeichnung der Tat im Internet zu veröffentlichen, muss dies beendet werden, sobald die Personalien des Täters feststehen.

2. **Ein unter Fortdauer der Veröffentlichung erwirktes notarielles Schuldanerkenntnis, den pauschaliert geschätzten Betriebsschaden zu ersetzen, ist anfechtbar, wenn es unter der Drohung zustande gekommen ist, die Veröffentlichung erst nach einem derartigen Zahlungsversprechen zu beenden. Eine derartige Drohung kann auch konkludent zum Ausdruck gebracht werden.**

Sachverhalt:

Die Beklagte vermietet in einem in Gebäude Zimmer an Prostituierte. Dort warf der Kläger am 12.01. und 25.01.2013 Stinkbomben. Es gelang der Beklagten, ihn zu identifizieren, nachdem sie in ihrer Videoüberwachungsanlage gespeicherte Fotos seiner Person ins Internet gestellt hatte.

Der Versuch, den Kläger am 27.01.2013 in seiner Wohnung zur Rede zu stellen, schlug fehl. Danach kam es am 28.01.2013 zu notariellen Termin, bei dem der Kläger im Hinblick auf die durch sein Verhalten entstandenen Schäden ein auf 12.000 € nebst Zinsen lautendes Schuldanerkenntnis gegenüber der Beklagten unterzeichnete und sich deswegen der sofortigen Zwangsvollstreckung in sein Vermögen unterwarf. Die Beklagte versprach in derselben Urkunde, die Fotos des Klägers aus dem Internet herauszunehmen und alle über den Kläger gespeicherten Daten unter Verschluss zu halten. Des Weiteren sollten die gegen ihn gestellten Strafanträge zurückgezogen werden, sobald er seine Zahlungszusage erfüllt hatte.

Im vorliegenden Rechtsstreit hat der Kläger beantragt, die Vollstreckung aus der notariellen Urkunde für unzulässig zu erklären. Das Schuldanerkenntnis stehe in keinem Verhältnis zu dem angerichteten Schaden und sei wucherisch. Unabhängig davon habe er es rechtswirksam angefochten, da er unter Druck gesetzt worden sei.

Das Landgericht hat die Klage abgewiesen: Der Kläger habe ein deklaratorisches Anerkenntnis abgegeben, das ihm den Einwand, betraglich überfordert worden zu sein, abschneide. Er sei auch nicht in verwerflicher Weise bedroht worden.

Das greift der Kläger mit der Berufung an.

Aus den Gründen:

Der angefochtene Titel hat keinen Bestand, so dass eine Zwangsvollstreckung daraus unzulässig ist (§§ 794 Abs. 1 Nr. 5, 795 S. 1, 767 Abs. 1 ZPO) und seine vollstreckbare Ausfertigung an den Kläger herausgeben werden muss (§ 371 BGB analog)....

Das streitigev deklaratorischen Anerkenntnis wurde durch unzulässig ausgeübten Zwang veranlasst. Dieser Zwang ging von der – möglicherweise nicht wörtlichen aber nach den Umständen zumindest konkludent vermittelteten Ankündigung der Beklagten aus, die laufende Veröffentlichung der Fotos des Klägers erst dann zu beenden, wenn dieser die notarielle Verpflichtungserklärung abgab. Ein entsprechender Zusammenhang wird aus dem Urkundstext selbst deutlich, demzufolge die Herausnahme der Fotos aus dem Internet als Gegenleistung zum Schuldanerkenntnis des Klägers ausgestaltet wurde. Es ist weder vorgetragen noch sonst ersichtlich, dass die Beklagte zum Ausdruck gebracht hätte, auch ohnedies – nämlich im Sinne einer eigenständigen, von jeder Verknüpfung mit dem Verhalten des Klägers freien Vorleistung – zu einem solchen Schritt bereit zu sein .... Indem die Beklagte die notarielle Zahlungszusage des Klägers durch den Hinweis auf die ansonsten fortdauernde Publikation der Fotos herbeiführte, übte sie eine widerrechtliche Drohung aus, weil die Veröffentlichung gegen das Gesetz verstieß und unabhängig von jedwedem Entgegenkommen des Klägers hätte beendet werden müssen (vgl. Ellenberger in Palandt, BGB, 73. Aufl., § 123 Rn. 16). Die Publikation war gemäß § 22 KunstUrhG verboten und damit ohne weiteres zu unterlassen. Die Vorschrift gestattet die Verbreitung und öffentliche Zurschaustellung von Bildnissen einer Person nur mit deren Erlaubnis, an der es im vorliegenden Fall fehlte.

c) Es bedarf keiner Auseinandersetzung mit der Auffassung des Landgerichts, die Beklagte habe ein legitimes Interesse daran gehabt, „denjenigen ausfindig" zu machen, „der die Stinkbomben im Bordell zerplatzen ließ", „nicht zuletzt, um weitere Anschläge zu vermeiden". Selbst wenn man darin – was aus der Sicht des Senats freilich eher fern liegt – primär einen Rechtfertigungsgrund gemäß § 227 BGB oder § 34 StGB (zu dessen Anwendung im Zivilrecht vgl. Ellenberger in Palandt, BGB, 73. Aufl., § 227 Rn. 10) sähe, war für einen solchen Rechtfertigungsgrund jedenfalls kein Raum mehr, nachdem die Beklagte die Identität des Klägers ermittelt hatte und dessen Urheberschaft feststand. Diese Situation war bei der Errichtung der notariellen Urkunde längst eingetreten.

Evangelische Kirche darf die Bewerbung um die Stelle eines „Antirassismus-Referenten" wegen Konfessionslosigkeit ablehnen (Ls)

(**Landesarbeitsgericht Berlin**, Urteil vom 28. Mai 2014 – 4 Sa 157/14; 4 Sa 238/14)

Ein kirchlicher Arbeitgeber darf die Besetzung einer Stelle eines Referenten/einer Referentin, der/die einen unabhängigen Bericht zur Umsetzung der Antirassismuskonvention der Vereinigten Nation durch Deutschland erstellen soll, von der Mitgliedschaft in einer christlichen Kirche abhängig machen. Der wegen Kofessionslosigkeit abgelehnten Bewerberin steht keine Entschädigung nach dem Allgemeinen Gleichbehandlungsgesetz zu.

(Nicht amtliche Leitsätze)

Umbaumaßnahmen im Betriebsratsbüro unterliegen nicht der Mitbestimmung (Ls)

(**Hessisches Landesarbeitsgericht**, Beschluss vom 3. März 2014 – 16 TABVGa 214/13)

Dem Betriebsrat steht kein Mitbestimmungs- oder Abwehrrecht zu, wenn der Arbeitgeber die Tür zum Betriebsratsbüro um einige Meter versetzen will. Die Tatsache, dass der Weg zur Damentoilette sich für das weibliche Ersatzmitglied des Betriebsrats dadurch um 200 m verlängert, ist zumutbar und keine unzulässige Behinderung der Betriebsratsarbeit.

(Nicht amtliche Leitsaätze)

Zur Sperrung personenbezogener Daten in einer Gesundheitsakte des Sozialpsychiatrischen Dienstes (Ls)

(**Oberverwaltungsgericht Berlin-Brandenburg**, Beschluss vom 21. Januar 2014 – OVG 12 S 84.13)

1. **Die Sperrung in einer Gesundheitsakte des Sozialpsychiatrischen Dienstes enthaltener personenbezogener Daten kann wegen der Befürchtung des Betroffenen, in einem Unterbringungsverfahren könnte auf diese Daten zurückgegriffen werden, nicht im Wege vorläufigen Rechtsschutzes verlangt werden. Der Betroffene kann darauf verwiesen werden, dass die Wahrheit oder Unwahrheit entsprechender Daten in einem etwaigen Unterbringungsverfahren eigenständig zu prüfen und er in diesem Verfahren anzuhören ist.**
2. **Die Sperrung einer Akte, die zu einer Person geführt wird, aber über einen längeren Zeitraum zu unterschiedlichen Sachverhalten angefallene personenbezogene Daten enthält, kann regelmäßig nicht beansprucht werden; der Betroffene muss die zu sperrenden Daten konkretisieren.**

Zulässigkeit eines Ärztebewertungsportals

(**Landgericht Kiel**, Urteil vom 6. Dezember 2013 – 5 O 372/13 –)

Ein Arzt muss subjektive, anonyme Bewertungen in einem Ärztebewertungsportal im Hinblick auf die Meinungsäußerungsfreiheit der Verfasser hinnehmen. Ein sich aus § 29 Abs. 1 Nr. 1 BDSG ergebendes Abwehrinteresse besteht erst, soweit falsche Tatsachenbehauptungen aufgestellt werden bzw. es sich um Schmähkritik handelt.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Parteien streiten über eine auf dem Internetportal der Beklagten veröffentlichte negative Bewertung des Klägers.

Der Kläger ist ein langjährig praktizierender Frauenarzt. Die Beklagte betreibt ein Portal im Internet, auf dem auch Bewertungen über Ärzte veröffentlicht werden können. Das Qualitätsmanagement der Beklagten umfasst u.a. die Maßgabe, dass vor Veröffentlichung einer Bewertung diverse Schritte durchlaufen werden müssen. So müssen sich die Bewertenden mit einer E-Mail-Adresse bei der Beklagten anmelden, bei Abgabe der Bewertung ausdrücklich bestätigen, dass sie vom bewerteten Arzt behandelt wurden und über einen an die angegebene E-Mail-Adresse gesendeten Aktivierungslink die Abgabe der Bewertung nochmals bestätigen. Am 30.01.2013 wurde auf dem Portal der Beklagten eine Bewertung über den Kläger eingestellt. Unter dem Profil des Klägers mit Namen und Praxisanschrift folgte ein Bewertungstext sowie eine Notenbewertung. Mit der Notenbewertung können einzelne Kriterien nach dem bekannten Schulnotensystem von 1 („Sehr gut“) bis 6 („Ungenügend“) bewertet werden. Der Kläger erhielt dabei die folgenden Noten:

Behandlung	5,0
Aufklärung	5,0
Vertrauensverhältnis	6,0
Genommene Zeit	4,0
Freundlichkeit	2,0
Wartezeit Termin	1,0
Wartezeit Praxis	4,0
Sprechstundenzeiten	2,0
Betreuung	4,0
Praxisausstattung	5,0
Telefonische Erreichbarkeit	5,0
Gesamtnote	**4,4**

Ein Screenshot der Notenbewertung ist als Anlage K 1 (Bl. 6 d. A.) zu sehen.

Auf eine Beanstandung durch den Kläger hin löschte die Beklagte den Text zur Bewertung, lehnte eine Löschung der Notenbewertung aber ab.

In mindestens zwei anderen Bewertungen auf dem Bewertungsportal der Beklagten erhielt der Kläger die Gesamtnoten 1,0 und 1,4.

Der Kläger ist der Auffassung, dass in den einzelnen Notenbewertungen zu den Punkten der „Behandlung“, der „Aufklärung“, der „Praxisausstattung“ und der „telefonischen Erreichbarkeit“ unwahre Tatsachenbehauptungen lägen, die den Tatbestand der üblen Nachrede erfüllten. Ohnehin könne die Bewertung nicht unter den Schutz der Meinungsfreiheit fallen, da mit Nichtwissen bestritten werde, dass eine Patientin des Klägers oder überhaupt eine dritte Person die Bewertung abgegeben habe. Mit Nichtwissen bestreitet der Kläger weiter, dass der angebliche Autor der Bewertung der Beklagten auf deren Rückfrage hin die abgegebene Bewertung ausführlich bestätigt habe. Ebenfalls mit Nichtwissen bestreitet der Kläger, dass das Qualitätsmanagement der Beklagten sicherstelle, dass nur Patienten des jeweiligen Arztes Bewertungen über diesen abgeben könnten. Vielmehr könne jede dritte Person die Veröffentlichung entsprechender Bewertungen bei der Beklagten bewirken, so dass das System der Beklagten völlig unzureichend sei.

Aus den Gründen:

I. Dem Kläger steht gegen die Beklagte kein Anspruch auf Löschung der Notenbewertung vom 30.01.2013 bezüglich der Punkte „Behandlung“, „Aufklärung“, „Praxisausstattung“ und „telefonische Erreichbarkeit“ zu.

Ein entsprechender Anspruch des Klägers ergibt sich nicht aus § 35 Abs. 2 S. 2 Nr. 1 BDSG. Demnach sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist. Wenngleich die streitgegenständliche Bewertung auch personenbezogene Daten enthält, ist deren Speicherung jedoch zulässig. Die Speicherung der Bewertung ist nach § 29 Abs. 1 Nr. 1 BDSG dann zulässig, wenn ein Grund zur Annahme eines schutzwürdigen Interesses an dem Ausschluss der Datenerhebung und -speicherung nicht gegeben ist. Dies ist hier der Fall. Der Anwendungsbereich des § 29 BDSG ist vorliegend eröffnet, da die gespeicherten Daten ungeachtet weiterer verfolgter Zwecke der Beklagten jedenfalls auch der Übermittlung dienen, nämlich der Information der interessierten Nutzer bzw. der Allgemeinheit (vgl. hierzu den parallel gelagerten Fall des OLG Frankfurt NJW 2012, 2896 f.). Die Prüfung, ob ein schutzwürdiges Interesse vorliegt, verlangt eine Abwägung zwischen dem Recht des Klägers auf informationelle Selbstbestim-

mung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG als Ausfluss des allgemeinen Persönlichkeitsrechts auf der einen Seite und dem Recht auf Meinungs- und Kommunikationsfreiheit nach Art. 5 Abs. 1 GG auf der anderen Seite. Die Abwägung ergibt, dass dem Grundrecht auf Meinungsfreiheit der Vorrang einzuräumen ist, so dass ein schutzwürdiges Interesse des Klägers i.S.d. § 29 BDSG nicht besteht.

Zweifellos ist durch die streitgegenständliche Notenbewertung das allgemeine Persönlichkeitsrecht des Klägers betroffen. Die Bewertung bezieht sich auf die berufliche Tätigkeit des Klägers als Arzt und fällt damit in die sogenannte Sozialsphäre des Klägers, die im Verhältnis zur Intim- und Privatsphäre allerdings nicht gleichermaßen geschützt ist. Äußerungen im Rahmen der Sozialsphäre dürfen nur im Falle schwerwiegender Auswirkungen auf das Persönlichkeitsrecht mit negativen Sanktionen verknüpft werden, so etwa dann, wenn eine Stigmatisierung, soziale Ausgrenzung oder Prangerwirkung zu besorgen sind (BGH NJW 2009, 2888 ff.).

Die angegriffenen Notenbewertungen stellen sich im vorliegenden Fall als Meinungsäußerungen, nicht aber als Tatsachenbehauptungen dar. Tatsachenbehauptungen unterscheiden sich von Meinungsäußerungen und Werturteilen dadurch, dass bei den letztgenannten die subjektive Beziehung zwischen der Äußerung und der Wirklichkeit im Vordergrund steht, während für Tatsachenbehauptungen die objektive Beziehung des sich Äußernden zum Inhalt seiner Äußerung charakteristisch ist. Für die Einstufung als Tatsachenbehauptung kommt es wesentlich darauf an, ob die Aussage einer Überprüfung auf ihre Richtigkeit mit den Mitteln des Beweises zugänglich ist, was bei Meinungsäußerungen und Werturteilen ausscheidet, weil sie durch das Element der Stellungnahme und des Dafürhaltens gekennzeichnet werden und sich deshalb nicht als wahr oder unwahr erweisen lassen (BGH NJW 2005, 279 ff.; BVerfG NJW 2003, 1855 f.). Meinungsäußerungen und Werturteile fallen in den Schutzbereich der Meinungsfreiheit nach Art. 5 Abs. 1 S. 1 GG, soweit die Grenze zur Schmähkritik nicht überschritten ist. Von der Meinungsfreiheit geschützt sind auch Äußerungen, die zwar einen tatsächlichen Kern aufweisen, in denen sich aber Tatsachen und Meinungen vermengen und die insgesamt durch die Elemente der Stellungnahme, des Dafürhaltens oder Meinens geprägt werden (BGH NJW 2009, 3580 ff.). So verhält es sich hier.

Die Bewertungskriterien „Behandlung", „Aufklärung", „Praxisausstattung" und „telefonische Erreichbarkeit" knüpfen zwar an einen Tatsachenkern wie eben die Praxisausstattung oder die telefonische Erreichbarkeit an. Die Bewertung dieses Tatsachenkerns in der Form von Noten stellt aber ein Werturteil dar, das von der Meinungsfreiheit geschützt ist. So hat der Bundesgerichtshof (NJW 2009, 2888 ff.) in einem vergleichbaren Fall entschieden, dass Notenbeurteilungen, durch die eine Lehrerin in den Bewertungskriterien "guter Unterricht", "fachlich kompetent", "motiviert", "faire Noten", "faire Prüfungen" und "gut vorbereitet" benotet wurde, in den Bereich der Meinungsäußerungen fallen, auch wenn sie einen tatsächlichen Kern haben. Innerhalb der Verknüpfung von Tatsachenkern und Werturteil überwiegen hier die Elemente der Stellungnahme, des Dafürhaltens oder Meinens deutlich. Es wird gerade nicht gesagt, dass der Kläger beispielsweise nicht über ein bekanntes Risiko einer von ihm empfohlenen Behandlungsmethode aufgeklärt habe, sondern es wird der Punkt „Aufklärung" mit einer „5", also mit einem „Mangelhaft" bewertet. Es wird nicht behauptet, dass der Kläger beispielsweise bei 5 Anrufversuchen zu verschiedenen Uhrzeiten an zwei aufeinander folgenden Tagen nicht erreichbar gewesen sei, sondern der Punkt der „telefonischen Erreichbarkeit" wird ebenfalls mit einer „5" benotet. Dass eine Bewertung etwa der Praxisausstattung auch nach zertifizierten Prüfverfahren möglich ist oder bestimmte Qualitätsstandards eingehalten worden sein mögen, ist dabei unerheblich. Die Note „5" bringt eine persönliche Meinung zum Ausdruck, die auch irrational oder nicht nachvollziehbar sein kann, die aber gerade nicht objektiv ist und dies auch nicht sein muss.

Soweit der Kläger der Auffassung ist, dass es sich bei dem Kriterium der „telefonischen Erreichbarkeit" um eine unwahre Tatsachenbehauptung handele, da er belegen könne, dass er für seine Patientinnen jederzeit erreichbar sei, kann dem nicht gefolgt werden. Selbst wenn der Kläger – wie von ihm im Rahmen der persönlichen Anhörung geschildert – jeder Patientin eine Visitenkarte aushändigt, auf der sowohl seine Festnetz- als auch seine Handynummer abgedruckt sind und er für seine Patientinnen auch im Urlaub erreichbar ist, betrifft dies beispielsweise nicht die telefonischen Erreichbarkeit der Praxis für Erstpatientinnen. So ist keinesfalls ausgeschlossen, dass – wie es bei Arztpraxen erfahrungsgemäß durchaus häufiger vorkommt – der Anschluss wegen anderweitiger Telefongespräche zeitweise häufiger besetzt ist. Gleichfalls wird der Kläger zu Sprechstundenzeiten nicht ununterbrochen telefonisch erreichbar sein, da er seine Patientinnen behandelt. Ein Rückruf des Klägers mag einer Patientin verspätet erschienen sein. Zwar wären die vorgenannten Aspekte aus vernünftiger Sicht objektiv nicht unbedingt nachvollziehbar. Dies kann letztlich aber dahinstehen, da eine Notenbewertung, wie sie hier vorgenommen wird, keinen objektiven Standards folgt, sondern letztlich Teil einer subjektiven Meinung ist, die auch unvernünftig sein darf. Ob ein Dritter etwas für gut, ausreichend oder schlecht befindet, ist stets der persönlichen Einschätzung und Überzeugung und damit der eigenen, subjektiven Meinung geschuldet. Nicht anders verhält es sich bei der Vergabe von Noten, die einem Äquivalent von „Gut" oder auch „Mangelhaft" entsprechen. Dass diese Schulnoten ohne den ursprünglich zugehörigen begleitenden Bewertungstext gänzlich isoliert wahrgenommen werden, unterstreicht den Charakter des persönlichen Werturteils zusätzlich.

Soweit der Kläger mit Nichtwissen bestreitet, dass die beanstandete Bewertung von einer von ihm behandelten Patientin verfasst wurde und der Auffassung ist, dass die Bewertung daher nicht in den Schutzbereich der Meinungsfreiheit fallen könne, führt dies zu keinem anderen Ergebnis. Ein Arzt, der sich Bewertungen in einem frei zugänglichen Internetportal ausgesetzt sieht, hat keinen Anspruch gegen den Betreiber des Portals auf Löschung der Einträge, auch wenn diese anonym erfolgen (OLG Frankfurt NJW 2012, 2896 f.). Zwar ist es auch nach dem von der Beklagten dargestellten System des Qualitätsmanagements aufgrund der dennoch gewährleisteten Anonymität ersichtlich nicht ausgeschlossen, dass das Bewertungssystem missbräuchlich verwendet werden kann, um einem Arzt zu schaden. Dies muss aber letztlich hingenommen werden, um einen effektiven Schutz der Meinungsfreiheit zu garantieren. Es kann nicht vorausgesetzt werden, dass sich die Bewertenden vor Abgabe einer Bewertung durch Vorlage von Nachweisen wie etwa Arbeitsunfähigkeitsbescheinigungen, Rezepten oder Terminszetteln legitimieren und damit identifizieren, wie es der Kläger verlangt. Die anonyme Nutzung ist dem Internet immanent. Eine Beschränkung der Meinungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugeordnet werden können, ist mit Art. 5 Abs. 1 S. 1 GG nicht vereinbar. Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen eine Selbstzensur vornimmt und davon absieht, seine Meinung zu äußern (BGH NJW 2009, 2888 ff.; OLG Frankfurt NJW 2012, 2896 f.; OLG Hamm CR 2012, 128 ff.). Ein Schutz des bewerteten Arztes findet letztlich

dadurch statt, dass unwahre Tatsachenbehauptungen oder Schmähkritik nicht hingenommen werden müssen. In Anbetracht des – unstreitig vorhandenen – Qualitätsmanagements der Beklagten, reicht, auch wenn die Effektivität des Qualitätsmanagements streitig ist, der latente Verdacht der Manipulation von Bewertungen aber nicht aus, um eine Löschung der beanstandeten Bewertungskriterien zu erreichen (vgl. OLG Frankfurt a.a.O.).

Die Grenze zur Schmähkritik ist hier nicht überschritten. An die Bewertung einer Äußerung als Schmähkritik sind strenge Maßstäbe anzulegen, weil anderenfalls eine umstrittene Äußerung ohne Abwägung dem Schutz der Meinungsfreiheit entzogen und diese damit in unzulässiger Weise verkürzt würde. Erst wenn bei einer Äußerung nicht mehr die Auseinandersetzung in der Sache, sondern die Herabsetzung der Person im Vordergrund steht, die jenseits polemischer und überspitzter Kritik herabgesetzt und gleichsam an den Pranger gestellt werden soll, nimmt die Äußerung den Charakter einer unzulässigen Schmähung an (BGH NJW 2009, 3580 ff.). Eine reine Notenbewertung erfüllt den Charakter einer Schmähkritik jedoch nicht (BGH NJW 2009, 2888 ff.).

Dass der Kläger im Wettbewerb mit anderen Frauenärzten steht und durch die Negativbewertung berufliche Nachteile erleiden könnte, ist ebenfalls kein ausreichender Grund, um ein schutzwürdiges Interesse des Klägers zu begründen, das stärker als das Grundrecht auf Meinungsfreiheit wiegen würde. Auch Ärzte unterliegen den Marktmechanismen, zu denen heute – wie in vielen anderen Lebensbereichen auch – Bewertungsmöglichkeiten in öffentlich zugänglichen Quellen, zu denen auch das Internet zählt, gehören. Da die Meinungsfreiheit auch das Recht des Äußernden umfasst, die Modalitäten einer Äußerung und damit das Verbreitungsmedium frei zu bestimmen, muss ein Arzt es grundsätzlich hinnehmen, wenn die Möglichkeit besteht, ihn in einem öffentlich zugänglichen Portal zu bewerten, und diese Möglichkeit genutzt wird (OLG Frankfurt NJW 2012, 2896 f.). Selbst wenn sich die Benotung in Form einer Negativempfehlung, also eines Abratens von einem Arzt, auswirken sollte, muss ein Arzt eine entsprechend geäußerte negative Meinung gegen sich gelten lassen (vgl. LG Köln, Urteil vom 18.07.2012 – 28 O 89/12 –, juris sowie (zum Bewertungsportal der Beklagten) LG Düsseldorf, Urteil vom 09.04.2013 – 5 O 141/12 –, juris).

Nochmals deutlich unterstrichen werden soll an dieser Stelle allerdings, dass gerichtlicherseits die im Rahmen der mündlichen Verhandlung zum Ausdruck gekommene Sorge, Verärgerung und Frustration des Klägers über die streitgegenständliche Bewertung ohne weiteres verständlich und nachvollziehbar ist. Dennoch muss im Rahmen der Interessenabwägung zwischen dem allgemeinen Persönlichkeitsrecht des Klägers und dem Recht auf Meinungs- und Informationsfreiheit letzterem der Vorrang eingeräumt werden, da das schützenswerte Interesse der Nutzer von Bewertungsportalen im Internet an Meinungs- und Informationsfreiheit überwiegt. So sollen Internet-Bewertungsportale ihrem Sinn und Zweck nach Nutzern Gelegenheit bieten, sowohl positive als auch negative Meinungen zu äußern. Das Interesse der Allgemeinheit an kritischen, unabhängigen Informationen, die über derartige Bewertungsportale im Internet erlangt werden können, ist als sehr hoch zu bewerten, weil solche Informationen für den Verbraucher unabdingbar sind, um gewerbliche Produkte und Dienstleistungen zu bewerten und sich insoweit eine Meinung bilden zu können (Urteil LG Nürnberg-Fürth vom 13.01.2010 – 3 O 3692/09, zitiert nach juris). Das große Interesse an derartigen Informationen wird durch die zunehmende Beliebtheit von Bewertungsportalen im Internet belegt. Insoweit sind negative Meinungsäußerungen und Werturteile in Internet-Bewertungsportalen, soweit sie nicht in Schmähkritik bestehen oder in unwahren Tatsachenbehauptungen ihren Grund finden, nicht rechtswidrig (OLG Hamburg WRP 2012, 485 ff.). Hinzu tritt im vorliegenden Fall, dass gerade aufgrund des Umstands, dass es sich um eine reine Notenbewertung handelt, Nutzer des Bewertungsportals dieser Bewertung naturgemäß keine sonderlich hohe Bedeutung beimessen werden, da die Noten gerade nicht mit Tatsachenbehauptungen unterfüttert sind und damit klar erkennbar lediglich eine subjektive Einschätzung geäußert wird.

Ein Anspruch des Klägers auf Löschung der beanstandeten Noten ergibt sich auch nicht nach §§ 823 Abs. 2, 1004 BGB i.V.m. § 186 StGB unter dem Gesichtspunkt einer üblen Nachrede, da, wie bereits ausgeführt, keine Tatsachenbehauptungen vorliegen, die Gegenstand einer üblen Nachrede sein könnten.

Unerheblich ist, ob – wie von der Beklagten gerügt – der Kläger eine Rechtsverletzung nicht hinreichend substantiiert hat. Denn eine Störerhaftung der Beklagten als Host-Provider scheidet bereits deshalb aus, weil es sich hier nicht um Tatsachenbehauptungen handelt, die richtig oder falsch sein können (vgl. LG Nürnberg-Fürth CR 2012, 541 ff.). Ohnehin läge unter Abwägungsgesichtspunkten keine beseitigungspflichtige Rechtsverletzung vor. Auch insoweit wird auf die vorangegangenen Ausführungen Bezug genommen.

Ein Anspruch des Klägers folgt auch nicht unter dem Gesichtspunkt eines unzulässigen Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb nach §§ 823 Abs. 1, 1004 BGB. Dahinstehen kann, ob die streitgegenständlichen Benotungen überhaupt einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb darstellen. Ist eine gewerbliche Leistung durch eine wertende Äußerung betroffen, ist mit der Annahme eines rechtswidrigen Eingriffs jedenfalls grundsätzlich Zurückhaltung geboten (Sprau, in: Palandt, BGB, 72. A., § 823 Rn. 129). Im vorliegenden Fall wären im Rahmen der vorzunehmenden Interessenabwägung die Benotungen jedenfalls nicht als widerrechtlich einzustufen, da das schützenswerte Interesse der Nutzer von Bewertungsportalen im Internet an Meinungs- und Informationsfreiheit überwiegt.

Datenschutzrechtliches Verbot des Scannens von Personalausweisen

(**Verwaltungsgericht Hannover**, Urteil vom 28. November 2013 – 10 A 5342/11 –)

1. **Soweit die Erhebung und Verwendung personenbezogener Daten aus dem Personalausweis oder mithilfe des Personalausweises betroffen ist, enthalten die Vorschriften des dritten Abschnitts des Personalausweisgesetzes eine abschließende, § 28 BDSG verdrängende Regelung.**

2. **Das Scannen und Speichern von Personalausweisen durch nicht öffentliche Stellen ist nach den datenschutzrechtlichen Bestimmungen des Personalausweisgesetzes unzulässig.**

Sachverhalt:

Die Beteiligten streiten um die Rechtmäßigkeit einer datenschutzrechtlichen Anordnung des Beklagten.

Die Klägerin ist eine Logistikdienstleisterin, die insbesondere im Bereich der Automobillogistik und Autotransporte tätig ist. Auf ihrem Betriebsgelände lagern ständig mehrere tausend Fahrzeuge. Täglich werden zahlreiche Fahrzeuge – insbesondere von Fahrern von Spediti-

onen – abgeholt. Um den Speditionsvorgang zu überwachen, werden die Personalausweise der Abholer eingescannt und auf einem Rechner gespeichert.

Nachdem die Beklagte (die zuständige Datenschutzaufsichtsbehörde) durch mehrere Eingaben von Betroffenen Kenntnis von dieser Praxis erhalten hatte, wandte er sich im Juli 2011 an die Klägerin, teilte ihr mit, dass sie das Einscannen von Personalausweisen für unzulässig halte und bat um Stellungnahme. Hierauf äußerte die Klägerin gegenüber der Beklagten, die von ihr geübte Praxis sei mit den datenschutzrechtlichen Bestimmungen vereinbar. Die eingescannten Personalausweise der Abholer würden auf einem gesonderten Rechner gespeichert und gelöscht, sobald eine positive Rückmeldung über die Fahrzeugauslieferung vorliege; in der Regel sei dies nach spätestens fünf Tagen der Fall. Das Wachgebäude, in dem sich der Rechner befinde, sei während der Geschäftszeiten ständig besetzt und werde auch ansonsten überwacht; unbefugte Dritte könnten sich daher die Daten nicht zugänglich machen. Nach § 28 Abs. 1 Nr. 2 des Bundesdatenschutzgesetzes (BDSG) sei das Erheben, Speichern und Nutzen von personenbezogenen Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen erforderlich sei und kein Grund zu der Annahme bestehe, dass ein schutzwürdiges Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiege. Unter Berücksichtigung der hohen Werte, die den Spediteuren oder Fahrern übergeben würden, könne ein berechtigtes Interesse an der Datenerhebung, die gerade dazu diene, den reibungslosen Speditionsvorgang zu überwachen und gegebenenfalls einen Ansprechpartner zu haben, nicht ernstlich in Zweifel gezogen werden. Vorwiegend komme es in diesem Zusammenhang zwar auf den Namen und die Adresse der Fahrzeugabholer an, aber auch das Lichtbild und die weiteren Informationen zum Erscheinungsbild wie Körpergröße und Augenfarbe könnten insbesondere im Falle einer Straftat der Erleichterung der polizeilichen Ermittlungen dienen. Überwiegende schutzwürdige Interessen der Betroffenen seien nicht ersichtlich. Werde der Speditionsvorgang erfolgreich abgeschlossen, würden die Daten nicht anderweitig genutzt, sondern gelöscht.

Mit Bescheid vom 07.11.2011 gab die Beklagte der Klägerin unter Androhung eines Zwangsgeldes für den Fall der Nichtbefolgung auf, innerhalb von einer Woche nach Bestandskraft der Anordnung das Einscannen von Personalausweisen zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen: Die Voraussetzungen des § 28 BDSG lägen nicht vor. Zu Unrecht berufe sich die Klägerin darauf, die von ihr erhobenen Daten dienten insbesondere im Falle einer Straftat der Erleichterung der polizeilichen Ermittlungen. Da die Ermittlungsbehörden die Daten wie Lichtbild, Körpergröße, Augenfarbe usw. bei den Meldebehörden abrufen könnten, sei die Erhebung durch die Klägerin nicht erforderlich und damit unzulässig. Darüber hinaus sei nach dem Personalausweisgesetz das Scannen von Ausweisdaten untersagt. Der Ausweis dürfe lediglich als Identitätsnachweis und Legitimationspapier verwendet, d.h. zur Einsichtnahme vorgelegt werden.

Zur Begründung ihrer am 08.12.2011 erhobenen Klage wiederholt die Klägerin unter Vertiefung im Einzelnen ihr Vorbringen aus dem Verwaltungsverfahren. Aus Zeitgründen sei es gerechtfertigt, eine Kopie der Personalausweise anzufertigen. Die eingescannten Unterlagen dienten der Ermittlung von Straftätern; dem von ihr praktizierten Verfahren komme zugleich eine präventive Wirkung zu. Sobald der jeweilige Speditionsvorgang abgeschlossen sei – in der Regel spätestens nach 5 Tagen –, würden die Daten wieder gelöscht.

Aus den Gründen:

Die zulässige Klage ist nicht begründet.

Der angefochtene Bescheid ist rechtmäßig und verletzt die Klägerin daher nicht in ihren Rechten (vgl. § 113 Abs. 1 Satz 1 VwGO).

Rechtsgrundlage für die vom Beklagten getroffenen Anordnungen ist § 38 Abs. 5 Satz 2 BDSG. Nach § 38 Abs. 5 Satz 1 BDSG kann die Aufsichtsbehörde zur Gewährleistung der Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz gegenüber nicht öffentlichen Stellen Maßnahmen u.a. zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten anordnen. Gemäß § 38 Abs. 5 Satz 2 BDSG kann sie bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Die Anordnung des Beklagten, das Verfahren „Einscannen von Personalausweisen" einzustellen und die bisher rechtswidrig erhobenen Daten zu löschen, stellt eine Maßnahme im Sinne der letztgenannten Vorschrift dar.

Die von dem Beklagten angeordneten Maßnahmen sind inhaltlich nicht zu beanstanden. Das von der Klägerin praktizierte Scannen und Speichern von Personalausweisen stellt einen schwerwiegenden Verstoß gegen datenschutzrechtliche Vorschriften dar, so dass es der Beklagte auf der Grundlage von § 38 Abs. 5 Satz 2 BDSG verbieten und die Löschung der bisher rechtswidrig erhobenen Daten anordnen kann.

Die Zulässigkeit des Scannens und Speicherns von Personalausweisen beurteilt sich nach den in Abschnitt 3 des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis – Personalausweisgesetz – (PAuswG) getroffenen Regelungen über den Umgang mit personenbezogenen Daten; die von den Beteiligten herangezogene Vorschrift des § 28 BDSG über die Datenerhebung und -speicherung für eigene Geschäftszwecke durch nicht öffentliche Stellen ist hingegen nicht anwendbar.

Nach § 1 Abs. 2 Nr. 3 BDSG gilt das Bundesdatenschutzgesetz zwar grundsätzlich auch für die Datenerhebung, -nutzung und -verarbeitung durch nicht öffentliche Stellen. Soweit aber andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften des Bundesdatenschutzgesetzes vor (§ 1 Abs. 3 Satz 1 BDSG). Die Konkurrenz von Rechtsvorschriften des Bundes innerhalb und außerhalb des Bundesdatenschutzgesetzes, deren Gegenstand die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist, wird durch diese Regelung im Sinne des Vorrangs der spezielleren – bereichsspezifischen – Norm geklärt (vgl. Dix in Simitis, Bundesdatenschutzgesetz, 7. Aufl., Rn. 158 zu § 1). Inwieweit sich der Vorranggrundsatz konkret auswirkt, bestimmt sich nach dem Inhalt der mit dem Bundesdatenschutzgesetz konkurrierenden Vorschrift. Soweit diese eine abweichende Regelung für einen Sachverhalt trifft, der ebenfalls im Bundesdatenschutzgesetz geregelt ist, verdrängt sie die Normen dieses Gesetzes.

Soweit es um die Erhebung und Verwendung personenbezogener Daten aus dem Personalausweis oder mithilfe des Personalausweises geht, enthalten die Vorschriften des dritten Abschnitts des Personalausweisgesetzes eine abschließende, § 28 BDSG verdrängende Regelung. Denn § 14 PAuswG mit der amtlichen Überschrift „Erhebung und Verwendung personenbezogener Daten" bestimmt, dass die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises ausschließlich erfolgen darf durch

1. zur Identitätsfeststellung berechtigte Personen nach Maßgabe der §§ 15 bis 17,

2. öffentliche Stellen und nicht öffentliche Stellen nach Maßgabe der §§ 18 bis 20.

Damit ist diese Norm die zentrale bereichsspezifische Datenschutzvorschrift des Personalausweisrechts (so Möller in Hornung/Möller, PassG – PAuswG, Kommentar 2011, Rn. 1 zu § 14), die keinen Raum für eine vorrangige oder auch nur ergänzende Heranziehung der Regelungen des dritten Abschnitts des Bundesdatenschutzgesetzes über die Datenverarbeitung nicht öffentlicher Stellen lässt.

Die Klägerin ist unstreitig keine zur Identitätsfeststellung berechtigte Behörde im Sinne von § 14 Nr. 1 PAuswG. Maßgeblich für die Zulässigkeit des beanstandeten Verfahrens ist daher § 20 PAuswG. Abs. 1 dieser Norm bestimmt, dass der Inhaber den Personalausweis bei öffentlichen und nicht öffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden kann und ist damit die Grundlage für die Verwendung als Ausweis und Legitimationspapier auch im privaten Rechtsverkehr (Möller in Hornung/Möller, PassG – PAuswG, Kommentar 2011, Rn. 3 zu § 20). Dem entsprechend gesteht der Beklagte der Klägerin auch ohne weiteres zu, dass sie sich von den Fahrzeuge abholenden Personen den Personalausweis zeigen lässt und darin enthaltene Daten (Namen, Geburtsdatum, Adresse) herausschreibt.

Das mit der angefochtenen Verfügung beanstandete Verfahren hingegen ist § 20 Abs. 2 PAuswG zuzuordnen, wonach außer zum elektronischen Identitätsnachweis der Personalausweis durch öffentliche oder nicht öffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden darf. Nach der zur Konkretisierung der datenschutzrechtlichen Bestimmungen des Personalausweisgesetzes heranzuziehenden Begriffsbestimmung in § 3 Abs. 2 Satz 1 BDSG (vgl. BT-Drs. 16/10489 S. 40 zu § 14) ist eine automatisierte Verarbeitung die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen, wobei zum Verarbeiten das Speichern von personenbezogenen Daten gehört (§ 3 Abs. 4 Satz 1 BDSG). Ungeachtet der dabei angewendeten Verfahren ist Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung (§ 3 Abs. 4 Satz 2 Nr. 1 BDSG). Angesichts dieses Regelungsgefüges kann es nicht ernsthaft zweifelhaft sein, dass das von der Klägerin praktizierte Verfahren, bei dem Personalausweise gescannt und unter Verwendung einer speziellen Software auf einem Rechner gespeichert werden, um im Bedarfsfall verwendet zu werden, als automatisierte Speicherung personenbezogener Daten im Sinne von § 20 Abs. 2 PAuswG zu qualifizieren ist; auch die Klägerin hat substantiierte Einwände insoweit nicht erhoben.

Dieses Ergebnis wird durch die Entstehungsgeschichte von §§ 14 und 20 PAuswG bestätigt. So heißt es in der Begründung des Regierungsentwurfs zu § 14, der unverändert Gesetz geworden ist, u.a. (BT-Drs. 16/10498 S. 40):

„§ 14 stellt klar, dass die Erhebung und Verwendung personenbezogener Daten aus oder mithilfe des Ausweises künftig nur über die dafür vorgesehenen Wege erfolgen darf. Dies sind für nichtöffentliche und öffentliche Stellen der elektronische Identitätsnachweis und für zur hoheitlichen Identitätsfeststellung berechtigte Behörden der Abruf der elektronisch gespeicherten Daten einschließlich der biometrischen Daten. Weitere Verfahren z.B. über die optoelektronische Erfassung („scannen“) von Ausweisdaten oder den maschinenlesbaren Bereich sollen ausdrücklich ausgeschlossen werden.“

Dem entsprechend wird in der Begründung zu § 20 Absätze 2 und 3, der ebenfalls im Gesetzgebungsverfahren nicht verändert wurde, ausgeführt (BT-Drs. 16/10498 S. 42):

„Die Vorschrift ist erforderlich, weil der Einsatz des elektronischen Identitätsnachweises sowohl zu einem automatischen Abruf von Daten (z.B. bei der erneuten Anmeldung bei einem Dienstekonto) als auch zur automatischen Speicherung personenbezogener Daten (z.B. nach Übermittlung von Daten zur Anlage eines Dienstekontos) führen kann. Jenseits dieser engen Ausnahmen – die der Ausweisinhaber über die Eingabe seiner Geheimnummer steuern kann – bleiben die Verwendungsverbote der bisherigen Fassung von § 3 Abs. 4 Satz 1 PersAuswG und § 16 Abs. 4 Satz 1 PassG, § 3a Abs. 1 Satz 1 und Abs. 2 erster Halbsatz und § 4 Abs. 2 und 3 des Personalausweisgesetzes erhalten. Von der Vorschrift erfasst sind alle Formen des automatischen Abrufs, insbesondere Scannen, Fotokopieren und Ablichten der Daten. …“

Ob tatsächlich schon das bloße Kopieren von Personalausweisen – von ausdrücklich gesetzlich zugelassenen Ausnahmen wie in § 8 Abs. 1 Satz 3 Geldwäschegesetz, § 95 Abs. 4 Satz 2 Telekommunikationsgesetz und § 64 Abs. 1 Nr. 2 Fahrerlaubnisverordnung abgesehen – nach Wortlaut sowie Sinn und Zweck der datenschutzrechtlichen Vorschriften des Personalausweisgesetzes verboten ist, bedarf hier keiner Entscheidung, da das von der angefochtenen Verfügung erfasste Scannen und automatisierte Speichern mit der Möglichkeit der Weiterverarbeitung und Nutzung eine andere rechtliche Qualität aufweist. Lediglich vorsorglich ist deshalb darauf hinzuweisen, dass nach dem vom Beklagten vorgelegten Schreiben des Bundesministeriums des Innern an den Bundesbeauftragten für den Datenschutz vom 01.02.2013 zwar kein grundsätzliches rechtliches Kopierverbot (mehr) besteht, für das Anfertigen von Kopien des Personalausweises (bzw. des Reisepasses) aus sicherheits- und datenschutzrechtlichen Gründen jedoch strenge Maßstäbe gelten sollen. Bei einer Identifizierung unter Anwesenden sei die Erstellung einer Kopie grundsätzlich unzulässig, weil regelmäßig kein Bedarf dafür bestehe.

Ohne Einfluss auf die rechtliche Zulässigkeit des von der Klägerin praktizierten Verfahrens ist die Frage, ob im Einzelfall eine wirksame Einwilligung des Personalausweisinhabers vorliegt. Das Scannen und Speichern von Personalausweisen ist nach den zuvor dargestellten Normen gesetzlich verboten, ohne dass dem Ausweisinhaber die Möglichkeit eingeräumt worden wäre, das Verbot durch sein Einverständnis zu suspendieren. Eine die Erhebung, Verarbeitung und Nutzung personenbezogener Daten rechtfertigende Einwilligung des Betroffenen, wie sie in § 4 Abs. 1, § 4a BDSG geregelt ist, sieht das Personalausweisgesetz als hier einschlägige Spezialvorschrift nicht vor.

Das von der Klägerin praktizierte Verfahren des Scannens und Speicherns von Personalausweisen stellt einen schwerwiegenden Verstoß gegen die datenschutzrechtlichen Bestimmungen des Personalausweisgesetzes dar, so dass der Beklagte hiergegen auf der Grundlage von § 38 Abs. 5 Satz 2 BDSG einschreiten kann. Grundsätzlich setzt eine Untersagung nach dieser Vorschrift zwar voraus, dass zuvor nach § 38 Abs. 5 Satz 1 BDSG vergeblich die Beseitigung des Mangels verlangt wurde und auch die Festsetzung eines Zwangsgeldes nicht zum Erfolg geführt hat. Steht jedoch die Unmöglichkeit der Fehlerbeseitigung von vornherein fest, kann ausnahmsweise unmittelbar das Datenverarbeitungsverfahren untersagt werden (Petri in Simitis, Bundesdatenschutzgesetz, 7. Aufl., Rn. 75 zu § 38). So verhält es sich hier, da eine Legalisierung des von der Klägerin praktizierten Verfahrens durch bloße Modifikationen nicht möglich ist.

Berichte, Informationen, Sonstiges

Studie der Initiative Markt- und Sozialforschung:

Vertrauen in Datenschutz hängt von der bearbeitenden Einrichtung ab. Vertrauen bei Gesundheitseinrichtungen und Staat am häufigsten – bei IT und Telekommunikation am seltensten: Soziale Medien liegen hinter NSA

Das Vertrauen in Datenschutz hängt maßgeblich von der Einrichtung ab, die die Daten bearbeitet. Dabei vertrauen die Deutschen am häufigsten den abgefragten Einrichtungen der Gesundheitsbranche – am seltensten hingegen IT- und Telekommunikationsunternehmen.

Ein knappes Jahr nach den Veröffentlichungen Edward Snowdens stellt die Initiative Markt- und Sozialforschung e.V. (ISMF) zum Start der 1. Tour der Marktforschung aktuelle Ergebnisse einer repräsentativen Studie zum Vertrauen in den Datenschutz bei verschiedensten Einrichtungen und Institutionen vor. Zwischen dem 5. und 9. Mai wurden Personen ab 14 Jahren befragt. Die Studie zeigt: Vertrauen in den Schutz persönlicher Daten hängt maßgeblich von der Einrichtung ab, bei welcher die Daten bearbeitet werden.

Insgesamt wurde bei der Studie das Vertrauen in den Datenschutz bei 23 Einrichtungen verschiedenster Branchen abgefragt. Dabei vertrauen 44 Prozent der Befragten dem Datenschutz bei den abgefragten Einrichtungen eher oder sehr. Spitzenreiter sind die Einrichtungen der Gesundheitsbranche, deren Datenschutz mit 76 Prozent die meisten vertrauen. Knapp 55 Prozent der Befragten vertrauen dem Datenschutz öffentlicher Einrichtungen, 51 Prozent vertrauen dem Datenschutz bei Finanzunternehmen und nur 19 Prozent dem Datenschutz bei den abgefragten IT- und Telekommunikationsunternehmen. Bei der Betrachtung der einzelnen Einrichtungen zeigt sich: Am häufigsten vertrauen die Deutschen dem Datenschutz bei der Polizei (82 Prozent) – und trotz des NSA Skandals wird dem Datenschutz bei ausländischen Geheimdiensten (7 Prozent) noch häufiger vertraut als dem Datenschutz bei Sozialen Medien (5 Prozent).

Während Geschlecht und Bildung auf das allgemeine Vertrauen in den Datenschutz keinen Einfluss hat, zeigt sich mit steigendem Alter ein sinkendes Vertrauen in den Umgang mit Daten. Auch der Wohnort hat einen Einfluss – Befragte aus den neueren Bundesländern vertrauen schlechter. Am stärksten ist das Vertrauen in den Datenschutz in Baden-Württemberg.

Das Vertrauen in öffentliche Einrichtungen ist im Mittel mit 55 Prozent überdurchschnittlich stark – ohne Einbezug von Geheimdiensten vertrauen hier sogar 70 Prozent der Deutschen dem Datenschutz. Hier hat der Grad der formalen Bildung einen positiven Einfluss auf das Vertrauen. Während dem Datenschutz bei der Polizei (82 Prozent), Gesetzlichen Pflichtversicherungen (72 Prozent), Kommunalen Einrichtungen (69 Prozent), dem Finanzamt (67 Prozent) und Landes- und Bundeseinrichtungen (60 Prozent) überdurchschnittlich stark vertraut wird, liegen deutsche Geheimdienste (27 Prozent) sowie Ausländische Geheimdienste (7 Prozent) deutlich unter dem Schnitt.

Dem Datenschutz bei allen abgefragten IT- und Telekommunikationsunternehmen wird hingegen unterdurchschnittlich oft vertraut. Im Schnitt vertrauen dem Datenschutz der abgefragten IT-Unternehmen nur knapp 19 Prozent der Befragten. Hier sinkt das Vertrauen in den Datenschutz mit dem Grad der formalen Bildung, der Unterschied zwischen Ost- und Westdeutschland ist hingegen nicht mehr eindeutig. Telefongesellschaften (28 Prozent) schneiden noch am besten ab, gefolgt von Emailkontobetreibern (25 Prozent), Handyherstellern (24 Prozent), Suchmaschinenbetreibern (16 Prozent) und Sozialen Medien (5 Prozent).

Dem Datenschutz aller abgefragten Finanzunternehmen wird hingegen überdurchschnittlich häufig vertraut. Im Schnitt vertrauen 51 Prozent der Befragten den Unternehmen hinsichtlich des Datenschutzes. Vorne liegen Banken und Sparkassen (68 Prozent), gefolgt von Kreditkartengesellschaften und Versicherungen (jeweils 42 Prozent). Bei den abgefragten Finanzunternehmen allgemein ist ein sinkendes Vertrauen in den Umgang mit Daten mit steigendem Alter zu beobachten. Regional betrachtet vertrauen die Baden-Württemberger dem Datenschutz bei Finanzunternehmen am häufigsten, Personen aus Nordrheinwestfalen sowie dem Nordosten am seltensten.

Am stärksten ist das Vertrauen in den Datenschutz in der Gesundheitsbranche (77 Prozent). Trotz der Berichterstattung über den Umgang mit Patientendaten durch Apotheken wird hier dem Datenschutz mit 78 Prozent der Deutschen am zweithäufigsten vertraut. Auch Ärzten und Krankenhäusern vertrauen mit 75 Prozent überdurchschnittlich viele der Deutschen. Zwar hat die Bildung auf das Vertrauen in die Gesundheitsbranche keinen Einfluss, doch die Gruppe der über 59-Jährigen, die ansonsten dem Datenschutz am kritischsten gegenübersteht, vertraut hier deutlich mehr als die 40 bis 59-Jährigen. Die jüngsten bleiben jedoch Spitzenreiter. Mit steigendem Einkommen sinkt jedoch das Vertrauen in den Umgang mit Daten bei Gesundheitseinrichtungen.

Neben diesen Branchen wurde ferner das Vertrauen in den Datenschutz bei Vereinen und Clubs (51 Prozent) Energieversorgern (50 Prozent), Kirchen und Religionsgemeinschaften (49 Prozent), Lotteriegesellschaften (19 Prozent) und Werbeagenturen (8 Prozent) erhoben.

Auch das Vertrauen in den Datenschutz bei Marktforschungsinstituten wurde abgefragt, wobei trotz der strengen und deutlich über das gesetzliche Maß hinausgehenden standesrechtlichen Selbstregulierung mit 40 Prozent der Deutschen nur unterdurchschnittliche viele dem Datenschutz vertrauen. Um den Deutschen die Markt- und Sozialforschung näher zu bringen, über den strengen Datenschutz

der Branche sowie den Mehrwert von Erhebungen für die Gesellschaft und jeden Einzelnen aufzuklären, startete die Initiative Markt- und Sozialforschung am 19. Mai 2014 die 1. Bundesweite Tour der Marktforschung. Alle Infos hierzu unter www.deutsche-marktforscher.de

Nutzung privater E-Mail-Postfächer für dienstliche Zwecke

Eine pauschale Weiterleitung dienstlicher E-Mails auf private E-Mail-Konten von Bediensteten ist nach Auffassung des LfDI Rheinland-Pfalz (Bericht 2012/2013, III, 1 Nr. 1.1) grundsätzlich nicht zulässig. Die Art privater E-Mail-Lösungen und die dabei bestehenden Zugriffsmöglichkeiten sind höchst unterschiedlich und entziehen sich in aller Regel der Beurteilung und Einflussnahme des Dienstherrn sowie in Teilen auch der Inhaberinnen und Inhaber der privaten Postfächer. Aus Sicht des LfDI kann damit der nach § 9 Abs. 2 Nr. 4 LDSG geforderte Schutz vor unbefugter Kenntnisnahme nicht verlässlich sichergestellt werden (vgl. 20. Tb., Tz. 21.3.1).

Die Nutzung privater E-Mail-Konten von Beschäftigten mit dem Ziel, außerhalb der Dienstzeit oder auf Dienstreisen einen Zugriff auf dienstliche Unterlagen zu eröffnen, begegnet damit datenschutzrechtlichen Bedenken. Soweit entsprechende Anforderungen bestehen, sollte hierfür stattdessen ein gesicherter externer Zugriff auf die dienstlichen Postfächer eingerichtet werden (VPN-Zugang, Terminal-Server-Lösung etc.).

In begründeten Einzelfällen mag die Nutzung privater E-Mail-Postfächer fallweise erforderlich sein, etwa bei unvermuteter Abwesenheit und Dringlichkeit einer Rückantwort. Dies muss jedoch auf Ausnahmefälle beschränkt bleiben und darf nicht als allgemeine Form der dienstlichen Kommunikation zugelassen werden. Soweit personenbezogene Daten betroffen sind, sind dabei angemessene Schutzvorkehrungen zur Wahrung der Vertraulichkeit zu treffen (z.B. Verschlüsselung der betroffenen Dokumente).

Die Weiterleitung von Nachrichten ohne Personenbezug ist aus datenschutzrechtlicher Sicht grundsätzlich unbedenklich, es bestehen jedoch Zweifel, ob bei einer routinemäßigen Nutzung in der Praxis eine entsprechende Abschätzung und Differenzierung vorgenommen wird und entsprechende Vorkehrungen getroffen werden.

Im Rahmen einer allgemeinen Regelung sollten damit folgende Punkte berücksichtigt werden:

- Eine pauschale Weiterleitung dienstlicher E-Mails auf private E-Mail-Konten von Bediensteten ist grundsätzlich nicht zugelassen; eingehende Nachrichten sind bei Abwesenheit zunächst entsprechend der bestehenden Vertretungsregelungen weiterzuleiten.
- Die Weiterleitung dienstlicher E-Mails zu privaten E-Mail-Adressen ist nur im Ausnahmefall zulässig und nur, wenn dies aus sachlichen und zeitlichen Gründen zwingend geboten ist. Derartige Ausnahmen bedürfen der Genehmigung.
- Soweit personenbezogene Daten betroffen sind, sind geeignete Maßnahmen zur Wahrung der Vertraulichkeit und Integrität der Daten zu treffen (Verschlüsselung). Für Unterlagen, die im öffentlichen Interesse geheimhaltungsbedürftig sind (Verschlusssachen) gelten die Anforderungen der Verschlusssachenanweisung.
- Die genutzten privaten E-Mailkonten dürfen nur im Zugriff von Beschäftigten der Verwaltung stehen; ein Zugriff

weiterer Nutzerinnen und Nutzer (z.B. von Familienmitgliedern) muss ausgeschlossen sein.

- Die weitergeleiteten dienstlichen Nachrichten sind, wenn ihre Speicherung nicht mehr erforderlich ist, unverzüglich zu löschen.

Werbung und Adresshandel

Ethnomarketing

Eine Auswertung von Namen nach ethnischer und rassischer Herkunft oder Religionszugehörigkeit der Betroffenen für Werbezwecke ist unzulässig. Das Verbot darf nicht durch begriffliche Verschleierung umgangen werden.

Unter der Überschrift „Ethnomarketing" offerierte ein in der Datenanalyse und im Adresshandel tätiges Unternehmen personenbezogene Daten zur ethnischen Herkunft von über 15 Millionen in Deutschland lebenden Konsumenten. Interessenten konnten außerdem ihren vorhandenen Kundendatenbestand im Hinblick auf die wahrscheinliche ethnische Zugehörigkeit des jeweiligen Kunden analysieren lassen. Das Unternehmen warb damit, es könne sowohl für jeden Straßenabschnitt Deutschlands als auch auf Personenebene Wahrscheinlichkeiten der Zugehörigkeit zu den folgenden „Kulturkreisen" ausweisen: deutsch – italienisch – türkisch – griechisch – spanisch – Balkan – osteuropäisch – nordasiatisch – afrikanisch (südlich der Sahara) – außereuropäisch-islamisch – süd-/ost-/südostasiatisch (Indien/Vietnam) – sonstige (Benelux, Frankreich, Großbritannien, Nordeuropa, USA, Kanada) – Spätaussiedler aus der früheren Sowjetunion. Die Zuordnung einer Person erfolge aufgrund einer Vor- und Nachnamenanalyse und eines Abgleichs mit amtlichen Informationen zur Anzahl der Ausländer. „Wer …weiß, wo die unterschiedlichen ethnischen Gruppen wohnen, ist klar im Vorteil!" lautete die Werbebotschaft, und weiter hieß es, „Erkenntnisse aus der Analyse können sofort vertrieblich nutzbar gemacht werden, zum Beispiel für Postwurfsendungen oder zur Selektion kulturkreisbezogener Zielgruppenadressen…".

Im Laufe des datenschutzrechtlichen Überprüfungsverfahrens bestritt das Unternehmen, eine Zuordnung nach ethnischen, rassischen oder religiösen Kriterien vorzunehmen, sondern lediglich nach „Kulturkreisen", die es wechselnd auch als „Sprachkreise" oder „Sprach- und Kulturräume" bezeichnete. Die Zuordnung außereuropäisch-islamischer Kulturkreis wollte das Unternehmen in „außereuropäisch-arabischstämmiger Sprachraum" ändern.

Die angebotene Dienstleistung war rechtswidrig. Das Bundesdatenschutzgesetz erlaubt die Erhebung, Verarbeitung und Nutzung bestimmter sensitiver Daten wie Angaben über die rassische und ethnische Herkunft oder religiöse Überzeugungen nur sehr eingeschränkt (§§ 3 Abs. 9, 28 Abs. 6 bis 9 BDSG).

Das Regierungspräsidium Darmstadt hatte als Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich vor einigen Jahren zugestanden, dass bei einer Auswertung von Namen nach Sprachzugehörigkeit für Werbezwecke der Schutzbereich des § 3 Abs. 9 nicht berührt sei, solange die ausgewählten Personen nicht eindeutig einer Ethnie zugeordnet werden können. In der Regel ist mit einer Sprachzuordnung keine Zuordnung zur ethnischen Herkunft verknüpft. Der Begriff „ethnische Herkunft" ist im ethnologischen Sprachgebrauch durch mehrere Merkmale definiert: Bestimmend sind Religion, Sprache, Abstammung, Herkunft aus oder Ansässigkeit in einer bestimmten geografischen Region, Teilhabe am sozialen Zusammenhang der ethnischen Gruppe, Selbstdefinition als Mitglied der ethnischen Gruppe, Praktizieren der gemeinsam geteilten Kultur der ethnischen Gruppe oder Wissen um diese Kultur. Da die Sprache bei der Bestimmung der ethnischen Herkunft nur ein Element ist, lässt sich aus ihr allein nicht auf die ethnische Herkunft der Person schließen.

Das Angebot beschränkte sich jedoch – entgegen der Meinung des Unternehmens – nicht auf eine Zuordnung zu einem Sprachraum. Es gibt weder einen osteuropäisch-nordasiatischen, afrikanischen (südlich der Sahara) noch einen süd-/ost-/südostasiatischen Sprachraum. Ein osteuropäisch-nordasiatischer Raum würde von Polnisch im Westen bis Jakutisch im Nordosten reichen. Allein in Russland gibt es schätzungsweise 100 Sprachfamilien. Wenn man sich nicht auf die beiden Sprachräume frankophon und anglophon beschränkt, gibt es in Afrika (südlich der Sahara) ca. 2000 Sprachen. Wenig einleuchtend ist auch die Kategorisierung süd-/ost-/südasiatischer Sprachraum mit Sprachen wie z.B. Hindi, Taglog, Koreanisch, Thai, Vietnamesisch, Japanisch oder Chinesisch.

Die als Sprach- oder Kulturkreiszuordnung bezeichnete Kategorisierung vermittelte vielmehr den Eindruck einer verdeckten Klassifizierung nach ethnischen und rassischen Kriterien: Slawen, Eurasier, Mongolenvölker, Asiaten, Schwarzafrikaner. Bezeichnenderweise schlug das Unternehmen daher auch die Kategorie arabischstämmiger (Araber) Sprachraum vor. Dass es sich bei „islamisch" um eine Zuordnung zu einer Religion handelte, war offensichtlich. Das Unternehmen verarbeitete mithin sensitive Daten gem. § 3 Abs. 9 BDSG.

Der Gesetzgeber hat die Verarbeitung der in § 3 Abs. 9 aufgezählten Datenarten an besonders restriktive Anforderungen geknüpft. Diese Beschränkungen dürfen nicht dadurch umgangen werden, dass die Datenarten in andere Datenarten umdefiniert werden, um so dem Anwendungsbereich des § 3 Abs. 9 zu entgehen. Das geschieht, wenn Ethnie und Rasse definitorisch im Begriff Kulturraum, der sich wiederum durch beliebige räumliche Beschränkung oder Erweiterung auf eine Ethnie oder Rasse reduzieren lässt, versteckt werden. Ein Kulturkreis (Kulturraum) kann, muss aber keineswegs weiträumig sein. Der Begriff kann einen globalen (westlicher oder östlicher Kulturkreis), aber auch seinen sehr regionalen Bezug haben (hessischer Kulturraum). Die Bezeichnung Ethnomarketing, mit dem das Unternehmen warb, war durchaus eine adäquate Beschreibung der mit dem Produkt verbundenen Intention, nämlich Werbung, die auf eine nach ethnischen und/oder rassischen Merkmalen definierte Gruppe ausgerichtet ist, zu ermöglichen.

Die Zuordnung erfolgte ohne Wissen und Einwilligung der Betroffenen. Da die Anforderungen des § 28 Abs. 6 bis 9 BDSG nicht erfüllt waren, war sie rechtswidrig. Das Unternehmen hat die Werbung für das Produkt aus seiner Webseite entfernt.

(Hess LfD, 42. TB (2013), 4.4)

Literaturhinweise

Buchbesprechungen

Kevin Marschall, **Entwicklung einer Handlungsanleitung für ein unternehmensinternes Compliance-Management-System.** Optionen zur Begrenzung der rechtlichen Risiken des betrieblichen Datenschutzbeauftragten
Beiträge zu Datenschutz und Informationsfreiheit, Band 3, Verlag Dr. Kovač, Hamburg, 2014, 134 S., 74,80 €

Unter den Risiken, denen durch ein Compliance Management System begegnet werden soll, widmet sich der Autor vorrangig der möglichen strafrechtlichen Haftung des DSB. Bislang sind keine Urteile zur strafrechtlichen Verantwortung von betrieblichen Datenschutzbeauftragten bei Nicht- oder fehlerhafter Wahrnehmung ihrer Pflichten ergangen. Auch in der Literatur finden sich bislang nur sehr wenige Stimmen und Stellungnahmen zur strafrechtlichen Haftungsproblematik von gesetzlich Beauftragten und deren konkreten Handlungspflichten. Es fehlt eine gefestigte Rechtsprechung, an der sich Entscheidungsträger und insbesondere Datenschutzbeauftragte in der Praxis orientieren können.

Der Autor analysiert zunächst die Haftungsrisiken im Bereich Täterschaft durch aktives Tun. Darauf aufbauend beschäftigt er sich mit der Frage, ob und unter welchen Voraussetzungen der Datenschutzbeauftragte als „Gehilfe durch Unterlassen" zu qualifizieren ist und somit für sein (Nicht-)Handeln strafrechtlichen Risiken unterliegt. Eine Handlungsanleitung soll es dem Datenschutzbeauftragten ermöglichen, die Auswirkungen seines Handelns besser abzuschätzen und einen möglichen Reputationsverlust für das Unternehmen und für ihn selbst zu vermeiden.

Abschließend integriert der Autor die Handlungsanleitung in ein 7-stufiges Compliance-Management-System (nach IDW-PS 980), um neben der theoretischen und praktischen Verwertbarkeit der Arbeit den Bezug zu unternehmensinternen Risikomanagement-Systemen herzustellen und um hierdurch die betriebliche Umsetzung der gegebenen Empfehlungen zu erleichtern.

Redaktion

Stephan Weth/Maximilian Herberger/Michael Wächter (Hrsg.), **Daten- und Persönlichkeitsschutz im Arbeitsverhältnis** – Praxishandbuch zum Arbeitnehmerdatenschutz, Verlag C.H.Beck, München, 2014, XXII, 614 S., 89,– €

Die 16 Autoren, zu denen auch die 3 Herausgeber zählen, haben sich mit dem im Titel des Buches ausgewiesenen Thema aus verschiedenen Blickwinkeln befasst. Es handelt sich im Kern um die Zusammenstellung monographischer Einzelbeiträge, die durchweg gut aufeinander abgestimmt sind, wenngleich manche Abgrenzungen (etwa zwischen den Kapiteln A IV und B IX) etwas künstlich wirken.
Über den 32 Kapiteln finden sich beispielsweise folgende Überschriften:

- Internetgegebenheiten mit Bezug zu Persönlichkeitsrecht und Datenschutz (A IV)
- Compliance und interne Revision (A VIII)
- Beschwerderecht des Arbeitnehmers (A XIV)
- Biometrische Verfahren (B IV)
- GPS-Ortung (B V)
- Betriebsrat und Datenschutz (C I)
- Internationaler Datentransfer (C III)
- Outsourcing von IT-Dienstleistungen (C V)

Die Struktur des Buches löst sich im Aufbau von den zu der Thematik bereits vorliegenden Werken und folgt einer Systematik, die manchem nach Lösungen für seine Probleme suchenden Praktiker sehr entgegenkommen dürfte. Die Ausführungen zeichnen sich durchgängig durch eine bemerkenswerte gedankliche Tiefe und dogmatische Durchdringung des behandelten Stoffs aus. Nur ganz vereinzelt erscheint der Bezug zum Arbeitnehmerdatenschutz nicht ganz so eindeutig (vgl. etwa Kapitel A XIII) – interessant bleibt die Lektüre allemal.

Dass sich Schreibstil und Diktion bei den einzelnen Themenblöcken unterscheiden, liegt bei der Vielzahl der Mitwirkenden in der Natur der Sache und behindert die gute Lesbarkeit der Artikel überhaupt nicht – Zwischenüberschriften oder sonstige Untergliederungen z.B. bei einem 20 Druckseiten umfassenden Text (S. 61-83) würden sie allerdings noch erhöhen.

Die Autoren vertreten bisweilen Standpunkte, die sich von der h.M. oder der Rspr. unterscheiden. Dies ist zweifellos als eine zu begrüßende Bereicherung der Diskussion strittiger Fragen anzusehen. Zumindest unschädlich wäre aber ein Hinweis, wenn von höchstrichterlichen Entscheidungen abgewichen wird (z.B. bei der behaupteten Inkompatibilität der Funktion des betrieblichen DSB mit seiner Mitgliedschaft im BR; vgl. S. 167 und demgegenüber BAG, Urteil vom 23.3.2011 – 10 AZR 562/09).

Fazit: Das Werk füllt in überzeugender Weise eine Lücke in den zum Thema schon existierenden Gesamtdarstellungen. Die Lektüre verspricht großen Informationsgewinn und ist sehr empfehlenswert für alle, die sich mit der Materie des Arbeitnehmerdatenschutzes näher auseinandersetzen wollen.

RA Dr. Georg Wronka, Bonn

Thomas Sassenberg/Reto Mantz, **WLAN und Recht. Aufbau und Betrieb von Internet-Hotspots,** Erich Schmidt Verlag, Berlin, 2014, 270 S., kartoniert, 38,–€

Der Internetzugang mittels eines Wireless Local Area Networks (WLAN) hat in

den letzten 15 Jahren einen enormen Erfolg verzeichnet und längst Einzug in unseren Alltag gehalten. Entsprechende Netzwerke kommen nicht mehr nur im privaten Umfeld, sondern z.B. auch in Cafes, Hotels oder Zügen etc. zum Einsatz. Neben punktuellen Anbindungen nehmen auch Lösungen für größere Flächen zu. In vielen Städten gibt es innerstädtisches WLAN, teils von privaten Unternehmen, teils von Kommunen betrieben. Bei ihrer Realisierung gibt es jedoch zahlreiche Rechtsfragen, u.a. zur Störerhaftung. Zudem werden die umfangreichen regulatorischen Bestimmungen als bürokratisches Hemmnis empfunden.

Das Buch nimmt diese Ausgangslage zum Anlass, sich dem Thema WLAN und Recht näher ausführlich zu widmen. Aufgezeigt werden die nach den typischen Betreibermodellen entstehenden Rechtsfragen und die daraus resultierenden Handlungsmöglichkeiten.

Nach einer allgemeinen und einer technischen Einführung werden die aus dem Telekommunikationsrecht für den Betreiber folgenden Anforderungen dargelegt. Dabei werden neben typischen Fragen, z.B. zu Meldepflicht und Datenschutz, auch die Anforderungen an die Öffentliche Sicherheit dargestellt. Die Behandlung der Verantwortlichkeit des Anbieters erschöpft sich nicht in der Darstellung der aktuellen Rechtsprechung zur Störerhaftung sowie der Haftungsprivilegierung nach dem Telemediengesetz. Das Werk

- nennt im Einzelnen mögliche Maßnahmen aus tatsächlicher und rechtlicher Sicht,
- stellt die Konsequenzen für Aufbau und Betrieb eines WLANs dar,
- erläutert, wie sich Anbieter bei Inanspruchnahme, z.B. durch Abmahnung, verhalten sollten.

Auch das Verhältnis zwischen Anbieter und Nutzer wird behandelt. Sie erfahren, wie dieses Rechtsverhältnis – insbesondere bei unentgeltlicher Leistung – einzuordnen ist und welche (AGB-)Regelungen getroffen werden sollten. Weitere erörterte Themen lauten

- Anforderungen aus den Regelungen zum Verbraucherschutz,
- Gestaltung und Webseiten des WLAN-Angebots ,
- Anwendungsbereich des Telemediendatenschutzes,
- Realisierung des Betriebs.

Abgerundet wird das Werk durch Übersichten und Checklisten. Diese ermöglichen nicht nur den schnellen Einstieg in die Materie. Sie dienen auch der Überprüfung interner Prozesse sowie der Durchführung von ersten Compliance-Maßnahmen.

Schriftleitung

Christina Schmidt-Holtmann, **Der Schutz der IP-Adresse im deutschen und europäischen Datenschutzrecht. Zur Auslegung des Begriffs des personenbezogenen Datums,** Beiträge zum Informationsrecht, Band 34, Duncker & Humblot, Berlin, 2014, 212 S., Print: 69,90 €, E-Book: 62,90 €, Print & E-Book: 83,90 €

Sobald ein Internetnutzer online geht, hinterlässt er als Spur seine IP-Adresse, welche die Grundvoraussetzung für das Surfen im Netz ist. Kennt der Staat oder ein Privater die IP-Adresse, kann er den Nutzerweg durch das Internet problemlos nachverfolgen und unter Umständen die Identität des Nutzers ermitteln. So entsteht das Bedürfnis nach einem wirksamen Schutz von IP-Adressen während und nach der Internetnutzung.

Ergebnis der Arbeit ist, dass IP-Adressen personenbezogene Daten sind und somit dem Datenschutzrecht unterfallen. Die Frage nach dem Personenbezug von IP-Adressen kann aber nicht alleine auf Grundlage des deutschen Rechts beantwortet werden, denn das Bundesdatenschutzgesetz wird von weiteren, insbesondere europäischen, Regeln bestimmt und geprägt. So kennen insbesondere die allgemeine Datenschutzrichtline und Artikel 8 der Grundrechtscharta den Begriff der personenbezogenen Daten. Die deutsche Norm muss daher einer richtlinien- und europakonformen Auslegung unterzogen werden. Nach dem Ergebnis der Untersuchung gibt auch das europäische Recht vor, dass IP-Adressen als personenbezogene Daten zu behandeln sind.

Die Arbeit wurde mit dem Wissenschaftspreis 2012 des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und dem Förderpreis 2013 des Freundeskreises Trierer Universität ausgezeichnet.

Der Inhalt ist im Einzelnen wie folgt gegliedert:

A. Einführung in die Thematik und Darstellung der Untersuchung

B. Einführung in die technischen Grundlagen und Regelungsansätze des Datenschutzes im Internet. Technische Grundlagen – Regelungsansätze für das Datenschutzrecht im Internet

C. Die nationale datenschutzrechtliche Situation in Bezug auf den Schutz von IP-Adressen. Die Behandlung von IP-Adressen im deutschen Recht – Fazit

D. Europarechtliche Vorgaben für den Datenschutz. Sekundärrecht – Grundrechtliche Gewährleistungen – Primärrecht – Bestimmung des europäischen Prüfungsmaßstabs (Ergebnis)

E. Zusammenfassende Bewertung
Literatur- und Sachwortverzeichnis

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.

Stefan Brink/Tim Wybitul, **Der „Neue Datenschutz" des BAG, ZD 2014, S. 225**
Der Beitrag versucht an Hand einer Reihe aktueller Entscheidungen des BAG zu belegen, dass das BAG der Zulässigkeitsnorm des § 32 BDSG durch wesentliche Auslegungshinweise mehr Klarheit und Gewicht gegeben hat. Zutreffend ist insoweit, dass das grundsätzlich maßgebende Verhältnismäßigkeitsprinzip noch deutlicher herausgearbeitet wurde und der Umfang des Persönlichkeitsschutzes im Beschäftigungsverhältnis nicht davon abhängt, ob § 75 Abs. 2 BetrVG, Art. 2 Abs. 1 GG oder § 32 BDSG als Maßstab herangezogen wird.

Holger Greve, **Korruptionsbekämpfung und Whistleblowing, ZD 2014, S. 336**
Der Beitrag widmet sich der Auflösung des Konflikts zwischen Transparenz der Datenverarbeitung, Informationsfreiheit und dem Informantenschutz (externer) Whistleblower. Die für die Zulässigkeit der Hinweisweitergabe geltenden Grundsätze, nämlich dass die Vorwürfe berechtigt sind, nicht aus unlauteren Motiven heraus erhoben wurden, die Veröffentlichung im öffentlichen Interesse liegt und vor der Anzeige grundsätzlich ein Versuch interner Klärung durchgeführt wird, sollten nach Auffassung des Autors Gegenstand einer gesetzlichen Normierung werden.

Jens Hammersen/Ulrich Eisenried, **Ist „Redlining" in Deutschland erlaubt?, ZD 2014, S. 342**
Als Redlining wird ein Procedere bezeichnet, bei dem nach Auswertung soziodemografischer Daten Bewohnern eines bestimmten Gebiets Waren (z.B. nur gegen Vorkasse) oder Dienstleistungen (speziell Kredite) nicht oder nur verteuert angeboten werden. Die Bestimmung des § 28b Abs. 3 BDSG untersagt es zwar, für Verhaltensprognosen ausschließlich Adressdaten heranzuziehen. Im Rahmen des die Prognose aufstellenden Algorithmuses muss auch anderen Daten eine wesentliche Bedeutung zukommen. Diese Einschränkung soll nach § 10 Abs. 2 KWG jedoch für Finanzdienstleister nicht gelten. Den Interessen des Betroffenen müsse durch eine extensivere Auslegung des Auskunftsanspruchs des § 34 Abs. 4 S. 2 Nr. 4 BDSG Rechnung getragen werden.

Jochen Konrad-Klein, **„Recht auf Vergessen" im Personalwesen, CuA 6/2014, S. 13**
Auf die Höchsthaltbarkeitsdaten für Personaldaten bzw. auf die Einhaltung gesetzlicher Löschungsfristen weist der Beitrag hin und sieht in der Kontrolle der Einhaltung dieser Verpflichtung eine wichtige Aufgabe der Mitarbeitervertretung.

Matthias Lachenmann/Sebastian Schwiering, **Betrieb von Videokameras in PKW: Datenschutzrechtliche (Un-)Zulässigkeit des Betriebs von On-Board-Kameras in PKWs, NZV 2014, S. 291**
Die Autoren untersuchen die rechtliche Zulässigkeit von Kameras im Straßenverkehr. Die Innenüberwachung des öffentlichen Nachverkehrs halten Sie bei Einhaltung formaler Anforderungen für zulässig, in Taxis hingegen für unzulässig. Den Einsatz von Dashboard-Kameras bei privaten PKW halten die Autoren regelmäßig für unzulässig.

Robert Rothmann, **Videoüberwachung und Auskunftsrecht, DuD 2014, S. 405**
Nachgewiesen wird, dass ein visueller Auskunftsanspruch bei Videoaufzeichnung in der Praxis auf erhebliche Widerstände stößt.

Annika Selzer, **Datenschutz bei internationalen Cloud Computing Services, DuD 2014, S. 470**
Der Beitrag zeigt die Notwendigkeit einer zweistufigen Zulässigkeitsprüfung bei der Nutzung eines Cloud Services, der von einem Cloud Anbieter in einem Drittstaat betrieben wird.

Katrin Sommer, **Personalinformationssysteme im radikalen Wandel, CuA 6/2014, S. 4**
Lag bisher der Schwerpunkt von Personalinformationssystemen noch oft auf dem Verwalten der Personaldaten, wächst der Markt für Software zur strategischen Personalplanung und zum Talent-Management, wobei zunehmend subjektive Bewertungen und per Algorithmen ermittelte Vermutungen über zukünftiges Mitarbeiterhalten unter dem Aspekt des Successfaktors einfließen. Diese Entwicklungen gilt es sorgsam datenschutzkritisch zu beobachten.

Tim Wybitul, **Neue Spielregeln bei Betriebsvereinbarungen und Datenschutz, NZA 2014, S. 225**
Der Autor nimmt die Entscheidung des BAG (NZA 2013, 1433 und NZA 2014, 551) zur Zulässigkeit von Tor- bzw. Taschenkontrollen zum Anlass, die von dem Gericht erstellten Kriterien für eine das BDSG verdrängende Zulässigkeitsregelung darzustellen. Die Regelung wurde als rechtmäßig angesehen, da sie unter Beachtung des Verhältnismäßigkeitsprinzips die Interessen des Arbeitgebers und der Beschäftigten angemessen berücksichtigte. Bemerkenswert ist, dass der Umfang der Pflicht zur Wahrung des Persönlichkeitsrechts an der Vorgabe des § 75 Abs. 2 BetrVG gemessen wurde und die Prüfung des § 32 BDSG dahingestellt wurde, weil der Schutzanspruch des Beschäftigten nach § 75 Abs. 2 BetrVG und § 32 BDSG deckungsgleich sei.

Freund und Helfer

In den USA hat jemand darauf geklagt, seinen Computer heiraten zu dürfen. Er sei ihm in allen Belangen lieb und alles andere als das Recht ihn zu heiraten sei eine Ungleichbehandlung von Computerliebenden. Wer Gefallen an diesem Gedanken findet, der kann es ja mal bei Siri versuchen. Das ist die freundliche Stimme aus dem iPhone, die in allen Lebenslagen für einen da ist. Auch sie kann man fragen: „Willst Du mich heiraten?“ Siri antwortet immer, auch in diesem Fall. Das fällt dann aber abweisend oder ausweichend aus. Sie fragt etwa zurück, ob man sich für Brautmoden oder für eine Partnervermittlung interessiert.

Auch wenn sie selbst keine Heiratsabsichten hat, geht Siri aber im Gegenzug ganz schön ran. Sie schickt dann Nachrichten wie: „Ich weiß nicht, wo Du bist. Du kannst es mir aber zeigen. Aktiviere dazu einfach in den Einstellungen unter „Datenschutz“ sowohl die „Ortungsdienste“ als auch unter „Ortungsdienste“ die Option „Siri“.“ Das hört sich nach Interesse an. Siri fragt aber noch genauer nach, und legt mit folgenden Worten nach: „Ich kenne Deine Privatadresse nicht. Ich weiß eigentlich gar nichts über dich. Tippe in den Siri-Einstellungen auf „Meine Info“ und wähle dann in den Kontakten deinen Namen. Dann weiß ich, wer Du bist.“

Das macht man vielleicht besser nicht, denn schließlich weiß man ja auch nicht wer Siri ist. Sicher ist nur, dass sie Amerikanerin und ein öffentlicher Cloud-Dienst ist, der nicht nur auf alles antwortet, was man ihn fragt, sondern der auch alles behält, was man ihm anvertraut. Als Cloud-Dienst ist Siri keine Wolke, aus dem sich alles verflüchtigt, sondern ein Stahlschrank, zu dem Apple einen Schlüssel hat und den die NSA und sicher auch der chinesische Geheimdienst und wer weiß wer noch alles überwachen. Auch wenn man Siri also noch so schätzt und sie einem hilfreich erscheint, sollte man ihr keine Geheimnisse anvertrauen.

Für 100%ige Datenschutzkonzepte

Bundesdatenschutzgesetz (BDSG)

Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften

Von **Dr. jur. Hans-Jürgen Schaffland**, RA und Justitiar des Deutschen Genossenschafts- und Raiffeisenverbandes e. V. i. R., und **Dipl.-Kfm. Noeme Wiltfang**, Abteilungsleiter Datenverarbeitung i. R. im Deutschen Genossenschafts- und Raiffeisenverband e. V.

Loseblattwerk und Datenbank

Die Grundlage für optimalen Datenschutz ist eine verlässliche, aktuelle Informationsquelle. Genau das bietet Ihnen der „**Schaffland/Wiltfang**". Er macht den Zugriff auf andere Gesetzesveröffentlichungen überflüssig, denn er enthält

- das vollständig kommentierte BDSG,
- alle Landesdatenschutzgesetze und Auszüge aus wichtigen, vom BDSG tangierten Gesetzen.

Umfassende Regelungen zu Werbung, Scoring, Arbeitnehmerdaten sowie Meldepflichten bei Datenschutzpannen – der Gesetzgeber hat das Problem Datenschutz erkannt. Bei der täglichen Umsetzung helfen Ihnen

- praktische Beispiele und Hinweise,
- konkrete Formulierungsvorschläge,
- Checklisten zur Prüfung der Zulässigkeit der Datenverarbeitung, der Datennutzung und zu Benachrichtigungspflichten,
- Lösungsvorschläge für die Bewältigung der Datensicherungsmaßnahmen nach § 9 und der Anlage zu § 9,
- der Leitfaden zum PC-Einsatz.

www.BDSGdigital.de

ESV ERICH SCHMIDT VERLAG

Auf Wissen vertrauen

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