ISSN 0178-8930

G 20 141

RDV

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

6/2014

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

GOLA/WRONKA, Individuelle und pauschale Mitarbeiterbefragungen – arbeits- und datenschutzrechtliche Grenzen von Auskunftspflichten

LÜDEMANN/SENGSTACKEN/VOGELPOHL, Pay as you drive: Datenschutz in der Telematikversicherung

NEUMANN, Telekommunikationsdatenschutz für geschlossene Benutzergruppen nach der TKG-Novelle 2012. Sind Betreiber von Krankenhäusern, Hotels und Gaststätten beim Angebot von Telekommunikationsdiensten noch an §§ 91 ff. TKG gebunden?

Kurzbeiträge

GOLA, Aus den aktuellen Berichten der Aufsichtsbehörden (16): Datenschutz in der Schule

BITTNER, Das Datenschutzaudit bei Auftragsdatenverarbeitern – Ein Überblick über Anforderungen und bisherige Entwicklungen

WEIß, Die Struktur der Aufsichtsbehörden in den EU-Staaten und deren Kompetenzen – ein aktueller Überblick

KIESCHE, Datenschutz im BEM

Rechtsprechung

Aus dem Inhalt

BGH, Sorgfaltspflicht bei elektronischer Rechtsanwalts Handakte (Ls)

BGH, Islamisches Kopftuch und Annahmeverzug (Ls)

BAG, Deutliche Mitteilung der Schwerbehinderung bei der Bewerbung (Ls)

BAG, Anhörung des Arbeitnehmers vor einer Verdachtskündigung

30. Jahrgang
Dezember 2014
Seiten 291–356

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

30. Jahrgang 2014
Heft 6
Seiten 291–356

RDV
Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 291

Veranstaltungen 292

Aufsätze

Prof. Peter GOLA/RA Dr. Georg WRONKA
Individuelle und pauschale Mitarbeiterbefragungen – arbeits- und datenschutzrechtliche Grenzen von Auskunftspflichten 293

Prof. Dr. Volker LÜDEMANN, Christin SENGSTACKEN, LL.M., Kerstin VOGELPOHL
Pay as you drive: Datenschutz in der Telematikversicherung 302

Andreas NEUMANN
Telekommunikationsdatenschutz für geschlossene Benutzergruppen nach der TKG-Novelle 2012. Sind Betreiber von Krankenhäusern, Hotels und Gaststätten beim Angebot von Telekommunikationsdiensten noch an §§ 91 ff. TKG gebunden? 307

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten der Aufsichtsbehörden (16): Datenschutz in der Schule 313

Timo BITTNER
Das Datenschutzaudit bei Auftragsdatenverarbeitern. Ein Überblick über Anforderungen und bisherige Entwicklungen 315

Steffen WEIß, LL.M.
Die Struktur der Aufsichtsbehörden in den EU-Staaten und deren Kompetenzen – ein aktueller Überblick 319

Dr. Eberhard KIESCHE
Datenschutz im BEM 321

Rechtsprechung

Sorgfaltspflicht bei elektronischer Rechtsanwalts Handakte (Ls)
(BGH, Beschluss vom 09.07.2014) 328

Islamisches Kopftuch und Annahmeverzug (Ls)
(BAG, Urteil vom 24.09.2014) 328

Deutliche Mitteilung der Schwerbehinderung bei der Bewerbung (Ls)
(BAG, Urteil vom 18.09.2014) 328

Anhörung des Arbeitnehmers vor einer Verdachtskündigung
(BAG, Urteil vom 20.03.2014) 328

Zur Pflicht zur Angabe von Vorstrafen
(BAG, Urteil vom 20.03.2014) 331

Manipulation von Akten zur Verschleierung von Pflichtverstößen
(BAG, Urteil vom 23.01.2014) 336

Videoüberwachung im Eingangsbereich eines Bürogebäudes
(OVG Lüneburg, Urteil vom 29.09.2014) 337

Zur Mitbestimmung des Personalrats bei der Bestellung des Vertreters des behördlichen Datenschutzbeauftragten (Ls)
(HessVGH, Beschluss vom 22.07.2014) 343

Tätowierung im Eignungsauswahlverfahren zum Polizeivollzugsdienst der Bundespolizei (Ls)
(HessVGH, Beschluss vom 09.07.2014) 343

Anspruch auf Löschung intimer Bilder nach Beziehungsende (Ls)
(OLG Koblenz, Urteil vom 20.05.2014) 343

Unzulässige Verwendung von Bestandsdaten zu Werbezwecken (Ls)
(OLG Koblenz, Urteil vom 26.03.2014) 344

Keine Bereitstellung eines separaten Telefon- und Internetanschlusses für den Betriebsrat
(LAG Niedersachsen, Beschluss vom 30.07.2014) 344

Pflicht zur Vorlage eines erweiterten Führungszeugnisses (Ls)
(ArbG Gelsenkirchen, Urteil vom 04.07.2014) 345

Private Aufnahmen mit einer Dash-Cam unterliegen einem Beweisverwertungsverbot
(AG München, Beschluss vom 13.08.2014) 345

Keine mutmaßliche Einwilligung für E-Mail-Fortbildungsangebot an Rechtsanwälte
(AG Leipzig, Urteil vom 18.07.2014) 347

Berichte, Informationen, Sonstiges

Marktmacht und informationelle Selbstbestimmung 349

Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert 349

EU-DS-GVO: Datenschutzneuregelung in Europa 350

9 Millionen Deutsche haben Partner im Internet gesucht 350

Bundesinnenministerium legt am 19.8.2014 Entwurf für IT-Sicherheitsgesetz vor 350

DSRI Herbstakademie 2014 351

Literaturhinweise

Buchbesprechungen

Michael Wächter, Datenschutz im Unternehmen
(REDAKTION) 353

Ute Schliesky/Christian Hoffmann/Anika D. Luch/Sönke E. Schulz/Kim Corinna Borchers, Schutzpflichten und Drittwirkung im Internet. Das Grundgesetz im digitalen Zeitalter (REDAKTION) 353

Stefan Strohmeier/Franca Piazza (Hrsg.), Human Resource Intelligence und Analytics (SCHRIFTLEITUNG) 354

Spiros Simitis (Hrsg.), Bundesdatenschutzgesetz (GOLA) 354

Neuerscheinungen

Aufsätze 355

Nachgefasst 356

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

Prof. Dr. Rolf SCHWARTMANN, Fachhochschule Köln

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

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

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

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

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

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

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

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

Prof. Dr. Karl LINNENKOHL, Universität Kassel

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

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

Prof. Dr. Michael RONELLENFITSCH, Hessischer Datenschutzbeauftragter

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

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

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

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

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis GDD-Mitteilungen 6/2014; 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.

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

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

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

Erscheinungsweise
6 x jährlich

Bezugspreis

Jahresabonnement	€ 139,–
Einzelheft	€ 25,–

MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Bestellungen
DATAKONTEXT
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 6
Seiten 291–356

RDV
Recht der Datenverarbeitung

30. Jahrgang · Dezember 2014 · Seiten 291–356

Editorial

30 Jahre RDV

Der mit diesem Heft abgeschlossene 30. Jahrgang der RDV bietet Gelegenheit für einen Rückblick.

Anlass für die Herausgabe der Zeitschrift war das Anliegen der 1976 gegründeten GDD, ihrem ständig wachsenden Mitgliederkreis ein auf die vielfältigen Ausprägungen des Datenschutzrechts eingehendes Publikationsorgan an die Hand zu geben. Da die GDD-Mitglieder ein breites Spektrum wirtschaftlicher, wissenschaftlicher und gesellschaftlicher Bereiche repräsentieren, sollten auch die zu behandelnden Themen möglichst weit gefächert werden. Allerdings wurde die RDV nicht als verbandstypisches Mitgliederperiodikum konzipiert, sondern als unabhängige Fachzeitschrift, die auch sonstige Interessenten ansprechen sollte.

Dies geschah zu einem Zeitpunkt, als sich das Datenschutzrecht mit einer besonderen Dynamik entwickelte. Die Diskussion über die Notwendigkeit der Novellierung des am 1. Februar 1977 verkündeten BDSG war in vollem Gang. Konkrete Änderungsvorschläge waren bereits Anfang 1980 eingebracht worden; die nächsten Gesetzentwürfe folgten 1983 und 1984. Das vom Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 kreierte „Recht auf informationelle Selbstbestimmung" befruchtete das Schrifttum und die Rechtsprechung in nicht geahntem Ausmaß, und nicht zuletzt spielte das europäische Datenschutzrecht eine immer stärkere Rolle.

Die Schriftleitung legte stets Wert auf eine ausgewogene Balance von wissenschaftlich ausgerichteten Aufsätzen und stärker praxisorientierten Beiträgen, wobei sie ein besonderes Interesse am Arbeitnehmerdatenschutz nicht verhehlen will. Die RDV, inzwischen wohl die auflagenstärkste sich dem Datenschutzrecht widmende Fachzeitschrift, erscheint im Zweimonats-Turnus. Die Zeit zwischen den Druckausgaben überbrückt die jüngst ins Leben gerufene RDV-Online. Sie beschränkt sich inhaltlich auf wenige, kurz abgehandelte Themen und einen Nachrichtendienst.

Es ist sicherlich nicht verwunderlich, dass sich im Lauf der Jahre die Akzente bei den in der Zeitschrift behandelten Themen etwas verlagerten. Sie beziehen sich heute vielfach auf Probleme, die vor 30 Jahren noch keine Bedeutung hatten, ja noch nicht einmal in Fragen gekleidet werden konnten. Soziale Netzwerke – um ein Beispiel zu nennen – bieten inzwischen den Einstieg in eine zweite Lebenswelt, die die reale Welt aus dem Blick geraten lässt. Was wir nicht wissen. liefert Google, und weil wir das wissen, wissen wir immer weniger. Trotz alledem: Das gedruckte Wort hat sein Gewicht und seinen eigenen Wert nicht verloren und wird sich gegenüber der Online-Information in ihren diversen Erscheinungsformen auch weiterhin behaupten.

Deshalb: Ad multos annos, RDV!

RA Dr. Georg Wronka,
verantwortlicher Schriftleiter
1985 - 1994

Prof. Peter Gola,
verantwortlicher Schriftleiter
seit 1995

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

Dr. Georg Wronka
Rechtsanwalt, beratende und gutachterliche Tätigkeit auf dem Gebiet des Datenschutz- und Wettbewerbsrechts; betrieblicher Datenschutzbeauftragter

Termin	Thema	Ort	Kontakt
26.-27.01.2015	GDD-Winter-Workshop	Garmisch-Partenkirchen	GDD e.V. und DATAKONTEXT
19.02.2015	Datenschutz und Videoüberwachung – Was geht und was geht nicht?	Köln	GDD e.V. und DATAKONTEXT
24.02.2015	Personalprozesse datenschutzkonform organisieren	Köln	GDD e.V. und DATAKONTEXT
23.-27.02.2015	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
03.03.2015	Internationaler Datenverkehr – Wie organisiere ich den Datenschutz?	Köln	GDD e.V. und DATAKONTEXT
05.03.2015	Big Data-Analysen und der Datenschutz	Köln	GDD e.V. und DATAKONTEXT
02.-06.03.2015	Der Auditor zur Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
09.-10.03.2015	Datenschutz Kompakt	Münster	GDD e.V. und DATAKONTEXT
09.-10.03.2015	ARGE Datenschutz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
16.03.2015	SAP-Funktionen für den Datenschutz	Köln	GDD e.V. und DATAKONTEXT
18.03.2015	Die neue Herausforderung im Datenschutz: Connected Car bei der Dienstwagennutzung	Köln	GDD e.V. und DATAKONTEXT
17.-19.03.2015	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Köln	GDD e.V. und DATAKONTEXT
23.-25.03.2015	Das SAP-System für Datenschutzbeauftragte	Stuttgart	GDD e.V. und DATAKONTEXT
24.-25.03.2015	Was Betriebsräte vom Datenschutz wissen müssen	Frankfurt/M.	GDD e.V. und DATAKONTEXT
25.03.2015	Social Media im Unternehmen – aber sicher!	Düsseldorf	GDD e.V. und DATAKONTEXT
30.03.2015	Der Datenschutzbeauftragte mit wenig Zeitbudget	Frankfurt/M.	GDD e.V. und DATAKONTEXT
31.03.2015	Kundendatenschutz	Köln	GDD e.V. und DATAKONTEXT
14.04.2015	Dienstliche Nutzung privater IT – Bring Your Own Device aus Arbeitgebersicht	Köln	GDD e.V. und DATAKONTEXT
14.04.2015	Kontrolle von Auftragnehmern im Rahmen der Auftragsdatenverarbeitung	Stuttgart	GDD e.V. und DATAKONTEXT
15.04.2015	Datenschutzaudit leicht gemacht	Köln	GDD e.V. und DATAKONTEXT
21.04.2015	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
23.04.2015	Toolgestütztes Datenschutz-Management	Köln	GDD e.V. und DATAKONTEXT
23.-24.04.2015	Fachtagung Datenschutz International	Berlin	GDD e.V. und DATAKONTEXT
28.04.2015	Grundlagen der Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
27.-28.04.2015	Datenschutz Management – Teil 3	Köln	GDD e.V. und DATAKONTEXT

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

Aufsätze

Prof. Peter Gola/RA Dr. Georg Wronka

Individuelle und pauschale Mitarbeiterbefragungen – arbeits- und datenschutzrechtliche Grenzen von Auskunftspflichten

Der Beitrag zeigt an typischen Fällen der betrieblichen Praxis auf, wann Datenerhebungen im Rahmen der Durchführung des Beschäftigungsverhältnisses sowohl im Interesse des Arbeitgebers als auch des Arbeitnehmers erforderlich sind, wann eine Offenbarungspflicht des Mitarbeiters besteht bzw. wann die Erhebung nur anonym und auf freiwilliger Basis erfolgen darf.

I. Vorbemerkungen

Bei Befragungen von Mitarbeitern im laufenden Arbeitsverhältnis kann es einmal um individuelle, d.h. von dem jeweiligen einzelnen Mitarbeiter zu erhaltende, Informationen gehen; zum anderen kann es sich um pauschale Befragungen handeln, mit denen Zustände im Unternehmen oder ein Meinungsbild der Belegschaft zu bestimmten Sachverhalten ermittelt werden sollen. Individuelle Befragungen können ihren Anlass auch darin haben, dass dem Betroffenen ein Anhörungsrecht zusteht bzw. der Arbeitgeber Maßnahmen erst ergreifen kann, wenn er dem Betroffenen zumindest Gelegenheit zur Stellungnahme gegeben hat.

Im Übrigen hat der Arbeitgeber ebenso wie gegenüber Bewerbern auch gegenüber bereits Beschäftigten[1] ein „Fragerecht", dem korrespondierend Auskunftspflichten der Mitarbeiter gegenüberstehen. Bestimmt wird der Gegenstand des Datenerhebungsrechts dadurch, ob die Information für die Durchführung des Beschäftigungsverhältnisses erforderlich ist (§ 32 Abs. 1 S. 1 BDSG; sowie z.B. für den öffentlichen Dienst: § 29 Abs. 1 S. 1 LDSG NW; § 100 BBG, § 34 Abs. 4 LBeamtG NW). Die Erforderlichkeit setzt voraus, dass der Arbeitgeber die Information zur Wahrnehmung seiner Rechte und Pflichten aus dem Beschäftigungsverhältnis benötigt und der Verhältnismäßigkeitsgrundsatz[2] gewahrt ist. Vorschriften für den öffentlichen Dienst erstrecken die zulässige Zweckbestimmung darüber hinaus darauf, dass auch zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, benötigte Verarbeitungen gestattet sind. Im Geltungsbereich des BDSG ist hinsichtlich dieser Verwendungen zu prüfen, ob die Organisation oder Planung noch im Zusammenhang mit der Durchführung des einzelnen Beschäftigungsverhältnisses steht; ansonsten wäre bei „beschäftigungsfremden" Verwendungen § 28 Abs. 1 S. 1 Nr. 2 BDSG als Rechtsgrundlage heranzuziehen[3].

Bei Verarbeitungen im Geltungsbereich des BDSG bedarf es bei sensiblen Daten eines „rechtlichen Anspruchs", zu dessen Wahrnehmung oder Abwehr die Information durch den Beschäftigten benötigt wird (§ 28 Abs. 6 Nr. 3 BDSG). Die Vorschriften für den öffentlichen Dienst weisen keine entsprechende Regelung auf.

Die Anforderungen des BDSG entfallen, wenn Befragungen der Mitarbeiter anonym erfolgen bzw. erfolgen müssen, weil – wie es bei allgemeinen Mitarbeiterumfragen regelmäßig der Fall ist – die Kenntnis der Informationsgeber nicht erforderlich ist.

II. Anhörungsrechte bzw. -pflichten

1. Allgemeines

Anhörungsrechte der Beschäftigten haben ihren Ursprung u.a. in dem Anspruch auf Persönlichkeitsrechtschutz des Mitarbeiters und der Fürsorgepflicht des Arbeitgebers. Relevant ist das Recht des Mitarbeiters, in betrieblichen Angelegenheiten, die seine Person betreffen, von den hierfür zuständigen Personen gehört zu werden. Im Besonderen kann er verlangen, dass die Beurteilung seiner Leistungen sowie die Möglichkeiten seiner beruflichen Entwicklung im Betrieb erörtert werden. Er ist berechtigt, zu Maßnahmen des Arbeitgebers, die ihn betreffen, Stellung zu nehmen sowie Vorschläge für die Gestaltung der Arbeitsplätze und des Arbeitsablaufs zu machen (§ 82 BetrVG)[4].

„Erörterung" bedeutet einen Dialog zwischen Arbeitgeber und Mitarbeiter. Die Ansprache von Möglichkeiten des beruf-

1 Zu „Fragerecht und Offenbarungspflicht" im Zusammenhang mit der Begründung des Beschäftigungsverhältnisses vgl. Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, 6. Aufl., Rn. 456 ff.

2 Zu diesem Grundsatz zuletzt BAG, RDV 2014, S. 272.

3 Zur Verarbeitung sog. beschäftigungsfremder Daten vgl. Gola/Schomerus, BDSG, 12. Aufl. § 32 Rn. 45 ff.

4 Im Beamtenverhältnis kann eine Auswahlentscheidung, die auf eine dem Beamten nicht bekanntgegebene Beurteilung zurückgreift, rechtlich fehlerhaft und nicht verwertbar sein; OVG NRW vom 15.3.2013 – 1 B 133/13–; vom 27.6.2013 – 6 A 63/12 –.

lichen Aufstiegs, die damit ggf. verbundene Notwendigkeit weiterer Qualifizierungsmaßnahmen oder geplante Schritte im Hinblick auf die künftige Einordnung des Mitarbeiters infolge veränderter Arbeitsbedingungen führen in der Regel zu einem wechselseitigen Informationsaustausch. Fragen des Arbeitgebers an den Mitarbeiter etwa zur Bereitschaft, an Schulungen teilzunehmen, oder nach persönlichen Interessen, die für die Besetzung eines Arbeitsplatzes relevant sein können („IT-Freak"), liegen im Zulässigkeitsspektrum des arbeitgeberseitigen Fragerechts nach § 82 BetrVG bzw. Erhebungsrechts gem. § 32 BDSG.

2. Personalakten

Dem aus dem Recht auf informationelle Selbstbestimmung fließenden Gebot der Transparenz trägt das Anhörungsrecht Rechnung, das Beschäftigten vor Aufnahme negativer Vorgänge in ihre Personalakte eingeräumt ist. Für Angehörige des öffentlichen Dienstes ist dieses Recht ausdrücklich normiert (z.B. § 109 BBG; § 86 LBeamtG NW, § 3 Abs. 6 TV-L)[5].

Nimmt der Arbeitgeber für den Arbeitnehmer nachteilige Vorgänge und Unterlagen unter Verstoß gegen das Anhörungs- und Erörterungsrecht zu den Personalakten, so ist die Speicherung rechtswidrig; ob die Rechtswidrigkeit durch eine nachträgliche Anhörung geheilt werden kann, ist strittig.

Daraus ergibt sich, dass der Arbeitgeber auch gehalten ist, eine den Arbeitnehmer betreffende Beurteilung zu begründen und vor ihrer endgültigen Fassung mit dem Arbeitnehmer zu erörtern und eventuelle berechtigte Einwände bereits bei der endgültigen Abfassung zu berücksichtigen[6].

Es herrscht Übereinstimmung, dass diese Anhörungsrechte auch für sonstige Arbeitsverhältnisse, in denen derartig formulierte Ansprüche nicht bestehen, Geltung haben, sei es, dass hierzu § 82 Abs. 1 BetrVG herangezogen wird, sei es, dass das Anhörungs- und Erörterungsrecht aus einer vertraglichen Nebenverpflichtung des Arbeitgebers abgeleitet wird. Im Rahmen der das Verhältnis zwischen Dienstherrn/Arbeitgeber und Mitarbeiter gestaltenden Prinzipien der Offenheit und des Vertrauens verlangt die Fürsorgepflicht vom Arbeitgeber, aus einem Sachverhalt nur dann eine für den Beschäftigten ungünstige Folgerung zu ziehen, wenn er diesem zuvor Gelegenheit gegeben hat, zu diesem Sachverhalt Stellung zu nehmen und Erklärungen darüber abzugeben, wie er zu seiner Handlungsweise gekommen ist. Ein Beispiel ist der Ablauf einer Verdachtskündigung.

3. Verdachtskündigung

Verdächtigt der Arbeitgeber den Arbeitnehmer einer Straftat oder schweren Vertragsverletzung, so kann bereits der diesbezügliche Verdacht den Grund für eine Kündigung darstellen. Im Streitfall muss der Arbeitgeber nachweisen, dass er vor Ausspruch der Kündigung alle zumutbaren Anstrengungen unternommen hat, um den Sachverhalt umfassend aufzuklären. Insoweit gebietet die aus dem Rechtsstaatsprinzip abgeleitete Unschuldsvermutung, auch entlastenden Indizien nachzugehen. Bereits deshalb ist dem Beschäftigten die Möglichkeit zur Entlastung durch eine eigene Stellungnahme zu geben[7]. Ohne die Anhörung bzw. die Gelegenheit hierzu ist die Kündigung nicht ultima ratio[8] und damit unwirksam[9]. Eine Pflicht des Arbeitgebers zur persönlichen Anhörung besteht zwar nicht; gleichwohl ist es zweckmäßig und in der Praxis üblich, den Sachverhalt in einem zu dokumentierenden Gespräch zu erörtern. Bei der Einladung zu dem Anhörungsgespräch muss das Thema konkret benannt sein, damit der Betroffene sich hierauf einstellen kann[10].

Das alles hat, wenn es um eine außerordentliche Kündigung geht, unter Beachtung der Zwei-Wochen-Frist des § 626 Abs. 2 BGB zu geschehen. Die Frist des § 626 Abs. 2 BGB beginnt erst nach einem im Allgemeinen innerhalb einer Woche angesetzten Anhörungstermins zu laufen[11]. Bleibt der Arbeitnehmer der Anhörung fern oder verzögert er diese, hat der Arbeitgeber die an ihn gestellten Anforderungen erfüllt[12].Dies kann auch bei unfreiwilligem Schweigen des Arbeitnehmers gelten. Anders ist es bei Nichterscheinen wegen Krankheit oder Urlaub. Hier ist aber im jeweiligen Einzelfall zu prüfen, ob der Ablauf der Kündigungsfrist gehemmt ist, weil die Einholung der Stellungnahme des Beschäftigten tatsächlich unmöglich ist und ob weiteres Zuwarten zumutbar ist.

III. Personenbezogene Befragungen

1. Allgemeines

Inhalt und Art und Weise, wie die Arbeitnehmer relevante Informationen mitzuteilen haben, kann der Arbeitgeber auf Grund seines Direktionsrechts festlegen. Sein Weisungsrecht betrifft die Konkretisierung der Hauptleistungspflicht. Es ermöglicht dem Arbeitgeber nicht nur, dem Arbeitnehmer bestimmte Aufgaben zuzuweisen und den Ort und die Zeit ihrer Erledigung verbindlich festzulegen. Seine Weisungsbefugnis umfasst generell die Regelung der Ordnung und das Verhalten der Arbeitnehmer im Betrieb (§ 106 GewO).

Dazu gehört auch die Anordnung von allgemeinen von einer konkreten Aufforderung unabhängigen Meldepflichten. Beispiele sind die Pflicht zur unverzüglichen Mitteilung von für das Arbeitsverhältnis relevanten Änderungen in den persönlichen Verhältnissen des Arbeitnehmers[13], das Verlangen nach Vorlage eines ärztlichen Attests bereits ab dem ersten Tag der Erkrankung[14] oder einer Arztbesuchsbescheinigungen über die Notwendigkeit des Arztbesuches während der Arbeitszeit[15]. Ein weiteres Beispiel sind Meldepflichten als sog. Whistleblower.

5 Vgl. ArbG Frankfurt/Oder, RDV 2000, 227 mit Nachweisen der Rechtsprechung und Literatur.

6 So gesetzlich geregelt u.a. in § 93 Abs. 1 S. 5 LBeamtG NW.

7 BAG, NZA 2008, 809.

8 BAG, NZA 2013, 1416.

9 BAG, RDV 2014, 328.

10 LAG Berlin-Brandenburg vom 17.2.2011 – 25 Sa 2421/10 –.

11 BAG, RDV 2014, 328.

12 BAG, NZA 2008, 809.

13 Zur Mitteilung einer Schwangerschaft siehe § 5 Abs. 1 MuSchG; zur Mitteilung ihres vorzeitigen Endes vgl. BAG, NZA 2000, 2276 sowie RDV 2002, 313.

14 BAG, RDV 2013, 155 = NZA 2013, 322.

15 BAG, RDV 1997, 208 = NZA 1997, 785.

Besteht keine unaufgeforderte Offenbarungspflicht, so ergibt sich ggf. jedoch eine Mitteilungspflicht spätesten bei Nachfrage des Arbeitgebers[16], die Gegenstand eines Personalgesprächs sein kann. Voraussetzung ist, dass die vom Mitarbeiter erbetenen Informationen sich im Zulässigkeitsrahmen des BDSG bewegen und dass es sich um eine Angelegenheit handelt, die im Rahmen des Direktionsrechts besprochen werden soll[17]. Eine Anweisung zu einem Gespräch über eine ausschließlich von dem Arbeitgeber gewünschte und bereits abgelehnte einvernehmlichen Beendigung des Arbeitsverhältnisses gehört nicht hierzu. Die Weisung, an dem Gespräch teilzunehmen, betrifft weder die Arbeitsleistung noch die Ordnung oder das Verhalten im Betrieb und damit keinen der von § 106 GewO abgedeckten Bereiche. Stets muss der Arbeitgeber bei Weisungen billiges Ermessen walten lassen. Das schließt die Achtung grundrechtlich geschützter Interessen ein[18].

2. Krankenrückkehrergespräche

Ein kritisches Beispiel von Mitarbeiterbefragungen bilden Krankenrückkehrergespräche[19]. So kann es, wenn ein Mitarbeiter nach wiederholter oder längerer Erkrankung seine Arbeit wieder aufnimmt, angezeigt sein, mit ihm die weiteren Einsatzmöglichkeiten zu erörtern. Der Arbeitnehmer muss der Einladung nachkommen. Existiert ein Betriebsrat, darf der Arbeitnehmer ein Betriebsratsmitglied zum Gespräch hinzuziehen, §§ 82 Abs. 2, 84 Abs. 1 BetrVG. Bei der Einladung zu dem Gespräch ist der Betroffene über den Zweck des Gesprächs und die Reichweite seiner Auskunftspflicht zu belehren, d.h. dass er zu konkreten medizinischen Diagnosen keine Angaben machen muss[20], da § 28 Abs. 6 Nr. 3 BDSG keine Rechtsgrundlage bildet. Ebenso kann der Arbeitgeber von den Arbeitnehmern nicht verlangen, dass diese den sie behandelnden Arzt von seiner Schweigepflicht entbinden.

Eine Erhebung und Verarbeitung mittels förmlicher Einwilligung (§§ 4 Abs.1, 4a BDSG) scheidet überdies aus, da angesichts der besonderen widerstreitenden Interessenlage und des typischen Ungleichgewichts zwischen Arbeitnehmer und Arbeitgeber in diesen Fällen grundsätzlich Mängel an der Entschließungsfreiheit anzunehmen sind. Anders verhält es sich allein dann, wenn der Beschäftigte die Informationen unaufgefordert preisgibt, um in seinem Interesse liegende Vergünstigungen bzw. Veränderungen am Arbeitsplatz herbeizuführen, beispielsweise Arbeitserleichterungen, einen Arbeitsplatzwechsel oder den Erhalt anderer Arbeitsgerätschaften.

Ausnahmen hinsichtlich konkreter Nachfrage gelten jedoch, wenn ein berechtigtes betriebliches Interesse besteht, etwa wegen Ansteckungsgefahr für Kollegen oder auf Grund der Vermutung, dass der Arbeitnehmer seine Tätigkeit aus gesundheitlichen Gründen nicht mehr ausüben kann oder schließlich auch bei einem durch Indizien begründeten Verdacht der Vortäuschung einer Erkrankung. Zulässig sind weiter Fragen nach der voraussichtlichen Dauer der Krankheit, etwa wegen der Berechnung der Entgeltfortzahlung, oder danach, ob die Erkrankung durch die betrieblichen Bedingungen verursacht wurde, damit diese verbessert werden können und im Falle von Arbeitsunfällen über den Unfallhergang und dessen Ursache, um der Anzeigepflicht gegenüber der Berufsgenossenschaft (BG) nachkommen zu können

Sollen die Ergebnisse der Rückkehrgespräche aufgezeichnet werden, ist aus datenschutzrechtlichen Gründen der Arbeitnehmer darüber zu informieren und dessen Einwilligung einzuholen.

3. Betriebliches Eingliederungsmanagement

Die Durchführung des betrieblichen Eingliederungsmanagement ist in der Zielrichtung und im Verfahren von Krankenrückkehrergesprächen strikt zu unterscheiden[21]. § 84 Abs. 2 SGB IX sieht für alle Mitarbeiter, die innerhalb eines Jahres länger als 6 Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, das „betriebliche Eingliederungsmanagement" vor. Ziel dieses unter Beteiligung der Arbeitnehmer-Interessenvertretung durchzuführenden Verfahrens ist die Klärung, wie die Arbeitsunfähigkeit überwunden bzw. ihr künftig vorgebeugt werden kann. Letztlich soll mit ihm die Sicherung des Arbeitsplatzes verfolgt werden.

Bei der Praktizierung des Verfahrens werden in der Regel (abgefragte) Informationen des Mitarbeiters erörtert werden, die das Merkmal der personenbezogenen Daten i. S. von § 3 Abs. 1 BDSG erfüllen. Zur Wahrung seiner Persönlichkeitsrechte muss folgendes beachtet werden:

- Das gesamte Verfahren kann grundsätzlich nur mit Zustimmung des betroffenen Arbeitnehmers durchgeführt werden (§ 84 Abs. 2 Satz 1). Dies setzt einen informierten Betroffenen voraus (§ 84 Abs. 2 S. 3 SGB IX)[22]. Da die Zustimmung vor Verfahrensbeginn vorliegen muss, erfüllt sie das Kriterium der Einwilligung (§ 183 BGB).
- Der Betroffene ist auf „Art und Umfang der hierfür erhobenen und verwendeten Daten" hinzuweisen (§ 84 Abs. 2 Satz 2). Die Zustimmung muss sich, insbesondere da regelmäßig auch sensible Daten (§ 3 Abs. 9 BDSG) zur Sprache kommen werden, jetzt bzw. nachfolgend auch auf die das Verfahren ermöglichende, nachfolgende Datenverwendung erstrecken. Ob insoweit trotz der Spezialregelung des § 84 Abs. 2 S. 3 SGB IX § 4a Abs. 3 BDSG zur Anwendung kommt, ist strittig[23].
- Widerruft der Mitarbeiter seine Einwilligungserklärung, endet das Eingliederungsverfahren mit sofortiger Wirkung.

16 Zur Angabe einer Schwerbehinderteneigenschaft auf Nachfrage nach Ablauf der Probezeit: BAG, RDV 2012, 141 = NZA 2012, 555.

17 BAG, NJW 2009, 3115 = NZA 2009, S. 1011.

18 ErfK/Preis § 106 GewO Nr. 6.

19 Vgl. weitgehend ablehnend: Kynast, in: Behling/Abel (Hrsg.), Praxishandbuch Datenschutz im Unternehmen, Kap. 8 Rn. 178; Däubler, Gläserne Belegschaften, 5. Aufl., Rn. 274.

20 Vgl. LfD Baden-Württemberg, 30. TB (2010/2011), S. 136.

21 Vgl. bei Kiesche, Datenschutz im BEM, RDV 2014, 321; Kiper/Schierbaum, Krankheit, BEM und Datenschutz, CuA 12/2012, 25.

22 Zu den mitzuteilenden Informationen im Einzelnen vgl. bei Kiesche (Anm. 21).

23 Seifert, in: Simitis (Hrsg.) BDSG, 8. Aufl., § 32 Rn. 67

Bereits erhobene Daten müssen gelöscht werden, weil das mit ihnen verfolgte Ziel entfallen ist. Gleiches gilt wohl auch bei abgeschlossenen Verfahren[24].

4. Meldepflichten als Whistleblower

Billigem Ermessen unterliegt auch die Festlegung von Meldepflichten im Rahmen des sog. Whistleblowing, bei dem die Mitarbeiter angehalten werden, arbeitsrechtlich relevante Verstöße von Kollegen in einem in der Regel besonders gestalteten Meldeverfahren mitzuteilen. Konkretisiert der Arbeitgeber mit dieser Anweisung zur Datenmeldung nur die sich für den Arbeitnehmer bereits aus § 241 BGB und der arbeitsvertraglichen Treuepflicht ergebende Verpflichtung, Schaden vom Arbeitgeber abzuwenden, und sei dies auch im Rahmen ihm zumutbarer Anzeigen von „kriminellen" Kollegen, so handelt es sich um ein in seinem Direktionsrecht liegendes und durch § 32 Abs. 1 S. 1 BDSG abgedecktes Datenerhebungsverfahren.

Ist die Anzeigepflicht Gegenstand einer besonderen Abrede im Arbeitsvertrag oder einer Betriebsvereinbarung, so dürfen auch hier die Zumutbarkeitsgrenzen (vgl. auch §§ 305 ff. BGB) nicht überschritten werden. Der Informationsbedarf des Arbeitgebers ist im Rahmen einer Interessenabwägung und unter Beachtung des Verhältnismäßigkeitsprinzips mit dem Anspruch des Arbeitnehmers auf Wahrung seines Persönlichkeitsrechts (§ 75 Abs. 2 BetrVG) abzuwägen.

Gleiches gilt für die zur Aufklärung der gemeldeten Sachverhalte im Betrieb im Rahmen sog. Internal Investigations[25] durchführten Befragungen, wobei es um Aussagen von Zeugen und Verdächtigten geht. Der Pflicht, über im Zusammenhang mit seinem Arbeitsverhältnis stehenden Fragen Auskunft zu geben[26], kann hier im Spannungsfeld mit dem im Strafrecht geltenden Grundsatz stehen, dass niemand sich selbst belasten muss.

5. Verbesserungsvorschläge

Im Gegensatz zu der zuvor genannten Verpflichtung, Schaden vom Unternehmen abzuwenden, erfasst das Weisungsrecht nicht die Pflicht des Mitarbeiters, über den konkreten arbeitsvertraglichen Rahmen hinaus mit Verbesserungsvorschlägen das Unternehmen zu unterstützen.

Vorschläge der Arbeitnehmer, die der Vereinfachung, Beschleunigung oder sicheren Gestaltung betrieblicher Arbeitsabläufe dienen, die zur Kostensenkung beitragen oder die den sozialen Bereich betreffen, werden vom Arbeitgeber in der Regel gern entgegengenommen. Vielfach werden die Mitarbeiter durch Prämien oder sonstige Vergünstigungen sogar ermuntert, Vorschläge zu unterbreiten – abgesehen von dem Anreiz, den bei qualifizierten technischen Verbesserungsvorschlägen das ArbNErfG bietet, das dem Mitarbeiter bei Umsetzung einen Anspruch auf angemessene Vergütung gewährt. Sogar Belohnungen für nicht realisierte Vorschläge sind nicht selten, da mit Belohnungen die Motivation der Mitarbeiter zum kreativen Denken und eine Bewusstseinschärfung für betriebliche Probleme und die Aufgeschlossenheit gegenüber technischen und organisatorischen Entwicklungen geschaffen oder gefördert werden kann. Allein unter dieser Zweckbestimmung ist die personenbezogene Datenerhebung gerechtfertigt[27].

Häufig werden Regelungen für die Behandlung von Vorschlägen im Rahmen eines betrieblichen Vorschlagwesens getroffen, dessen Einführung wie auch die Durchführung gem. § 87 Abs. 1 Nr. 12 BetrVG der Mitbestimmung des Betriebsrats unterliegen. Die festzulegenden allgemeinen Grundsätze für die Praktizierung des Verfahrens können sich beziehen auf das Ausmaß und die Art der vorgeschlagenen Verbesserungen, auf die Außenwirkung des Vorschlags oder den mit dem Vorschlag erzielbaren wirtschaftlichen Effekt.

Es liegt in der Natur der Sache, dass bei derartigen Vorschlägen der Arbeitgeber berechtigt ist, Nachfragen an seinen Mitarbeiter zu stellen, sei es zu Details des Vorschlags selbst, sei es zu den Umständen, die den Mitarbeiter zu seiner Entwicklung veranlasst haben (betrieblicher Anlass oder private Anstöße), oder auch, wer an der Entwicklung außer ihm noch beteiligt war usw.

IV. Allgemeine Mitarbeiterbefragung

1. Gegenstand der Befragung

Im Gegensatz zu diesen „Einzelgesprächen" stehen „pauschale" Mitarbeiterbefragungen der gesamten oder von nach bestimmten Kriterien festlegten Teilen der Belegschaft. Derartige Datenerhebungen sollen helfen, Stärken oder Schwächen eines Unternehmens zu erkennen. Sie dienen zum einen dem Arbeitgeber zur Analyse und Diagnose der erfragten Sachverhalte und zum anderen der Beteiligung der Beschäftigten bei Veränderungs- und Modernisierungsprozessen. Abgefragt werden Bewertungen des Arbeitsumfelds, der Führung und Zusammenarbeit, die Arbeitszufriedenheit oder die Motivation. Gegenstand der Erhebung können auch sensible Tatbestände wie das Gesundheits- und Stressbild der Beschäftigten sein. Gleichwohl ist von Interesse nicht der einzelne Beschäftigte, sondern das Meinungsbild von Teilen oder der Gesamtheit der Belegschaft.

Je nach Zielstellung im Unternehmen ergeben sich verschiedene Formen einer Mitarbeiterbefragung[28]: Dazu zählen

- Zufriedenheitsumfragen (Erhebung der Zufriedenheit der Mitarbeiter mit verschiedenen Aspekten im Unternehmen)
- Klima-/Kulturbefragung (spezielle Abfrage der Themen Betriebsklima und Unternehmenskultur)
- Engagement-Befragungen (Untersuchung von Performance, Motivation, Bindung und Leistungsfähigkeit der Mitarbeiter)
- Prozess-Evaluationen (Bewertung des Planungsprozesses, Unterstützung des Change Managements).

24 Seifert, in: Simitis (Hrsg.) (Anm. 23), § 32 Rn. 67; a.A. Gundermann/Oberberg, Datenschutzrechtliche Gestaltung des betrieblichen Eingliederungsmanagements und Beteiligung des Betriebsrats, RDV 2007, 103 zu den Aufbewahrungsfristen bei abgeschlossenen Verfahren vgl. bei Kiesche (Anm. 21).

25 Zur Teilnahme- und Auskunftspflicht vgl. Momsen, ZIS 6/2011, 567: ZIS-online.com/dat/artikel/2011_6_586; Dann/Schmidt, NJW 2009, 1851.

26 Göpfert/Merten/Siegrist, NJW 1998, 1705.

27 Kynast, in: Behling/Abel (Hrsg.), Praxishandbuch Datenschutz im Unternehmen, Kap. 8, Rn. 228.

28 Vgl. SKOPOS, Institut für Markt- und Kommunikationsforschung GmbH & Co. KG, www.skopos.de.

2. Zulässigkeit von Umfragen im Betrieb

Werden Umfragen im Betrieb wie vorstehend beschrieben durchgeführt, ist zu unterscheiden:

Erfolgen sie anonym, d.h. können die Stellungnahmen der Mitarbeiter nicht den einzelnen Arbeitnehmern zugerechnet werden, ergibt sich kein datenschutzrechtliches Problem, da keine personenbezogenen/-beziehbaren Daten anfallen (vgl. dazu im Einzelnen nachfolgend). Die Anordnung der Durchführung derartiger anonymer Umfragen liegt im Direktionsrecht des Arbeitgebers; Mitbestimmungsrechte der Arbeitnehmervertretung – etwa nach § 87 Abs. 1 Nr. 1 BetrVG – kommen nicht zum Tragen.

Bisweilen legt der Arbeitgeber aber Wert darauf festzustellen, wem er den Fragebogen bzw. die Antworten zuordnen kann. Stellt er es dem Mitarbeiter völlig frei, einem ihm (z.B. über die Personalnummer) zurechenbaren Fragebogen auszufüllen, drohen ihm für den Fall, dass er seine Beteiligung verweigert, keine Nachteile. Beteiligt er sich, erklärt er mit der Rückgabe des ausgefüllten Formulars sein Einverständnis mit der Befragung, d.h. die Zulässigkeit der Datenerhebung beruht auf einer konkludenten Einwilligung[29].

Bei der dritten Variante fordert der Arbeitgeber die Mitarbeiter auf, auch gegen ihren Willen den ihnen zuzurechnenden Fragebogen auszufüllen. Bei dieser Vorgehensweise kann der Arbeitgeber nicht von einer freiwillig konkludent erteilten Einwilligung in die Erhebung der Angaben ausgehen. Auch § 32 Abs. 1 Satz 1 BDSG dürfte keine Legitimationsgrundlage bieten. Erzwungene Aussagen des Mitarbeiters werden nicht selten „frisiert" sein, um evtl. negative Reaktionen des Arbeitgebers zu vermeiden. Die Erhebung das Meinungsbild des Arbeitnehmers verfälscht abbildender Informationen ist zweifellos nicht zur Durchführung des Beschäftigungsverhältnisses erforderlich.

3. Pauschale Befragungen zu Gesundheitsgefährdungen

Ausgangspunkt für pauschale Mitarbeiterumfragen kann auch das Arbeitsschutzgesetz sein. Es verpflichtet den Arbeitgeber, durch eine Beurteilung der für die Beschäftigten mit ihrer Arbeit verbundenen Gefährdung zu ermitteln, welche Maßnahmen zum Arbeitsschutz erforderlich sind (§ 5 Abs. 1 ArbSchG) und das Ergebnis der Gefährdungsbeurteilung zu dokumentieren (§ 6 Abs. 1 ArbSchG). Das Gesetz enthält keine zwingende Vorgabe, wie diese Gefährdungsbeurteilung vorzunehmen ist, d.h. dem Arbeitgeber ist insoweit ein Handlungs- und Beurteilungsspielraum eingeräumt[30]. Ein gängiges Verfahren ist, dazu als einen ersten Schritt Mitarbeiterbefragungen durchzuführen. Informationen sollen gesammelt werden über Belastungsschwerpunkte im Betrieb sowie Zusammenhänge zwischen Arbeitsbedingungen und Gesundheitsbeschwerden. Erfragt werden detailliert konkrete bei der Arbeit auftretende Beschwerden (Kopfschmerzen, Rückenschmerzen, Augenbeschwerden etc.) ebenso wie psychische Belastungen. Die Erhebung dient der Entscheidung über Maßnahmen zur Vermeidung von Gefährdungen und zur betrieblichen Gesundheitsförderung. Die Meinung des Einzelnen ist zwar gefragt, sie dient aber dazu, allgemeine und nicht subjektive Belastungen und Gefährdungen zu erkennen. Demgemäß sind die Mitarbeiter zwar auf Grund des hier einschlägigen Weisungsrechts des Arbeitgebers gehalten, an der Befragung teilzunehmen, eine personenbezogene Erhebung wird aber regelmäßig als nicht erforderlich anzusehen sein. Die Erhebung hat also in anonymisierter Form zu erfolgen.

4. Anonyme Datenerhebung

Keine arbeits- und datenschutzrechtlichen Probleme entstehen, wie zuvorgesagt, wenn die Befragung in anonymisierter Form erfolgt, d.h. der Arbeitgeber nicht erkennen kann, wer an der Befragung teilgenommen bzw. Aussagen zu den Fragestellungen abgelehnt hat. Damit ist dann einerseits auch die Freiwilligkeit der Teilnahme sichergestellt. Zum anderen besteht nicht die Gefahr, dass die Fragen nicht wahrheitsgemäß, sondern „geschönt" beantwortet werden.

4.1 Der Begriff der Anonymität

Nicht unter den Schutz des BDSG fallen Angaben, die nicht (mehr) auf eine bestimmte Person beziehbar sind. Derartige anonyme Datenbestände können bestehen, weil die Daten bereits ohne Personenzug erhoben wurden, wie es ggf. bei einer anonymen Mitarbeiterbefragung der Fall sein kann. Daten können aber auch nachträglich anonymisiert werden. Insoweit definiert § 3 Abs. 6 BDSG das Anonymisieren von Daten als das Verändern personenbezogener Daten, wobei es sich aber nicht um das Verändern im Sinne des § 3 Abs. 4 Nr. 2 BDSG handelt[31]. Die Anonymisierung kann nämlich derart erfolgen, dass die Daten, die zur Bestimmung des Betroffenen führen, gelöscht werden. Es entsteht ein neuer Datenbestand nicht personenbeziehbarer Daten. Sie kann aber auch so erfolgen, dass ein fortbestehender personenbezogener Datenbestand genutzt wird, indem bestimmte Daten in einem anonymisierten Datenbestand gespiegelt werden, z.B. um diesen an einen Empfänger ohne Verstoß gegen das BDSG weitergeben zu können. Eindeutig muss dabei sein, dass bei dem Empfänger keine Möglichkeit der Reidentifizierung besteht.

Eine andere Art der Anonymisierung kann in der Aggregierung von Daten liegen, d.h. in der Zusammenführung von Einzeldatensätzen zu Gruppendatensätzen. Dabei ist aber darauf zu achten, dass die Merkmalsdaten so abstrakt bleiben, dass nicht auf Grund einzelner Merkmale noch Einzelnennungen erfolgen können. Solche Möglichkeiten der Einzelerkennung können auch dadurch entstehen, dass verschiedene Gruppendatensätze zusammengeführt werden. Zu beachten ist schließlich, dass Analysen und Algorithmen auf der Auswertung von Charakteristika der anonymisierten Personen beruhen und die Anonymität dadurch aufgehoben werden kann, dass die die Basis der Auswertung bildenden Charakteristika eine Person so deutlich in ihrem Persönlichkeitsprofil beschreiben, dass der Personenbezug herstellbar ist.

29 Däubler (Anm. 19), Rn. 268.

30 BAG, NZA 2009, 102.

31 Gola/Schomerus (Anm. 3) § 3 Rn. 31; vgl. zu möglichen „Veränderungsweisen" bei Wojtowicz, Wirksame Anonymisierung im Kontext von Big Data, PinG 2013, 65.

Aufzuzeigen ist, ob diese der Anonymisierung dienenden Tatbestände des Nutzens, des Veränderns oder Löschens von Daten dem Verbot mit Erlaubnisvorbehalt des § 4 Abs. 1 BDSG unterliegen. In allen Fällen führt das Ergebnis der Verarbeitung bzw. Nutzung dazu, dass die Beeinträchtigungen, vor denen das BDSG schützen soll (§ 1 Abs. 1 BDSG), nicht mehr eintreten können. Ergebnis ist daher, dass eine Nutzung oder ein Verändern[32] personenbezogener Daten nur vorliegt, wenn sich die Verwendung auch auf den Personenbezug erstreckt[33]. Eine automatisierte Auswertung ohne personenbezogenes Ergebnis unterliegt nicht dem BDSG[34] – vorausgesetzt, dass die personenbezogenen Zwischendateien alsbald gelöscht werden[35]. Gleiches gilt für das Verändern, wobei eine Löschung des Personenbezugs nach § 35 Abs. 2 S. 1 BDSG jederzeit möglich ist, sofern nicht Aufbewahrungsvorschriften oder entgegenstehende schutzwürdige Interessen des Betroffenen verletzt werden.

Zu beachten ist jedoch, dass der Begriff einer Anonymisierung in der Literatur unterschiedlich definiert wird. Eine Auffassung fordert die „absolute" Anonymität, bei der eine Reanonymisierung unmöglich ist. Personenbeziehbarkeit besteht danach bereits, wenn das für die Herstellung des Personenbezugs erforderliche Zusatzwissen theoretisch-abstrakt vorhanden ist. Auf die Zugänglichkeit für die verantwortliche Stelle soll es nicht ankommen[36].

Jedoch ist es eine Tatsache, dass eine absolute Anonymisierung angesichts der Möglichkeiten der ADV nur in den seltensten Fällen möglich ist. Dem folgte auch der Gesetzgeber, indem er es für das Erreichen der Anonymität genügen lässt, dass die Reanonymisierung einen unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft erfordern würde. Insofern ergibt sich die Trennlinie zwischen Anonymisierung und Pseudonymisierung, da bei der Pseudonymisierung diese Rückführung beabsichtigt ist. Maßgebend ist die Verfügbarkeit des zur Reanonymisierung erforderlichen Wissens. „Verfügbarkeit" heißt aber zum einen nicht, dass die Zusatzinformation schon oder noch bei der verantwortlichen Stelle vorhanden ist, und zum anderen nicht, dass eine Absicht der Reanonymisierung bestehen muss. Dieser Ausschluss einer personellen Zuordnung ist umso weniger möglich, je mehr qualifizierte Daten von möglichweise unterschiedlichen Quellen zu Auswertungen zusammengeführt werden. Andererseits muss nach der Lebenserfahrung eine derartige Möglichkeit mit gewisser Wahrscheinlichkeit auch erwartet werden können, was eine unter dem Gesichtspunkt der Verhältnismäßigkeit vorzunehmende Risikoanalyse voraussetzt[37]. Der Begriff des „unverhältnismäßig" hohen Aufwands macht deutlich, dass es sich immer um eine aus objektiver Sicht zu treffende Einzelfallentscheidung handelt. Insoweit wird auch das mögliche Interesse der speichernden Stelle an einer Reanonymisierung einzelner Daten und der damit gewonnene wirtschaftliche Nutzen, der ggf. auch hohe Kosten gerechtfertigt erscheinen lässt, maßgebend sein. Ist die verantwortliche Stelle in der Lage und bereit, den unverhältnismäßig hohen Aufwand zu betreiben, so sind die Daten nicht anonym.

Der Begriff des Personenbezugs ist daher relativ, d. h. dieselben Daten können für den einen anonym und für den anderen der betroffenen Person zuordbar sein. Werden anonyme Daten an eine Stelle übermittelt, die in der Lage ist, den Personenbezug herzustellen, so ist der Übermittlungstatbestand des BDSG erfüllt. Der Begriff der Anonymität ist somit als Gegenpart zum Personenbezug zu sehen.

Nach der aufgezeigten Gegenmeinung[38] soll der Personenbezug jedoch bereits bei der theoretisch abstrakten Möglichkeit, das Datum mit einer natürlichen Person in Verbindung zu bringen, fortbestehen. Auf das Wissen der speichernden Stelle komme es nicht an. Für die Stimmen, die von einem „absoluten" Begriff des Personenbezugs ausgehen, reicht eine „faktische" Anonymisierung nicht aus, so dass sich Anonymität und Personenbezug nicht ausschließen[39]. Diese Auffassung übersieht die vom Gesetzgeber vorgesehene Unterscheidung zwischen anonymen und pseudonymen Daten[40]. Bei einer Pseudonymisierung soll im Bedarfsfall der Personenbezug wieder herstellbar sein. So ist es jedenfalls im Normalfall[41]. Dabei ist zu unterscheiden, wer die Pseudonymisierung vornimmt. Wenn der Betroffene die Pseudonyme ausschließlich selbst vergibt, so kann der Personenbezug auch nur von ihm wiederhergestellt werden. Vergibt ein vertrauenswürdiger Dritter die Pseudonyme und verfügt ausschließlich er über die Zuordnungsregel, so ist für andere die Anonymität hergestellt. Nimmt die verantwortliche Stelle die Pseudonymisierung vor, so kann dadurch Zweckmissbrauch vermieden werden; für sie bleibt aber der Personenbezug bestehen[42]. Das Pseudonym bewirkt Anonymität gegenüber Dritten, denen die Daten übermittelt werden, dies jedoch nur, wenn der Dritte keine Möglichkeit hat, durch Zugriff auf die Referenzdatei den Personenbezug wieder herzustellen[43]. Insofern obliegt der datenverarbeitenden Stelle bei der Weitergabe „relativ" anonymisierter Daten die Verpflichtung, die Zwecke und Verwendung beim Empfänger und seine Möglichkeiten der Reanonymisierung festzustellen. Liegen letzte vor, müssen die Voraussetzungen für die Zulässigkeit der Übermittlungstatbestände der §§ 28, 29 gegeben sein. Wird jedoch ein großer nicht personenbezogener oder ein eine Personengruppe betreffender Datenbestand übermittelt, bei dem der Empfänger ggf. nur einige wenige Betroffene aufgrund eines im Einzelfall eventuell vorhandenen Zusatzwissens möglicherweise identifizieren kann, kann die übermittelnde Stelle noch von hinreichender Anonymisierung ausgehen[44].

32 Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 4. Aufl., § 3 Rn. 46.

33 Dammann, in: Simitis (Hrsg.) (Anm. 23) § 3 Rn. 191.

34 Ulmer, Big Data – Neue Geschäftsmodelle, neue Verantwortlichkeiten?, RDV 2013, 227; Weichert, Big Data und Datenschutz, ZD 2013, 257.

35 Dammann, in: Simitis (Hrsg.) (Anm. 23), § 3 Rn. 195.

36 Weichert, in: Däubler/Klebe/Wedde/Weichert (Anm. 32) § 3 Rn. 15; Wojtowicz, Wirksame Anonymisierung im Kontext von Big Data, PING 2013, 66.

37 Vgl. Dammann, in: Simitis (Hrsg.), (Anm. 23) § 3 Rn. 16.

38 Weichert, in: Däubler/Klebe/Wedde/Weichert, (Anm. 32), § 3 Rn. 3.

39 Vgl. im Detail bei Härting, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065.

40 Vgl. auch Buchner, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl., § 3 Rn. 50; Scholz, in: Simitis (Hrsg.), (Anm. 23) § 3 Rn. 320a.

41 Buchner, in: Taeger/Gabel (Hrsg.) (Anm. 40), § 3 Rn. 47.

42 Scholz, in: Simitis (Hrsg.), (Anm. 23) § 3 Rn. 220a ff.; Schild, in: Wolff/Brink (Hrsg.), Datenschutzrecht, BDSG, § 3 Rn. 102 ff.

43 Zur „absoluten" Anonymisierung, vgl. Plath/Schreiber, in: Plath (Hrsg.), BDSG § 3 Rn. 63; Scholz, in: Simitis (Hrsg.) (Anm. 23) § 3 Rn. 220a; Schild, in: Wolff/Brink (Hrsg.) (Anm. 42), § 3 Rn. 106.

44 Zur Zulässigkeit dieses Restrisikos vgl. Wojtowicz, Wirksame Anonymisierung im Kontext von Big Data, PING 2013, 66; vgl. auch Härting, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065.

Angaben über eine bestimmte einzelne Person sind ferner nicht mehr gegeben bei aggregierten Daten sowie bei Sammelangaben über Personengruppen. Werden im Rahmen des strategischen HRM aggregierte Daten zur Ermittlung von Risiken ausgewertet, die das gesamte Unternehmen betreffen, so z.B. über das kumulierte Abwanderungsrisiko hochqualifizierter Mitarbeiter, so greift das BDSG nicht.

Wenn jedoch eine Einzelperson als Mitglied einer näher beschriebenen Personengruppe bekannt ist, so handelt es sich auch um Einzelangaben zu dieser Person, wenn die Daten auf die Einzelperson „durchschlagen"[45]. Dies gilt selbst dann, wenn es sich bei den Angaben zur Beschreibung der Personengruppe um statistische oder auf Durchschnittswerten beruhende Angaben handelt. Maßgebend ist die Zweckbestimmung der erfassten Information, d. h. ob sie auch dazu dienen soll, das einzelne Gruppenmitglied zu bewerten[46]. Nach § 35 Abs. 2 BDSG dürfen auch Daten, die nur möglicherweise eine bestimmte Person betreffen, möglicherweise aber auf diese Person bezogen unrichtig sind, nicht verwendet werden[47]. Nach alledem wird die Nutzung von sog. Big Data für die Personalplanung weitgehend ohne die Verwendung von personenbezogenen Daten auskommen können und daher nicht im Spannungsfeld mit datenschutzrechtlichen Normen stehen[48]. Die gilt solange, wie es darum geht, abstrakte Aussagen über den der Zukunftsplanung des Unternehmens entsprechenden quantitativen und qualitativen Personalbedarf und die diesbezüglichen Risikobereiche wie beispielsweise Gesundheits-, Wissens- oder Demografierisiken darzustellen.

4.2 Aufhebung der Anonymität durch Umfang der erhobenen Daten

Diese Anonymität ist aber nur gewahrt, wenn nicht nachträglich auf Grund der Struktur der Befragung und der jeweiligen Antworten auf bestimmte Beschäftigte rückgeschlossen werden kann. Das ist häufig der Fall, wenn statistische Angaben erfragt werden, etwa zu dem Alter, der Betriebszugehörigkeit, dem Geschlecht sowie nach Voll- oder Teilzeitbeschäftigung und Abteilungszugehörigkeit.

Derartige Probleme ergeben sich auch, wenn die Befragung online erfolgen soll, da hier der Befragte durch IP-Adresse, Benutzername, Browser Fingerprint und Cookies ermittelt werden kann[49]. Gleiches gilt, wenn die Beantwortung der Fragen aus dem E-Mail-Postfach des Mitarbeiters erfolgt[50]. An dem Personenbezug der Erhebung ändert nichts, wenn die Auswertung der erhobenen Daten anschließend aggregiert in Gruppenangaben erfolgt, um damit den Rückschluss auf einzelne Personen auszuschließen[51].

Ansonsten müsste bei personenbezogener Erhebung deren Erforderlichkeit nach § 32 Abs. 1 S. 1 BDSG oder § 28 Abs. 1 S. 1 Nr. 2 BDSG gegeben sein.

5. Personenbezogene Datenerhebung

5.1 Erlaubnistatbestände

Ob diese Erforderlichkeit bei derartiger und sonstiger pauschaler Erhebung besteht und ob die Mitarbeiter zur Teilnahme an der Umfrage verpflichtet werden können, ist Gegenstand der nachfolgenden Betrachtung.

Ist der Personenbezug der Datenerhebung nicht ausgeschlossen, d.h. wenn die Teilnehmer an der Umfrage näher bestimmt oder bestimmbar sind, stellt sich die Frage nach der datenschutzrechtlichen Zulässigkeit.

Vor dem Schritt zur personenbezogenen Datenerhebung steht jedoch zunächst das Gebot der Datenvermeidung und Datensparsamkeit des § 3a BDSG zur Prüfung an, d.h. ob das Umfrageziel nicht auf dem Weg der anonymen oder pseudonymen Durchführung der Erhebung erreicht werden kann. Hieraus kann sich auch zumindest die Verpflichtung einer Anonymisierung im zweiten Schritt der Erhebung ergeben, d.h. die vom Erhebungsbogen getrennte Erfassung der Daten des Absenders. Anzumerken ist jedoch, dass auch eine pseudonymisierte Erhebung nicht die Personenbeziehbarkeit grundsätzlich ausschließt. Sie bewirkt im Gegensatz zu der Anonymisierung, dass die Bestimmung des Betroffenen nur „relativ" ausgeschlossen oder wesentlich erschwert wird. Dies gilt insbesondere dann, wenn die verantwortliche Stelle auch zur Aufhebung der Pseudonymisierung in der Lage bleibt.

Als Rechtsgrundlage für eine personenbezogene Datenerhebung ist § 32 Abs. 1 S. 1 oder ggf. § 28 Abs. 1 S. 1 Nr. 2 BDSG in Betracht zu ziehen.

§ 32 Abs. 1 S. 1 BDSG verlangt, dass die Zweckbestimmung der Datenerhebung im Rahmen der Durchführung des mit dem Beschäftigten bestehenden Arbeitsverhältnisses erforderlich ist. Zur Durchführung des Arbeitsverhältnisses erforderlich sind die Daten, die der Arbeitgeber zur Wahrnehmung seiner Rechte und zur Erfüllung seiner Pflichten gegenüber dem betroffenen Beschäftigten vernünftigerweise benötigt[52]. Für die Durchführung der individuellen Vertragsbeziehung ist die Teilnahme an einer allgemeinen Mitarbeiterbefragung nicht erforderlich.

Der bei Nichtvorliegen der Zweckbestimmung des § 32 Abs. 1 S. 1 BDSG weiterhin anwendbare § 28 Abs. 1 S. 1 Nr. 2 BDSG[53] scheidet ebenfalls regelmäßig als Zulässigkeitsnorm aus, da den berechtigten Interessen des Arbeitgebers an der Durchführung der Umfrage zumeist überwiegende schutzwürdige Interessen der Beschäftigten entgegenstehen. Der Beschäftigte muss dem Arbeitgeber nicht seine subjektive Einschätzung der Arbeitsbedingungen, seine Motivation bzw.

45 Vgl. BAG, RDV 1986, 138 und 1995, 29 = NZA 1995, 185.

46 Vgl. bei Gola/Wronka (Anm. 1), Rn. 1104 ff.

47 OLG Hamburg, NJW 1987, 659 zur Löschung zweifelhafter mit dem Vermerk „Identität nicht feststellbar" gespeicherter Negativdaten.

48 Vgl. das Beispiel bei Jentzsch, Nutzung von Big Data für die strategische Personalplanung, HR Performance 7/2013, 48.

49 Zum Ausschluss derartiger Möglichkeiten: LfD Baden-Württemberg, (Anm. 20), 144 f.

50 Siehe die Hinweise zu diesbezüglichen Anonymisierungsmöglichkeiten: Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, Empfehlungen zum Datenschutz bei Mitarbeiterbefragungen: www.datenschutz-hamburg.de.

51 Bayerisches Landesamt für Datenschutz, Tätigkeitsbericht 2011/2012, 67 f.

52 Gola/Schomerus (Anm.3), § 32 Rn. 11.

53 Vgl. Gola/Wronka (Anm. 1), Rn. 664 ff.

stattgefundene „innere Kündigung“ oder von ihm empfundene Probleme mit der Zusammenarbeit mit Kollegen oder Vorgesetzten offenbaren und damit die Erstellung eines Persönlichkeitsbilds eröffnen. Hier gilt der Grundsatz „Die Gedanken sind frei“. Eine Verpflichtung der Mitarbeiter, dem Arbeitgeber ihre subjektive Meinung über ihre Arbeitsbedingungen mitzuteilen oder beispielsweise Verbesserungsvorschläge für betriebliche Abläufe zu machen, besteht daher regelmäßig nicht[54].

5.2 Einwilligung

5.2.1 Freiwilligkeit

Damit bleibt die Frage, ob die Datenerhebung bei den Mitarbeitern zulässig ist, die hierin einwilligen und sich bei eindeutig freigestellter Teilnahme[55] an der Umfrage beteiligen. Eine „informierte“ Einwilligung setzt zunächst voraus, dass der Zweck der Befragung, die beabsichtigten Auswertungen und die die Befragung durchführende bzw. die Befragungsergebnisse auswertende Stelle offengelegt werden. Zugesichert werden muss, dass den Beschäftigten im Falle der Nichtbeteiligung keine Nachteile entstehen[56]. Gleichwohl wird die nach § 4a Abs. 1 BDSG erforderliche Freiwilligkeit auf Grund der wirtschaftlichen Abhängigkeit des Arbeitnehmers häufig fraglich sein[57].

5.2.2 Einschaltung eines Dienstleisters

Das die Freiwilligkeit in Frage stellende Risiko eventueller Benachteiligung bei Versagung der Einwilligung kann entfallen, wenn der Arbeitgeber durch Einschaltung eines die Befragung durchführenden und insoweit zur Vertraulichkeit verpflichteten Dienstleisters nicht erfährt, wer an der Befragung teilgenommen hat, und ihm die Auswertung der Befragungsergebnisse in hinreichender Aggregierung mitgeteilt[58] und dieses Vorgehen mit einer erforderlichen Betriebsvereinbarung abgesichert werden. Die Einschaltung des Dienstleisters kann sich, je nachdem, ob er als „Personalforschungsinstitut“ die Befragung in eigener Regie durchführt oder ob er auf Weisung des Arbeitgebers handelt, als Funktionsübertragung oder Auftragsdatenverarbeitung darstellen. Die Frage der Zulässigkeit der Weitergabe von Mitarbeiterdaten an den Dienstleister stellt sich nicht, wenn diese – ggf. in pseudonymisierter Form unter Einschaltung eines Codes – durch den jeweiligen Mitarbeiter erfolgt. Doppelbeteiligungen können hierdurch ausgeschlossen werden.

V. Konzernweite Befragung

1. Grundsätzliches

Auch wenn der Wunsch der Mitgliederbefragung von der Konzernmutter ausgeht, ist eine Übermittlung der Mitarbeiterdaten an die Konzernmutter, damit von dort die Befragung personenbezogen gestartet werden kann, weder durch § 32 Abs. 1 S. 1 BDSG noch durch § 28 Abs. 2 S. 2 BDSG gerechtfertigt. Jedenfalls kann das Streben nach einem einheitlichen Personalmanagement oder einer einheitlichen Personalsteuerung allein kein den schutzwürdigen Interessen der Beschäftigten vorrangiges berechtigtes Interesse begründen. Gemäß dem Aspekt der Freiwilligkeit der Teilnahme genügt es, wenn die Tochter die Mitarbeiter über den Wunsch der Mutter informiert und diese die von der Mutter vorgegebenen Fragen unmittelbar beantworten. Dieses kann in anonymer oder pseudonymisierter Form erfolgen[59].

2. Beteiligung des Betriebsrats

Als Beteiligungsrechte des Betriebsrats kommen vorrangig in Betracht

- *Das Informationsrecht des § 80 Abs. 2 BetrVG*
  Der Betriebsrat kann auch bei nicht mitbestimmungspflichtiger anonymer Befragung Auskunft über die Auswertungsergebnisse verlangen, wenn die hinreichende Wahrscheinlichkeit besteht, dass diese Bezug zu Aufgaben des Betriebsrates haben[60].
- *Das Mitbestimmungsrecht bei Personalfragebögen und Beurteilungsgrundsätze nach § 94 BetrVG.*
  Der Einsatz eines „Personalfragebogens“ erfolgt, wenn Beschäftigte einer standardmäßigen Befragung unterzogen werden und sich die Fragen auf ihre persönlichen Verhältnisse und nicht auf eine von den Beschäftigten losgelöste Arbeitsplatzbeschreibung erstrecken[61]. Das Mitbestimmungsrecht erfasst den Gegenstand der Fragen ebenso wie den Verwendungszweck der erhobenen Daten. Es gilt unabhängig davon, ob die Beantwortung der Fragen freigestellt ist oder ob die Befragung durch einen Dritten erfolgt[62]. Es entfällt, wenn die Befragung anonym erfolgt.
- *Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG.*
  Erfolgt die Befragung online oder werden die Daten automatisiert ausgewertet, unterliegt das Verfahren so lange der Mitbestimmung, wie ein Personenbezug der Daten vorliegt bzw. noch herstellbar ist, auch wenn eine Absicht nicht besteht, Erkenntnisse zu Leistung oder Verhalten der Beschäftigten zu gewinnen.
- *Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 7 BetrVG*
  Der Betriebsrat hat nach § 87 Abs. 1 Nr. 7 BetrVG mitzubestimmen bei betrieblichen Regelungen, die dem Gesundheitsschutz dienen. Mitbestimmungsrecht besteht auch, bei

54 ULD, www.datenschutzzentrum.de/wirtschaft/praxis/20070313.htm; LfD Baden-Württemberg (Anm. 20), 145.

55 Dieser Hinweis hat auf dem Fragebogen selbst und drucktechnisch hervorgehoben zu geschehen, vgl. LfD Baden-Württemberg (Anm. 20), 138; www.bfdi.bund.de Thema Arbeitnehmerdatenschutz/Mitarbeiterbefragungen.

56 Der hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Anm. 51), Ziff. 5a und b, akzeptiert in diesem Fall die Einwilligung als Erlaubnistatbestand, sofern keine sensiblen, die Persönlichkeit des Befragten betreffenden Daten erfragt werden.

57 So ULD (Anm. 55) für den Regelfall.

58 LfD Baden-Württemberg (Anm. 20), S. 138.

59 Vgl. LfD Baden-Württemberg (Anm. 20), S. 144 f.

60 BAG, ArbuR 2000, S. 267 = RDV 2000, S. 23 (Ls).

61 Zum Begriff und dem Umfang der Mitbestimmung im Einzelnen: Gola/Wronka (Anm. 1), Rn. 1806 ff.

62 Vgl. Hess LAG, RDV 2002, S. 131 zur Mitbestimmung bei einer von der Konzernmutter über das Computersystem der Tochter durchgeführten anonymen Befragung.

gesetzlichen Handlungspflichten, wenn zu ihrer Umsetzung betriebliche Regelungen erforderlich sind. Daher hat der Betriebsrat ein Mitbestimmungsrecht bei der Gefährdungsbeurteilung nach § 5 ArbSchG und § 3 BildschArbV[63]. Basis der Gefährdungsbeurteilung kann eine Datenerhebung bei den Mitarbeitern sein[64], über deren Inhalt im Nichteinigungsfall die Einigungsstelle entscheidet.

VI. Vorabkontrolle durch den Datenschutzbeauftragten

Sollen die Mitarbeiterumfragen personenbezogen erfolgen, unterliegt die Durchführung des Verfahrens der Vorabkontrolle durch den betrieblichen bzw. behördlichen DSB. (§ 33a Abs. 1 S. 5 LDSG NW; § 4d Abs. 6 BDSG). Während die Prüfpflicht für den behördlichen DSB den Regelfall bildet (§ 10 Abs. 3 LDSG), wird sie für den betrieblichen DSB ausgelöst, wenn automatisierte Verfahren besondere Risiken für die Rechte und Freiheiten der Betroffenen auslösen. Dies wird insbesondere unterstellt, wenn besondere Arten personenbezogener Daten verarbeitet werden oder die Daten der Bewertung der Persönlichkeit des Betroffenen dienen können. Die Vorabkontrolle entfällt, wenn § 28 Abs. 1 S. 1 Nr. 1 oder § 32 Abs. 1 Nr. 1 BDSG den Arbeitgeber zur Datenerhebung oder -verarbeitung berechtigt oder er diese nur bei Einwilligung durchführen will. Abhängig von der Art der abgefragten Daten ist damit die Vorabkontrolle geboten, da die Erlaubnisnorm nicht greift und die Wirksamkeit der Einwilligung zumindest vorab zunächst in Frage gestellt werden muss. Zudem sind die in § 4d Abs. 6 BDSG genannten Gefährdungsfälle nur beispielhaft, d.h. Gegenstand der Vorabkontrolle ist der Ausschluss der Verarbeitung der oben genannten sensiblen Daten unter Personenbezug oder Personenbeziehbarkeit zu den Befragten.

Vorgegangen werden kann gemäß nachstehender Checkliste[65]:

- Werden Mitarbeiterdaten in direkter oder indirekter Form verarbeitet?
- Lassen sich Fragen oder Antworten auf eine Person beziehen?
- Insbesondere: Ist der Personenkreis auf einen kleinen Personenkreis beschränkt und somit ein Personenbezug möglich?
- Ist die Freiwilligkeit sichergestellt?
- Ist der Feedback-Bogen anonymisiert oder pseudonymisiert?
- Wer hat bei pseudonymisierten Daten die Möglichkeit der Rückführung zu den Personen?
- Wird idealerweise ein neutraler Dienstleister eingesetzt?
- Handelt es sich um eine Funktionsübertragung oder Auftragsdatenverarbeitung?
- Bei festgestelltem Personenbezug: Auf welcher Rechtsgrundlage basiert die Mitarbeiterbefragung?

VII. Fazit

Die Zulässigkeit einer Mitarbeiterbefragung hängt zunächst davon ab, ob der Arbeitgeber im Rahmen seines sich aus dem Direktionsrecht ergebenden Weisungsrechts den Mitarbeiter anweisen kann, an der Befragung teilzunehmen.

Sodann ist – bei pauschalen Befragungen – relevant, ob die bei der Befragung beabsichtigte Datenerhebung mit den Datenschutzansprüchen der Mitarbeiter vereinbar ist. Ggf. ist die Erhebung zwar einerseits z.B. zu organisatorischen Zwecken erforderlich, wobei andererseits jedoch eine anonymisierte Erhebung genügt.

Ist die Teilnahmeanweisung nicht durch das Direktionsrecht gedeckt, kann die Befragung nur freiwillig erfolgen. Erfolgt die Datenerhebung in anonymisierter Form, stehen Datenschutzfragen nicht entgegen, d. h. es bedarf z.B. keiner datenschutzrechtlichen Einwilligung des Betroffenen.

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

Dr. Georg Wronka
Rechtsanwalt, beratende und gutachterliche Tätigkeit auf dem Gebiet des Datenschutz- und Wettbewerbsrechts; betrieblicher Datenschutzbeauftragter

63 BAG, NZA 2011, 651.
64 BAG, NZA 2014, 990.
65 Entnommem bei Keck, DatenschutzPraxis 10/11, 3.

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

Pay as you drive: Datenschutz in der Telematikversicherung

Das Angebot ist verführerisch. Daten gegen Geld. Wer der KfZ-Versicherung Einblick in sein Fahrverhalten gibt, kann bei vorsichtigem Fahrstil die Prämie senken. Seit Anfang des Jahres ist dies auch in Deutschland möglich. Kunden müssen dafür nur eine Box im Auto installieren, die Daten über das Fahrverhalten speichert und an den Versicherer übermittelt. In der Automobil- und Versicherungsbranche sind maßgeschneiderte Tarife schon seit langer Zeit ein Thema. Bislang stehen neben Datenschutzbedenken vor allem die hohen Infrastrukturkosten dem breiten Einsatz entgegen. Die Einführung des gesetzlich verpflichtenden eCalls ab Herbst 2015 ändert die Situation grundlegend. Mit dem Einbau der hierfür erforderlichen Technik ist künftig jedes Auto telematikfähig. Das Argument der hohen Infrastrukturkosten ist dann hinfällig. Versicherungsexperten gehen davon aus, dass pay-as-you-drive-Tarife bereits in wenigen Jahren eine feste Größe im Kfz-Versicherungsmarkt darstellen. Aus Sicht des Datenschutzes spricht nichts gegen Telematiktarife, wenn die Kunden einwilligen und die Datenschutzgrundsätze eingehalten werden. Risiken entstehen jedoch abseits des eigentlichen Tarifmodells. Diesen versteckten datenschutzrechtlichen Gefahren geht der Beitrag nach.

I. Einleitung

Die Kfz-Versicherung befindet sich im Umbruch. Im Zuge intelligenter und vernetzter Automobile hält die Telematikversicherung Einzug in den Haftpflichtversicherungsmarkt. Nicht zuletzt die Car2Car Kommunikation und der automatische Notruf eCall[1] verändern das Fahrverhalten auf deutschen Straßen, auch Versicherungen bemühen sich um das Auto der Zukunft. Als erster deutscher Versicherer bietet die „Sparkassen Direkt Versicherung" (S-Direkt) seit Beginn des Jahres ein Tarifmodell an, dessen Versicherungsprämie in Abhängigkeit des Fahrverhaltens bemessen wird. Dieses Versicherungsmodell ist bisher einmalig auf dem deutschen Markt. Neu ist es hingegen nicht, amerikanische und britische Agenturen bieten bereits seit Jahren erfolgreich fahrbezogene Telematikversicherungen an[2].

Das Tarifmodell erfordert eine detaillierte und dauerhafte Datenverwendung, um die fahrbezogene Versicherungsprämie bestimmen zu können[3]. Datenschützer befürchten dadurch eine Überwachung des Autofahrers, die ungewollte und ausufernde Datenverwendungen nach sich ziehen könnten[4]. Denn bereits erhobene Daten wecken Begehrlichkeiten auf Seiten weiterer Wirtschaftsteilnehmer abseits des Versicherungsmarktes. Durch die Möglichkeit, mithilfe der Daten Bewegungs-, Nutzungs- und Kommunikationsprofile zu erstellen[5], erlangen die Fahrdaten einen Wert, dessen wirtschaftliche Bedeutung vom Fahrzeugnutzer nicht abschätzbar ist. Kritische Auseinandersetzungen müssen jedoch berücksichtigen, dass es sich bei diesem Versicherungsmodell nicht um eine zwingende Datenpreisgabe handelt. Die Telematikversicherung ist lediglich ein neues Tarifangebot an den Versicherungskunden. Die datenschutzrechtliche Risikobewertung muss sich daher an der vertraglichen Gestaltung der vorhandenen Versicherungsbedingungen orientieren. Die Art und Weise der Datenverwendung sollte dem Kunden größtmöglichen Schutz bieten, wenn er sich für das Angebot entscheidet. Dafür müssen die gesetzlichen Datenschutzmaßnahmen ausreichend berücksichtigt und eingehalten werden. Es steht daher nicht zur Debatte, ob Telematikversicherungen aus Datenschutzsicht grundsätzlich zulässig sind, sondern ob ihre jeweilige Umsetzung datenschutzkonform ist.

Der vorliegende Beitrag bietet zunächst eine Übersicht des neuen Versicherungsmodells (II.) und bewertet dieses vor ausgewählten datenschutzrechtlichen Gesichtspunkten (III.), abschließend wird das Versicherungsmodell einer kritischen Würdigung unterzogen (IV.).

II. Darstellung des Versicherungsmodells am Beispiel S-Drive[6]

Die Telematikversicherung ist auf dem deutschen Versicherungsmarkt ein Novum. Das Verständnis ihres Ablaufs bedingt die Erklärung anhand existierender Vertragsregelungen. Da die „Sparkassen Direkt Versicherung" bisher einziger Anbieter des Versicherungsmodells ist, sollen hier stellvertretend deren Vertragsbestimmungen zur Beschreibung der Funktionsweise herangezogen werden.

Der Versicherungsnehmer erhält nach Abschluss des Vertrags eine Messbox, die in seinem Fahrzeug installiert wird. Die Box zeichnet auf, wann, wo und wie schnell gefahren wurde. Ebenfalls registriert sie starke Beschleunigungen und abrupte Bremsvorgänge. Der Kunde erhält einen kennwortgeschützten Zugang zu einem Webportal und einer Smartphone-App, wodurch er jede einzelne Fahrt nachträglich betrachten und nachvollziehen kann. Gleichzeitig beinhaltet der Service eine Fahrzeugortungs-Funktion und einen automatischen Notruf. Bei Diebstahl des Pkws können Versicherungsnehmer oder Versicherungsgeber eine Ortung durchführen. Zudem registrieren Crash-Sensoren

1 Zum Datenschutz beim automatischen Notruf siehe auch Lüdemann/Sengstacken, Lebensretter eCall: Türöffner für neue Telematikdienstleistungen, RDV 2014, 177; Rohwetter, Geheimfunk im Notruf, Die Zeit 29/2014, S. 25.

2 Die Versicherungsmodelle besitzen eine große Popularität auf dem Markt der Fahranfänger bspw. mit dem Versicherungspaket „drive like a girl", abrufbar unter: http://www.drivelikeagirl.com/.

3 Roßnagel, Datenschutz in der künftigen Verkehrstelematik, NZV 2006, 281.

4 So unter anderem der ehemalige Bundesdatenschutzbeauftragte Schaar, abrufbar unter: http://www.autohaus.de/telematik-telefonica-vernetzt-auto-und-versicherung-1237602.html.

5 Weichert, Datenschutz im Auto – Teil 2, SVR 2014, 241.

6 Die folgenden Darstellungen sind den Vereinbarungen zum Telematik-Sicherheits-Service (S-Drive-Service) der Sparkassen-Direkt-Versicherung entnommen, abrufbar unter: https://www.sparkassen-direkt.de/fileadmin/pdf/telematik/Endkundenvertrag.A2.2.pdf. Zudem bietet nun die Signal-IDuna Tochter Sijox eine pay as you drive-Versicherung an, siehe www.aap-drive.de.

eine Kollision anhand von Beschleunigungskräften. Das System übermittelt den exakten Unfallort, die Stärke der Beschleunigungskräfte, Uhrzeit und Fahrtrichtung an eine Notrufstelle.

Die Datenverarbeitung findet in zwei voneinander getrennten Datenkreisen statt. Die von der Box gemessenen Werte werden in Form von Rohdaten alle 20 Sekunden an einen Kooperationspartner gesendet[7]. Dort werden sie im Auftrag gegen eine Kunden-ID erhoben und verarbeitet. Persönliche Daten, die Rückschlüsse auf eine bestimmte Person zulassen, besitzt nur der Versicherungsgeber. Der Kooperationspartner und von ihm beauftragte Subunternehmen ermitteln auf Grundlage der Datensätze Score-Werte. Nach der Bearbeitung erhält die Versicherung monatlich insgesamt fünf Score-Werte. Vier Score-Werte ergeben sich für Geschwindigkeit, Fahrweise, Nachtfahrten und Stadtfahrten, aus ihnen wird ein Gesamtscore durch Gewichtung der Einzelscores ermittelt. Dem Versicherungsgeber ist es nicht möglich, dem Versicherungsnehmer einzelne Fahrten zuordnen. Diese Möglichkeit besitzt lediglich der Kunde, indem der Kooperationspartner die aufbereiteten Daten auf dem Webportal bzw. der App zur Verfügung stellt.

Auf Grundlage der Score-Werte ermittelt der Versicherungsgeber die zu zahlende Versicherungsprämie. Erreicht der Kunde einen guten Jahres-Gesamtpunktwert, erhält er einen Rabatt von 5% auf seine nächste Jahres-Beitragsrechnung. Liegt der Score unter dem festgelegten Zielwert, wird kein zusätzlicher Beitrag fällig, es bleibt bei der zum Vertragsabschluss vereinbarten Versicherungsprämie. Zusätzlich werden dem Kunden jährlich 71,40 EUR für die Bereitstellung der Telematikbox in Rechnung gestellt.

III. Datenschutzrechtliche Beurteilung

Die Telematikversicherung im Kfz-Bereich ist grundsätzlich rechtskonform[8]. Die datenschutzrechtliche Legitimation ergibt sich aus dem Versicherungsvertrag und umfasst gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG jene Datennutzung, die für die Erfüllung des Vertragszwecks erforderlich ist. Da die freiwillige Entscheidung des Versicherungsnehmers die Datenverwendung bestimmt und auslöst, handelt es sich um ein in den Grenzen des Bundesdatenschutzrechts frei zu gestaltendes Vertragsverhältnis. Die proklamierten Risiken der Fahrerüberwachung und der Erstellung von Bewegungsprofilen werden durch die vorhandene Vertragsgestaltung nicht erfüllt.

Denn obgleich die installierte Messbox personenbezogene Daten erhebt, werden diese zur weiteren Verarbeitung an den Kooperationspartner sowie dessen beauftragte Subunternehmer pseudonymisiert übermittelt. Die Erhebung unter Nutzung der Kunden-ID verhindert den Rückschluss auf den Versicherungsnehmer. Eine Herstellung des Personenbezugs ist an dieser Stelle nur mit einer entsprechenden Referenzliste möglich[9]. Der Versicherungsgeber selbst erhält lediglich aggregierte Datensätze als Scorewerte. Diese können dem Versicherungsnehmer zwar zugeordnet werden, besitzen jedoch nicht die erforderliche Informationstiefe, um eine Erstellung von Bewegungsprofilen zu ermöglichen. Der Versicherungsgeber erhält keine detaillierten Datensätze, damit er keine fahrtgenaue Überwachung betreiben kann. Das System zweier getrennt gestalteter Datenverwendungskreise ermöglicht hinsichtlich der Fahrtüberwachung durch die Versicherung einen ausreichenden Datenschutz.

Darüber hinaus eröffnen sich jedoch Risikopotentiale, die in der bisherigen Kritik kaum Beachtung gefunden haben. Diese betreffen insbesondere die Fahrzeugnutzung durch Dritte, die automatische Bemessung der Versicherungsprämie sowie Datenverwendungsmöglichkeiten über den Versicherungsgeber hinaus.

1. Überwachungsrisiko durch den Versicherungsnehmer

Ein Überwachungsrisiko ergibt sich nicht durch den Versicherungsgeber, sondern in Person des Versicherungsnehmers. Eine vertragliche Regelung und damit eine datenschutzrechtliche Erlaubnis existiert nur zwischen der Versicherung und ihrem Kunden. Mittels Kennwortzugang zum Webportal bzw. zur App erhält ausschließlich der Versicherungsnehmer Einsicht in die Fahrtdaten des Pkw. Dadurch besitzt er die uneingeschränkte Möglichkeit, das betroffene Fahrzeug und dessen Nutzung ständig überwachen zu können. Weichen Fahrzeugnutzer und Versicherungsnehmer voneinander ab, können die Fahrdaten von Letzterem uneingeschränkt eingesehen werden. Der Versicherungsgeber bestimmt in den Vertragsbedingungen, dass der Versicherungsnehmer jeden anderen Nutzer des Fahrzeugs darauf hinzuweisen hat, dass eine Erfassung der Fahrtdaten erfolgt und diese von ihm eingesehen werden können[10].

Bei der privaten Pkw-Nutzung mag dieses Risiko gering erscheinen, da im familiären Bereich eine Überwachung der Fahrdaten und des Aufenthaltsortes nur private Konsequenzen nach sich zieht[11]. Gleichwohl ist das Recht auf informationelle Selbstbestimmung eines dritten Fahrers gefährdet, wenn die Datenerhebung nicht offensichtlich ist. Denn sein Recht kann er nur wahrnehmen, wenn er weiß, ob und wie Daten über ihn erhoben werden. Die Transparenz der Datenverarbeitung müsste an dieser Stelle den Datenschutz gewährleisten[12]. Kommt der Versicherungsnehmer seiner Hinweispflicht zur Datenverarbeitung nicht nach, müsste die technische Gestaltung der Messbox die Transparenz der Datenverarbeitung gewährleisten. Der Vorgang der Datenerhebung sollte dem Fahrer stets im Pkw angezeigt werden, so dass er sich des Eingriffs in sein Recht auf informationelle Selbstbestimmung bewusst ist. Gleichwohl müsste ihm die Möglichkeit zugestanden werden, die Datenverarbeitung unterbrechen zu können. Dies ist nicht möglich, da ein Ausbau oder eine Stilllegung des Geräts ohne vorheriges Einverständnis des Versicherungsgebers nicht erlaubt ist[13]. Diese technisch bedingte Wahlbehinderung müsste

7 Im Rahmen des S-Drive-Service werden die Daten an den Téléfonica Digital Instance Server im Hosting Center der TeleCityGroup nach London gesendet und dort von der Firma Masternaut verarbeitet.

8 So auch der Landesdatenschutzbeauftragte Schleswig-Holsteins Weichert, abrufbar unter: http://www.heise.de/newsticker/meldung/Datenschuetzer-warnt-vor-Versicherungstarif-mit-Wanze-im-Auto-2074881.html.

9 Gola, in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 3a Rn. 10.

10 § 7 der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

11 Ebenfalls möglich ist ein Anwendungsausschluss des BDSG gem. § 1 II Nr. 3 BDSG, da die Datenerhebung ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt; a. M. Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl., § 1 Rn. 10, welcher den Ausschluss nur begründet, wenn die Datenverarbeitung nicht automatisiert erfolgt; ebenso restriktive Auslegung lt. Dix, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl. 2011, § 1 Rn. 148 m. w. N.

12 In diese Richtung auch Roßnagel, 281 (Fn. 3).

13 § 5c der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

zumindest für anderweitige Nutzer offensichtlich gemacht werden, indem die Transparenz der Datenerhebung durch Signale oder Icons im Fahrzeug hergestellt würde[14].

Problematischer erweist sich das Überwachungsrisiko bei dienstlicher Fahrzeugnutzung, etwa bei Außendienstmitarbeitern. Der Abschluss einer Telematikversicherung für Dienstfahrzeuge ermöglicht dem Arbeitgeber die Überwachung des Arbeitnehmers auf unkomplizierte Weise. Für den Arbeitgeber ist es lohnenswert zu wissen, ob sich der Außendienstmitarbeiter auf dem schnellsten Weg zum Kunden begibt, ob er während der Fahrt an anderen Orten verweilt und wie lange er sich tatsächlich beim Kunden aufhält. Der Vorgang der telematikbasierten Standortnutzung ist vergleichbar mit der Ortungsmöglichkeit eines Betriebsmobiltelefons[15]. Dabei besteht eine vertragliche Vereinbarung ebenfalls nur zwischen dem Telekommunikationsdienstleister und dem Arbeitgeber als Vertragskunde. Der Arbeitgeber ist gem. § 98 Abs. 1S. 2 TKG verpflichtet, weitere Nutzer über die erteilte Einwilligung in die Handyortung zu informieren. Unterlässt er dies, besteht die Gefahr der heimlichen Überwachung des Arbeitnehmers. Eine Rechtfertigung für den Einsatz dieser Überwachungsmöglichkeit könnte gem. § 32 Abs. 1 S. 1 BDSG durch das arbeitsvertragliche Kontrollinteresse des Arbeitgebers gegeben sein[16]. In diesem Zusammenhang dürfen personenbezogene Daten des Beschäftigten verarbeitet werden, wenn dies für die Durchführung des Beschäftigtenverhältnisses erforderlich ist. Erlaubt ist eine Datennutzung etwa für die Optimierung des Fuhrparkeinsatzes oder das Aufspüren gestohlener Fahrzeuge[17]. Eine vollständige Kontrolle des Arbeitnehmers am externen Arbeitsplatz würde jedoch einen unzulässigen Eingriff in das Persönlichkeitsrecht darstellen, insbesondere wenn der Pkw auch der zusätzlichen privaten Nutzung unterliegt[18]. Diese Grundsätze müssten auch für die Überwachung des Arbeitnehmers durch die Standortbestimmung mittels Telematikversicherung gelten. Denn es könnte ein zusätzlicher Druck auf den Arbeitnehmer entstehen, indem sein Fahrverhalten der ständigen Kontrolle unterliegt. Eine Konfliktsituation zwischen Fahrüberwachung und termingerechter Wahrnehmung von Außendienstterminen wäre die Folge.

Ebenso stellt sich bei der Mehrfachnutzung des Fahrzeugs die Frage, wem die erzeugten Versicherungsscores zuzurechnen sind. Die Scores werden ausschließlich auf Grundlage der Fahrleistung ermittelt, eine Autorisierung des Fahrers erfolgt nicht. Sie werden grundsätzlich dem Versicherungsnehmer zugeordnet. Eine nachträgliche Berichtigung der Fahrtdaten erscheint ausgeschlossen. Dies folgt allein schon aus den Versicherungsbedingungen, die gleichfalls einen nachträglichen Korrekturanspruch von Fehlmessungen durch das Messsystem ausschließen[19].

2. Risiko der automatisierten Einzelentscheidung

Bedenklich erscheint vor dem Hintergrund des Verbots der automatisierten Einzelentscheidung die Berechnung der telematikbasierten Versicherungsprämie. Denn eine Bewertung, die den Betroffenen auf ein bloßes Objekt eines automatisierten Entscheidungsverfahrens reduziert, unterliegt dem Verbot des § 6a BDSG. Der Gesetzgeber beabsichtigt, vor automatisierten, beeinträchtigenden Entscheidungen zu schützen, die ausschließlich aufgrund der Bewertung von Persönlichkeitsprofilen ergehen, ohne dass der Betroffene die Möglichkeit der Einflussnahme oder der Nachvollziehbarkeit hat[20].

Die durch Telebox erhobenen personenbezogenen Daten bilden die ausschließliche Datenbasis, auf welcher mithilfe des Scoreverfahrens eine unmittelbare Entscheidung über den Versicherungsnehmer getroffen wird[21]. Grundlage der automatisierten Einzelentscheidung bildet die Bewertung von Persönlichkeitsmerkmalen, welche laut Art. 15 Abs. 1 EU-DatSchRl auch Verhalten und Zuverlässigkeit von Personen umfassen. Persönlichkeitsmerkmale setzten somit eine gewisse Komplexität voraus[22]. Der Versicherungsgeber erhält Score-Werte über Geschwindigkeit, Fahrweise sowie Nacht- und Stadtfahrten. Der Score Geschwindigkeit erfasst die Einhaltung von Geschwindigkeitsbegrenzungen und verschlechtert sich bei Überschreitungen. Mithilfe des Scorewertes kann daher ein Rückschluss auf Verhalten und Zuverlässigkeit des Versicherten erfolgen. Ein weiterer Rückschluss auf das Verhalten ist durch die Score-Werte Stadtfahrt und Nachfahrt möglich. Sie veranschaulichen, zu welcher Tageszeit und auf welche Art der Versicherte sein Fahrzeug nutzt. Zusätzlich wird die Fahrweise bewertet. Diese vier Score-Werte stellen Aspekte der Persönlichkeit des Versicherungsnehmers dar; werden sie miteinander verknüpft, kann die Persönlichkeit des Versicherungsnehmers abgelesen und bewertet werden.

Die Ausschließlichkeit der automatisierten Entscheidung liegt vor, wenn keine inhaltliche Bewertung und eine darauf gestützte Entscheidung durch eine natürliche Person stattfindet. Eine Umgehung des Verbots soll insbesondere verhindert werden, indem lediglich eine mehr oder minder formale Bearbeitung durch einen Menschen erfolgt, der keine Befugnis oder ausreichende Datengrundlage besitzt, um von der automatisierten Entscheidung abweichen zu können[23]. Der Entscheidung muss daher ein menschliches Ermessen zugrunde liegen. Die profane Übernahme einer vorbereiteten automatisierten Entscheidung ist dabei nicht angebracht, der menschliche Entscheidungsträger muss einen Spielraum für abweichende Entscheidungen besitzen. Für die Ermittlung der Versicherungsprämie ist ausschließlich die Gesamtsumme der Score-Werte entscheidend, weitere Faktoren oder gar eine Überprüfung der ermittelten Datensätze findet nicht statt[24].

Auch weitere Gesichtspunkte zur Ermittlung der Versicherungsprämie fließen nicht in die Entscheidung ein. Vielmehr wird nicht einmal die auftretende Fehlerquote von falsch gemessenen Daten der Telebox berücksichtigt[25]. Bisher besteht auch keine Möglichkeit der Korrektur[26]. Durch menschliche

14 So auch für andere Bereiche in der Kfz-Telematik gefordert von Weichert, Datenschutz im Auto – Teil 2, SVR 2014, 241.

15 Gola, Datenschutz bei der Kontrolle „mobiler" Arbeitnehmer, NZA 2007, 1139.

16 Hallaschka/Jandt, Standortbezogene Dienste im Unternehmen, MMR 2006, 436.

17 Wedde, in: BDSG, § 32 Rn. 104 (Fn. 11).

18 Gola, 1139 (Fn. 15); so auch die permanente Ortung verneinend Wedde, in: BDSG, § 32 Rn. 108 (Fn. 11).

19 § 1e der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

20 Klug, in: Gola/Schomerus, BDSG § 6a Rn. 1 (Fn. 9).

21 Vgl. Scholz, in: Simitis (Hrsg.), BDSG, § 6a Rn. 5 (Fn. 11).

22 Klug, in: Gola/Schomerus, BDSG, § 6a Rn. 7 und 9 (Fn. 9).

23 So die Begründung zur Novellierung des § 6a I BDSG und der Einführung des Satz 2 im Jahr 2009, siehe BT-Drs. 16/10529 S. 13; Abel, Die neuen BDSG-Regelungen, RDV 2009, 147.

24 § 9e der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

25 § 1d der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

26 § 1e der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

Überprüfung könnte jedoch ein höheres Vertrauenspotenzial in das Versicherungsmodell generiert werden.

Die rechtliche Folge der automatisierten Entscheidung beeinträchtigt den Betroffenen in erheblichem Maße, denn mit ihr gehen relevante negative Folgen für den Betroffenen einher[27]. Ungeachtet der Folge einer möglichen höheren Versicherungsprämie kommt grundsätzlich eine erhebliche Beeinträchtigung des Versicherungsnehmers in seinem Persönlichkeitsrecht in Betracht. Denn der Zweck des BDSG ist es gemäß § 1 Abs. 1 BDSG, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird[28]. Es soll gewährleisten, dass der Einzelne selbst bestimmt, wann welche Informationen über ihn preisgegeben werden, um ein selbständiges Gesellschaftsmitglied zu sein[29]. Andernfalls würde der Einzelne zum Adressat von „optimierten" Verhaltenserwartungen degradiert werden[30]. Es stellt sich die Frage, inwiefern der Versicherungsnehmer sich bei dieser Entscheidungsgrundlage eigenständig verhalten kann. Zwar erteilt er seine Erlaubnis, dass seine personenbezogenen Daten erhoben und verarbeitet werden, allerdings wird ihm die Möglichkeit entzogen, deren Auswertung inhaltlich zu kontrollieren. Dadurch wird er gezwungen, sein Verhalten anzupassen, um in den Genuss eines Rabatts zu gelangen.

Darüber hinaus liegt eine erhebliche Beeinträchtigung vor, wenn der Betroffene durch die Entscheidung in seiner wirtschaftlichen oder persönlichen Entfaltung nachhaltig gestört wird[31]. Wenn anzunehmen ist, dass sich telematikbasierte Versicherungsmodelle auf dem Versicherungsmarkt durchsetzen, wird sich auch die Kostenstruktur alternativer Versicherungsmodelle verändern. Daraus würde folgen, dass durch einen hohen Zuspruch der Versicherungsnehmer die Preise für alternative Angebote steigen. Versicherungsnehmer könnten gezwungen sein, telematikbasierte Angebote annehmen zu müssen. Sie wären damit in ihrer Wahlfreiheit eingeschränkt und müssten ihre Daten unfreiwillig zur Verfügung stellen, obgleich sie dies nicht wünschen. Ein derartiger Zwang würde gleichfalls eine Beeinträchtigung der informationellen Selbstbestimmung bedeuten, da ein datenschützendes Verhalten nur noch unter unverhältnismäßigem Aufwand möglich wäre.

3. Risiko weiterer Datenverwendungen

Werden Daten für einen bestimmten Zweck erhoben, bergen sie grundsätzlich die Gefahr der Begehrlichkeit weiterer Wirtschaftsteilnehmer zu unterliegen. Datenverwendungsmöglichkeiten eröffnen sich dabei nicht nur im privatwirtschaftlichen Umfeld, sondern auch im Bereich der Unfallaufklärung bis hin zur Verfolgung von Straftaten. Mittels Telematikversicherung erhobene Daten könnten insbesondere genutzt werden, um die Aufklärung von Verkehrsdelikten zu beschleunigen und zu vereinfachen[32]. Ihre Nutzung durch Strafverfolgungsbehörden ist dabei eine naheliegende Verwendungsmöglichkeit, die unter dem Deckmantel der Unfallaufklärung begründet werden könnte.

Rückblickend betrachtet, hat sich das Strafverfolgungsinteresse auch auf neue technische Entwicklungen und moderne Kommunikationsmöglichkeiten ausgeweitet. Mithilfe von modernen Kommunikationsmedien erhobene Daten müssen gem. § 100a ff StPO unter Umständen den Strafverfolgungsbehörden zur Verfügung gestellt werden[33]. Dieses Interesse könnte auch auf mittels Telematikversicherung erhobene Daten ausgeweitet werden, dafür bedürfte es jedoch einer gesetzlichen Erlaubnis. Eine Parallele ergibt sich zur strafrechtlichen Verwertung von Autobahnmautdaten, sog. „TollCollect Daten". Das LG Magdeburg hatte zu entscheiden, ob eine Herausgabe dieser Daten an die Strafverfolgungsbehörden im Diebstahlsfall gemäß § 100 g f. StPO rechtmäßig ist[34]. Dieses wurde mit der Begründung verneint, dass die Erhebung der Daten unter strenger gesetzlicher Zweckbestimmung des Autobahnmautgesetzes erfolgte. Eine darüber hinausgehende Datenverwendung würde eine Zweckänderung mit sich bringen, die der Gesetzgeber ausdrücklich verweigert[35]. Eine derartige gesetzliche Zweckbestimmung existiert für Daten aus Telematikversicherungen nicht. Ihre Verwendung wird lediglich durch zugrundeliegende Vertragsbedingungen bestimmt. Eine Ausweitung auf andere Zwecke erscheint daher möglich. Mit dieser Maßnahme könnten Verkehrsunfälle effektiver aufgeklärt werden, dies gilt auch für leichte Verkehrsverstöße z.B. Geschwindigkeitsübertretungen. Denn die Daten liegen erhoben vor und werden, obgleich für einen anderen Zweck, zunächst gespeichert. Zu beachten ist dabei, dass eine Verwendung für andere Zwecke vor dem Hintergrund des § 28 II BDSG zu beurteilen ist. Demzufolge ist eine Übermittlung von Daten für einen Zweck zulässig, der der Verfolgung von Straftaten dient, und wenn kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. An der Interessenabwägung lässt sich bereits eine restriktive Auslegung des Ausnahmetatbestandes erkennen, nicht zuletzt muss sich auch die ursprüngliche Datenerhebung der verantwortlichen Stelle auf die Erfüllung eigener Geschäftszwecke beschränken. Als Beispiel sei genannt, dass auch der Arbeitgeber die Fahrtdaten seiner Dienstwagenflotte nur bei schwerwiegenden Verkehrsverstößen an die Polizei herausgeben wird[36].

Eine weitere Ähnlichkeit lässt sich zum Einsatz von Unfalldatenspeichern erkennen. Auch diese erfassen die Fahrdaten und können bei Unfällen zur Aufklärung der Sachlage dienen. Entscheidender Unterschied bei der Datenerfassung ist, dass die Daten im Unfalldatenspeicher im Abstand von 45 Sekunden überschrieben werden und der Fahrzeugführer die Möglichkeit hat, mittels Knopfdruck gespeicherte Daten zu löschen[37]. Diese Möglichkeit bleibt dem Versicherungsnehmer bei Telematikdaten verwehrt. Diese Tatsache fällt besonders ins Gewicht, wenn der Fahrzeugführer sich durch die erfassten Daten selbst belas-

27 Scholz, in: Simitis (Hrsg.), BDSG, § 6a Rn. 28 (Fn. 11).

28 Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl., § 1 Rn. 1.

29 Gola, in: Gola/Schomerus, BDSG, § 1 Rn. 7 (Fn. 9); Roßnagel, 281, 282 (Fn 3).

30 Simitis, in: Simitis (Hrsg.), BDSG, § 1 Rn. 36 (Fn. 11).

31 Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Aufl. 2008, S. 159.

32 Roßnagel, 281, 281 (Fn. 3).

33 Roßnagel, 281, 285 (Fn. 3); zu dieser Problematik auch Mielchen, Daniela, Verrat duch den eigenen PKW – wie kann ich mich schützen, SVR 3/2014, 81.

34 LG Magdeburg, NStZ 2006, 34.

35 Vgl. LG Magdeburg, Beschluss vom 03.02.2006 – 25 Qs 7/06; ebenso das Bundesamt für Datenschutz und Informationssicherheit, abrufbar unter http://www.bfdi.bund.de/DE/Themen/WirtschaftUndFinanzen/Verkehr/Artikel/MautdatenFuerVerbrechensbekaempfung.html?nn=409802.

36 Gola, in: Gola/Schomerus, BDSG, § 28 Rn. 38 (Fn. 9).

37 Informationen zum Kienzle UDS, abrufbar unter http://www.rgvs.de/Angebote/UDS/uds.html.

ten könnte. Denn einen tatsächlichen Zugriff auf die gespeicherten Daten hat lediglich der Versicherungsgeber durch Anfrage beim datenverarbeitenden Subunternehmen. Nur dort kann eine Löschung veranlasst werden. Fraglich ist, ob der Versicherungsgeber bei Anfrage der Verfolgungsbehörde die Daten tatsächlich bereitstellt. Diese Praxis ist wahrscheinlich, da Versicherungen bereits jetzt Auskunft erteilen über Angaben, die im Rahmen von Schadensanzeigen getätigt werden. Es ist zwar möglich, diesen Eingriff in das Grundrecht auf informationelle Selbstbestimmung des Einzelnen zu rechtfertigen, wenn es dem überwiegenden Interesse der Allgemeinheit dient. Ein derartiger Eingriff wird in der Regel jedoch nicht bei geringfügigen Unfallschäden gerechtfertigt sein[38].

Derartige Datenauskünfte könnten gegen den nemo-tenetur-Grundsatz verstoßen[39]. Diesem Grundsatz zufolge ist niemand verpflichtet, sich selbst anzuklagen bzw. sich selbst zu belasten[40]. Bei der Verwendung von Telematikdaten, die ursprünglich freiwillig und mittels Einwilligung des Versicherungsnehmers für die Bemessung der Versicherungsprämie erhoben wurden, würde durch die Beschlagnahmung der Daten der nemo-tenetur-Grundsatz vollständig ausgehöhlt[41]. Um diesen Umstand zu umgehen, müsste der Versicherungsnehmer als erstes einen Zugriff auf die erhobenen Daten haben. Dies könnte durch eine Autorisierung der Rohdaten zur weiteren Verarbeitung erfolgen oder eine nachträgliche Löschungsmöglichkeit. Diese Maßnahme würde jedoch dem Versicherungsprinzip zuwider laufen, da der Versicherungsgeber nicht mehr zwingend alle relevanten Daten erhalten würde. Zudem erschwert sich die Lage, wenn nicht der Versicherungsnehmer sondern ein Dritter gefahren ist. Sodann wäre der Versicherungsgeber in der Lage, die Daten an die Verfolgungsbehörden herauszugeben. Dabei könnte es sich jedoch um Daten handeln, deren Erhebung nicht durch den Dritten autorisiert wurde, da kein Vertragsverhältnis zwischen ihm und der Versicherung besteht. Eine Übermittlung wäre in diesem Fall unzulässig.

Vor dem Hintergrund der Datenverwendungsmöglichkeiten ist es daher unzureichend, dass der Versicherungsnehmer derzeit keinen Einfluss auf die Weitergabe oder ihre Löschung hat.

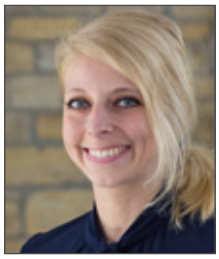
IV. Fazit

Die Telematikversicherung kann grundsätzlich die Datenschutzregelungen erfüllen. Individuelle vertragliche Vereinbarungen verhindern es nicht, dass der Versicherungsnehmer einen ausreichenden Schutz seiner Datenverwendungen erwarten darf. Dieser Schutz steht allerdings in Abhängigkeit des Vertragspartners und darf nicht zu Lasten ausufernder Versicherungsbedingungen in den Hintergrund gedrängt werden.

Die Betrachtung des derzeitigen Versicherungsmodells zeigt ungeklärte Sachverhalte auf, die sich rechtlich in einer Grauzone bewegen. So könnte ein Verbot der automatisierten Einzelfallentscheidung vorliegen, indem die Prämienbemessung vollständig ohne menschliches Ermessen erfolgt. Dieser Vorgang wird nicht allen Fahrtsituation gerecht, da es oftmals auf die spontane Reaktion des Fahrers im Einzelfall ankommt. Eine pauschalierte Delegierung an eine automatische Entscheidungseinheit verkennt diesen menschlichen Aspekt. Ebenso ist es fraglich, die Informationspflicht über die Datenverwendung bei der Pkw-Nutzung durch Dritte an den Versicherungsnehmer zu delegieren. Eine Datenverwendung durch den Versicherungsgeber als verantwortliche Stelle beinhaltet auch die Informationspflicht des Betroffenen. Insbesondere im Bereich der Arbeitnehmerüberwachung ergibt sich eine gefährliche Korrelation zum Arbeitnehmerschutz.

Grundsätzlich gilt es zu beachten, dass im hart umkämpften Versicherungsmarkt der Datenschutz nicht auf Kosten des Versicherungsnehmers ausgehöhlt wird und zu einer Randbedingung degradiert wird. Obgleich bisher nur ein einziger Anbieter von Telematikversicherungen auf dem deutschen Markt existiert, könnten weitere Versicherungsgesellschaften nachziehen. Das verführerische Versprechen des Anbieters, durch zusätzliche Datenpreisgabe die Versicherungskosten zu senken, darf das Datenschutzbewusstsein der Versicherungsnehmer nicht verdrängen. Nahezu unausweichlich wird die restriktive Datenpreisgabe für den risikobewussten Verbraucher jedoch dann, wenn das Versicherungsmodell sich durchsetzt und alternative Angebote zur Ausnahme werden. An dieser Stelle wäre der Gesetzgeber gefordert, zu Beginn kritischer Auseinandersetzungen rechtliche Klarheiten zu schaffen. Dies gilt nicht zuletzt mit Hinblick auf mögliche Datenverwendungen durch die Strafverfolgungsbehörden, sondern auch auf jene im privatwirtschaftlichen Bereich. Ansonsten droht dem Autofahrer eine dauerhafte Überwachung durch das eigene Fahrzeug.

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, LL.M.
ist Referentin für Datenschutz und Compliance bei der Amprion GmbH in Dortmund. Zuvor war sie wissenschaftliche Mitarbeiterin und Projektleiterin am Forschungszentrum Energiewirtschaft und Energierecht (fee) der Hochschule Osnabrück und beschäftigte sich schwerpunktmäßig mit aktuellen datenschutzrechtlichen Fragestellungen.

Kerstin Vogelpohl
studiert an der Hochschule Osnabrück Wirtschaftsrecht LL.B. Neben ihrem Studium ist sie als studentische Hilfskraft am Forschungszentrum für Energiewirtschaft und Energierecht (fee) der Hochschule Osnabrück im Bereich Datenschutzrecht tätig.

38 Mielchen, 81, 85 (Fn. 33).

39 Vgl. § 136 I S. 2 StPO.

40 Pfeiffer, in: Pfeiffer, Strafprozessordnung Kommentar, 5. Aufl. 2005, § 136 StPO Rn. 4.

41 Mielchen, 81, 85 (Fn. 33).

Andreas Neumann

Telekommunikationsdatenschutz für geschlossene Benutzergruppen nach der TKG-Novelle 2012

Sind Betreiber von Krankenhäusern, Hotels und Gaststätten beim Angebot von Telekommunikationsdiensten noch an §§ 91 ff. TKG gebunden?

Seit Inkrafttreten des TKG 1996 unterlagen Anbieter von Telekommunikationsdiensten spezifischen Datenschutzvorschriften des Telekommunikationsrechts. Das galt unabhängig davon, ob sich das betreffende Angebot an die Öffentlichkeit oder nur an einen (mehr oder weniger) eng abgegrenzten Kreis von Nachfragern, eine sog. „geschlossene Benutzergruppe", richtete. Damit mussten z.B. auch Betreiber von Krankenhäusern, Hotels und Gaststätten, die ihren Patienten bzw. Gästen die Nutzung eines Telefon- oder Internetanschlusses anboten, grundsätzlich die gegenüber dem allgemeinen Datenschutzrecht strengeren Vorgaben des Telekommunikationsdatenschutzrechts einhalten. Der Beitrag geht der Frage nach, ob sich mit der TKG-Novelle 2012 hieran etwas geändert hat.

I. Einleitung

Neben den klassischen Telekommunikationsanbietern im Festnetz- und Mobilfunkbereich, deren Hauptgeschäftszweck im Angebot von Telekommunikationsdiensten liegt, bieten auch viele zumeist kleinere Unternehmen ihren Kunden telekommunikative Leistungen im Rahmen eines davon unabhängigen Geschäftszwecks an. Typische Beispiele für solche eigentlich telekommunikationsfremden[1] Anbieter sind Betreiber von Krankenhäusern, Hotels und Gaststätten, die ihren Patienten bzw. Gästen die Nutzung eines Telefon- oder Internetanschlusses anbieten[2]. Diese Angebote richten sich explizit nur an solche Personen, die unabhängig von der Inanspruchnahme der jeweiligen Telekommunikationsdienste eine spezifische rechtliche – zumeist vertragliche – Beziehung mit dem jeweiligen Anbieter eingegangen sind oder sonst einem abgrenzbaren Personenkreis angehören: Das Telefon in einem Krankenhauszimmer wird dem dortigen Patienten zur Verfügung gestellt, und der Internetzugang in einem Internet-Café den anwesenden Gästen. Man spricht deshalb insoweit auch von einer geschlossenen Benutzergruppe[3]. Zu einer solchen zählen nach herrschender und zutreffender Auffassung auch die Arbeitnehmer eines Unternehmens, denen der Arbeitgeber die private Nutzung der betrieblichen Telekommunikationsmöglichkeiten gestattet[4]. Die Angebote der klassischen Telekommunikationsunternehmen richten sich demgegenüber an beliebige Dritte, stehen also – unter den üblichen Voraussetzungen für einen Vertragsschluss – der Öffentlichkeit zur Verfügung[5].

Während das Telekommunikationsrecht in weiten Teilen nur solche Anbieter spezifischen Verpflichtungen unterwirft, galten die Vorschriften über den Telekommunikationsdatenschutz seit Inkrafttreten des TKG 1996 explizit auch für Anbieter, die ihre Dienste lediglich den Teilnehmern geschlossener Benutzergruppen anbieten[6]. Das ergibt sich nicht nur deutlich aus den Gesetzesmaterialien zum TKG 1996[7] wie auch zum geltenden TKG[8]. Es kommt auch im Normtext dadurch zum Ausdruck, dass sich die betreffenden Vorgaben allgemein an diejenigen richten, die geschäftsmäßig Telekommunikationsdienste erbringen, also, vereinfacht formuliert, an alle, die Dritten – mit oder ohne Gewinnerzielungsabsicht – Telekommunikation anbieten, soweit dieses Angebot von gewisser Dauer („nachhaltig"[9]) ist (§ 3 Nr. 5 TKG 1996 bzw. § 3 Nr. 10 TKG). Nicht erforderlich ist demgegenüber, dass sich dieses Angebot an die Öffentlichkeit, also an beliebige Dritte, richtet[10].

Formal ist es zwar auch nach der großen TKG-Novelle im Jahr 2012 hierbei geblieben. Geändert wurden allerdings die

1 Lau, in: Manssen, Telekommunikations- und Multimediarecht, Loseblattsammlung, Stand: 33. Ergänzungslieferung (11/2013), C § 88 Rn. 19.

2 Siehe z.B. die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (88) (zu § 89 TKG-RegE); Braun, in: Beck'scher TKG-Kommentar, 4. A., 2013, § 91 Rn. 12; Hartung, in: Wilms/Masing/Jochum, TKG, Loseblattsammlung, Stand: 8. Ergänzungslieferung (3/2007), § 91 Rn. 25.

3 Büttgen, in: Beck'scher TKG-Kommentar (Fn. 2), § 103 Rn. 6; Hartung (Fn. 2), § 91 Rn. 25; Ohlenburg, K&R 2003, 265 (267); Trute, in: Trute/Spoerr/Bosch, TKG mit FTEG, 2001, § 89 Rn. 4. Schütz, in: Beck'scher TKG-Kommentar (Fn. 2), § 6 Rn. 52, der – in einem marktzugangsrechtlichen Zusammenhang – den Begriff über die Zugehörigkeit zu derselben juristischen Person oder zum selben Konzern bestimmen will. Zur Notwendigkeit eines kontextabhängigen Begriffsverständnisses siehe Eckhardt, in: Heun, Handbuch Telekommunikationsrecht, 2. Aufl., 2007, Teil B Rn. 21.

4 Vgl. Neumann, IRNIK-Diskussionspapier Nr. 3, 2014, S. 32 m. w. N.

5 Büttgen, in: Scheurle/Mayen, TKG, 2. Aufl., 2008, § 91 Rn. 15. Zur Definition des Angebots an die Öffentlichkeit als Angebot an einen grundsätzlich unbeschränkten bzw. unbestimmten Personenkreis respektive an jedermann siehe die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (60) (zu § 6 TKG-RegE); Büttgen, RDV 2001, 6; Eckhardt (Fn. 3), Teil B Rn. 26; Fetzer, in: Arndt/Fetzer/Scherer, TKG, 2008, § 3 Rn. 75; Holznagel/Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl., 2011, § 3 TKG Rn. 26; Schütz (Fn. 3), § 6 Rn. 44 ff.

6 Braun (Fn. 2), § 91 Rn. 12 f.; Büttgen (Fn. 5), § 91 Rn. 15.

7 Stellungnahme des Bundesrates, BT-Drs. 13/4438, S. 5 (7) (Nr. 12 [zu § 3 TKG-E]); ausdrücklich zu der auf Grundlage des § 89 Abs. 1 TKG 1996 ergangenen Rechtsverordnung dann auch die Verordnungsbegründung, BR-Drs. 300/00, S. 13 (zu § 1).

8 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (88) (zu § 89 TKG-RegE).

9 Siehe hierzu Neumann (Fn. 4), S. 9 m. w. N.

10 Eckhardt (Fn. 3), Teil B Rn. 55; Fetzer (Fn. 5), § 3 Rn. 43, § 91 Rn. 6; Gramlich, in: Manssen (Fn. 1), C § 3 Rn. 9, § 91 Rn. 45; Holznagel/Ricke (Fn. 5), § 3 TKG Rn. 13; Koenig/Neumann, K&R 2000, 417 (418); Königshofen, RDV 1997, 97 (97 f.).

Legaldefinitionen, mit denen der Kreis jener Dritten näher abgesteckt wurde. Nach der Bestimmung über den Anwendungsbereich der Vorschriften zum Telekommunikationsdatenschutz regelt der betreffende Gesetzesabschnitt nämlich „den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten" (§ 91 Abs. 1 S. 1 TKG). Vor der TKG-Novelle 2012 war „Teilnehmer" gemäß der Legaldefinition in § 3 Nr. 20 TKG 2004 noch „jede natürliche oder juristische Person, die mit einem Anbieter von Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat". Und „Nutzer" war nach § 3 Nr. 14 TKG 2004 „jede natürliche Person, die einen Telekommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne notwendigerweise Teilnehmer zu sein". Seit 2012 kommt es für die Einstufung als „Teilnehmer" demgegenüber darauf an, dass der Vertrag „mit einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten" geschlossen wurde, also mit dem Anbieter von „der Öffentlichkeit zur Verfügung stehende[n] Telekommunikationsdienste[n]" (§ 3 Nr. 17a TKG). Und „Nutzer" ist ebenfalls nur noch, wer einen solchen „öffentlich zugänglichen Telekommunikationsdienst" in Anspruch nimmt (oder – nunmehr auch – beantragt).

Liest man diese Änderungen im Zusammenhang mit dem insoweit unveränderten[11] § 91 Abs. 1 S. 1 TKG, so liegt die Annahme nahe, dass der Anwendungsbereich des Telekommunikationsdatenschutzrechts nunmehr auf öffentlich zugängliche Telekommunikationsdienste beschränkt ist[12]. Vor allem aber beziehen sich die operativen Bestimmungen der §§ 93 ff. TKG auf Pflichten, die gegenüber „Teilnehmern" und „Nutzern" bestehen[13]. Sollte die Qualifikation als „Teilnehmer" oder „Nutzer" davon abhängen, ob ein öffentlich zugänglicher Telekommunikationsdienst in Rede steht, so ergeben sich aus diesen Bestimmungen keine Verpflichtungen für Diensteanbieter, die ihre telekommunikativen Leistungen gerade nicht der Öffentlichkeit, sondern nur den Mitgliedern einer geschlossenen Benutzergruppe anbieten. Geschlossene Benutzergruppen unterfielen bei einer solchen Lesart also nicht mehr den Vorschriften des TKG über den Telekommunikationsdatenschutz.

Soweit sich das Schrifttum überhaupt mit dieser Problematik befasst, wird diese Konsequenz überwiegend als ungewolltes Versehen des Gesetzgebers abgelehnt[14]. Unlängst hat jedoch die Annahme, dass nicht öffentliche Angebote bzw. geschlossene Benutzergruppen nicht mehr dem Telekommunikationsdatenschutz unterfallen, explizite Zustimmung erfahren[15]. Angesichts der oben dargestellten Zusammenhänge lässt sich auch kaum leugnen, dass im Lichte der novellierten Legaldefinitionen für „Teilnehmer" und „Nutzer" die Anwendbarkeit der §§ 91 ff. TKG jedenfalls nach dem Wortlaut der einschlägigen Vorschriften ernsthaft in Frage gestellt ist[16]. Insbesondere ist nicht nachvollziehbar, wenn vereinzelt behauptet wird, „Nutzer" i.S.v. § 3 Nr. 14 TKG sei „auch der Nutzer privater Telekommunikationsdienste, die nicht der Öffentlichkeit bereitgestellt werden"[17]. Das widerspricht offensichtlich der auf § 3 Nr. 14 (und 20) TKG bezogenen Definition öffentlich zugänglicher Telekommunikationsdienste in § 3 Nr. 17a TKG als gerade „der Öffentlichkeit zur Verfügung stehende Telekommunikationsdienste". Es ist deshalb zu klären, ob für das Angebot von Telekommunikation gegenüber Mitgliedern geschlossener Benutzergruppen tatsächlich nur (noch) die allgemeinen Bestimmungen des BDSG gelten.

II. Gesetzgebungsgeschichte

Beim Versuch, die Gründe für die Änderung der Legaldefinitionen in § 3 Nr. 14 und 20 TKG zu ergründen, wird man die Gesetzesmaterialien zur TKG-Novelle 2012 heranziehen müssen. Aus diesen ergibt sich nur, dass die Begriffsbestimmungen an die entsprechenden Legaldefinitionen in Art. 2 lit. h und k der Rahmenrichtlinie 2002/21/EG angepasst werden sollten[18]. Den Gesetzesmaterialien – insbesondere zu den Änderungen im Bereich der §§ 91 ff. TKG[19] – ist demgegenüber nicht zu entnehmen, dass mit den Änderungen eine Beschränkung der bisherigen Anwendbarkeit des Telekommunikationsdatenschutzes auf geschlossene Benutzergruppen bezweckt war[20]. Es ist noch nicht einmal ersichtlich, dass der Gesetzgeber sich dieser potentiellen Konsequenz auch nur ansatzweise bewusst gewesen wäre.

Das ist insoweit bemerkenswert, als die richtlinienrechtlichen Legaldefinitionen schon von jeher einen öffentlich zugänglichen Kommunikationsdienst voraussetzten. Es handelt sich mithin nicht um Neuerungen, zu denen es im Zusammenhang mit den Änderungsrichtlinien im Jahr 2009 gekommen wäre, die unmittelbarer Anlass der TKG-Novelle 2012 waren. Blickt man auf das Gesetzgebungsverfahren aus dem Jahr 2004, so fällt auf, dass bereits damals die Legaldefinitionen in § 3 Nr. 14 und 20 TKG der Umsetzung richtlinienrechtlicher Begriffsbestimmungen dienen sollten[21]. Während die Definition des Begriffs „Teilnehmer" schon seinerzeit Art. 2 lit. k der Rahmenrichtlinie 2002/21/EG folgte, sollte der Begriff „Nutzer" aber gerade nicht dem allgemeinen Nutzerbegriff aus Art. 2 lit. h der Rahmenrichtlinie 2002/21/EG entsprechen, sondern der spezifischen Legaldefinition für den „Nutzer" in Art. 2 lit. a der Datenschutzrichtlinie für elektronische Kommu-

11 Zu den hier nicht relevanten Änderungen des § 91 TKG im Rahmen der TKG-Novelle 2012 siehe etwa Ferik, RDV 2012, 240 (240 f.); Pokutnev/Schmid, CR 2012, 360 (362).

12 Sander, CR 2014, 176 (182); etwas vorsichtiger Jenny, in: Plath, BDSG, 2013, § 91 TKG Rn. 7; Pokutnev/Schmid, CR 2012, 360.

13 Siehe auch Eckhardt/Schmitz, CR 2011, 436 (436 f.).

14 Jenny (Fn. 12), § 91 TKG Rn. 7; Munz, in: Taeger/Gabel, BDSG, 2. Aufl., 2013, § 91 TKG Rn. 11; Pokutnev/Schmid, CR 2012, 360 (361).

15 Sander, CR 2014, 176 (182).

16 Eckhardt/Schmitz, CR 2011, 436 (437); Pokutnev/Schmid, CR 2012, 360 (366). Die fehlende Abstimmung der §§ 91 ff. TKG auf die Änderung von § 3 Nr. 20 TKG rügt zu Recht auch Braun (Fn. 2), § 3 Rn. 71.

17 So Säcker, in: Säcker, TKG, 3. Aufl., 2013, § 3 Rn. 45.

18 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 17/5707, S. 43 (49) (zu Nr. 3 lit. l [§ 3 Nr. 14]) u. 50 (Nr. 3 lit. t [§ 3 Nr. 20]).

19 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 17/5707, S. 43 (79 f.) (zu Nr. 75 ff.).

20 Siehe auch Pokutnev/Schmid, CR 2012, 360.

21 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (58) (zu § 3 Nr. 14 u. 20 TKG-RegE).

nikation 2002/58/EG[22]. Dieser setzte und setzt zwar auch die Nutzung eines öffentlich zugänglichen Kommunikationsdienstes voraus[23]. Der Umstand, dass dieser explizite Paradigmenwechsel bei der Legaldefinition des Begriffs „Nutzer" in den Gesetzesmaterialien zur TKG-Novelle 2012 nicht einmal erwähnt wird, verdeutlicht jedoch, dass der Zusammenhang, in den die jeweiligen Rechtsbegriffe eingebettet sind, weder reflektiert noch auch nur erkannt wurde.

Das gilt namentlich für die Auswirkungen auf den Bereich des Telekommunikationsdatenschutzes. Zwar findet sich in den Materialien aus dem Jahr 2004 zu den Begriffsbestimmungen in § 3 Nr. 14 und 20 TKG auch kein Hinweis darauf, dass bewusst auf das Merkmal der öffentlichen Zugänglichkeit des Telekommunikationsdienstes verzichtet wurde, um die Anwendbarkeit der §§ 91 ff. TKG auf geschlossene Benutzergruppen zu ermöglichen. Aus den Materialien ergibt sich jedoch, dass im damaligen Gesetzgebungsverfahren ohne weiteres ausdrücklich von einer Geltung des Telekommunikationsdatenschutzes auch für Angebote an „Teilnehmer geschlossener Benutzergruppen" ausgegangen wurde[24].

Das dürfte auf den Umstand zurückzuführen sein, dass die Frage nach dem Anwendungsbereich des Telekommunikationsdatenschutzes bereits im Zusammenhang mit dem TKG 1996 umfassend diskutiert worden war[25]. Denn bereits in Art. 2 lit. a und b der Telekommunikationsdatenschutzrichtlinie 97/66/EG, die dann von der Richtlinie 2002/58/EG abgelöst wurde, wurden die Begriffe „Teilnehmer" und „Benutzer" als Schutzsubjekte der Richtlinienvorgaben nur für den Bereich öffentlich zugänglicher Telekommunikationsdienste definiert. Obwohl bereits seinerzeit die Bundesrepublik Deutschland somit richtlinienrechtlich nur zur Schaffung entsprechender Schutzvorkehrungen verpflichtet war, hatte man sich ausdrücklich für einen weitergehenden, auch geschlossene Benutzergruppen einbeziehenden Anwendungsbereich des Telekommunikationsdatenschutzes auf nationaler Ebene entschieden.

Gerade auch weil seinerzeit die Richtlinie 97/66/EG überhaupt noch nicht in Kraft war, spielte dieser Aspekt zwar im Gesetzgebungsverfahren zum TKG 1996 nur eine untergeordnete Rolle[26]. Vielmehr ging er damals weitgehend in der – bejahten – Frage auf, ob der Telekommunikationsdatenschutz auch für nicht gewerbliche Angebote gelten sollte[27], zu denen etwa sog. „Corporate Networks" zählen können[28], also ein weiteres Beispiel für eine geschlossene Benutzergruppe[29]. Im Zusammenhang mit dem Erlass der seinerzeit in § 89 Abs. 1 TKG 1996 vorgesehenen Telekommunikations-Datenschutzverordnung (TDSV) wurde jedoch ausdrücklich die grundsätzliche Anwendbarkeit des Telekommunikationsdatenschutzes auf geschlossene Benutzergruppen festgelegt[30]. An die TDSV und damit auch an ihren Anwendungsbereich knüpfte das Gesetzgebungsverfahren zum TKG im Jahr 2004 dann ausdrücklich an[31]. Es sollte lediglich „nunmehr statt des Begriffs, der an der Telekommunikation Beteiligten'", der noch für den Anwendungsbereich der TDSV maßgeblich war (§ 1 Abs. 1 S. 1 TDSV), „auf Teilnehmer und Nutzer hingewiesen" werden[32]. Eine inhaltliche Engerführung des Anwendungsbereichs war damit jedoch nicht intendiert[33]. Das zeigen die ausdrückliche Nennung geschlossener Benutzergruppen an selber Stelle der Entwurfsbegründung[34] und die unveränderte Übernahme der relevanten Bestimmungen trotz entsprechender Kritik im Rahmen des damaligen Gesetzgebungsverfahrens[35]. Damit im Einklang steht es, dass in den Legaldefinitionen für die Begriffe „Nutzer" und „Teilnehmer" in § 3 Nr. 14 und 20 TKG 2004 darauf verzichtet wurde, auf einen öffentlich zugänglichen Telekommunikationsdienst Bezug zu nehmen.

Dieser Blick in die Gesetzgebungsgeschichte verdeutlicht, dass der Gesetzgeber bei den Änderungen der Legaldefinitionen in § 3 Nr. 14 und 20 TKG im Jahr 2012 die Hintergründe der bisherigen Begriffsbestimmungen und damit auch die potentiellen Auswirkungen auf den Telekommunikationsdatenschutz schlichtweg nicht im Blick hatte, der stattdessen damals auf ganz andere Themen (Breitbandausbau, Kundenschutz, Netzneutralitätsdebatte usw.) gerichtet war[36]. Es dürfte sich also bei den hier dargestellten Konsequenzen, die sich bei wortlautgetreuer Betrachtung für die Anwendbarkeit der §§ 91 ff. TKG ergeben, in der Tat um ein legislatorisches Versehen handeln.

22 Siehe auch Fetzer (Fn. 5), § 3 Rn. 72; Lünenbürger, in: Scheurle/Mayen (Fn. 5), § 3 Rn. 36; Ohlenburg, K&R 2003, 265 (266); Säcker (Fn. 17), § 3 Rn. 44; Schütz (Fn. 3), § 3 Rn. 54.

23 Zweifelhaft erscheint deshalb die Erwägung von Pokutnev/Schmid, CR 2012, 360 (360 f.), dass mit der „Rechte der Bürger"-Richtlinie 2009/136/EG u. a. die Rechte im Bereich des Datenschutzes gestärkt werden sollten, womit sich eine Beschränkung des Anwendungsbereichs der Vorschriften zum Telekommunikationsdatenschutz nicht vertrage. Denn diese Entwicklung – hierzu auch Ferik, RDV 2012, 240 (240 f.); Roßnagel/Johannes/Kartal, K&R 2012, 244 (250) – bezieht sich gerade nicht auf die vorliegend relevante Frage, ob der Telekommunikationsdatenschutz auch für nicht öffentliche Angebote gelten soll.

24 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (88) (zu § 89 TKG-RegE); auch in der Literatur wurde dementsprechend angenommen, dass die §§ 91 ff. TKG 2004 insoweit über die richtlinienrechtlichen Vorgaben hinausgehen, die auf öffentlich zugängliche Telekommunikationsdienste beschränkt sind, siehe Fetzer (Fn. 5), § 91 Rn. 9.

25 Vgl. etwa Dix, DuD 1997, 278 (279 f.).

26 Siehe aber die Stellungnahme des Bundesrates, BT-Drs. 13/4438, S. 5 (7) (Nr. 12 [zu § 3 TKG-E]).

27 Bericht der Abgeordneten Elmar Müller (Kirchheim), Hans Martin Bury, Dr. Manuel Kiper, Dr. Max Stadler und Gerhard Jüttemann, BT-Drs. 13/4864 (neu), S. 70 (83) (zu § 86 TKG-E).

28 Bericht der Abgeordneten Elmar Müller (Kirchheim), Hans Martin Bury, Dr. Manuel Kiper, Dr. Max Stadler und Gerhard Jüttemann, BT-Drs. 13/4864 (neu), S. 70 (83) (zu § 86 TKG-E).

29 Siehe hierzu die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (95) (zu § 110 TKG-RegE); Verordnungsbegründung, BR-Drs. 300/00, S. 13 (zu § 1); Eckhardt (Fn. 3), Teil B Rn. 23; Fetzer (Fn. 5), § 91 Rn. 7; Munz (Fn. 14), § 91 TKG Rn. 11; Ohlenburg, K&R 2003, 265 (267); Trute (Fn. 3), § 89 Rn. 4.

30 Verordnungsbegründung, BR-Drs. 300/00, S. 13 (zu § 1).

31 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (88) (zu Abschnitt 2 u. zu § 89 TKG-RegE).

32 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (88) (zu § 89 TKG-RegE).

33 Siehe auch Eckhardt (Fn. 3), Teil L Rn. 153; Ohlenburg, K&R 2003, 265 (266).

34 Siehe erneut die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (88) (zu § 89 TKG-RegE).

35 Vgl. dazu Hartung (Fn. 2), § 91 Rn. 26. Entsprechenden Forderungen wurde ausdrücklich nicht Rechnung getragen, siehe Ohlenburg, K&R 2003, 265 (267).

36 Zu der Fokussierung auf diese Themen siehe auch Ferik, RDV 2012, 240.

III. Gesetzessystematischer Sinnzusammenhang

Bei aller Bedeutung der Gesetzgebungsmaterialien für die Gesetzesauslegung und -anwendung ist nach gefestigter Rechtsprechung des BVerfG für die Auslegung einer Gesetzesvorschrift allerdings der in dieser zum Ausdruck kommende objektivierte Wille des Gesetzgebers maßgebend, so wie er sich aus dem Wortlaut der Gesetzesbestimmung und dem Sinnzusammenhang ergibt, in den diese hineingestellt ist[37]. Der Entstehungsgeschichte einer Vorschrift kommt für deren Auslegung nach den verfassungsgerichtlichen Vorgaben deshalb nur insofern Bedeutung zu, als sie die Richtigkeit einer nach dem durch den Wortlaut und Sinnzusammenhang zum Ausdruck gebrachten objektivierten Willen des Gesetzgebers ermittelten Auslegung bestätigt oder Zweifel behebt, die ansonsten nicht ausgeräumt werden können[38]. Es ist daher zu untersuchen, ob gerade auch systematisch-teleologische Aspekte für die Annahme sprechen können, dass der Anwendungsbereich des Telekommunikationsdatenschutzrechts insoweit nach der TKG-Novelle 2012 unverändert geblieben ist.

1. Widerspruch in § 91 TKG?

In diesem Zusammenhang wird z. T. darauf hingewiesen, dass sich bei einem Rückgriff auf die novellierten Legaldefinitionen bereits innerhalb des § 91 Abs. 1 S. 1 TKG ein Widerspruch ergebe: Während der verpflichtete Diensteanbieter gerade keinen öffentlich zugänglichen Telekommunikationsdienst erbringen müsse, wären nur diejenigen Personen geschützt, die einen solchen öffentlichen Dienst in Anspruch nehmen[39]. Das ist zwar zutreffend, zwingt für sich genommen aber nicht zur Annahme interpretatorischer Konsequenzen. Es ist vielmehr nicht unüblich, dass gesetzliche Vorschriften nur einen bestimmten Ausschnitt des Verhaltens der dem persönlichen Anwendungsbereich unterfallenden Personen regeln.

So adressieren beispielsweise bestimmte Vorschriften des TKG zunächst alle „Diensteanbieter", legen ihnen aber nur Verpflichtungen im Umgang mit Rufnummern auf (siehe etwa § 66e TKG). Das führt nicht dazu, dass man nun diese Vorschriften auch auf anderen Telekommunikationskennungen anwenden würde, um insoweit einen norminternen „Widerspruch" zwischen dem formalen Adressatenkreis und dem tatsächlichen Anwendungsbereich der Norm zu vermeiden. Vielmehr wird die Norm nur angewendet, soweit der betreffende Diensteanbieter auch tatsächlich Rufnummern nutzt. Vergleichbares gilt innerhalb des Telekommunikationsdatenschutzes selbst etwa für die Regelung über die Mitteilung ankommender Verbindungen nach § 101 TKG: Sie betrifft formal alle „Diensteanbieter", regelt in der Sache aber nur den Umgang mit „bedrohende[n] oder belästigende[n]" Anrufen und wird deshalb (jedenfalls grundsätzlich[40]) auch nur auf Anbieter von Sprachkommunikation angewendet[41]. Es ist nicht ersichtlich, warum mit Blick auf § 91 Abs. 1 S. 1 TKG nicht entsprechend verfahren werden könnte. Aus dem Telekommunikationsdatenschutzrecht würden sich dann nur für solche Diensteanbieter Verpflichtungen ergeben, die öffentlich zugängliche Telekommunikationsdienste anbieten.

2. Sondervorschriften für geschlossene Benutzergruppen

In systematischer Hinsicht kommt allerdings den Sondervorschriften für geschlossene Benutzergruppen Bedeutung zu, mit denen aus Gründen der Verhältnismäßigkeit der Anwendungsbereich des Telekommunikationsdatenschutzrechts punktuell beschränkt wird[42]. Insbesondere § 99 Abs. 1 S. 8, Abs. 2 S. 7, § 101 Abs. 1 S. 4, § 102 Abs. 3, § 103 S. 2 TKG[43] sehen auch nach der TKG-Novelle 2012 unverändert Ausnahmen vor für „Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten". Diese Ausnahmeregelungen wären sinn- und funktionslos, wenn das Telekommunikationsdatenschutzrecht schon grundsätzlich nur noch für Anbieter öffentlich zugänglicher Dienste gelten würde. Nimmt man nur die spezifischen Vorschriften zum Telekommunikationsdatenschutz in den Blick, so wird man angesichts dieser systematischen Zusammenhänge auch weiterhin ohne weiteres von der grundsätzlichen Anwendbarkeit der §§ 91 ff. TKG auf geschlossene Benutzergruppen ausgehen[44].

3. Zusammenspiel mit § 88 TKG

Zu berücksichtigen ist des Weiteren das Zusammenspiel mit dem einfachgesetzlichen Fernmeldegeheimnis in § 88 TKG. Diese Vorschrift verpflichtet jeden Diensteanbieter zur Wahrung des Fernmeldegeheimnisses (§ 88 Abs. 2 S. 1 TKG), dem insbesondere „der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war", unterliegen (§ 88 Abs. 1 S. 1 TKG). Diensteanbieter ist aber nach § 3 Nr. 6 TKG, vereinfacht formuliert, jeder, der Dritten – ob mit oder ohne Gewinnerzielungsabsicht – Telekommunikation anbietet, soweit dieses Angebot von gewisser Dauer ist (siehe bereits oben, unter I.). Ob sich dieses Angebot an die Öffentlichkeit oder nur an die Mitglieder einer geschlossenen Benut-

37 Vgl. etwa BVerfGE 59, 128 (153); BVerfGE 1, 299 (312); siehe auch BVerwGE 142, 84 (86) Rn. 12; BGH, NJW 2012, 376 (377) Rn. 14.

38 BVerfGE 59, 128 (153); BVerfGE 1, 299 (312).

39 Munz (Fn. 14), § 91 TKG Rn. 11; insoweit auf „Inkonsistenzen" hinweisend auch Eckhardt/Schmitz, CR 2011, 436 (437).

40 Zur Diskussion um eine punktuelle Ausdehnung auf Anbieter von Telefax- und/oder Kurztextnachrichtendiensten siehe Hartung (Fn. 2), § 101 Rn. 9 m. w. N.

41 Büttgen, RDV 2001, 6 (10); Klesczewski, in: Säcker (Fn. 17), § 101 Rn. 3; Neumann/Koch, Telekommunikationsrecht, 2. Aufl., 2013, Kap. 5 Rn. 48.

42 Siehe zu dieser Zwecksetzung die Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (88) (zu § 89 TKG-RegE), sowie bereits zu § 1 TDSV die Verordnungsbegründung, BR-Drs. 300/00, S. 13 (zu § 1); vgl. des Weiteren Büttgen, RDV 2001, 6 (7); Ohlenburg, MMR 2004, 431; Klesczewski (Fn. 41), § 91 Rn. 31; auf beschränkte technische Möglichkeiten der betreffenden Anbieter abstellend Büttgen (Fn. 5), § 91 Rn. 16.

43 Auch § 91 Abs. 2 TKG dürfte ein entsprechendes Verständnis zugrunde liegen, vgl. Eckhardt (Fn. 3), Teil B Rn. 55; Fetzer (Fn. 5), § 91 Rn. 7; Gramlich (Fn. 10), C § 91 Rn. 45; Munz (Fn. 14), § 91 TKG Rn. 11. Nicht ohne weiteres ausgeschlossen ist insoweit allerdings auch die – im Ergebnis aber abzulehnende, vgl. Koenig/Neumann, RDV 2001, 117 (120) – Auffassung, dass durch die Vorschrift der Anwendungsbereich des Telekommunikationsdatenschutzrechts auf geschlossene Benutzergruppen öffentlicher Stellen der Länder erweitert wird.

44 Ähnlich wohl die „Kontrollüberlegung" von Pokutnev/Schmid, CR 2012, 360 (361). So im Ergebnis auch Munz (Fn. 14), § 91 TKG Rn. 11, wenngleich unter Rückgriff auf § 91 Abs. 2 TKG, siehe hierzu Fn. 43.

zergruppe richtet, spielt keine Rolle[45]. Da § 88 TKG nicht auf „Teilnehmer" oder „Nutzer" als geschützte Personen abstellt, hat sich an dieser Rechtslage durch die TKG-Novelle 2012 auch bei bloßer Wortlautbetrachtung nichts geändert[46].

Nach § 88 Abs. 3 S. 1 TKG dürfen Diensteanbieter sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste (einschließlich des Schutzes ihrer technischen Systeme) erforderliche Maß hinaus keine Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen. Eine Verwendung dieser Kenntnisse für andere Zwecke ist gemäß § 88 Abs. 3 S. 3 TKG nur zulässig, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Solche Ermächtigungen ergeben sich insbesondere aus den Vorschriften über den Telekommunikationsdatenschutz[47]. Zu denken ist etwa an § 97 TKG für die Ermittlung und Abrechnung des Entgelts oder namentlich auch an § 100 TKG, der u. a. die Verarbeitung von Bestands- und Verkehrsdaten zum Zwecke der Missbrauchsbekämpfung erlaubt.

Würden §§ 91 ff. TKG nicht (mehr) für geschlossene Benutzergruppen gelten, könnten sich die betreffenden Diensteanbieter auch nicht auf diese Ermächtigungen zur Verarbeitung solcher Daten stützen, die jedenfalls in weiten Teilen unter das einfachgesetzliche Fernmeldegeheimnis aus § 88 TKG fielen. Zugleich käme ein Rückgriff auf die Verarbeitungsermächtigungen des allgemeinen Datenschutzrechts (etwa § 28 BDSG) nicht in Betracht, da sich diese nicht „ausdrücklich auf Telekommunikationsvorgänge" beziehen[48]. Die Betreiber geschlossener Benutzergruppen wären damit zwar von den spezifischen Verpflichtungen des Telekommunikationsdatenschutzrechts befreit. Sie unterlägen aber bei der Verwendung der Daten weiterhin datenschutzrechtlichen Vorgaben (aus dem BDSG) und dem einfachgesetzlichen Fernmeldegeheimnis. Zugleich könnten sie sich nicht auf die Verarbeitungsermächtigungen des allgemeinen Datenschutzrechts stützen – und auch nicht auf die spezifisch telekommunikationsrechtlichen Ermächtigungen in §§ 91 ff. TKG.

Denkbar wäre zwar, dass die betreffenden Diensteanbieter sich die erforderlichen Datenverarbeitungen durch Einwilligungen der Mitglieder ihrer geschlossenen Benutzergruppen legitimieren lassen[49]. Es ist aber schon sehr umstritten, inwieweit solche Einwilligungen auch mit Blick auf den jeweiligen Kommunikationspartner wirken können[50]. Vor allem aber würde die Möglichkeit einer Einwilligung bei geschlossenen Nutzergruppen nicht weiterhelfen, die – wie etwa „Corporate Networks" – auf Dauer angelegt sind und schon bei Inkrafttreten der TKG-Novelle 2012 Bestand hatten. Hier hätte die Beschränkung des Anwendungsbereichs zur Folge gehabt, dass bis zur nachträglichen Erteilung entsprechender Einwilligungen die Verarbeitung der unter § 88 TKG fallenden (Verkehrs-) Daten unzulässig geworden wäre. Jedenfalls aber würde die Notwendigkeit, sich die Datenverarbeitung im Einzelnen durch Einwilligungen gestatten zu lassen, zu einer zusätzlichen Belastung derjenigen Diensteanbieter führen, deren Angebote sich gerade nur an geschlossene Benutzergruppen und nicht an die Öffentlichkeit richten.

Betrachtet man den vorstehend skizzierten Sinnzusammenhang, in den die §§ 91 ff. TKG gestellt sind, hätte ein Auseinanderfallen des Anwendungsbereichs von § 88 TKG und des Telekommunikationsdatenschutzrechts mithin einen Bruch in der gesetzlichen Regelungssystematik zur Folge. Die Erleichterungen, die mit einer Befreiung von den Vorgaben des Telekommunikationsdatenschutzes einhergingen, wären mit erheblichen Einschränkungen im Umgang mit den (Verkehrs-) Daten verbunden, die weiterhin von § 88 TKG geschützt werden. Auch das Zusammenspiel mit § 88 TKG spricht somit dafür, dass es nicht dem gesetzlichen Regelungsplan entspricht, geschlossene Benutzergruppen aus dem Anwendungsbereich der §§ 91 ff. TKG herauszunehmen.

IV. Interpretatorische Schlussfolgerungen

Während bei einer streng wortlautgetreuen Ausfüllung der Begrifflichkeiten in §§ 91 ff. TKG geschlossene Benutzergruppen nicht mehr dem Telekommunikationsdatenschutz unterlägen, spricht der Sinnzusammenhang der einschlägigen Vorschriften für das Gegenteil[51]. Nur letztgenanntes Verständnis wird durch die Betrachtung der Gesetzgebungsgeschichte gestützt: Während die Entscheidung für die Einbeziehung geschlossener Benutzergruppen mehrfach ausdrücklich in den einschlägigen Gesetzesmaterialien dokumentiert ist, enthalten die Materialien zur TKG-Novelle 2012 keinen Hinweis darauf, dass diese Entscheidung durch die Anpassung der Legaldefinitionen in § 3 Nr. 14 und 20 TKG revidiert werden sollte.

Zu klären ist damit noch, wie dieser Befund methodisch zu verarbeiten ist. Da die Begriffe „Nutzer" und „Teilnehmer" auch in anderen Vorschriften des TKG verwendet werden[52] und der Gesetzgeber ausdrücklich die allgemeinen Legaldefinitionen an die Begriffsbestimmungen der (allgemeinen) Rahmenrichtlinie anpassen wollte, wird es nicht angängig sein, die Definitionen in § 3 Nr. 14 und 20 TKG als solche erweiternd auszulegen[53]. Eine solche Vorgehensweise hätte einen überschießenden Eingriff in den Wortlaut des Gesetzes zur Folge,

45 Siehe die Nachweise in Fn. 10.

46 Dementsprechend geht auch die Literatur unverändert ohne weiteres von der Geltung des Fernmeldegeheimnisses nach § 88 TKG auch bei nicht an die Öffentlichkeit gerichteten Angeboten, aus, vgl. Bock, in: Beck'scher TKG-Kommentar (Fn. 2), § 88 Rn. 24, also in geschlossenen Benutzergruppen; siehe auch Munz (Fn. 14), § 88 TKG Rn. 13.

47 Eckhardt (Fn. 3), Teil L Rn. 60; Jenny (Fn. 12), § 88 TKG Rn. 18 f.; Lau (Fn. 1), C § 88 Rn. 27; Trute (Fn. 3), § 89 Rn. 16. Sehr weitgehendes Verständnis von § 88 Abs. 3 S. 1 TKG bei Voßhoff, K&R 10/2014, Editorial.

48 Vgl. auch Hartung (Fn. 2), § 91 Rn. 45, zur Möglichkeit einer etwaigen Beschränkung auf – gerade auch hier relevante – telekommunikationsspezifische Sachverhalte a. a. O., Rn. 46 f.

49 Zur Möglichkeit entsprechender Einwilligungen siehe etwa BVerfGE 120, 274 (341); Burkard, NJW-Spezial 2011, 370 (370 f.); Hartmann/Pröpper, BB 2009, 1300 (1301); Hoppe/Braun, MMR 2010, 80 (84); Neumann (Fn. 4), S. 35 f.

50 Siehe zum Streitstand ausführlich (die Streitfrage bejahend) Neumann (Fn. 4), S. 35 f. m. w. N.; nunmehr auch Voßhoff, K&R 10/2014, Editorial

51 Entsprechend aus nicht näher spezifizierten „teleologischen Erwägungen" Jenny (Fn. 12), § 91 TKG Rn. 7.

52 Siehe zum „Nutzer" etwa § 16, § 45 Abs. 3 S. 4, § 45i Abs. 1 S. 2, § 47 Abs. 1 S. 1, § 66 Abs. 2 S. 2 TKG und zum „Teilnehmer" insbesondere §§ 45a ff. und § 66k TKG.

53 So aber der Vorschlag von Munz (Fn. 14), § 91 TKG Rn. 11.

mit dem überdies die in den Gesetzesmaterialien dokumentierte Regelungsabsicht in vollem Umfang ignoriert würde.

Der methodisch richtige Weg dürfte deshalb darin bestehen, die Auslegung der Begriffe „Nutzer" und „Teilnehmer" in §§ 91 ff. TKG von den allgemeinen Begriffsbestimmungen zu entkoppeln und stattdessen weiterhin an den bisherigen Begriffsbestimmungen in § 3 Nr. 14 und 20 TKG 2004 auszurichten. Ein solches „gespaltenes" Begriffsverständnis, bei dem derselbe Begriff in einzelnen Vorschriften des Gesetzes anders ausgelegt wird als in den ausdrücklichen Begriffsbestimmungen der allgemeinen Legaldefinition, ist zwar ungewöhnlich und in der Regel abzulehnen[54]. Ein derartiges Verständnis ist aber auch nicht per se ausgeschlossen, wenn die Gesetzesauslegung ergibt, dass nur auf diese Weise der gesetzliche Regelungsplan erreicht werden kann. Insbesondere ist deshalb sogar dem TKG selbst ein derartiges Begriffsverständnis nicht fremd, bei dem in einem konkreten Sachzusammenhang von einer allgemeinen Legaldefinition abgewichen wird. So hat namentlich der Begriff „Zugang" in § 18 TKG einen anderen Bedeutungsgehalt als der in § 3 Nr. 32 TKG legaldefinierte Begriff „Zugang"[55]. Zwar findet sich im Gegensatz zu jenem Beispiel[56] für die Begriffe „Nutzer" und „Teilnehmer" keine ausdrückliche Aussage in den Gesetzesmaterialien, aus denen sich eine solche Begriffsspaltung ergibt. Dass die Begriffe in §§ 91 ff. TKG nicht dasselbe meinen können wie die in § 3 Nr. 14 und 20 TKG legaldefinierten Begriffe, ergibt sich aber aus dem Sinnzusammenhang dieser Vorschriften. Dieser ist, wie (oben, unter III.) gezeigt, nach der verfassungsgerichtlichen Rechtsprechung für die Gesetzesauslegung aber sogar von stärkerer Bedeutung als die Gesetzesmaterialien. Damit sind zur Vermeidung einer sinnwidrigen Gesetzesauslegung die Begriffe „Nutzer" und „Teilnehmer" in §§ 91 ff. TKG im Sinne der bisherigen Legaldefinitionen nach § 3 Nr. 14 und 20 TKG 2004 und nicht im Sinne der entsprechenden Begriffsbestimmungen des geltenden TKG auszulegen.

Auch wenn man sich damit den Grenzen des rechtsmethodisch Zulässigen annähern dürfte, erscheint diese Vorgehensweise sinnvoller als beispielsweise eine analoge Anwendung der §§ 91 ff. TKG[57]. Deren Voraussetzungen dürften – wenn man eine Lösung des Problems im Wege der Auslegung für nicht möglich halten wollte – hier zwar durchaus vorliegen. Da den Verhaltensvorgaben der §§ 91 ff. TKG grundrechtliche Relevanz zukommt, würde sich hier aber die Folgeproblematik stellen, inwieweit durch die analoge Anwendung von Gesetzesvorschriften in Grundrechte eingegriffen werden kann[58]. Soweit die §§ 91 ff. TKG überdies durch Bußgeldtatbestände flankiert werden (§ 149 Abs. 1 Nr. 16 bis 17c TKG), stünde schließlich das strenge Bestimmtheitsgebot aus Art. 103 Abs. 2 GG einer analogen Anwendung auch grundsätzlich entgegen. Zwar können diese Überlegungen nicht entscheidend für die Beantwortung der Frage sein, ob eine bestimmte Normanwendung sich noch im Rahmen der Auslegung bewegt oder deren Grenzen bereits in Richtung einer analogen Anwendung überschreitet. Sie verdeutlichen aber, dass die methodisch (noch) zulässige Auslegung der Begriffe „Nutzer" und „Teilnehmer" im Sinne der *früheren* Legaldefinitionen auch dem Regelungsplan des Gesetzes entspricht, der ansonsten nicht oder nur unvollständig verwirklicht werden könnte.

V. Fazit

Im Schatten der politischen Diskussion insbesondere um den Breitbandausbau, die Netzneutralität und den Ausbau des Kundenschutzes hat der Gesetzgeber mit der TKG-Novelle 2012 auch die Legaldefinitionen der Begriffe „Nutzer" und „Teilnehmer" in § 3 Nr. 14 und 20 TKG geändert. Bei einem am Wortlaut dieser Begriffsbestimmungen ausgerichteten Verständnis der §§ 91 ff. TKG hätte das zur Folge, dass der Telekommunikationsdatenschutz seither nicht mehr in geschlossenen Benutzergruppen (Krankenhäuser, Hotels, Gaststätten, Arbeitsverhältnisse, sog. „Corporate Networks" usw.) gilt. Die Gesetzgebungsmaterialien zeigen aber deutlich, dass diese Konsequenz im Gesetzgebungsverfahren nicht bedacht und schon gar nicht gewollt war. Die ausdrückliche Bezugnahme auf „geschlossene Benutzergruppen" in mehreren Vorschriften zum Telekommunikationsdatenschutz und das Zusammenspiel mit dem insoweit unbeeinträchtigten Fernmeldegeheimnis nach § 88 TKG zeigen, dass auch der gesetzliche Sinnzusammenhang dagegen spricht, den Anwendungsbereich des Telekommunikationsdatenschutzrechts auf öffentlich zugängliche Telekommunikationsdienste zu beschränken. Die Begriffe „Nutzer" und „Teilnehmer" sind im Rahmen der §§ 91 ff. TKG daher weiterhin im Sinne der früheren Legaldefinitionen in § 3 Nr. 14 und 20 TKG 2004 zu verstehen. Das Telekommunikationsdatenschutzrecht gilt deshalb nach wie vor auch im Falle geschlossener Benutzergruppen. Zur Vermeidung von Rechtsunsicherheit böte allerdings die derzeit (vor allem mit Blick auf weitere Regelungen zur Infrastrukturmitnutzung) geplante TKG-Novelle 2015 eine evtl. nutzenswerte Gelegenheit, die unklarheitsauslösenden Änderungen in den Legaldefinitionen rückgängig zu machen.

Andreas Neumann
ist Geschäftsführer des privaten Instituts für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie (IRNIK) und assoziierter Wissenschaftler (‚Senior Fellow') am Zentrum für Europäische Integrationsforschung (ZEI) der Universität Bonn. Zuvor Tätigkeit an der Forschungsstelle für Rechtsinformatik der Universität Marburg und als wissenschaftlicher Mitarbeiter am ZEI, dort zuletzt als Leiter der Forschungsgruppe Telekommunikationsrecht.

54 Siehe etwa Saueressig, Jura 2005, 525 (526); wohl auch Wank, Die Auslegung von Gesetzen, 5. Aufl., 2011, S. 19 f.

55 Siehe hierzu Neumann/Koch (Fn. 41), Kap. 3 Rn. 422; Nolte, in: Säcker (Fn. 17), § 18 Rn. 15; Schütz (Fn. 3), § 18 Rn. 16.

56 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, S. 55 (64) (zu § 18 TKG-RegE).

57 Diese Möglichkeit erwägend Neumann (Fn. 4), S. 31.

58 Bejahend BGHZ 147, 39 (44); Sachs, in: Sachs, GG, 6. Aufl., 2011, Art. 20 Rn. 21; Schwabe, DVBl. 1997, 352 (352 f.). Verneinend Gusy, DÖV 1992, 461 (464), sowie hinsichtlich der analogen Anwendbarkeit von Ermächtigungsgrundlagen für belastende Verwaltungsakte BVerfG, NJW 1996, 3146; VG Minden, NVwZ 2003, 370. Siehe zum Ganzen auch Gern, DÖV 1985, 558; Wolff/Neumann, NStZ 2003, 404 (407 f.).

Kurzbeiträge

Aus den aktuellen Berichten der Aufsichtsbehörden (16): Datenschutz in der Schule

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter*

Für Schulen und Lehrer gilt, dass Kinder ebenso ein Recht auf Datenschutz haben wie Erwachsene. Da sie dieses Recht häufig noch nicht verstehen oder einfordern, ist die Schule umso mehr gefordert, zumal neue Verarbeitungsformen per Internet, Computer, Schulverwaltungs- und Zeugnisprogrammen oder elektronischen Klassenbüchern (hierzu BlnBDI, JB 2013, Zoff 12.1.2) praktiziert werden. So müssen es Schüler nicht akzeptieren, dass Noten von Klausurarbeiten offen verlesen oder Zeugnisse nach einer Rangliste ausgegeben werden (ThürLfDI, 10. TB, öffent. Bereich, Ziff. 13.7) – was natürlich nichts daran ändert, dass gute Leistungen auch gelobt werden dürfen.

I. Schüler- und Lehrerdaten im Internet

Als eine nicht zulässige Praxis bewertet der ThürLfDI (a.a.O. Ziff. 13.5), Vertretungspläne unter Nennung der Namen der Lehrkräfte und anderer Daten im Internet zu veröffentlichen. Zwar könne eine solche Vertretungsliste im Schulgebäude selbst zur Aufgabenerfüllung und internen Information ausgehängt werden, eine für jedermann zugängliche Internetveröffentlichung sei jedoch nicht erforderlich. Die Übermittlung personenbezogener Daten an private Stellen außerhalb der Schulöffentlichkeit ist nur gestattet, wenn die Lösung schulischer Aufgaben und Organisationsfragen sie gebietet. Daher ist es unverhältnismäßig, die gewünschte Information der Vertretungslehrer bzw. der Eltern mit der gleichzeitigen Informationsmöglichkeit für Unbefugte zu verbinden. Auch eine Einwilligung der betroffenen Lehrkräfte führt nicht weiter, da sie einen nicht notwendigen Zweck gestatten soll und aufgrund des beschäftigungsbedingten Abhängigkeitsverhältnisses ggf. nicht mit der gebotenen Freiwilligkeit erfolgt.

Nicht in das Internet gehören auch vertrauliche Information über Aussagen von Lehrern oder über das Abstimmungsverhalten in Schulgremien. Die Zulässigkeit der Verarbeitung personenbezogener Daten durch schulische Gremien und deren Mitglieder richtet sich ggf. nach dem jeweiligen Schulgesetz und wäre auch nach dem Landesdatenschutzgesetz nur rechtmäßig, wenn sie zur Erfüllung der den Gremien zugewiesenen schulbezogenen Aufgaben erforderlich ist. Dies ist hinsichtlich der Veröffentlichung von Daten über Lehrkräfte im Hinblick auf die Aufgaben eines Mitglieds der Schulkonferenz nicht gegeben und damit unzulässig; zumal die Mitglieder der Schulkonferenz in Angelegenheit der Gremienarbeit zur Verschwiegenheit verpflichtet sind (BlnBDI, JB 2013, Ziff. 12.1.5).

Im Rahmen ihrer Öffentlichkeitsarbeit möchten Schulen Ereignisse aus dem Schulleben publizieren, sei es in einer Schulzeitschrift, sei es auf der Homepage der Schule. Der bayerische LfD (25. TB, 2013, Ziff. 10.3) weist darauf hin, dass es hierfür grundsätzlich einer freiwilligen, informierten und schriftlichen Einwilligung der betroffenen Schüler, Eltern oder Lehrer bedarf. Eine gesetzliche Ausnahme gilt u.a. für den in Bayern geregelten papiergebundenen Jahresbericht (Art. 85 Abs. 3 BayEUG). Fotos sind in dem Katalog der dort zu veröffentlichten Daten nicht genannt und daher auch hier einwilligungspflichtig. Für die in der Regel bei jeder schulischen Veröffentlichung einzuholende Einwilligung hat der BayLfD verschiedene fallbezogene Muster-Einwilligungserklärungen entwickelt, die unter www.datenschutz-bayern.de unter der rubrik „Themen“, Unterrubrik „Schulen“ abrufbar sind.

Auf Probleme stieß auch das Vorhaben einer privaten Ersatzschule in Berlin, die Daten ihrer Schüler und Lehrer von dem Anbieter einer US-amerikanischen Website verwalten zu lassen. Nach Auffassung des BlnBDI (JB 2013, Ziff. 12.1.3) ist die – trotz der faktischen Auftragsdatenverarbeitung – erfolgende Datenübermittlung in das Drittland USA nur zulässig bei Einwilligung der Betroffenen. An deren Freiwilligkeit fehlte es, da sie bei Schuleintritt im Zusammenhang mit dem Abschluss des Schulvertrages als conditio sine qua non eingeholt werden sollte. Zudem wurde die von dem US-Anbieter eingesetzte Software „engrade“ als zur Authentifizierung der zugriffberechtigten Lehrkräfte nicht ausreichend bewertet, da die Begrenzung des Zugriffsschutzes auf die Kombination aus Nutzername und Passwort für den Zugriffsschutz im Umfeld Schule nicht genüge. Insbesondere bei einer dezentralen Nutzung (über Rechner in den Unterrichtsräumen) hätten unbefugte Dritte (z.B. Schüler) durch Einsatz von Spionagesoftware leicht die Möglichkeit des Zugriffs auf das System. Ein Verzicht der Betroffenen auf höhere Sicherheitsanforderungen sei mit den zwingenden Vorgaben des Schulgesetzes unvereinbar.

II. Interne Vertraulichkeit

Die für die Fehlzeiten eines Schülers eingegangen Begründungen sind nur den Lehrern und Personen zugänglich zu machen, die die Angaben aus organisatorischen oder pädagogischen Gründen benötigen. Mitschüler zählen nicht hierzu. Ob diese Vertraulichkeit gewährleistet ist, wenn die Schule die Übermittlung der Entschuldigung per unverschlüsselter e-mail

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

vorgibt, wird vom LfD Baden-Württemberg (31. TB, 2012/2013, Ziff. 8.2.5) in Frage gestellt, wobei hier auch der Identität des Absenders nicht immer vertraut werden könne. Zu regeln ist die sichere Aufbewahrung der Entschuldigungen und deren Löschung. Sollten Fehlzeiten Ausfluss auf die Notenbildung haben, so ist die Speicherung bis zur Bestandskraft des Zeugnisses erforderlich.

Fehlt ein Schüler unentschuldigt, so sollen im Rahmen eines Pilotprojekts an Berliner Schulen die Eltern direkt aus dem Klassenzimmer per SMS unmittelbar darüber informiert werden. Mit dem BlnBDI (JB 013, Ziff. 12.1.2) wurde hierüber Einvernehmen erzielt, nachdem eine „neutrale" Formulierung der Benachrichtigung gewählt wurde. Der BDI hatte geltend gemacht, dass bei der Versendung der SMS nicht festgestellt werden kann, wer das Handy gerade (physisch) in Besitz hat und die Information zur Kenntnis nimmt.

Wechselt ein Schüler z.B. im Folge eines Umzugs die Schule, so darf (vgl. z.B. § 115 Abs. 3 SchulG B.-W.) die aufnehmende Schule die zu Verwaltungszwecken notwendigen Daten bei der abgebenden Stelle erheben, was deren Befugnis zur Übermittlung indiziert. Daten, die zur Aufgabenerfüllung der neuen Schule nicht erforderlich sind, dürfen nur mit Einwilligung des Erziehungsberechtigten weitergegeben werden (§ 4 Abs. 1 Nr. 2 LDSG-BW). Das gilt beispielsweise für die Grundschulempfehlung zum Besuch weiterführender Schulen (LfD Bad.-Würt. 31. TB, 2012/2013, Ziff. 8.2.6).

Gestattet eine Schule Dritten (z.B. Krankenkasse, Bank) im Rahmen ihres pädagogischen Konzepts die Durchführung einer Informationsveranstaltung, so muss sie sicherstellen, dass die Veranstaltung nicht dazu genutzt wird, Schülerdaten zu werblichen Zwecken zu erheben (LDA Brandenburg, TB, 2012/2013, Ziff. 13.3).

III. Soziale Netzwerke im Schulbetrieb

Ob im Schulbetrieb oder in der Kommunikation zwischen Lehrern und Schülern Facebook oder andere soziale Netze zum Einsatz kommen dürfen, ist Gegenstand fast aller aktuellen Tätigkeitsberichte. Dabei werden verschiedene Facetten beleuchtet, wobei jedoch die Vereinbarkeit mit dem Datenschutz generell in Frage steht. So ist nach dem HmbBfDI (24. TB, 2012/2013, Ziff. 7.2) die Nutzung von sozialen Medien zur Verarbeitung personenbezogener Daten zu dienstlichen Zwecken nach dem Landesdatenschutzgesetz verboten (ebenso BlnBDI, JB 2013, Ziff. 12.1.1. oder LfDI Rheinl.-Pfalz, 24. Bericht, 2012/2013, Ziff. 6.1.1). Selbst wenn man deutsches Datenschutzrecht aufgrund des Hauptsitzes des Netzwerkanbieters im Ausland für nicht anwendbar ansieht, so greifen die Gesetze, die das Lehrer-Schülerverhältnis regeln (vgl. für Mecklenburg-Vorpommern, LfDI, TB 2012/2013, Ziff. 6.9.6). In Baden-Württemberg besteht sogar ein ministerielles Verbot, gleiches gilt für Bayern und Schleswig-Holstein (vgl. bei BlnBDI, TB 2013, Ziff. 12.1.1). Weiterhin möglich bleibt jedoch die Verwendung von Facebook bei der Behandlung des Themas im Unterricht zu Demonstrationszwecken (LfD Bad.-Würt. 31. TB, 2012/2013, Ziff. 8.2.7)

IV. Schulbedingte Kommunikation per Facebook

Im schulischen Alltag besteht für Lehrkräfte ggf. das Erfordernis, mit Schülern auch nach dem Unterricht noch in schulischen Angelegenheiten zu kommunizieren. Dafür steht den Schulen teilweise eigene Software zur Verfügung. Eine Nutzung von Facebook zur Schüler-Lehrer-Kommunikation ist jedoch datenschutzrechtlich aus folgenden Gründen nicht gestattet: Abgestellt wird zunächst auf eine Verletzung des Grundsatzes der Erforderlichkeit, da der Einsatz von Facebook für Unterrichtszwecke nicht zur Erfüllung des Bildungs- und Erziehungsauftrages der Schule geboten ist; ferner liegt ein Verstoß gegen die Bestimmungen zum technisch organisatorischen Datenschutz vor, da die Datensicherheit bei einer Datenverarbeitung in den USA nicht sichergestellt werden kann; die Lehrkräfte können nicht gewährleisten, dass die personenbezogenen Verkehrs- und Inhaltsdaten der Kommunikation vertraulich bleiben, da das Geschäftsmodell des Unternehmens darauf ausgerichtet ist, die Informationen aus dem Kommunikations- und Nutzungsverhalten der jugendlichen Mitglieder zu vermarkten. Würde eine Schule Facebook als Lernplattform nutzen, würde ferner gegen die Bestimmungen zur Auftragsdatenverarbeitung und zum Telemedienschutz verstoßen.

V. Facebook-Freundschaften zwischen Lehrkräften und Schülern

Wenn eine Lehrkraft über einen eigenen privaten Facebook-Account verfügt, stellt sich die Frage, ob sie sich mit den Schülern im Sinne der Facebook-Terminologie „befreunden" darf. Die Aufsichtsbehörden verneinen dies zu Recht (vgl. LfDI M.-V., a.a.O., Ziff. 6.9.6)

Anderenfalls hätte aus datenschutzrechtlicher Sicht, worauf der LfDI Rheinl.-Pfalz (a.a.O.) hinweist, eine Facebook-Freundschaft zur Folge, dass Lehrkräfte und Schüler wechselseitig Einblick in die jeweils anderen Profile und die dort hinterlegten Daten und Fotos erhalten. Sie könnten erfahren, wer, wann und auf welcher Webseite den Like Button betätigt hat, welche Nachricht auf einer „befreundeten" Pinnwand gepostet wurde und was sonst noch aus dem realen Leben bei Facebook preisgegeben wird. Über die „benutzerdefinierten Freundeslisten" könne man zwar die Zugriffsmöglichkeiten der Facebook-Freunde in Bezug auf das eigene Profil einschränken; dies sei aber mit einem gewissen Aufwand verbunden und dürfte schon aus Bequemlichkeit in der Praxis kaum genutzt werden.

VI. Facebookkontakt aufgrund Einwilligung der Schüler

An der Problematik ändert sich nichts, wenn der Facebookkontakt auf „freiwilliger" Basis geschieht. Der BlnBDI (a.a.O) weist zutreffend darauf hin, dass die Lehrkraft, ganz gleich, in welchem Zusammenhang sie mit ihren Schülern in Kontakt tritt, in der Regel immer auch eine Vertreterin der Schule bleibt. Die Schüler können sich daher nicht freiwillig für eine Freund-

schaft mit der Lehrkraft entscheiden, da für sie nicht auszuschließen ist, dass mit der Absage der Freundschaftsanfrage schulische Nachteile verbunden sind. Zudem würde der Schüler die Bedeutung und Tragweite seiner Einwilligung selten überblicken, da bei großen sozialen Netzwerken Datenverarbeitungsvorgänge komplex, unvollständig und weitgehend unverständlich dargestellt werden (vgl. LfDI M.-V. Ziff. 6.9.6), wobei dieser fehlende Überblick bei einer Einholung der Einwilligung bei den Eltern kaum anders wäre.

Bei Freundschaftsanfragen durch Schüler besteht, wie der LfDI Rheinl.-Pfalz (a.a.O.) anführt, umgekehrt für die Lehrkraft das Problem der Ungleichbehandlung und die Gefahr, dass die gebotene Trennung zwischen schulischen und privaten Angelegenheiten unterlaufen wird. Darüber hinaus könne nicht ausgeschlossen werden, dass die Facebook-Nutzung durch Lehrkräfte Schüler überhaupt erst zu einer Facebook-Mitgliedschaft veranlasst, an Facebook bindet oder den Entschluss, das Angebot von Facebook nicht mehr zu nutzen, erschwert.

Letztendlich ist es mit dem Bildungs- und Erziehungsauftrag der Schule nicht zu vereinbaren, wenn das Geschäftsmodell von Facebook – „Verkauf" persönlicher Daten für kommerzielle Zwecke – durch die Institution Schule und ihre Repräsentanten zumindest indirekt unterstützt wird.

VII. Schülerfoto auf dem Lehrermobiltelefon

Einem Lehrer, der eine neue Klasse übernimmt, mag ein Sitzplan mit Namen und Fotos der Schüler die Arbeit zum Einstieg erleichtern. Gleichwohl ist er nicht befugt, hierzu auf seinem privaten Mobiltelefon Portraitfotos der Klasse zu machen. Der LfDI Rheinl.-Pfalz (a.a.O, Ziff. III-6.1.5) verneint einerseits die nötige „Erforderlichkeit für die Erfüllung schulischer Aufgaben (§ 67 Abs. 1 SchulG)" und sieht zudem in dem Fall keine Befugnis zur Speicherung der Fotos auf dem privaten Handy.

VIII. Videokameraattrappen auf der Mädchentoilette

Auch an Schulen bestehen „höchstpersönliche Bereiche der Privat- und Intimsphäre" wie z.B. Toiletten, Duschen oder Umkleideräume. Sie sind zwar nicht der Kontrolle der Schule entzogen, eine Überwachung durch Videokameras ist jedoch generell unzulässig. Daran würde sich auch nichts ändern, dass die Elternschaft der Maßnahme zustimmt. Gleiches gilt für den Einsatz von Videoattrappen (ThürLfDI, 10. TB öffentl. Bereich, 2012/2013, Ziff. 13.6)

Das Datenschutzaudit bei Auftragsdatenverarbeitern

Ein Überblick über Anforderungen und bisherige Entwicklungen

Timo Bittner, LL.M., LL.M., Irmenseul*

I. Einleitung

Auslagerungen von vormals internen Aufgaben und Beauftragungen von Fremdfirmen mit neuen Aufgaben sind in der Wirtschaft ein beliebtes Mittel, um Kosten zu senken oder sich auf das Kerngeschäftsfeld zu konzentrieren. Beliebtes Outsourcing dieser Art betrifft z.B. Personaldienstleistungen, IT-Support, Marketingdienstleistungen oder Datenentsorgungen. Diese Aufgaben umfassen häufig die Erhebung, die Verarbeitung oder die Nutzung von personenbezogenen Daten[1], was eine Funktionsübertragung darstellen kann. Werden die personenbezogenen Daten jedoch nicht eigenständig, sondern durch eine externe Stelle im Auftrag für die verantwortliche Stelle erhoben, verarbeitet oder genutzt, liegt eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG vor. Diese Konstellation setzt die Verarbeitung von personenbezogenen Daten durch eine andere Stelle, in Bezug auf die datenschutzrechtliche Zulässigkeit, einer internen Verarbeitung gleich[2]. Dies kann als eine Herabsetzung der Zulässigkeitshürde angesehen werden. Um einen sicheren und datenschutzkonformen Rahmen für die Verarbeitung zu gewährleisten, werden dem Auftraggeber und dem Auftragnehmer jedoch entsprechende Pflichten durch § 11 BDSG auferlegt.

Diese Pflichten bestehen zum einen darin, dass der Auftraggeber für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich bleibt. Ferner obliegt es dem Auftraggeber, den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftragnehmer hingegen hat, insofern er beauftragt werden möchte, die technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten sicherzustellen. Sollte dies erfüllt sein, so muss der Auftrag schriftlich erteilt werden, wobei gesetzlich vorgeschriebene Mindestinhalte geregelt sein müssen.

* Der Autor ist Berater bei der s-con Datenschutz und schreibt eine Dissertation über Datenschutzaudits bei Auftragsdatenverarbeitern.

1 Staub, DuD 2014, 159 (159).

2 Spoerr, in: Wolff/Brink, Beck'scher Online-Kommentar zum Datenschutzrecht, Edition 7, Stand 01.02.2014, § 11 Rn. 4; Gola/Schomerus, Bundesdatenschutzgesetz, 11. Aufl., München 2012, § 11 Rn. 3.

Die Pflicht des Auftraggebers, sich regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten zu überzeugen und das Ergebnis zu dokumentieren, scheint nicht nur eine Regelung zu sein, der häufig nicht durch den Normadressaten entsprochen wird, sondern auch eine sehr schwierige Aufgabe. Die Auftraggeber müssen sich entscheiden, auf welchem Weg und mit welchem Aufwand diese Vergewisserung vorgenommen werden soll. Hierbei wäre es für die verantwortliche Stelle von großem Vorteil, wenn ein Datenschutzsiegel bestätigt, dass der Auftragsdatenverarbeiter bei seiner Tätigkeit die gesetzlichen Bestimmungen zum Datenschutz einhält und die Umsetzung kontinuierlich verbessert[3] sowie darüber hinaus gehende Maßnahmen zum Schutz von personenbezogenen Maßnahmen ergreift[4].

Solch ein Vorteil bietet sich in der Praxis jedoch höchst selten. Die wenigsten Auftragsdatenverarbeiter lassen sich durch ein externes Audit zertifizieren. Hinzu kommt das Problem, dass es bisher keine gesetzlichen Vorgaben für eine Durchführung entsprechender Audits oder Anforderungen an Auditoren gibt[5]. Dies kann Zweifel darüber aufkommen lassen, dass bestehende Angebote alle erforderlichen Inhalte zum Gegenstand haben. Hierunter und unter der Tatsache, dass Audits für die verantwortliche Stelle bislang nicht ausreichend transparent sind, leidet wiederum momentan die Aussagekraft und Bedeutung solcher Datenschutzsiegel.

Derzeit kommen Auftragsdatenverarbeiter nicht immer ausreichend ihrer Pflicht nach, technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu ergreifen. Insbesondere eine stete Verbesserung und Reflexion der eigenen Umsetzung von datenschutzrechtlichen Bestimmungen ist oftmals praxisfern. Auch im Hinblick auf eine kontinuierliche Steigerung des Datenschutzstandards beim Auftragsdatenverarbeiter könnte ein zielgerichtetes Audit von Vorteil sein[6].

II. Gegenstand und Inhalt

Die Hauptfrage, welche sich zunächst stellt, ist, was der eigentliche Gegenstand eines solchen Datenschutzaudits sein sollte. Dies umfasst die Fragen, wer an dem Audit teilnimmt sowie in welchem räumlichen Bereich was auditiert wird[7]. Eine Orientierung an dem Umweltschutzaudit kommt in Bezug auf diese Fragestellung nicht in Betracht[8], da bei diesem das gesamte Umweltmanagementsystem eines Standortes betrachtet wird. Auch ein Datenschutzaudit, welches den Auftragsdatenverarbeiter selbst oder eines seiner Produkte zertifiziert, scheint nicht fähig zu sein, für die vorgenannten Probleme Abhilfe zu schaffen. Eine Ausrichtung an Begrifflichkeiten wie Datei oder Verwendungszweck wäre ebenfalls ungünstig, weil diese zu einem zu begrenzten Prüfungsrahmen führen würde. Hingegen würde eine Auditierung des gesamten Auftragsdatenverarbeiters zu einem zu großem Umfang führen, der über das Ziel hinaus führen würde, es sei denn, der Auftragsdatenverarbeiter betreibt nur eine Anwendung[9]. Des Weiteren darf die Auditierung aber sich gerade nicht nur auf den Auftragsdatenverarbeiter beschränken. Alle konkret einbezogenen Unterauftragnehmer sollten vom Audit mit erfasst werden.

Denkbarer Gegenstand des Audits könnte vielmehr eine konkrete Anwendung sein. Unter dieser muss ein Prozess verstanden werden, der aus dem Zusammenwirken von technisch-organisatorischen Komponenten zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten besteht und dabei einer übergreifenden Zielsetzung einer oder mehrere datenverarbeitenden Stellen dient[10]. Im Fall einer Auftragsdatenverarbeitung wäre dies die Anwendung aller involvierten Systeme durch den Auftragsdatenverarbeiter und dessen Unterauftragnehmer, welche die Anbahnung, die Durchführung und die Beendigung des Vertragsverhältnisses umfasst. Bespielhaft wäre ein ausgelagertes Bewerbungsmanagement, bei dem der Auftragsdatenverarbeiter für den Auftraggeber Stellenausschreibungen vornimmt, die Bewerber einlädt, unter Einhaltung von Vorgaben eine Vorauswahl vornimmt und ein Unterauftragnehmer eine zugehörige Bewerberdatenbank führt. Sollten Schnittstellen zu anderen Anwendungen bestehen, so bilden diese die Grenzen des Prüfungsgegenstands[11]. Der Auftragsdatenverarbeiter müsste vor dem jeweiligen Audit die Anwendung genau beschreiben, damit der Auditor diese anschließend überprüfen kann[12].

III. Nutzen und Aussagekraft

Ob ein solches Audit den bezweckten Lerneffekt beim Auftragsdatenverarbeiter erfüllt, hängt davon ab, ob das Audit auch als ein Lernsystem verstanden wird[13]. Selbstverständlich wird bereits dadurch der Datenschutzstandard beim Auftragsdatenverarbeiter in geringem Umfang gesteigert, dass dieser den Prozess eines Datenschutzaudits auf sich nimmt und dabei die Beschäftigten mit der Thematik konfrontiert[14]. Diese werden zukünftig den Datenschutz nicht gänzlich vergessen und diesem einen gewissen Stellenwert beimessen. Bemerkenswert ist, dass der Lerneffekt nicht immer als eines der Ziele angesehen wird[15].

Die Erreichung weiterer möglicher Ziele, wie eine Stärkung der Selbstverantwortung des Auftragsdatenverarbeiters und des Wettbewerbs sowie eine Verringerung des Vollzugsdefizits des Datenschutzrechts[16], hängt davon ab, ob der Auftragsda-

3 Mester, DuD 2014, 141 (141).

4 So auch: Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 5 f.

5 Weichert, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 4. Auflage, Frankfurt am Main 2104, § 9a Rn. 2.

6 Roßnagel/Pfitzmann/Garstka, Gutachten zur Modernisierung des Datenschutzrechts, 2001, S. 134; Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 6.

7 Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 70.

8 Ebenda.

9 Roßnagel/Pfitzmann/Garstka, Gutachten zur Modernisierung des Datenschutzrechts, 2001, S. 136; Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 73; anderer Meinung wohl: Bizer, DuD 2006, 5 (5 ff.); Zwick, DuD 2006, 24 (27).

10 Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 71.

11 Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 72.

12 Ebenda.

13 Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 6.

14 Ebenda.

15 Dieser findet zumindest nicht Erwähnung in der Aufzählung der Ziele bei: Behrendt, DuD 2006, 20 (22).

16 Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 4; siehe auch Roßnagel/Pfitzmann/Garstka, Gutachten zur Modernisierung des Datenschutzrechts, 2001, S. 132 f.

tenverarbeiter tatsächlich dazu bereit ist, den Datenschutz zu verbessern. Eine reine Vorspiegelung von Fortschrittsabsichten sowie reinen Verbesserungen auf dem Papier werden keinen tatsächlichen Nutzen haben, sondern nur eine reine Täuschungswirkung gegenüber der verantwortlichen Stelle bzw. den Betroffenen. Eine Minderung des Vollzugsdefizits korreliert mit einer tatsächlichen Erhöhung des Datenschutzniveaus beim Auftragsdatenverarbeiter. Die Steigerung der Selbstverantwortung ist nicht nur eine Zielsetzung, die mittels eines Audits verwirklicht werden soll, sondern ist bereits wichtiger Bestandteil des gesamten Prozesses. Darüber hinaus sind Nutzen hinsichtlich Prozessoptimierung und Qualitätssteigerung möglich[17].

Die Aussagekraft eines Audits hängt offensichtlich davon ab, ob dieses in irgendeiner Art standardisiert oder vergleichbar ist[18]. Das bedeutet im Einzelnen, dass Audits nur eine angemessene Aussagkraft haben, wenn sie transparent sind, also das Auditverfahren selbst, dessen Inhalt, Anforderungen und Ergebnis allen berechtigten Stakeholdern zur Einsicht überlassen wird und sich das Audit nicht in erheblichem Umfang von den angebotenen Audits anderer Anbieter unterscheidet. In Bezug auf diese Anforderungen stellt sich die weitere Frage, ob ein Audit transparent sein kann, wenn dessen Verfahren und Ergebnis nicht veröffentlicht wird und ob eine Vergleichbarkeit gegeben ist, wenn das Audit bei einer Gegenüberstellung mit den Angeboten anderer Anbieter in Bezug auf Umfang, Vorgehensweise, Zeitrahmen, Niveau und Intensität eine abweichende Auffassung erkennen lässt. Für eine Aussagekraft eines Auditergebnisses ist ferner sehr entscheidend, ob der durchführende Auditor über alle erforderlichen Fähigkeiten und Kenntnisse verfügt[19].

Damit das Audit eine erstrebenswerte Aussagekraft vorweisen kann, dürfen aber auch Staatsgrenzen bei der Auditierung keine Barrieren darstellen[20]. Das heißt nicht nur, dass bei solchen Audits grenzüberschreitende Datenverarbeitungen betrachtet werden müssen, sondern diese in Folge von Aufdeckungen entsprechender Mängel auch verbessert werden müssen. Dabei stellen sprachliche Unterschiede, verschiedene Auffassungen von Datenschutz bzw. dessen Vollzug als auch differierende Gesetze und deren Interpretationen Hindernisse dar, die im schlechtesten Fall kumulierend auftreten können. Im europäischen Datenschutz ist bislang der einzige gemeinsame Nenner Art. 17 der Richtlinie 95/46/EG. Dieser bildet die Grundlage für § 11 BDSG und ist, aufgrund des Richtliniencharakters, unbestimmter als die deutsche Vorschrift. Wichtig ist jedoch, dass dort bereits die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Maßnahmen umrissen werden, der verantwortlichen Stelle die Pflicht auferlegt wird, dass diese sich von der Angemessenheit dieser Maßnahmen überzeugt, sowie dass das Schriftformerfordernis des Vertrages gefordert wird.

Für Auftragsdatenverarbeiter, welche als Servicerechenzentren agieren, wurde schon vor längerer Zeit ein konkreter Bedarf für Datenschutzaudits bestätigt[21]. Hinzu kommt, dass die immer ausgeprägtere Nutzung von im Ausland angesiedelten Cloud-Diensten ein weiteres Erfordernis für die Etablierung von Datenschutzaudits schafft. Aus diesen Gründen scheint die Einführung entsprechender Audits notwendig zu sein und einen sinnvollen Nutzen zu stiften[22].

IV. Rechtliche Fragen

Wie oben dargestellt, sind die Anforderungen an ein entsprechendes Audit, dass eine solche Maßnahme nicht ins Leere läuft und die eigentlichen Ziele nicht verfehlt werden, nicht unerheblich. Gerade im Hinblick auf die Probleme, die durch eine grenzüberschreitende Datenverarbeitung auftreten können, stellt sich die Frage, ob ein Regelungsrahmen für Datenschutzaudits bei Auftragsdatenverarbeitern erforderlich ist. Weiterhin bleibt offen, welche Form ein entsprechender Regelungsrahmen haben sollte. Diverse Modelle kommen dabei in Frage.

Mit der Implementierung des § 9a in das BDSG wurde der Form einer gesetzlichen Regelung bereits im Jahr 2001 der erste Anstoß gegeben. Diese Programmnorm[23] stellt ein Gesetz in Aussicht, das nicht nur die Durchführung entsprechender Audits, sondern auch das Verfahren und die Anforderungen und die Zulassung der Auditoren regelt. Dem Wortlaut entsprechend zielt das Vorhaben darauf ab, den Datenschutz und die Datensicherheit bei der zu auditierenden Stelle zu verbessern. Obwohl im Bundestag ein Gesetzesentwurf[24] diskutiert wurde, ist bis heute kein entsprechendes Gesetz verabschiedet worden[25]. Hierfür ist insbesondere die umfangreiche Kritik des Bundesrates[26] verantwortlich[27]. Obwohl sich die Politik mit der Programmnorm bereits darauf festgelegt hat, ein entsprechendes Gesetz zu verabschieden[28], und ein zweiter, wesentlich kompakterer Vorschlag[29] dem Bundesministerium des Inneren vorgelegt wurde, deutet nichts darauf hin, dass in absehbarer Zukunft ein nationales Gesetz beschlossen wird.

Neben einem nationalen Gesetz kommt auch eine supranationale Regelung des Themas in Betracht. Die geltende Richtlinie 95/46/EG erwähnt ein Datenschutzaudit nicht. Derzeit würde die aktuelle Entwicklung in der Europäischen Union jedoch die Gelegenheit bieten, dass Thema in allen Mitgliedsstaaten verbindlich zu regeln. Der durch die Europäische Kommission erstellte Entwurf für eine Datenschutzgrundverordnung[30] beinhaltet mit Art. 38 jedoch eher ein etwas ausführlicheres Ab-

17 Behrendt, DuD 2006, 20 (22).

18 So auch: Meissner, DuD 2008, 525 (525); Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 93.

19 Roßnagel/Pfitzmann/Garstka, Gutachten zur Modernisierung des Datenschutzrechts, 2001, S. 138.

20 Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 72.

21 Gesellschaft für Datenschutz und Datensicherheit, GDD-Mitteilungen 2/99, S. 4.

22 Selber Meinung: Bizer, DuD 2006 5 (9).

23 Scholz, in: Simitis, Bundesdatenschutzgesetz, § 9a BDSG, Rn. 1.

24 BT-Drs. 16/12011.

25 Scholz, in: Simitis, Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011, § 9a Rn. 40.

26 BR-Drs. 4/09, S. 1 ff.

27 Gola/Schomerus, Bundesdatenschutzgesetz, 11. Aufl., München 2012, § 9a Rn. 2.

28 Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 140; Scholz, in: Simitis, Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011, § 9a Rn. 40.

29 Roßnagel/Pfitzmann/Garstka, Gutachten zur Modernisierung des Datenschutzrechts, 2001, S. 140 ff.

30 Europäische Kommission, KOM(2012) 11 endgültig.

bild der deutschen Programmnorm, da die Vorschrift genauere Regelungen nur ankündigt und weitere Regelungsvorhaben legitimiert. In dessen Absatz 1 ist dabei jedoch nicht wörtlich die Rede von Datenschutzaudits, sondern von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -zeichen, anhand derer Betroffene rasch das von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern gewährleistete Datenschutzniveau in Erfahrung bringen können. Die Änderungsvorschläge vom Berichterstatter für den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments[31] brachten in der Hinsicht keine signifikanten Konkretisierungen. Ganz im Gegensatz dazu machte der inoffiziell konsolidierte Entwurf für die weiteren Verhandlungen[32] wesentlich präzisere Vorschläge. Fraglich ist, ob ein Audit in der Datenschutzgrundverordnung grundsätzlich ausreichend Berücksichtigung finden kann oder ob hierzu eine eigene Verordnung erforderlich wäre. Das Umweltschutzaudit ist durch die Umwelt-Audit-Verordnung 761/2001/EG geregelt. Diese legt den Mitgliedsstaaten die Pflicht auf, Zulassung und Aufsicht der Umweltgutachter sowie die Benennung der für die Standortregistrierung zuständigen Stellen durch nationales Recht näher zu bestimmen. Diese Aufgabe erfüllt in Deutschland das Umweltauditgesetz[33]. Da die Idee eines Datenschutzaudits auf das Umweltschutzaudit zurückzuführen ist[34], stellt sich die Frage, ob auch hier eine Kombination von nationalem und europäischem Recht denkbar wäre. Diese könnte, wie beim Umweltschutzaudit, in einer Umsetzung in nationales Recht bestehen, welches auf eine europäische Richtlinie oder einen dazu ermächtigenden Artikel in der geplanten Datenschutzgrundverordnung zurückzuführen ist.

Neben Gesetzen und anderen legislativen Maßnahmen gibt es aber auch andere Möglichkeiten für ein entsprechendes Regelwerk. Hierbei ist z.B. auf die ISO-Normen zu verweisen. Diese beschreiben bereits andere Audits, die für Unternehmen große Relevanz aufweisen. In erster Linie sind hier das QM-Audit ISO 9001 oder das IT-Sicherheitsaudit ISO 27001 zu nennen. Auch hier ist wieder das Umweltschutzaudit als Beispiel aufzuzählen, da die ISO-Norm 14001 das Vorgehen bei Umweltaudits konkretisiert. Angesichts dessen ist auch hier eine Abwägung dahingehend erforderlich, ob für das Datenschutzaudit eine ISO-Norm als Regelungsform zweckführend ist. Dabei darf nicht übersehen werden, dass auch solche Regelungen einen indirekten Zwang zur Durchführung des Audits auf den Auftragsdatenverarbeiter ausüben können[35].

Eine dritte Form für eine mögliche Regelung ist die nicht bindende Regelung durch entsprechende Interessensverbände bzw. -vereine. Solch ein Standard könnte der neue kooperative Datenschutzstandard DS-BvD-GDD-01[36] des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. sowie der Gesellschaft für Datenschutz und Datensicherheit e. V. sein. Da aber solche Modelle, wie grundlegend auch ISO-Normen, keinen Gesetzescharakter aufweisen und somit nicht zwingend anwendbar sind, wird sich zeigen, ob diese alle gewünschten Ziele erreichen können.

Letztendlich ist es auch möglich, entsprechende Audits durch die staatlichen Datenschutzaufsichten durchführen zu lassen oder es diesen zu überlassen, ein einheitliches Verfahren zu entwickeln, zu etablieren, zu überwachen und zu unterstützen. Dabei stellt sich jedoch die Frage, ob dies wirtschaftlich zu verwirklichen ist und ein solches Audit alle bezweckten Effekte erzielen kann. Um diese Fragen beantworten zu können, müssen bestehende Modelle betrachtet werden. In Schleswig-Holstein hat das ULD bereits ein eigenes Audit für öffentliche und nicht-öffentliche Stellen sowie die Landesdatenschutzaufsicht in Bremen für öffentliche Stellen ein Datenschutzaudit eingeführt[37]. Sollten diese die angestrebten Ziele erreichen, könnten sie als Vorbild dienen.

Neben der Frage des Regelungsrahmens stellen sich weitere rechtliche Fragen. Hierzu zählt die Frage, ob bei einer Regelung der Zulassung von Auditoren ein Eingriff in das Grundrecht auf Ausübung der Berufsfreiheit der Gutachter aus Art. 12 GG vorliegt. Dabei muss berücksichtigt werden, ob Gutachter eine anerkannte Prüfung ablegen können oder ob der Markt für Datenschutzaudits sogar nur zugelassenen Auditoren eröffnet sein soll[38]. Ferner könnte auch gegenüber dem Unternehmen, dem nach nicht erfolgreicher Auditierung das Zertifikat oder das Führen eines Datenschutzsiegels untersagt wird, ein Eingriff in die freie Berufsausübung und Gewerbefreiheit vorliegen[39].

Darüber hinaus stellt sich in Bezug auf das Führen eines Zertifikats die Frage, welche rechtlichen Folgen dies mit sich bringt und welche Auswirkrungen dies auf die Rechtssicherheit hat. In Bezug auf Haftung, Datenschutzpannen und Bußgelder wäre es denkbar, dass das Führen eines Zertifikats Effekte für die verantwortliche Stelle oder den Auftragsdatenverarbeiter hat. Dabei spielt es sicherlich eine Rolle, wie das Audit ausgestaltet ist bzw. welchem Regelungsrahmen das Audit unterworfen ist.

Diese weiteren Probleme rechtlicher Natur deuten bereits zumindest darauf hin, dass eine gesetzliche Regelung förderlich wäre. Sollte dieser Eindruck letztlich bestätigt werden, bedarf es der Klärung der Gesetzgebungs- und Verwaltungskompetenz[40]. Der bestehende Gesetzentwurf könnte dann vielleicht als Grundlage für einen neuen Vorschlag für ein Gesetz dienen und die Programmnorm § 9a BDSG könnte doch noch ihren Zweck erfüllen. Dazu müsste der Entwurf geprüft und in der Weise angepasst werden, dass dieser den Entwicklungen seit seiner Erstellung Rechnung trägt. Ebenso sollten die Vor- und Nachteile einer nationalen bzw. supranationalen Regelung abgewogen werden. Allerdings müssten bei dieser Abwägung auch wirtschaftliche und politische Aspekte eine angemessene Berücksichtigung finden.

31 Europäisches Parlament, 2012/0011(COD).

32 Inofficial consolidated version after LIBE COMMITTEE VOTE provided by the rapporteur 22.10.2013.

33 Kloepfer, Umweltschutzrecht, München 2008, § 4 Rn. 103.

34 Scholz, in: Simitis, Bundesdatenschutzgesetz, § 9a BDSG, Rn. 2; Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 40.

35 Näheres hierzu bei: Zwick, DuD 2006, 24 (25).

36 Http://www.dsz-audit.de/datenschutzstandard/; Staub, DuD 2014, 159 (159 ff.).

37 Gola/Schomerus, Bundesdatenschutzgesetz, 11. Aufl., München 2012, § 9a Rn. 14; für Details siehe: https://www.datenschutzzentrum.de/audit/index.htm; Behrendt, DuD 2006, 20 (20 ff.); https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen02.c.736.de; Bock, DuD 2007, 410 (410); https://www.datenschutzzentrum.de/presse/20131114-europrise.html.

38 Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 135.

39 Ebenda.

40 Roßnagel, Datenschutzaudit, Wiesbaden 2000, S. 137 f.

V. Stand der Wissenschaft

Bisher gibt es für die Datenschutzauditierung von Auftragsdatenverarbeitern weder im europäischen noch im nationalen Recht eine gesetzliche Pflicht oder einen geregelten Rahmen. Das Bundesdatenschutzgesetz enthält zwar mit § 9a BDSG eine Programmnorm für Datenschutzaudits. Der Entwurf für ein Ausführungsgesetz von 2009[41] ist jedoch nicht als Gesetz verabschiedet worden. Zu dem Thema gab es bereits in der Vergangenheit wie auch heute wissenschaftliche und praxisnahe Publikationen[42]. Diese befassen sich jedoch meist mit einem allgemeinen Datenschutzaudit und nicht mit der konkreten Auditierung von Auftragsdatenverarbeitern. Oftmals werden insbesondere die in der Praxis auftretenden Interessenkonflikte und Probleme bei der Umsetzung nicht angemessen berücksichtigt.

Besonders im Hinblick darauf, dass mittlerweile diverse privatwirtschaftliche Stellen und Landesdatenschutzaufsichtsbehörden Datenschutzaudits anbieten, sowie Datenschutz-Interessensverbände sich dem Thema widmen, indem sie eine Ausbildung für Datenschutzauditoren anbieten und ein Zertifizierungsprogramm einführen, hat das Thema nicht nur weiteren wissenschaftlichen Klärungscharakter, sondern befasst sich auch mit einem aktuellen Thema des Datenschutzes. Dieses weist aufgrund der immer engeren Verstrickung des internationalen Datenverkehrs eine globale Bedeutung auf. Auf Grund dieser Problematik hat die Arbeitsgruppe „Rechtsrahmen des Cloud Computing" des Bundesministerium für Wirtschaft und Energie ein rechtspolitisches Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing" erarbeitet. Dieses zielt auf eine Compliance-Zertifizierung ab, welcher eine unabhängige Prüfung vorausgeht. Der Cloud-Nutzer könnte zukünftig auf ein solches Zertifikat vertrauen. Die eigentliche Überzeugung über die technischen und organisatorischen Maßnahmen könnte dann entfallen[43].

VI. Zusammenfassung von derzeitigen Unklarheiten

Die verschiedenartigen Modelle, die derzeit eingeführt werden bzw. eingeführt worden sind, müssen dahingehend bewertet werden, ob sie die Ziele eines modernen Datenschutzaudits für Auftragsdatenverarbeiter erfüllen können. Ferner müssen die Fragen geklärt werden, ob ein Audit freiwillig bleiben sollte, ob ein Regelungsrahmen erforderlich ist und falls ja, welche Art eine Zielerfüllung ermöglichen könnte.

Darüber hinaus muss ausgearbeitet werden, welche Inhalte ein Audit haben muss und wie die Durchführung in Bezug auf die verschiedenen Formen von Auftragsdatenverarbeitungen ausgestaltet sein sollte. Dabei muss auch die Frage der Zulassung und Ausbildung von Auditoren geklärt werden. Alle anderen rechtlichen Fragen, welche mit dem Thema in Verbindung stehen, bedürfen einer Analyse. Diese könnte der Politik und allen anderen Beteiligten aufschlussreiche Erkenntnisse liefern, welche bei weiteren Maßnahmen Berücksichtigung finden könnten.

41 BT-Drs. 16/12011.

42 Gola/Schomerus, Bundesdatenschutzgesetz, 11. Aufl., München 2012, § 9a Rn. 2a.

43 Http://www.trusted-cloud.de/561.php.

Die Struktur der Aufsichtsbehörden in den EU-Staaten und deren Kompetenzen – ein aktueller Überblick

Steffen Weiß, LL.M., Bonn*

Auch wenn der europäische Gesetzgeber über die EU-Datenschutzrichtlinie 95/46/EG (EU-DSRL) Vorgaben für eine Vereinheitlichung der Datenschutzaufsicht in den Mitgliedstaaten gemacht hat, zeigen sich bei näherer Betrachtung strukturelle Unterschiede der behördlichen Aufsicht, die im Folgenden anhand ausgewählter Beispiele[1] aufgezeigt werden sollen.

Bereits die Frage nach der Etablierung einer oder mehrerer Kontrollstellen zur Wahrnehmung gesetzlich übertragender Aufgaben lässt dabei nationalstaatliche Abweichungen erkennen. Im Gegensatz zur föderalen Struktur der Aufsichtsbehörden in Deutschland und der Etablierung auf Bundes- und Länderebene werden verantwortliche Stellen im europäischen Vergleich in der Regel mit nur einer zentralen Aufsicht für Datenschutz-Fragen konfrontiert. Diese ist sodann sowohl für den öffentlichen als auch für den privaten Bereich zuständig. Abweichungen von diesem Grundsatz bestehen nur vereinzelt und betreffen sodann bestimmte Datenverarbeitungen im öffentlichen Bereich, die

* Der Autor ist Repräsentant Internationales bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn

1 In den durchgeführten Vergleich wurden folgende EU-Mitgliedstaaten einbezogen: Frankreich, Großbritannien, Irland, Italien, die Niederlande, Polen, Schweden und Spanien.

überdies aus gesetzlichen Autonomiestatuten resultieren[2]. Folglich erübrigen sich in Mitgliedstaaten mit nur einer zentralen Aufsicht beispielsweise zusätzliche Koordinierungstreffen, wie sie in Deutschland über den Düsseldorfer Kreis stattfinden. Ferner ist die Kontrolle der Datenverarbeitungen nicht vom Sitz des jeweiligen Unternehmens abhängig.

Ob die jeweilige Aufsicht sich allein auf die Einhaltung der Datenschutzgesetze bezieht oder auch andere Regelungsbereiche mit berücksichtigt, kann variieren. Ein besonderes Augenmerk ist dabei insbesondere auf die elektronische Kommunikation zu legen, die hierzulande primär unter den Begriff der Telemedien gefasst wird. Die diesbezüglichen Vorgaben der Richtlinie 2002/58/EG wurden innerhalb der Mitgliedstaaten in unterschiedlichen Normen bzw. Gesetzen verankert, was Auswirkungen auf die diesbezügliche Aufsicht hat. So wurde in Schweden die Kontrollstelle über den Electronic Communications Act (2003:389) der schwedischen Post- und Kommunikationsbehörde[3] und nicht der allgemeinen Datenschutzaufsicht[4] übertragen. Auch sind besondere Kompetenzzuweisungen möglich, so geschehen in Deutschland, das die Überwachung der datenschutzrelevanten Normen des Telemediengesetzes gem. § 59 Abs. 1 S. 1 Rundfunkstaatsvertrag (RStV) den für den Datenschutz zuständigen Kontrollbehörden zuweist.

Die Verwendung sog. Cookies, als Beispiel einer Querschnittsmaterie zwischen Datenschutz und elektronischer Kommunikation, wäre daher in Schweden[5] der Datenschutzaufsicht entzogen, während dies in Deutschland nicht der Fall ist. Ebenso unterfällt in den Niederlanden die Durchsetzung der Bestimmungen zum Einsatz von Cookies gem. Sect. 11.7a des Dutch Telecommunication Act (Telecommunicatiewet) der Kontrollbehörde für Verbraucher und Märkte[6] und nicht der allgemeinen Datenschutzaufsicht[7].

Die Aufgabenwahrnehmung der jeweiligen Kontrollstelle hat im Sinne der Vorgaben des Art. 28 Abs. 1 EU-DSRL in völliger Unabhängigkeit zu erfolgen, was in Teilen der Mitgliedstaaten nicht im Sinne der EU-DSRL umgesetzt wurde[8]. Neben der Unabhängigkeit sind auch die Kompetenzen der staatlichen Aufsicht europarechtlich geprägt und dementsprechend harmonisiert. Insbesondere verfügt jede Kontrollstelle über Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen. Ebenso stehen ihr Einwirkungsbefugnisse bis hin zur Löschung von Daten zu. Bezüglich der nationalstaatlichen Kompetenzzuweisungen lassen sich keine gravierenden Unterschiede im europäischen Vergleich ausmachen. Auch die in § 38 Abs. 4 BDSG normierten Zutrittsberechtigungen der Kontrollpersonen finden im europäischen Vergleich ein gesetzliches Pendant[9].

Dass die Kontrollbefugnisse der Aufsicht nicht nur im Falle von Beschwerden angewandt werden, sondern als Dienstleistung verstanden werden können, zeigt ein Blick nach Großbritannien. Das dortige Information Commissioner's Office (ICO) bietet die Möglichkeit eines einvernehmlichen Audits an, im Rahmen dessen sich öffentliche wie nicht-öffentliche Stellen einer behördlichen Kontrolle unterziehen lassen können. Die daraus gewonnenen Erkenntnisse werden sodann in einer Zusammenfassung veröffentlicht[10].

Ob die harmonisierten Grundsätze hinsichtlich Unabhängigkeit und Kompetenzen der Datenschutzaufsicht durch eine uneinheitliche Praxis der Rechtsdurchsetzung ins Leere laufen, lässt sich pauschal nicht beantworten. Zwar divergiert die Personalstärke unter den europäischen Aufsichtsbehörden zum Teil erheblich, jedoch ist dabei die Anzahl der datenverarbeitenden Stellen ebenso zu berücksichtigen wie Kompetenzüberschneidungen zu anderen staatlichen Kontrollorganen. Nichtsdestotrotz ist ein Vergleichswert von 400 Beschäftigen beim ICO Großbritanniens zu 40 Mitarbeitern der schwedischen Aufsicht bemerkenswert. Dass die Personalstärke Auswirkungen auf die Regelmäßigkeit von Datenschutzkontrollen haben kann, dürfte dabei nicht von der Hand zu weisen sein.

In engem Zusammenhang mit der personellen Ausstattung sind Budgets der Kontrollbehörden zu sehen, wobei an dieser Stelle für Italien ein Spitzenwert von 18,67 Mio. EUR an Ausgaben für 2013 zu Buche schlägt[11], an den sich Spanien mit einem Jahresbudget für 2012 in Höhe von 13,93 Mio. EUR zumindest annähert[12]. Schweden bildet mit Ausgaben für seine Datenschutzaufsicht in Höhe von 4,2 Mio. EUR[13] für 2013 das europäische Schlusslicht.

Mit Blick auf die Bußgeldpraxis europäischer Aufsichtsbehörden lassen sich gravierende Unterschiede ausmachen. Der Bußgeldrahmen, in dem ein Datenschutzverstoß sanktioniert wird, ist seitens des EU-Gesetzgebers nicht vorgegeben und variiert zwischen ermittelten maximalen 50.000 EUR[14] und 600.000 EUR[15]. Einzelne Mitgliedstaaten geben zwar eine maximale Bußgeldhöhe an, lassen aber ein Überschreiten des Höchstbetrags zu, um einen erzielten wirtschaftlichen Vorteil abzuschöpfen[16]. Überdies gibt es Datenschutzgesetze, die sich zum Bußgeldrahmen überhaupt nicht äußern[17].

Die im Zuge des vorgenommenen Vergleichs ebenfalls festgestellte stetige Erhöhung von Bußgeldern bzw. des zugrunde liegenden gesetzlichen Rahmens legt die Vermutung nahe, dass hierdurch zunehmend eine abschreckende Wirkung erzielt wer-

2 So in Spanien, vgl. Art. 148 de la Constitución española de 1978 i.V.m. Art. 41 Ley Ogánica 15/1999 bezogen auf die autonomen Regionen.

3 Post- och telestyrelsen.

4 Datainspektionen.

5 Vgl. Sect. 6 Electronic Communications Act.

6 Autoriteit Consument & Markt.

7 College bescherming persoonsgegevens (CBP).

8 EuGH C-518/07 – Europäische Kommission gegen Bundesrepublik Deutschland.

9 Vgl. § 38 BDSG; Art. 14 Act of August 29, 1997 on the Protection of Personal Data (Polen); Sect. 158 Data Protection Code (Italien); Sect. 24 Data Protection Acts 1988 and 2003 (Irland); Sect. 50 sowie schedule 9 Data Protection Act 1998 (Großbritannien).

10 Http://ico.org.uk/what_we_cover/audits_advisory_visits_and_self_assessments/audits.

11 Vgl. Garante per la protezione dei dati personali, relazione annnuale 2013, S. 231 („Totale spese").

12 Vgl. Agencia Española de la Protección de Datos, Memoria AEPD 2012, S. 111 („crédito ejercicio").

13 Datainspektionen, Årsredovisning 2013, S. 53 („Utgifter").

14 Art. 121 of the Act of 17 June 1966 on enforcement proceedings in administration (Polen).

15 Art. 45.4 Ley Orgánica 15/1999 (Spanien).

16 Vgl. § 43 Abs. 3 Satz 3 BDSG.

17 So Personal Data Act 1998:204 (Schweden).

den soll. So soll die Datenschutzaufsicht der Niederlande hinsichtlich einer unterbliebenen Meldung einer Verarbeitung personenbezogener Daten ein Bußgeld in Höhe von maximal 4.500 EUR verhängen können (vgl. Art. 66 Personal Data Protection Act), was sich nach einem neuen Gesetzesvorhaben[18] bei einem Verstoß gegen Vorgaben zur Meldung einer sog. Datenschutzpanne nunmehr auf bis zu 450.000 EUR erhöhen kann.

Spitzenreiter in Bezug auf jährlich verhängte Bußgelder ist die spanische Aufsichtsbehörde AEPD, die in 2012 einen Wert von 20.73 Mio. EUR[19] erreichte. Ein hoher Bußgeldwert muss jedoch nicht zwingend ein Indikator für ein schwaches nationales Datenschutzniveau sein, zumal die spanische Behörde ihre Ausgaben durch Sanktionierungen refinanziert[20]. In Kontrast hierzu steht die französische Aufsicht CNIL, die mit einem veröffentlichten Wert von 43.000 EUR[21] ihren Schwerpunkt eher auf die Sensibilisierung als die Sanktionierung zu setzen scheint.

Der kurze Aufriss zur europäischen Datenschutzaufsicht hat gezeigt, dass der europäische Gesetzgeber im Zuge seiner Reformbestrebungen über eine EU-Datenschutz-Grundverordnung (EU-DS-GVO) und den dabei geplanten Vereinfachungsgedanken, so insbesondere zum „one-stop-shop" Verfahren, vor der Herausforderung steht, bestehende strukturelle Unterschiede ebenso in Einklang bringen zu müssen, wie abweichende personelle und finanzielle Ausstattungen von Aufsichtsbehörden. Ob die dargelegte divergierende Bußgeldpraxis durch eine neue europarechtliche Vorgabe nivelliert werden kann, darf in Anbetracht des bestehenden Ermessenspielraums[22] im Übrigen bezweifelt werden.

18 Http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=1693.

19 Bezogen auf die Bereiche Telekommunikation, Finanzinstitute, Energie-, Wasserversorger, SPAM, Videoüberwachung, vgl. AEPD, Memoria AEPD 2012, S. 72.

20 So die AEPD, vgl. http://www.elmundo.es/encuentros/invitados/2009/04/3580/.

21 Commission Nationale de l'Informatique et des Libertés, rapport d'activité 2013, S. 55.

22 Vgl. Art. 79 Abs. 2 des Vorschlags für eine Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(29129) 11 endg.

Datenschutz im BEM

Dr. Eberhard Kiesche, Bremen*

I. Ordnungsgemäßes BEM nur mit Datenschutz möglich

Beschäftigte, die ein Angebot für die Durchführung eines betrieblichen Eingliederungsmanagements nach § 84 Abs. 2 SGB IX erhalten, sollen hochsensible gesundheitsbezogene Daten offenlegen, u. a. Einschränkungen der Leistungsfähigkeit und Einsatzflexibilität, Behinderungen, Krankheitsfolgen und Ursachen der Erkrankung. In Unternehmen und Dienststellen herrscht nach wie vor große Unsicherheit, wie Gesundheitsdaten und sonstige Daten im BEM rechtssicher zu schützen sind. Die Wahrung des Persönlichkeitsschutzes im Betrieblichen Eingliederungsmanagement (nachfolgend BEM) bereitet den betrieblichen BEM-Akteuren und den betroffenen Beschäftigten nach wie vor große Probleme.

Von daher ist der Frage nachzugehen, wie das Recht auf informationelle Selbstbestimmung und der Persönlichkeitsschutz im BEM-Verfahren, z.B. in einer BEM-Verfahrensordnung, sicherzustellen sind. Der Datenschutz ist das Kriterium, das ein ordnungsgemäßes BEM von Krankenrückkehrgesprächen abgrenzt. Unterlassener Datenschutz führt dazu, dass Vertrauen verspielt wird und die Beschäftigten BEM-Gespräche oftmals mit den ungeliebten disziplinierenden Krankenrückkehrgesprächen gleichsetzen.

Im Folgenden wird untersucht, welche Daten der Beschäftigten im BEM erhoben, verarbeitet und genutzt werden und welche gesetzlichen Grundlagen für die Datenverwendung in Frage kommen. Insbesondere ist zu klären, ob die in § 84 Abs. 2 Satz 1 SGB IX geforderte Zustimmung des Beschäftigten noch um eine datenschutzrechtliche Einwilligungserklärung ergänzt werden muss. Weiterhin ist darzulegen, wie die in § 84 Abs. 2 SGB IX geforderte datenschutzrechtliche Aufklärung praktisch umgesetzt werden kann. Anschließend werden einige Konsequenzen für Datenschutzvorkehrungen im BEM aufgezeigt.

II. Datenarten im BEM und gesetzliche Grundlagen bzw. Erlaubnistatbestände

Im BEM werden personenbezogene Daten der Beschäftigten von den handelnden Personen, z.B. einem Integrationsteam, benötigt, darunter auch Gesundheitsdaten im Sinne § 3 Abs. 9 BDSG.

Hilfreich erscheint die Unterteilung der Daten in sensitive und nicht-sensitive Daten der Beschäftigten. Nichtsensitive Daten des BEM-Betroffenen sind z.B. das jeweilige Arbeitszeitmodell, die zugeordnete Kostenstelle, die aktuelle Tätigkeit im Unternehmen oder Qualifikationen. Sensitive Daten im Sinne von Gesundheitsdaten sind Arbeitsunfähigkeitsdaten, Prozess- bzw. Ablaufdaten im BEM, ärztliche Diagnose- und Prognosedaten, maßnahmenbezogene Daten wie z.B. Reha-Entlas-

* Der Autor ist selbstständiger Berater für Beschäftigtendatenschutz und Betriebliches Eingliederungsmanagement, Bremen.

sungsberichte, stufenweise Wiedereingliederung und Arbeitsversuche, Leistungsdaten (aus Arbeitserprobung), Bescheide von Rehabilitationsträgern und personenbezogene Arbeitsschutz- und Beanspruchungsdaten aus der Gefährdungsbeurteilung am jeweiligen Arbeitsplatz.

Handelt es sich um Gesundheitsdaten im Sinne von § 3 Abs. 9 BDSG, so kommen als eine gesetzliche Rechtsgrundlage und als speziellere Regelungen nur § 28 Abs. 6-8 BDSG in Frage. Dies hat das Bundesarbeitsgericht (BAG) in einem Beschluss vom 7.2.2012 – 1 ABR 46/10 letztlich so entschieden[1]. Für sensible Daten, hier die Arbeitsunfähigkeitszeiten zur Einleitung des BEM, können nur die Regelungen in § 28 Abs. 6-8 BDSG und nicht § 32 Abs. 1 S. 1 BDSG herangezogen werden.

Das BAG prüft die Weitergabe einer Namensliste der BEM-Berechtigten an den Betriebsrat durch den Arbeitgeber ohne deren Einwilligung und greift auf § 28 Abs. 6 Nr. 3 BDSG zurück.

„6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn … 3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt (…)".

Der Arbeitgeber benötigt im BEM die Arbeitsunfähigkeitsdaten der Betroffenen zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche. Er muss das Angebot eines BEM als Rechtspflicht nachweisen können. Die Weitergabe an den Betriebsrat durch den Arbeitgeber ist eine gerechtfertigte Nutzung, benötigt nicht die Einwilligung der betroffenen Beschäftigten und dient vorrangig zum Schutz der Beschäftigten, damit der Betriebsrat seinem Überwachungsauftrag in § 84 Abs. 2 Satz 7 SGB IX und in § 80 Abs. 1 Nr. 1 BetrVG nachkommen kann.

Eine weitere Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Beschäftigten im BEM-Verfahren kann eine BEM-Betriebs-/Dienstvereinbarung als andere vorrangige Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG sein. Eine für das BEM entscheidende Rechtfertigung ist die freie und informierte Einwilligung der betroffenen Beschäftigten. Eine Einwilligung nach § 4a BDSG wird bei der Verarbeitung sensitiver und nicht-sensitiver Daten der Beschäftigten dann erforderlich, wenn § 28 Abs. 6 Nr. 3 BDSG als Rechtsgrundlage nicht mehr herangezogen werden kann, weil die schutzwürdigen Interessen der Betroffenen überwiegen. Das ist im BEM-Verfahren regelmäßig der Fall[2]. Allgemeine Vorbehalte gegen eine Einwilligung im BEM und damit im Arbeitsverhältnis müssen im Rahmen des § 84 Abs. 2 SGB IX zurücktreten[3].

III. Zustimmung und Einwilligung im BEM-Prozess

§ 84 Abs. 2 SGB IX Satz 1 setzt die Zustimmung und Beteiligung der betroffenen Personen im BEM voraus, damit der Klärungsprozess zur Erreichung der gesetzlich vorgegebenen BEM-Ziele beginnen kann. Die Zustimmung ist Ausdruck einer Freiwilligkeitskonzeption, die das BEM insgesamt prägt[4]. Sie ist eine rechtsgeschäftsähnliche Handlung oder Erklärung[5]. Ein Widerruf der Zustimmung ist aufgrund des Eingriffs in die informationelle Selbstbestimmung der betroffenen Person nicht auszuschließen. Gibt diese ihre Zustimmung zum BEM nicht, dann kann kein Klärungsverfahren durchgeführt werden. Beginnt der Arbeitgeber trotzdem das Klärungsverfahren, hat der Betroffene einen Unterlassungsanspruch.

Es handelt sich allerdings nur dann um eine wirksame Zustimmung, wenn vorher der Arbeitgeber umfassend über die BEM-Präventionsziele und die Datenverwendung im BEM aufgeklärt hat (§ 84 Abs. 2 Satz 3 SGB IX). Aus Beweisgründen sollte die Zustimmung der betroffenen Beschäftigten schriftlich dokumentiert werden.

Weiterhin ist zu klären, ob es noch zusätzlich zur Zustimmung einer Einwilligung in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Beschäftigten bedarf. Gelten Anforderungen des § 4 a BDSG zur freien und informierten Einwilligung auch im BEM-Verfahren? Hier gibt es noch zwei gegensätzliche Positionen.

Eine Meinung geht davon aus, dass eine zusätzliche Einwilligung nicht erforderlich ist[6]. Nach dieser Auffassung ist das BDSG nach § 1 Abs. 3 BDSG subsidiär, weil das SGB IX als Rechtsvorschrift des Bundes vorgeht. § 84 Abs. 2 Satz 1 wird als „lex specialis" zu § 4a BDSG angesehen. § 84 Abs. 2 SGB IX wäre also vorrangige Rechtsvorschrift, so dass § 3 Abs. 9 BDSG verdrängt wird. Damit wäre eine Einwilligung gemäß § 4a BDSG nicht erforderlich. Es bedarf bei der Zustimmung der betroffenen Person somit nicht der formalen Voraussetzungen des § 4a BDSG, so dass sogar eine mündliche Einverständniserklärung möglich wäre.

Die gegenteilige Auffassung geht davon aus, dass § 3 Abs. 9 und § 4 a Abs. 3 BDSG durch § 84 Abs. 2 SGB IX nicht verdrängt wird, weil keine „deckungsgleiche, tatbestandskongruente Norm" vorliegt[7]. Zwischen Zustimmung zum BEM und Einwilligung in die Datenverarbeitung ist zu unterscheiden[8]. Die formalen Voraussetzungen des § 4a Abs. 3 BDSG müssen eingehalten werden, wenn im BEM Gesundheitsdaten erhoben, verarbeitet und genutzt werden.

§ 84 Abs. 2 SGB IX Satz 1 ist zum Schutz der Betroffenen nicht umfassend datenschutzrechtlich formuliert und kann so

1 Zur berechtigten Kritik am BAG-Beschluss siehe Gola/Wronka, Handbuch Arbeitnehmerdatenschutz, 6. Aufl. 2013, Rn. 187.

2 Simitis/Seifert, BDSG, 8. Aufl. 2014, § 32 Rn. 67.

3 Gundermann/Oberberg, Datenschutzrechtliche Gestaltung des betrieblichen Eingliederungsmanagements und Beteiligung des Betriebsrats, RDV 2007, 103, 107.

4 BAG vom 7.2.2012 (1 ABR 46710), Rn. 33, ZD 2012, 481.

5 Boecken/Gebert, Zur Zustimmung des Beschäftigten nach § 84 Abs. 2 SGB IX, VSSR 2013, 77, 80, 84; Düwell, in: LPK SGB IX, 4. Aufl. § 84 Rn. 64.

6 Gola/Wronka, a.a.O., Rn. 725 ff.

7 Simitis-Dix 2014, § 1 Rn. 170; Gola/Wronka, a.a.O., Rn. 322.

8 Boecken/Gebert 2013, 77, 88-90; Gundermann/Oberberg, Datenschutzrechtliche Gestaltung des betrieblichen Eingliederungsmanagements und Beteiligung des Betriebsrats, RDV 2007, 103, 107; im Ergebnis zustimmend Düwell, LPK SGB IX, § 84 Rn. 72; Kiper/Schierbaum, Krankheit, BEM und Datenschutz, CuA 12/2012, 25, 28; Däubler, Gläserne Belegschaften, 5. Aufl. 2010, Rn. 399c; Schmidt, Schwerbehindertenarbeitsrecht, 2. Aufl. 2014, Rn. 355 ff. und 364; jetzt auch Simitis-Seifert, § 32 Rn. 67.

im Ergebnis §§ 3a, 4 und 4a BDSG nicht verdrängen. Nur dann, wenn der datenschutzrechtliche Sachverhalt unmittelbar in der anderen vorrangigen Rechtsvorschrift geregelt ist, tritt die Subsidiarität ein. In der allgemein gehaltenen Vorschrift § 84 Abs. 2 SGB IX fehlen datenschutzrechtliche Regelungen zur Verarbeitung personenbezogener Daten. Arbeitgeber sind zudem keine Sozialleistungsträger, so dass die Datenschutzvorschriften des SGB X und § 35 SGB I nicht gelten. Es muss auf das BDSG zurückgegriffen werden[9].

Damit ist stets in Betriebs-/Dienstvereinbarungen zum BEM eine gesonderte Einwilligung neben der Zustimmung zum BEM einzuholen[10]. Dabei sind die Anforderungen aus § 4 a BDSG umsetzen. Die Einwilligung muss in Schriftform vorgenommen werden und sich nach § 4 a Abs. 3 BDSG auf die Gesundheitsdaten beziehen. Der Gesetzgeber hat in § 84 Abs. 2 SGB IX dieses Erfordernis bei der Gesetzgebung sicherlich so deutlich nicht gesehen. Auch das BAG differenziert nicht ausreichend klar zwischen Zustimmung und Einwilligung[11]. Im Ergebnis ist die Einholung einer zusätzlichen Einwilligung jedoch notwendig, da sonst die strikte Zweckbindung der offenbarten BEM-Daten nicht gewährleistet werden kann[12].

Hinzu kommt, dass der Beschäftigte als „Herr des Verfahrens“[13] zu allen wesentlichen Schritten im BEM wiederum seine Einwilligung geben muss, z.B. dann, wenn der Betriebsarzt beteiligt wird oder wenn personenbezogene Daten an externe Stellen übermittelt werden. Daraus folgt, dass die Erhebung, Verarbeitung und Nutzung von insgesamt schutzwürdigen BEM-Daten der weiteren Einwilligungen der betroffenen Beschäftigten bedürfen und nicht auf § 32 Abs. 1 Satz 1 BDSG gestützt werden können. Auf § 28 Abs. 6 Nr. 3 BDSG kann allein die Ermittlung der Voraussetzungen für ein Angebot des BEM gestützt werden, d. h. zur Klärung der Voraussetzung, ob die betroffene Person mehr als 42 Tage Arbeitsunfähigkeitzeiten innerhalb der letzten zwölf Monate aufweist[14].

IV. Datenschutzrechtliche Aufklärung und Transparenz der Datenverarbeitung

§ 84 Abs. 2 Satz 3 SGB IX setzt eine umfassende Information der betroffenen Person über die Ziele des BEM und die Datenverwendung voraus. Erfolgen diese Hinweise nicht oder unvollständig, handelt es sich nicht um ein ordnungsgemäßes BEM. Die nicht gegebene Zustimmung des Betroffenen zum BEM hat dann keine Auswirkung auf die Beweis- und Darlegungslast im Kündigungsschutzprozess. Der Arbeitgeber muss sich darlegungs- und beweisrechtlich so behandeln lassen, als ob er das BEM nicht durchgeführt hätte.

Worüber ist der Beschäftigte im ordnungsgemäßen BEM zu informieren:

- BEM-Klärungsprozess, BEM-Präventionsziele, BEM-Beteiligte (Personen und Stellen)
- Freiwilligkeit BEM-Klärung; Zustimmungserfordernisse zu allen wesentlichen BEM-Schritten, Datenübermittlungen und -weitergaben
- Sanktionsfreier Abbruch des BEM; Folgen bzw. mittelbare Nachteile bei fehlender Zustimmung, dem Widerruf der Zustimmung oder der Ablehnung einer BEM-Maßnahme
- Art der Daten, aktenmäßiges Trennungsgebot und Aufbewahrungsort: prospektiv abzusehende erforderliche Daten/Informationen in der Personalakte, Daten in der besonders geschützten BEM-Akte; Zweckbestimmung und -bindung der Daten
- Verwendung und Erforderlichkeit von medizinischen Daten: Gesundheitsdaten und medizinische Daten in der Patientenakte beim Betriebsarzt
- Aufklärung über datenschutzrechtlich zulässige Fragen im BEM-Prozess
- Zugang/Regelung der Zugriffe zu den Daten in den Akten, Einbezug externer Stellen, Informationsaustausch mit dem Betriebsarzt bei Bedarf, Schweigepflicht aller am BEM-Verfahren Beteiligten
- Differenzierte Lösch- und Aufbewahrungsfristen für die Daten (in der Personalakte, BEM-Akte und in der Patientenakte beim Betriebsarzt), Löschung der gespeicherten Daten bei Widerruf
- Rechte des Betroffenen (u. a. Einsichtsrecht Akten, Auskunftsrecht gemäß § 34 BDSG) und
- Schutz der Akten vor unbefugtem Zugriff (technisch-organisatorische Maßnahmen).

Die Beratungspraxis zeigt, dass nur durch das BEM-Anschreiben an den betroffenen Beschäftigten die erforderliche Transparenz für ein ordnungsgemäßes BEM nicht hergestellt werden kann. Allein in einem Erstgespräch zur Entscheidungsfindung kann die gesetzlich geforderte Aufklärung vorgenommen werden, die sowohl für eine informierte Zustimmung zum BEM als auch für die Einwilligung gemäß § a BDSG notwendig ist[15]. Es sind für die umfassende Unterweisung der Beschäftigten verschiedene Informationskanäle zu nutzen, so das Anschreiben, das Erstgespräch, das Angebot von telefonischer Kontaktaufnahme nach Erhalt des BEM-Anschreibens und zusätzliche interne Aufklärung (Intranet, Versammlungen, Flyer, Unterweisungen).

V. Konsequenzen für ein datenschutzgerechtes ordnungsgemäßes BEM[16]

Es geht demnach nicht ohne eine gesonderte datenschutzrechtliche Einwilligung, die die Anforderungen von § 4a und § 4a Abs. 3 BDSG umsetzt.

9 Bergmann/Möhrle/Herb, Datenschutzrecht, § 32 BDSG, Rn. 157 ff.; Gola/Wronka, a.a.O., Rn. 318-319.

10 Siehe auch Deinert, Kündigungsprävention und betriebliches Eingliederungsmanagement, NZA 2010, 969, 973.

11 BAG, Urteil vom 24. März 2011 (Az. 2 AZR 170/10), Rn. 26.

12 Düwell, in: LPK SGB IX, § 84 Rn. 88.

13 Gagel, Betriebliches Eingliederungsmanagement – Rechtspflicht und Chance, NZA 2004, 1359 und Boecken/Gebert, a.a.O., 93.

14 Gola/Wronka, a.a.O., Rn. 728; Gundermann/Oberberg 2007, 107; Simitis-Seifert, a.a.O.; Müller-Glöge/Preis/Schmidt (Hrsg.), ErfK-Rolfs, 12. Aufl., SGB IX, Rn. 5.

15 Kiper/Schierbaum, a.a.O., 28.

16 Ausführlich Kiesche, Gesundheitsdaten schützen. Vorkehrungen im betrieblichen Eingliederungsmanagement, Gute Arbeit 3/2014, 24-26.

Die verfahrensrelevanten Beschäftigtendaten im Vorblatt zur BEM-Akte, in der Personalakte und in der BEM-Akte müssen vereinbart und in einer Anlage zur Betriebsvereinbarung als Datenblätter geführt werden. Es ist naturgemäß zu Beginn des BEM-Einzelfallmanagements nicht abzusehen, in welchem Umfang zusätzliche Daten, personenbezogene Informationen, Datenweitergaben oder Datenübermittlungen erforderlich werden. Immer wenn dies der Fall ist, müssen weitere Einzeleinwilligungen der Beschäftigten eingeholt werden[17]. Bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der BEM-Betroffenen sind vor allem die Datenschutzprinzipien der Datenvermeidung und Datensparsamkeit, der Transparenz und der Erforderlichkeit zu berücksichtigen.

Medizinische Daten als Unterfall von Gesundheitsdaten sind in der Regel im BEM-Einzelfallmanagement gar nicht erforderlich. Sollte dies doch in einem absoluten Ausnahmefall erforderlich werden, ist der Betriebsarzt hinzuziehen, und der Betroffene muss seine Einwilligung in die Schweigepflichtentbindung in jedem Einzelfall erteilen[18]. Selbst dann hat der Betriebsarzt dem Integrationsteam nur Leistungsmöglichkeiten des Beschäftigten und die Auswirkungen auf den konkreten Arbeitsplatz darzulegen. Medizinische Daten, die z.B. bei der Gewährung einer Arbeitsassistenz Leistungsträger anfordern, sind vom Betriebsarzt in einem verschlossenen Umschlag über den Arbeitgeber an die anfragende Stelle zu übermitteln. Hier sind erforderliche Datenflüsse im BEM-Verfahren datenschutzgerecht zu organisieren.

Der Arbeitgeber darf im BEM-Verfahren nicht sein von der Arbeitsrechtsprechung gebilligtes Fragerecht erweitern. Geben Beschäftigte von sich aus medizinische Daten preis, dürfen diese vom Arbeitgeber in der Regel nicht weiter verarbeitet oder genutzt werden. In dieser Frage gibt es in der Praxis große Unkenntnis und auch Unsicherheit.

Das Einzelfallmanagement im BEM-Verfahren hat von dem Gebot der Aktentrennung auszugehen. In die Personalakte gehören die Daten, die der Arbeitgeber unzweifelhaft zum Nachweis eines BEM-Angebots oder der Durchführung eines BEM in einem Kündigungsschutzprozess benötigt. In die BEM-Akte gehören alle Daten und Informationen, die zur Dokumentation des BEM-Verfahrens erforderlich sind. In die Patientenakte gehören die medizinischen Daten/Gesundheitsdaten, ärztliche Unterlagen/Berichte und Schriftwechsel mit Reha-Kliniken.

Der Zugang zur BEM-Akte ist so einzuschränken, dass ein unbefugter Zugriff nicht möglich ist. Das kann so erfolgen, dass die BEM-Akte in einem verschlossenen Umschlag aufbewahrt und jeder Zugriff dokumentiert wird[19]. Der jeweilige Fallmanager steuert den Zugriff des Integrationsteams auf die BEM-Akte. Eine elektronische Verarbeitung der BEM-Daten ist nicht möglich[20]. Elektronisch erstellte Protokolle sollten vorab vom betroffenen Beschäftigten in Absprache mit dem jeweiligen Fallmanager freigegeben werden. Dabei sind sensible Daten wie z.B. Diagnosen in den Protokollen unbedingt zu vermeiden (§ 3 a BDSG).

Zweckänderungen sind im BEM-Prozess nicht möglich, weil sich die Einwilligung ausschließlich auf den BEM-Zweck bezieht. Insbesondere dürfen die sensitiven und nichtsensiblen Daten im BEM nicht für krankheitsbedingte Kündigungen oder zur Abschätzung eines Prozessrisikos vom Arbeitgeber genutzt werden. Die Zweckbindung der BEM-Daten kann nicht durchbrochen werden.

Differenzierte Lösch- und Aufbewahrungsfristen sind zu beachten[21]. Widerruft der Betroffene seine Zustimmung zum BEM-Verfahren während des BEM-Prozesses, ist die BEM-Akte mit den bereits enthaltenden Daten datenschutzgerecht zu entsorgen.

Nach Abschluss des BEM-Verfahrens kann die BEM-Akte längstens drei Jahre aufbewahrt werden[22]. In dieser Zeit kann sich die Aufbewahrung für eine Wirksamkeitskontrolle des BEM-Einzelfallmanagement auch im schutzwürdigen Interesse des Betroffenen ergeben[23]. Das setzt aber voraus, dass weitere Zugriffe auf die BEM-Akte der Einwilligung des Betroffenen bedürfen, die Zugriffe protokolliert werden und die Akte geschützt in einem verschlossenen Umschlag geführt wird.

Die BEM-Daten in der Personalakte sind spätestens nach vier Jahren zu löschen. Während dieses Zeitraums kann der Arbeitgeber sie zum Nachweis der Rechtspflicht nach § 84 Ab. 2 SGB IX benötigen. Die vier Jahre ergeben sich analog zur möglichen Aufbewahrungsfrist von Arbeitsunfähigkeitstagen zur Begründung einer potenziellen krankheitsbedingten Kündigung[24].

Die betriebsärztlichen Unterlagen sind nach § 10 Abs. 3 (Muster-)Berufsordnung für Ärzte mindestens zehn Jahre aufzubewahren, soweit nicht andere Vorschriften eine längere oder kürzere Aufbewahrungsfrist vorsehen[25].

Datenschutzrechtlich schwierig wird die Abschottung der BEM-Daten von der Personalabteilung dann, wenn der Personalleiter Teil des Integrationsteams ist oder Mitarbeiter der Personalabteilung zum Fallmanager bestellt werden. Hiervon sollte die Praxis[26] Abstand nehmen.

Die Anzahl der BEM-Beteiligten im Integrationsteam oder am Runden Tisch des BEM ist möglichst auf ein Minimum zu beschränken. Die BEM-Akteure sind zusätzlich zu den ggf. bereits bestehenden Geheimhaltungspflichten auf das Datengeheimnis zu verpflichten. Eine Verschwiegenheitsverpflichtung ist Teil der Betriebs-/Dienstvereinbarung zum ordnungsgemäßen BEM.

17 Bergmann/Möhre/Herb, § 32 Rn. 160.

18 Landschaftsverband Rheinland (LVR), Handlungsempfehlungen zum Betrieblichen Eingliederungsmanagement, 4. Aufl. 2013, 27.

19 Siehe BAG, Urteil vom 12.9.2006, Az. 9 AZR 271/06.

20 Bergmann/Möhrle/Herb, § 32 Rn. 161.

21 Ausführlich und zum Teil abweichend FKS-Feldes, SGB IX, 3. Aufl. (Im Erscheinen), § 84 Rn. 52.

22 Früh Gundermann/Oberberg, a.a.O., 109.

23 Beyer/Jansen, Rechtsprobleme des Eingliederungsmanagements (Teil II), br 2010, 117, 122.

24 Siehe Weichert, Gesundheitsdaten von Bewerbern und Beschäftigten, RDV 2007, 189, 194.

25 Siehe z.B. Arbeitsmedizinische Regel Nummer 6.1, Fristen für die Aufbewahrung ärztlicher Unterlagen, Ausgabe: Dezember 2013 (GMBl Nr. 5 vom 24. Februar 2014, 90).

26 DGUV (Hrsg.), Leitfaden für Betriebsärzte zum Betrieblichen Eingliederungsmanagement, Berlin 2011, 11, 16-17.

VI. Datenschutz ist konkret umzusetzen und im ordnungsgemäßen BEM unerlässlich

Ein BEM, das Vertrauen bei den Beschäftigten genießt, muss den Beschäftigtendatenschutz umfassend und konkret regeln. Eine Betriebs- oder Dienstvereinbarung als andere vorrangige Rechtsvorschrift im Sinne von § 4 Abs. 1 BDSG kann die Persönlichkeitsrechte der Beschäftigten schützen und fördern, indem sie die Zustimmung zum BEM-Klärungsprozess, die Einwilligung in die Datenverwendung und die erforderlichen Datenschutzvorkehrungen im BEM-Prozess konkretisiert[27]. Der betriebliche Datenschutzbeauftragte ist für die Entwicklung einer BEM-Betriebs- oder Dienstvereinbarung rechtzeitig zu unterrichten und für eine Vorabkontrolle hinzuziehen[28]. Nur mit einem konkret umgesetzten Beschäftigtendatenschutz lässt sich das für ein gutes BEM unerlässliche Vertrauen bei den Beschäftigten gewinnen.

Materialien Bremen, für: Workshop Reha-Berater in Bremen am 17.10.2014

1. BV-BEM § 12 Datenschutz

1. Alle Mitglieder des Integrationsteams sind zur Wahrung des Datenschutzes verpflichtet und unterschreiben eine Verschwiegenheitsverpflichtung gemäß § 5 BDSG (Anlage 6). Die Mitglieder des Integrationsteams nehmen an Datenschutzschulungen des betrieblichen Datenschutzbeauftragten teil.
2. Das Integrationsteam darf im Rahmen des BEM ausschließlich die Daten erheben, nutzen und verarbeiten, die in Anlage 4 ausgewiesen sind. Eine Erhebung, Weitergabe und Verarbeitung von personenbezogenen Daten der betroffenen Beschäftigten erfolgt nur in dem Umfang, der für die Zwecke des BEM erforderlich ist. Der Zugang von Mitgliedern des Eingliederungsteams zu weiteren und insbesondere sensiblen Daten gemäß § 3 Abs. 9 BDSG setzt eine Einwilligung des Beschäftigten zur Weitergabe seiner Daten nach § 4 und § 4a BDSG voraus, ebenso die Übermittlung an Dritte außerhalb des Unternehmens.
3. Die Erhebung, Nutzung und Verarbeitung dieser Daten für Leistungs- und Verhaltenskontrollen ist unzulässig. Eine Aufhebung der Zweckbestimmung von BEM-Daten (§ 84 Abs. 2 SGB IX) ist unzulässig.
4. Das Erheben, Verarbeiten und Nutzen personenbezogener Daten im Rahmen des betrieblichen Eingliederungsmanagements erfordert die schriftliche freie und informierte Einwilligung des Beschäftigten, die jederzeit widerrufen werden kann. Anschließend sind die nicht mehr erforderlichen Daten unverzüglich zu löschen.
5. Im Rahmen des betrieblichen Eingliederungsmanagements ggf. bei Erforderlichkeit erfasste Unterlagen, Gutachten und Stellungnahmen mit medizinischen Daten und sonstige sensible Gesundheitsdaten müssen in einer von der Personalakte getrennten Patienten-Akte vom Betriebsarzt (§ 28 Abs. 7 BDSG) aufbewahrt werden. Der Beschäftigte muss der Aufnahme medizinischer Unterlagen, Informationen und Daten in die Patienten-Akte in jedem Einzelfall zustimmen, ebenso in jedem Einzelfall in die Weitergabe dieser Daten an Mitglieder des Integrationsteam durch den Betriebsarzt. Der betroffene Beschäftigte wird vorher über die betriebsärztliche Schweigepflicht aufgeklärt. Die Einwilligung bedarf der Schriftform.
6. Alle nichtmedizinischen und nichtsensiblen Unterlagen, Informationen und Daten werden in einer BEM-Akte vom Fallmanager geführt. Der Beschäftigte hat jederzeit ein Einsichtsrecht in seine BEM-Akte und Patienten-Akte. Jeder Zugriff auf die BEM-Akte in einem verschlossenen Umschlag erfolgt nach dem 4-Augenprinzip, d.h. unter Einbeziehung des Fallmanagers, und muss dokumentiert werden. Jede Einsichtnahme in die BEM-Akte durch BEM-Beteiligte bedarf der Zustimmung des betroffenen Beschäftigten. Eine automatisierte Datenverarbeitung im BEM-Verfahren findet nicht statt.
7. In der Personalakte dürfen ausschließlich Daten aufbewahrt werden, die zum Nachweis eines ordnungsgemäß durchgeführten BEM-Verfahrens erforderlich sind (Einleitung/Zustimmung zum BEM, Einwilligungserklärung, Abschluss, Nichtzustandekommen, Abbruch oder Unterbrechung des BEM-Verfahrens ohne Angabe von Gründen, Ergebnis des BEM). Der Beschäftigte kann jederzeit eine Darstellung zur Personalakte und zu seiner BEM-Akte hinzufügen lassen.
8. Die BEM-Akte wird drei Jahre nach Abschluss des Eingliederungsmanagements datenschutzgerecht aufbewahrt. Die Unterlagen sind dem betroffenen Beschäftigten anschließend im Original zu übergeben bzw. datenschutzgerecht zu entsorgen. In den Jahren der Aufbewahrung nach Abschluss des BEM ist die BEM-Akte in einem verschlossenen Umschlag aufzubewahren und jede Einsichtnahme zu protokollieren. Im Falle einer Beendigung des Arbeitsverhältnisses wird die BEM-Akte dem betroffenen Beschäftigten ausgehändigt. Die BEM-Daten in der Personalakte sind spätestens vier Jahre nach Abschluss des BEM zu löschen.

2. Einwilligung gemäß § 4a BDSG

Datenschutzrechtliche Einwilligung

in die Verwendung personenbezogener Daten im Rahmen des Betrieblichen Eingliederungsmanagement:

Name: _____

Vorname: _____

27 Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, 22. Tätigkeitsbericht 2008/2009, 125, www.datenschutz-hamburg.de/.

28 Kiper/Schierbaum, a.a.O., 33.

Ich erkläre meine Einwilligung, dass Daten über mich im Rahmen des BEM erhoben, verarbeitet und genutzt werden. Es handelt sich dabei ausschließlich um diejenigen Daten, die auf dem Datenblatt in Anlage 4 aufgeführt sind.

Diese Daten dürfen den Mitgliedern des Integrationsteams bekanntgegeben werden. Sie sind zur Verschwiegenheit und zur Wahrung des Datengeheimnisses verpflichtet.

In der Personalakte werden nur die erforderlichen Daten und Informationen ohne Angabe von Gründen aufgenommen, die der Arbeitgeber für den Nachweis eines BEM bzw. BEM-Angebots benötigt.

Medizinische und sonstige sensible Daten (z.B. Befunde, ärztliche Gutachten, Stellungnahmen, Reha-Berichte) werden nicht elektronisch verarbeitet und ausschließlich zur Patienten-Akte genommen. Die Aufnahme derartiger Daten in die Patienten-Akte bedarf in jedem Einzelfall meiner gesonderten Einwilligung gemäß § 4 und § 4a Bundesdatenschutzgesetz (BDSG). Zugriff auf die Patienten-Akte hat allein der Betriebsarzt. Zugriffe von BEM-Beteiligten auf meine BEM-Akte bedürfen in jedem Einzelfall meiner gesonderten Einwilligung.

Ich bin weiterhin damit einverstanden, dass die folgenden Verlaufsdaten im Rahmen des BEM bei Bedarf in der BEM-Akte dokumentiert und zum Zweck des BEM genutzt werden dürfen:

- Protokoll über Arbeitsversuche: Verlauf und Ergebnis
- Protokoll über „stufenweise Wiedereingliederung“: Verlauf und Ergebnis.

Eine Übermittlung von Daten, die im Rahmen des Betrieblichen Eingliederungsmanagements erhoben werden, an Dritte (z.B. Einrichtungen der Rehabilitation) außerhalb des Unternehmens, erfolgt nur nach vorheriger Zustimmung durch meine Person. Eine Weitergabe von weiteren personenbezogenen Daten und Informationen an die Mitglieder des Integrationsteams oder an weiteren internen Personen durch den Fallmanager erfolgt nur nach meiner vorherigen Einwilligung.

Ich bin darauf hingewiesen worden, dass ich jederzeit auch Einblick in meine BEM-Akte und in die Patientenakte nehmen und mir Kopien machen kann.

Ich erkläre, dass ich diese Einwilligung freiwillig abgebe. Mir ist bekannt, dass ich meine Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen kann. Ich bin auf die Folgen der Verweigerung oder Rücknahme der Einwilligung hingewiesen worden.

Ort, Datum

_____

Unterschrift

3. Datenblätter

Datenerhebung und -auswertung

a) Datenvorblatt zur BEM-Akte

Das *Datenblatt zum Betrieblichen Eingliederungsmanagement (Vorblatt zur BEM-Akte)* enthält folgende Datenfelder:

- o Name
- o Vorname
- o Geschlecht
- o Alter
- o Bereich/Kostenstelle
- o Vollzeit/Teilzeit
- o Schichtarbeit: ja/nein
- o Schwerbehindert oder gleichgestellt
- o Ausbildung/Qualifikationen
- o Aktuelle Tätigkeit im Unternehmen.

Diese Daten werden ausschließlich für die Zwecke des BEM erhoben, verarbeitet und genutzt und dürfen nur in anonymisierter Form nach Beteiligung des Betriebsrats ausgewertet werden.

b) Daten in der Personalakte

- Hinweis auf die BEM-Nebenakte
- Datum: BEM-Erstkontakt/Beginn des BEM
- Zustimmung zum BEM
- Durchschrift der datenschutzrechtlichen Einwilligung
- Nichtzustandekommen, Unterbrechung, Abbruch: ohne Angaben von Gründen, ggf. Hinzufügung einer Darstellung des Beschäftigten
- Abschluss des BEM
- Ergebnis der Eingliederung (umgesetzte BEM-Maßnahmen)

c) Daten in der BEM-Akte

- Protokolle über Gespräche mit Integrationsteam und externen Stellen
- Protokoll über Arbeitsversuche: Verlauf und Ergebnisse
- Protokoll zur stufenweisen Wiedereingliederung: Verlauf und Ergebnis
- Berichte, Gutachten und Stellungnahmen der Rehaträger oder des Integrationsfachdienstes ohne medizinische Daten und Informationen
- Maßnahmenplan
- Präventionsplan und Abschlussprotokoll
- Persönliche Stellungnahme(n) des Beschäftigten

4. Verschwiegenheitserklärung

Verschwiegenheitsverpflichtung

Ich verpflichte mich mit meiner Unterschrift, das Datengeheimnis gemäß § 5 Bundesdatenschutzgesetz (BDSG) zu wahren.

Hiermit erkläre ich, dass ich über die entsprechenden Vorschriften des BDSG und die Datenschutzbestimmungen innerhalb des BEM-Verfahrens vom Datenschutzbeauftragten ausreichend unterwiesen worden bin.

Ich werde alle personenbezogenen Daten, die ich im Laufe des BEM-Verfahrens erfahre, geheim halten und nicht Unbefugten im Unternehmen und Dritten offenbaren. Zu den Dritten gehören auch Arbeitgeber und die Personalabteilung.

Ein Verstoß gegen das Datengeheimnis führt zu eventuellen Schadensersatzansprüchen des betroffenen Beschäftigten, ggf. zu arbeits- und strafrechtlichen Maßnahmen und kann nach §§ 43, 44 BDSG als Ordnungswidrigkeit oder Straftat geahndet werden. In Extremfällen kann ordentlich bzw. außerordentlich gekündigt werden.

Meine Verpflichtung endet nicht mit meinem Ausscheiden aus dem Betrieblichen Eingliederungsmanagement. Sie besteht über das Ende meiner Tätigkeit im Unternehmen hinaus. Meine Verpflichtung auf das Datengeheimnis gemäß § 5 BDSG habe ich zur Kenntnis genommen.

Ort, Datum, Name

Unterschrift

§ 5 BDSG Datengeheimnis

Den beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

5. 1. Anschreiben

Anlage 1

Erstes Informationsanschreiben an den/die Beschäftigte/-n

Frau/Herrn

Vorname Name

Straße

PLZ Ort

Betriebliches Eingliederungsmanagement (BEM)

Sehr geehrte(r) Frau/Herr ,

wir möchten Sie über Hintergründe und Ziele des betrieblichen Eingliederungsmanagements (BEM) informieren. BEM dient dazu, aktuelle Arbeitsunfähigkeit zu überwinden, erneuter Arbeitsunfähigkeit vorzubeugen und Arbeitsplätze zu erhalten. § 84 Abs. 2 SGB IX verpflichtet unser Unternehmen zum BEM. Damit ist BEM die Aufgabe des Arbeitgebers. Ohne Zustimmung und Beteiligung der Beschäftigten ist jedoch die Durchführung eines BEM nicht möglich.

Im Rahmen des BEM haben wir festgestellt, dass Sie einen Anspruch auf die Teilnahme am BEM haben, weil Sie innerhalb der letzten 12 Monate länger als sechs Wochen arbeitsunfähig waren. Für ein Erstgespräch zum BEM stehen Ihnen die Mitglieder des Integrationsteams zur Verfügung. In diesem Gespräch können Sie sich alle Einzelheiten zum BEM erklären lassen. Telefonische Rücksprachen sind jederzeit möglich.

Bitte teilen Sie uns innerhalb der nächsten 3 Wochen auf dem Antwortbogen mit, ob Sie ein unverbindliches Erstgespräch zum betrieblichen Eingliederungsmanagement (BEM) in Anspruch nehmen möchten. Im Erstgespräch erläutern wir Ihnen die Ziele und Vorteile des BEM-Verfahrens, die beteiligten Stellen oder Personen, die damit verbundene Datenerhebung und -verwendung, Ihr Recht auf Auskunft über alle zu Ihrer Person im BEM gespeicherten Daten nach § 34 Bundesdatenschutzgesetz (BDSG) und die datenschutzrechtliche Einwilligung.

Wenn Sie von dem Angebot des BEM-Erstgesprächs Gebrauch machen wollen, vereinbaren Sie bitte mit dem Integrationsteam bzw. einer Person Ihrer Wahl aus dem Integrationsteam einen Termin für ein Erstgespräch. Nachdem Sie Ihre Zustimmung zur Teilnahme an einem BEM und die datenschutzrechtliche Einwilligung schriftlich erteilt haben, wird das Integrationsteam zur Entwicklung von Maßnahmen und Hilfen für ein Eingliederungsgespräch herangezogen.

Ganz wichtig: Das BEM und insbesondere alle erarbeiteten Maßnahmen im Verfahren sind für Sie freiwillig. Sämtliche Gespräche und Daten in diesem Zusammenhang unterliegen der Vertraulichkeit und dem Datengeheimnis. Sie entscheiden über die Erhebung und Weitergabe von personenbezogenen Daten und die Durchführung von Maßnahmen. Der Datenschutz ist umfassend auch durch eine Betriebsvereinbarung gewährleistet.

Wir freuen uns auf Ihre Antwort und hoffen auf eine gute vertrauensvolle Zusammenarbeit.

Mit freundlichen Grüßen

i. A.
Integrationsteam

Personen des Integrationsteams mit Mailadresse und Telefonnummer

1.

2.

3.

4.

5.

5.2 Lösch- und Aufbewahrungsfristen: siehe o. S. 324.

Rechtsprechung

Sorgfaltspflicht bei elektronischer Rechtsanwalts Handakte (Ls)

(**Bundesgerichtshof**, Beschluss vom 9. Juli 2014 – XII ZB 709/13–)

a) Wird die Handakte eines Rechtsanwalts allein elektronisch geführt, muss sie ihrem Inhalt nach der herkömmlich geführten entsprechen. Sie muss insbesondere zu Rechtsmittelfristen und deren Notierung ebenso wie diese verlässlich Auskunft geben können und darf keine geringere Überprüfungssicherheit bieten als ihr analoges Pendant.

b) Der Rechtsanwalt, der im Zusammenhang mit einer fristgebundenen Verfahrenshandlung – hier der Einlegung der Beschwerde – mit einer Sache befasst wird, hat dies zum Anlass zu nehmen, die Fristvermerke in der Handakte zu überprüfen. Auf welche Weise (herkömmlich oder elektronisch) die Handakte geführt wird, ist hierfür ohne Belang.

Islamisches Kopftuch und Annahmeverzug (Ls)

(**Bundesarbeitsgericht**, Urteil vom 24. September 2014 – 5 AZR 611/12 –)

Das Tragen eines Kopftuchs als Symbol der Zugehörigkeit zum islamischen Glauben und damit als Kundgabe einer abweichenden Religionszugehörigkeit ist regelmäßig mit der arbeitsvertraglichen Verpflichtung einer in einer Einrichtung der Evangelischen Kirche tätigen Arbeitnehmerin zu neutralem Verhalten nicht vereinbar.

Deutliche Mitteilung der Schwerbehinderung bei der Bewerbung (Ls)

(**Bundesarbeitsgericht**, Urteil vom 18. September 2014 – 8 AZR 759/13 –)

1. Ein schwerbehinderter Mensch, der bei seiner Bewerbung um eine Stelle den besonderen Schutz und die Förderung nach dem SGB IX in Anspruch nehmen will, muss die Eigenschaft, schwerbehindert zu sein, grundsätzlich im Bewerbungsschreiben oder unter deutlicher Hervorhebung im Lebenslauf mitteilen. Eine solche Mitteilung muss bei jeder Bewerbung erfolgen. Auf Erklärungen bei früheren Bewerbungen kommt es nicht an.

2. Entscheidend ist die Schwerbehinderteneigenschaft im Zeitpunkt der Bewerbung, nicht zu einem früheren Zeitpunkt. Nach dem Datenschutzrecht liegt es in der Entscheidung des schwerbehinderten Menschen, ob er die Schwerbehinderung bei der Bewerbung berücksichtigt haben will oder nicht.

(Nicht amtliche Leitsätze)

Anhörung eines Arbeitnehmers vor einer Verdachtskündigung

(**Bundesarbeitsgericht**, Urteil vom 20. März 2014 – 2 AZR 1037/12 –)

1. Für eine wegen des bloßen Verdachts einer Pflichtverletzung ergangene Kündigung ist die vorherige Anhörung des Arbeitnehmers Wirksamkeitsvoraussetzung. Die für die Anhörung gesetzte Frist darf auch im Hinblick auf den Beginn der Frist des § 626 Abs. 2 BGB im Allgemeinen nicht länger als eine Woche sein.

2. Die Anhörung kann unterbleiben, wenn der Arbeitnehmer von vornherein nicht bereit ist, sich zu den ihm gemachten Vorwürfen zu äußern bzw. wenn dem Arbeitnehmer Gelegenheit zur Stellungnahme gegeben wurde und dieser sich innerhalb der gesetzten angemessenen Frist nicht äußert. Auch wenn die Nichtäußerung nicht verschuldet ist, kann ein weiteres Zuwarten im Einzelfall unzumutbar sein.

(Nicht amtliche Leitsätze)

Sachverhalt:

Der 1958 geborene Kläger war seit September 1981 bei der beklagten Rundfunkanstalt beschäftigt, zuletzt als Techniker im IT-Service. Nach dem auf das Arbeitsverhältnis der Parteien anwendbaren Manteltarifvertrag war das Arbeitsverhältnis – es sei denn wegen Leistungsminderung – nur noch außerordentlich kündbar.

Im Juli und November 2010 wurden Räume der Beklagten durchsucht. Nach dem Vorbringen der Beklagten hatte es eine anonyme Anzeige gegeben, derzufolge mehrere ihrer Mitarbeiter, ua. der Kläger, bei Ausschreibungen über Telekommunikations- und Datennetzleistungen in Absprache mit einer beauftragten Firma die Leistungsverzeichnisse manipuliert hatten. Am 7. Dezember 2010 lag der Beklagten ein Bericht ihrer Innenrevision über die Leistungsabrufe der betreffenden Firma vor. Danach hat der Kläger von dieser ua. einen Barbetrag in Höhe von 200,00 Euro erhalten. Eine Schließanlage, die er von der Firma schon zuvor erhalten und bei sich eingebaut hatte, hatte der Kläger an die Beklagte zurückgegeben.

Mit Schreiben vom 8. Dezember 2010 lud die Beklagte den Kläger zu einer Anhörung für den 13. Dezember 2010 in ihre Geschäftsräume

ein. Der Kläger war seit dem 26. Juli 2010 erkrankt. Er teilte mit E-Mail vom 12. Dezember 2010 mit, er könne den Termin wegen einer Rehabilitationsmaßnahme nicht wahrnehmen. Er bat darum, ihn schriftlich anzuhören und die Fragen seinem Prozessbevollmächtigten zu schicken. Die Beklagte sandte daraufhin am 14. Dezember 2010 sowohl an den Kläger als auch an dessen Prozessbevollmächtigten einen zehn Seiten langen Fragenkatalog, der sich auf 13 einzelne Fragenbereiche bezog. Sie setzte dem Kläger eine Frist zur Beantwortung bis zum 17. Dezember 2010, 12:00 Uhr.

Mit Schreiben vom 15. Dezember 2010 – welches nach Angaben der Beklagten am 20. Dezember 2010 bei ihr einging –, teilten die Prozessbevollmächtigten des Klägers mit, dieser befinde sich noch bis zum 11. Januar 2011 in der Rehabilitationsmaßnahme. Es sei deshalb „kaum möglich", innerhalb der gesetzten Frist zu den Fragen Stellung zu nehmen. Es sei eine zeitaufwendige Besprechung mit dem Kläger erforderlich. Diese könne wegen der noch laufenden Rehabilitationsmaßnahme erst im Laufe des Monats Januar 2011 erfolgen. Eine Stellungnahme sei nach Ablauf der Maßnahme zu erwarten. Mit Schreiben vom 16. Dezember 2010, welches bei der Beklagten tags darauf einging, nahmen die Prozessbevollmächtigten auf ihr Schreiben vom 15. Dezember 2010 Bezug und rügten, die Zusendung des Fragenkataloges habe zu einem gesundheitlichen Rückschlag des Klägers geführt. Tatsächlich litt der Kläger an einer psychischen Erkrankung. Ob dies der Beklagten bekannt war, ist nicht festgestellt.

Mit Schreiben vom 20. Dezember 2010 hörte die Beklagte den bei ihr gebildeten Personalrat zu einer beabsichtigten Verdachts- und Tatkündigung an. Der Personalrat widersprach mit Schreiben vom 22. Dezember 2010 mit der Begründung, der Kläger sei nicht ausreichend angehört worden.

Mit Schreiben vom 27. Dezember 2010 kündigte die Beklagte das zwischen den Parteien bestehende Arbeitsverhältnis fristlos.

Dagegen hat der Kläger rechtzeitig die vorliegende Kündigungsschutzklage erhoben. Er hat gemeint, es fehle an einem wichtigen Grund iSv. § 626 Abs. 1 BGB. Außerdem habe die Beklagte die Frist des § 626 Abs. 2 BGB nicht gewahrt. Von dem Kündigungsschreiben habe er erst am 30. Dezember 2010 Kenntnis erlangt. Für eine auf den Verdacht einer Pflichtverletzung gestützte Kündigung fehle es an seiner ordnungsgemäßen Anhörung.

Aus den Gründen:

Die Revision ist begründet. Mit der gegebenen Begründung durfte das Landesarbeitsgericht die Kündigung vom 27. Dezember 2010 nicht als unwirksam ansehen. Ob sie wirksam ist, steht noch nicht fest.

I. Die Kündigung wegen vom Kläger tatsächlich begangener Pflichtverletzungen ist auf der Grundlage der bisherigen Feststellungen nicht deshalb unwirksam, weil die Beklagte die zweiwöchige Erklärungsfrist des § 626 Abs. 2 BGB nicht eingehalten hätte. Die Frist hat entgegen der Auffassung des Landesarbeitsgerichts nicht spätestens am Tag nach dem 7. Dezember 2010 zu laufen begonnen.

1. Gemäß § 626 Abs. 2 Satz 1 BGB kann eine außerordentliche Kündigung nur innerhalb von zwei Wochen erfolgen. Die Frist beginnt nach Abs. 2 Satz 2 der Norm mit dem Zeitpunkt, in dem der Kündigungsberechtigte von den für die Kündigung maßgebenden Tatsachen Kenntnis erlangt. Dies ist der Fall, sobald er eine zuverlässige und möglichst vollständige Kenntnis der einschlägigen Tatsachen hat, die ihm die Entscheidung darüber ermöglicht, ob er das Arbeitsverhältnis fortsetzen soll oder nicht. Zu den maßgebenden Tatsachen gehören sowohl die für als auch die gegen eine Kündigung sprechenden Umstände (BAG 21. Februar 2013 – 2 AZR 433/12 – Rn. 27; 27. Januar 2011 – 2 AZR 825/09 – Rn. 15, BAGE 137, 54). Der Kündigungsberechtigte, der bislang nur Anhaltspunkte für einen Sachverhalt hat, der zur außerordentlichen Kündigung berechtigen könnte, kann nach pflichtgemäßem Ermessen weitere Ermittlungen anstellen und den Betroffenen anhören, ohne dass die Frist des § 626 Abs. 2 BGB zu laufen begänne (BAG 21. Februar 2013 – 2 AZR 433/12 – a.a.O.; 25. November 2010 – 2 AZR 171/09 – Rn. 15). Dies gilt allerdings nur solange, wie er aus verständigen Gründen mit der gebotenen Eile Ermittlungen durchführt, die ihm eine umfassende und zuverlässige Kenntnis des Kündigungssachverhalts verschaffen sollen (BAG 31. März 1993 – 2 AZR 492/92 – zu II 1 der Gründe, BAGE 73, 42). Soll der Kündigungsgegner angehört werden, muss dies innerhalb einer kurzen Frist erfolgen. Sie darf im Allgemeinen nicht mehr als eine Woche betragen (BAG 27. Januar 2011 – 2 AZR 825/09 – Rn. 15, a.a.O.; 2. März 2006 – 2 AZR 46/05 – Rn. 24, BAGE 117, 168). Bei Vorliegen besonderer Umstände darf sie auch überschritten werden (BAG 2. März 2006 – 2 AZR 46/05 – a.a.O.). Unerheblich ist, ob die Ermittlungsmaßnahmen tatsächlich zur Aufklärung des Sachverhalts beigetragen haben oder nicht (BAG 21. Februar 2013 – 2 AZR 433/12 – a.a.O.; 25. November 2010 – 2 AZR 171/09 – a.a.O.). Gibt der Arbeitgeber dem Arbeitnehmer die Möglichkeit zur Stellungnahme, so gereicht ihm dies hinsichtlich des Beginns der zweiwöchigen Ausschlussfrist deshalb auch dann nicht zum Nachteil, wenn der Arbeitnehmer innerhalb angemessener Überlegungszeit keine Erklärung abgibt oder seine Stellungnahme rückblickend zur Feststellung des Sachverhalts nichts beiträgt (BAG 27. Januar 1972 – 2 AZR 157/71 – zu 3 der Gründe, BAGE 24, 99). Das bedeutet zugleich, dass der mit der beabsichtigten Anhörung verbundene Fristaufschub iSv. § 626 Abs. 2 BGB nicht nachträglich entfällt, wenn der Arbeitgeber das ergebnislose Verstreichen der Frist zur Stellungnahme für den Arbeitnehmer zum Anlass nimmt, nunmehr auf dessen Anhörung zu verzichten. Ein solcher nachträglicher Wegfall des ursprünglichen Aufschubs käme nur in Frage, wenn der betreffende Entschluss des Arbeitgebers auf Willkür beruhte. Davon kann die Rede nicht sein, wenn Anlass für den neuen Entschluss der Umstand ist, dass sich der Arbeitnehmer innerhalb einer ihm gesetzten, angemessenen Frist nicht geäußert hat.

2. Danach hat die Beklagte die Frist des § 626 Abs. 2 BGB nicht deshalb nicht gewahrt, weil diese spätestens mit dem auf den 7. Dezember 2010 folgenden Tag zu laufen begonnen hätte.

a) Das Landesarbeitsgericht hat angenommen, die Beklagte sei spätestens am 7. Dezember 2010 in der Lage gewesen, sich ein Bild darüber zu machen, ob die im Revisionsbericht aufgeführten Sachverhalte Grundlage für die Überzeugung sein konnten, der Kläger habe die ihm vorgeworfenen Pflichtverletzungen begangen. Um darauf eine Kündigung zu stützen, habe es für sie keiner weiteren Sachverhaltsaufklärung, insbesondere keiner Anhörung des Klägers bedurft. Sie sei schließlich auch ohne neue Erkenntnisse zu dem Schluss gekommen, der ihr bereits am 7. Dezember 2010 möglich gewesen sei. Die Frist für den Ausspruch einer auf tatsächlich begangene Pflichtverletzungen gestützten Kündigung habe damit am 21. Dezember 2010 geendet. Bis zu diesem Zeitpunkt sei die Kündigung dem Kläger – unstreitig – nicht zugegangen.

b) Diese Würdigung hält einer Überprüfung nicht stand. Zwar lag der Beklagten am 7. Dezember 2010 der Bericht ihrer Innenrevision vor. Sie durfte es aber nach pflichtgemäßem Ermessen für erforderlich halten, dem Kläger Gelegenheit zur Stellungnahme zu den darin enthaltenen Anschuldigungen zu geben. Es war nicht ausgeschlossen, dass sie dadurch von Umständen Kenntnis erlangen könnte, die den bisher ermittelten Sachverhalt in einem

anderen Licht erscheinen ließen. Darauf, ob die Anhörung tatsächlich neue Erkenntnisse erbrachte, kommt es nicht an.

3. Ob die Beklagte die Frist des § 626 Abs. 2 BGB gewahrt hat, steht noch nicht fest.

a) Allerdings hat die Beklagte, nachdem der Bericht der Innenrevision vorlag, den Kläger hinreichend zeitnah zu einer Anhörung eingeladen. Der vorgesehene Termin am 13. Dezember 2010 lag innerhalb einer Woche. Nachdem der Kläger mitgeteilt hatte, dass er den Termin wegen seiner Rehabilitationsmaßnahme nicht wahrnehmen könne, widersprach es auch nicht der gebotenen Eile, ihm zur Beantwortung des Fragenkatalogs eine Frist bis zum 17. Dezember 2010 zu setzen. Der Kläger selbst hatte um schriftliche Anhörung gebeten. Dies ist ein Umstand, der für die Anhörung das Überschreiten der Regelfrist von einer Woche rechtfertigt. Die Frist des § 626 Abs. 2 BGB begann demnach erst mit Ablauf der dem Kläger gesetzten Frist zur Stellungnahme, dh. am 18. Dezember 2010 zu laufen. Die Beklagte hätte die Kündigungserklärungsfrist selbst dann eingehalten, wenn die Kündigung dem Kläger erst am 30. Dezember 2010 zugegangen sein sollte.

b) Das Landesarbeitsgericht hat bisher aber keine Feststellungen dazu getroffen, ob eine für die Beklagte kündigungsberechtigte Person schon vor dem 17. Dezember 2010 von Umständen Kenntnis erlangt hatte, die darauf schließen ließen, der Kläger werde sich bis zum Ablauf der ihm gesetzten Frist ohnehin nicht mehr äußern. In diesem Fall käme ein entsprechend früherer Fristbeginn in Betracht. Dann wiederum könnte es für die Wahrung der Frist des § 626 Abs. 2 BGB darauf ankommen, wann genau die Kündigung dem Kläger im Rechtssinne zugegangen ist. Ebenso wenig hat das Landesarbeitsgericht bisher aufgeklärt, ob die Beklagte bis zur Vorlage des Berichts der Innenrevision am 7. Dezember 2010 die Aufklärungsmaßnahmen mit der gebotenen Eile vorgenommen hat.

c) Demgegenüber wurde der Fristbeginn nicht schon deshalb hinausgeschoben, weil der Kläger eine Stellungnahme erst nach dem Ende seiner Rehabilitationsmaßnahme in Aussicht gestellt hatte. Die Beklagte hatte die ihm bis zum 17. Dezember 2010 gesetzte Frist nicht verlängert. Darauf, ob andernfalls ein entsprechendes Zuwarten noch mit dem Gebot hinreichend zügiger Aufklärung vereinbar wäre, kommt es nicht an.

II. Sollte das Landesarbeitsgericht zu dem Ergebnis kommen, die Beklagte habe die Frist des § 626 Abs. 2 BGB eingehalten, wird es zu prüfen haben, ob ein wichtiger Grund iSv. § 626 Abs. 1 BGB vorliegt. Sofern es dies nicht wegen erwiesener Pflichtverletzung(en) des Klägers bejahen sollte, wird es prüfen müssen, ob ein solcher Grund zumindest wegen des Verdachts einer erheblichen Pflichtverletzung gegeben ist. Unter diesem Aspekt wäre die Kündigung auf der Basis der bisherigen Feststellungen nicht deshalb unwirksam, weil es an der erforderlichen Anhörung des Klägers fehlte.

1. Die vorherige Anhörung des Arbeitnehmers ist Voraussetzung für die Wirksamkeit einer Verdachtskündigung. Bei ihr besteht in besonderem Maße die Gefahr, dass der Arbeitnehmer zu Unrecht beschuldigt wird. Dessen Anhörung ist deshalb ein Gebot der Verhältnismäßigkeit. Unterbliebe sie, wäre die Kündigung nicht „ultima ratio“ (BAG 23. Mai 2013 – 2 AZR 102/12 – Rn. 31; 24. Mai 2012 – 2 AZR 206/11 – Rn. 32). Der Arbeitgeber muss dem Arbeitnehmer vor Ausspruch der Kündigung Gelegenheit geben, zu den Verdachtsmomenten Stellung zu nehmen, um dessen Einlassungen bei seiner Entscheidungsfindung berücksichtigen zu können (BAG 30. April 1987 – 2 AZR 283/86 – zu B I 2 c der Gründe). Versäumt er dies, kann er sich im Prozess nicht auf den Verdacht eines pflichtwidrigen Verhaltens des Arbeitnehmers berufen; die hierauf gestützte Kündigung ist unwirksam (BAG 30. April 1987 – 2 AZR 283/86 – zu B I 2 d der Gründe; 11. April 1985 – 2 AZR 239/84 – zu C III 3 der Gründe, BAGE 49, 39).

a) Der Umfang der Anhörung richtet sich nach den Umständen des Einzelfalls. Einerseits muss sie nicht in jeder Hinsicht den Anforderungen genügen, die an eine Anhörung des Betriebsrats nach § 102 Abs. 1 BetrVG gestellt werden (BAG 24. Mai 2012 – 2 AZR 206/11 – Rn. 33; 13. März 2008 – 2 AZR 961/06 – Rn. 15). Andererseits reicht es nicht aus, dass der Arbeitgeber den Arbeitnehmer lediglich mit einer allgemein gehaltenen Wertung konfrontiert. Die Anhörung muss sich auf einen greifbaren Sachverhalt beziehen. Der Arbeitnehmer muss die Möglichkeit haben, bestimmte, zeitlich und räumlich eingegrenzte Tatsachen ggf. zu bestreiten oder den Verdacht entkräftende Tatsachen aufzuzeigen und so zur Aufhellung der für den Arbeitgeber im Dunkeln liegenden Geschehnisse beizutragen. Um dieser Aufklärung willen wird dem Arbeitgeber die Anhörung abverlangt (BAG 24. Mai 2012 – 2 AZR 206/11 – a.a.O.; 13. März 2008 – 2 AZR 961/06 – a.a.O.).

b) Unterblieb die Anhörung, weil der Arbeitnehmer von vornherein nicht bereit war, sich auf die gegen ihn erhobenen Vorwürfe einzulassen und nach seinen Kräften an der Aufklärung mitzuwirken, steht dies der Wirksamkeit der Verdachtskündigung nicht entgegen. Erklärt der Arbeitnehmer, er werde sich zu dem gegen ihn erhobenen Vorwurf nicht äußern, und nennt er für seine Weigerung keine relevanten Gründe, muss der Arbeitgeber ihn über die Verdachtsmomente nicht näher informieren (BAG 13. März 2008 – 2 AZR 961/06 – Rn. 16; 28. November 2007 – 5 AZR 952/06 – Rn. 20). Eine solche Anhörung wäre überflüssig. Sie könnte zur Aufklärung des Sachverhalts und zur Willensbildung des Arbeitgebers nichts beitragen (BAG 13. März 2008 – 2 AZR 961/06 – a.a.O; 30. April 1987 – 2 AZR 283/86 – zu B I 2 d aa der Gründe).

c) Ein Unterlassen der Anhörung kann auch dann unschädlich sein, wenn der Arbeitgeber dem Arbeitnehmer – im Rahmen des Zumutbaren – Gelegenheit zur Stellungnahme gegeben, und dieser sich innerhalb der gesetzten – angemessenen – Frist gleichwohl nicht geäußert hat. Dies gilt einmal, wenn der Arbeitnehmer vorsätzlich schweigt, kann aber selbst bei unfreiwilligem Schweigen gelten. Ist etwa der Arbeitnehmer krankheitsbedingt nicht nur an einem persönlichen Gespräch, sondern längerfristig auch an einer schriftlichen Stellungnahme auf ihm übermittelte Fragen verhindert, muss der Arbeitgeber nicht notwendig die Zeit abwarten, zu der sich der Arbeitnehmer wieder äußern kann. Zwar mag die Frist des § 626 Abs. 2 BGB noch nicht zu laufen beginnen, solange der Arbeitgeber entsprechend zuwartet (vgl. dazu LAG Köln 25. Januar 2001 – 6 Sa 1310/00 -; Hessisches LAG 8. Oktober 1979 – 11 Sa 544/79 –). Wartet der Arbeitgeber diesen Zeitpunkt aber nicht ab, führt das nicht automatisch dazu, dass ihm eine Verletzung seiner Aufklärungspflicht vorzuwerfen wäre.

aa) Wartet der Arbeitgeber, dem der Arbeitnehmer mitteilt, er könne sich wegen einer Erkrankung nicht, auch nicht schriftlich äußern, dessen Gesundung ab, um ihm eine Stellungnahme zu den Vorwürfen zu ermöglichen, liegen in der Regel hinreichende besondere Umstände vor, aufgrund derer der Beginn der Frist des § 626 Abs. 2 BGB entsprechend lange hinausgeschoben wird. Dem Arbeitgeber, der die Möglichkeit einer weiteren Aufklärung durch den Arbeitnehmer trotz der Zeitverzögerung nicht ungenutzt lassen möchte, wird regelmäßig nicht der Vorwurf gemacht werden können, er betreibe keine hinreichend eilige Aufklärung, insbesondere dann nicht, wenn der Arbeitnehmer selbst um eine Fristverlängerung gebeten hat (ebenso Eylert/Friedrichs DB 2007, 2203, 2206; Menne-

meyer/Dreymüller NZA 2005, 382). Dies dient nicht zuletzt dem Interesse des Arbeitnehmers an der Vermeidung einer vorschnell, ohne Rücksicht auf mögliche Entlastungen erklärten Kündigung (vgl. dazu BAG 26. September 2013 – 2 AZR 741/12 – Rn. 23, 34).

bb) Umgekehrt verletzt der Arbeitgeber in einem solchen Fall nicht notwendig seine Aufklärungspflicht aus § 626 Abs. 1 BGB, wenn er von einem weiteren Zuwarten absieht. Ihm kann – abhängig von den Umständen des Einzelfalls – eine weitere Verzögerung unzumutbar sein. Das ist anzunehmen, wenn der Arbeitgeber davon ausgehen darf, der Arbeitnehmer werde sich in absehbarer Zeit nicht äußern (können). Hat etwa der Arbeitnehmer mehrmals um eine Verlängerung der gesetzten Frist zur Stellungnahme gebeten und hat sich seine Prognose, wann er sich werde äußern können, wiederholt als unzutreffend erwiesen, wird dem Arbeitgeber ein weiteres Zuwarten nicht zuzumuten sein. Mehrfache ergebnislose Fristverlängerungen können überdies die Annahme rechtfertigen, der Arbeitnehmer wolle sich in Wirklichkeit ohnehin nicht äußern. Einige weitere Tage warten zu müssen, wird der Arbeitgeber dabei in der Regel eher hinzunehmen haben als eine Wartezeit von mehreren Wochen. Es kann wiederum auch das Ende eines längeren Zeitraums abzuwarten sein, wenn schon die bisherigen Aufklärungsmaßnahmen längere Zeit in Anspruch genommen haben und keine Ansprüche des Arbeitnehmers aus Annahmeverzug drohen.

2. Danach ist das Landesarbeitsgericht auf der Grundlage seiner bisherigen Feststellungen rechtsfehlerhaft zu dem Ergebnis gelangt, es habe an der erforderlichen Anhörung des Klägers gefehlt.

a) Das Landesarbeitsgericht hat gemeint, die Beklagte habe nicht annehmen dürfen, der Kläger wolle sich einer Anhörung entziehen. Der Kläger habe seine Mitwirkung bei der Anhörung angekündigt, seine Prozessbevollmächtigten hätten sie für Mitte Januar 2011 in Aussicht gestellt. Der Kläger sei psychisch erkrankt gewesen und habe sich in einer Reha-Maßnahme befunden. „Hierüber" habe er die Beklagte unverzüglich in Kenntnis gesetzt.

b) Das Landesarbeitsgericht hat nicht alle relevanten Umstände in seine Prüfung mit einbezogen. Die bislang festgestellten Tatsachen tragen seine Begründung nicht.

aa) Das Landesarbeitsgericht hat nicht gewürdigt, dass der Kläger zunächst ohne einen Hinweis auf zeitliche Einschränkungen durch die Reha-Maßnahme um eine schriftliche Anhörung gebeten hatte. Erst anschließend stellten seine Prozessbevollmächtigten eine Äußerung für eine geraume Zeit später und zu einem recht vagen Zeitpunkt in Aussicht. Sie kündigten diese nicht für „Mitte Januar 2011" an – wovon das Landesarbeitsgericht ausgegangen ist –, sondern kündigten an, sie würde „im Laufe des Januar 2011" erfolgen. Die Prozessbevollmächtigten erläuterten überdies nicht, warum nicht schon während der noch laufenden Reha-Maßnahme eine Besprechung mit dem Kläger möglich wäre. Ob sich der Kläger dazu gesundheitlich nicht in der Lage sah, ob er möglicherweise überhaupt nicht äußerungsfähig war oder ob es nur Terminprobleme bzw. sonstige organisatorische Schwierigkeiten gab, die dem entgegenstünden, wird aus ihren Schreiben nicht ersichtlich.

bb) Dafür, dass die Beklagte aus der Art der Erkrankung des Klägers Rückschlüsse auf das Fehlen seiner Fähigkeit hätte ziehen können, sich – und sei es schriftlich – zu äußern, gibt es nach den bisherigen Feststellungen keine hinreichenden Anhaltspunkte. Es ist unklar, ob das Landesarbeitsgericht angenommen hat, der Kläger habe die Beklagte nicht nur über seinen Aufenthalt in einer Reha-Klinik, sondern auch über die Art seiner Erkrankung informiert. In der E-Mail vom 12. Dezember 2010 hatte der Kläger lediglich mitgeteilt, er befinde sich bis zum 11. Januar 2011 in der Klinik, sei gesundheitlich nicht in der Lage, an der Anhörung in den Räumen der Beklagten teilzunehmen, und bitte um eine schriftliche Anhörung. In den Schreiben seiner Prozessbevollmächtigten werden zur Art seiner Erkrankung keine Angaben gemacht.

c) Die Annahme des Landesarbeitsgerichts, dem Kläger sei es wegen seiner Erkrankung und der Durchführung der Reha-Maßnahme nicht möglich gewesen, den Fragenkatalog innerhalb der gesetzten Frist angemessen zu beantworten, beruht ebenfalls nicht auf hinreichenden Tatsachenfeststellungen. Sie rechtfertigt deshalb nicht die Würdigung, die Beklagte habe, weil sie dem Kläger keine längere Frist zur Stellungnahme gewährt habe, ihre Aufklärungspflicht verletzt.

aa) Das Landesarbeitsgericht stellt darauf ab, der Kläger sei von den betrieblichen Informationsquellen abgeschnitten gewesen, die ihm möglicherweise Entlastungsmaterial hätten liefern können. Es ist nicht ersichtlich, dass sich der Kläger darauf – insbesondere gegenüber der Beklagten – überhaupt berufen hätte. Abgesehen davon hätte er in seiner Antwort auf diesen Umstand hinweisen können.

bb) Soweit das Landesarbeitsgericht annimmt, die zeitliche Beanspruchung des Klägers durch Therapieeinheiten habe die ihm zur Verfügung stehende Zeit zur Stellungnahme erheblich eingeschränkt, fehlt es an Feststellungen zum konkreten zeitlichen Umfang dieser Einheiten. Ebenso wenig ist festgestellt, dass die Beklagte von dieser Beanspruchung Kenntnis gehabt hätte und sie bei ihrer Entscheidung, dem Kläger keine Nachfrist zu gewähren, hätte in Rechnung stellen müssen.

d) Unerheblich ist, ob die Beklagte das Gebot der zügigen Aufklärung aus § 626 Abs. 2 BGB verletzt hätte, wenn sie dem Kläger eine Nachfrist jedenfalls bis Mitte Januar 2011 gesetzt hätte. Selbst wenn dies zu verneinen wäre, folgt allein daraus – entgegen der Auffassung des Landesarbeitsgerichts – nicht, dass sie ihre Aufklärungspflicht nach § 626 Abs. 1 BGB verletzt hat, weil sie dem Kläger eine solche Frist nicht gewährte.

3. Das Landesarbeitsgericht wird – falls es darauf ankommt – die Frage, ob der Kläger vor Ausspruch der Verdachtskündigung im Rahmen des der Beklagten Zumutbaren Gelegenheit zur Stellungnahme zu den gegen ihn erhobenen Vorwürfen hatte, unter Berücksichtigung der vorstehenden Erwägungen und aller relevanten Umstände des Streitfalls erneut zu prüfen haben.

Zur Pflicht zur Angabe von Vorstrafen

(**Bundesarbeitsgericht**, Urteil vom 20. März 2014 – 2 AZR 1071/12 –)

Verurteilungen, die im Bundeszentralregister getilgt sind, braucht ein Stellenbewerber auf die pauschale Frage nach dem Vorliegen von Vorstrafen auch dann nicht anzugeben, wenn er sich um eine Stelle im Justizvollzugsdienst bewirbt.

Sachverhalt:

Die Parteien streiten über die Wirksamkeit einer Anfechtung und einer ordentlichen Kündigung ihres Arbeitsvertrags.

Der im Mai 1982 geborene, verheiratete Kläger bewarb sich Mitte Januar 2010 um eine Stelle im allgemeinen Vollzugsdienst des beklagten Landes. Zu den angeforderten Bewerbungsunterlagen gehörte die formularmäßige „Erklärung über Straftaten". Der Kläger gab an, er sei nicht vorbestraft; gegen ihn sei auch kein gerichtliches Strafverfahren und kein Ermittlungsverfahren der Staatsanwaltschaft anhängig oder innerhalb der letzten drei Jahre anhängig gewesen.

Im Rahmen eines Verfahrens zur Eignungsfeststellung wurde er erneut um Auskunft über gerichtliche Bestrafungen und gegen ihn geführte Ermittlungsverfahren gebeten. Der Kläger äußerte sich wie zuvor. Unter dem 28. April 2010 wurde auf seinen Namen ein Führungszeugnis zur Vorlage bei einer Behörde ausgestellt. Es enthielt keinen Eintrag.

Am 1. Juni 2010 wurde dem Kläger eine „Erklärung über Vorstrafen und anhängige Strafverfahren bei Einstellungen durch eine Justizvollzugsbehörde" vorgelegt. Er versicherte mit seiner Unterschrift, dass er „nicht gerichtlich bestraft" und gegen ihn „ein gerichtliches Strafverfahren oder ein Ermittlungsverfahren der Staatsanwaltschaft nicht anhängig" sei. Er bestätigte außerdem, darüber belehrt worden zu sein, dass er alle noch nicht getilgten oder nicht tilgungsreifen strafgerichtlichen Verurteilungen anzugeben und nach § 53 Abs. 2 iVm. § 41 Abs. 1 Nr. 1 BZRG auch über diejenigen Verurteilungen Auskunft zu geben habe, die nicht in ein Führungszeugnis oder nur in ein solches für Behörden aufzunehmen seien. Laut des Protokolls über ein Gespräch vom gleichen Tage erklärte bzw. bestätigte der Kläger außerdem: „Gegen mich ist weder ein Strafverfahren noch ein Ermittlungsverfahren anhängig oder in den letzten drei Jahren anhängig gewesen. Auf die möglichen Folgen, die sich aus dem Verschweigen solcher Verfahren ergeben könnten, bin ich hingewiesen worden".

Noch am 1. Juni 2010 unterzeichneten die Parteien einen Arbeitsvertrag. Seitdem ist der Kläger beim beklagten Land als Justizvollzugsbediensteter tätig. Auf das Arbeitsverhältnis finden kraft vertraglicher Bezugnahme der Tarifvertrag für den öffentlichen Dienst der Länder (TV-L) und die diesen ergänzenden, ändernden oder ersetzenden Tarifverträge in der für das beklagte Land geltenden Fassung Anwendung.

Im Rahmen einer Sicherheitsüberprüfung nach § 9 SÜG NRW erfuhr das beklagte Land, dass der Kläger im Juli 2003 zu einer Jugendstrafe von sechs Monaten wegen Körperverletzung und Betrugs verurteilt worden war. Die Vollstreckung der Strafe war zur Bewährung ausgesetzt worden. Zudem wurde bekannt, dass gegen ihn in den Jahren 2007 bis 2009 – teils aufgrund einer Selbstanzeige – acht Ermittlungsverfahren wegen des Verdachts auf Körperverletzung, Diebstahl, Hausfriedensbruch, Betrug, Beleidigung und gefährliche Körperverletzung geführt worden waren. Sechs Verfahren waren gemäß § 170 Abs. 2 StPO eingestellt worden. In zwei Verfahren war eine Einstellung nach § 153 Abs. 1 StPO erfolgt; die Geschädigten waren auf den Privatklageweg verwiesen worden. Die letzte Einstellungsverfügung datiert vom 24. August 2009.

Mit Schreiben vom 17. Dezember 2010 kündigte das beklagte Land das Arbeitsverhältnis der Parteien – nach Beteiligung des Personalrats – ordentlich zum 31. Januar 2011. Mit Schreiben vom 19. Januar 2011 focht es den Arbeitsvertrag wegen arglistiger Täuschung an. Im Termin der Güteverhandlung vor dem Arbeitsgericht am 20. Januar 2011 erklärte es – mündlich – die Anfechtung des Vertrags ein weiteres Mal.

Der Kläger hat sich gegen die Anfechtung und – fristgerecht – gegen die Kündigung gewandt. Er hat die Auffassung vertreten, ein Anfechtungsgrund liege nicht vor. Er sei nicht verpflichtet gewesen, das beklagte Land über seine Vorstrafe und die Ermittlungsverfahren zu unterrichten. Die Kündigung sei sozial ungerechtfertigt und auch deshalb unwirksam, weil es an einer ordnungsgemäßen Beteiligung des Personalrats fehle.

Das beklagte Land hat beantragt, die Klage abzuweisen. Es hat geltend gemacht, es habe den Arbeitsvertrag wegen arglistiger Täuschung wirksam angefochten. Der Kläger habe bewusst falsche Angaben zu Vorstrafen und gegen ihn geführten Ermittlungsverfahren gemacht. Bei wahrheitsgemäßer Erklärung wäre er nicht eingestellt worden. Vorschriften des Bundeszentralregistergesetzes einschließlich dort bestimmter Tilgungsfristen für strafgerichtliche Verurteilungen hätten ihrem Auskunftsverlangen nicht entgegengestanden. Die Kündigung sei wirksam. Der Kläger habe Fragen zu seiner Person in einem für seine Beschäftigung elementaren Bereich falsch beantwortet. Das habe dem Arbeitsverhältnis die Vertrauensgrundlage entzogen. Zugleich habe er sich damit für eine Tätigkeit im allgemeinen Justizvollzugsdienst als ungeeignet erwiesen. In diesem Bereich sei es unerlässlich, dass Arbeitnehmer in Offenheit und Ehrlichkeit Beispiele gäben und bereit seien, eigene Fehler und Schwächen einzugestehen. Abgesehen davon seien die gegen den Kläger geführten Ermittlungsverfahren in Anbetracht ihrer Anzahl und der ihnen zugrundeliegenden Tatvorwürfe Beleg für seine charakterliche Ungeeignetheit. Der Personalrat sei ordnungsgemäß beteiligt worden und habe der Kündigung zugestimmt.

Die Vorinstanzen haben den Klage stattgegeben. Mit seiner Revision begehrt das beklagte Land weiterhin, die Klage abzuweisen.

Aus den Gründen:

II. Die Kündigungsschutzklage ist begründet. Das beklagte Land hat den Arbeitsvertrag nicht wirksam angefochten (1.). Die ordentliche Kündigung vom 17. Dezember 2010 ist unwirksam (2.). Soweit das Arbeitsgericht und – ihm folgend – das Landesarbeitsgericht festgestellt haben, dass das Arbeitsverhältnis durch die Anfechtungserklärungen nicht aufgelöst worden ist, kommt ihren Entscheidungen keine eigenständige Wirkung zu.

1. Die Kündigungsschutzklage war nicht deshalb abzuweisen, weil zwischen den Parteien am 31. Januar 2011 kein Arbeitsverhältnis mehr bestanden hätte. Das beklagte Land war nicht zur Anfechtung des Arbeitsvertrags berechtigt.

a) Die Anfechtung war trotz der Kündigungserklärung nicht ausgeschlossen (BAG 12. Mai 2011 – 2 AZR 479/09 – Rn. 40; 16. Dezember 2004 – 2 AZR 148/04 – zu B II 1 a der Gründe). Beide Gestaltungsrechte bestehen grundsätzlich nebeneinander (vgl. BAG 6. September 2012 – 2 AZR 270/11 – Rn. 46 mwN).

b) Eine arglistige Täuschung iSv. § 123 Abs. 1 BGB liegt nicht vor.

aa) Die falsche Beantwortung einer dem Arbeitnehmer bei der Einstellung zulässigerweise gestellten Frage kann den Arbeitgeber nach § 123 Abs. 1 BGB dazu berechtigen, den Arbeitsvertrag wegen arglistiger Täuschung anzufechten, wenn die Täuschung für dessen Abschluss ursächlich war (BAG 6. September 2012 – 2 AZR 270/11 – Rn. 24; 7. Juli 2011 – 2 AZR 396/10 – Rn. 16).

bb) Der Arbeitgeber darf beim Arbeitnehmer bei der Anbahnung des Arbeitsverhältnisses Informationen zu Vorstrafen einholen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies „erfordert", dh. bei objektiver Betrachtung berechtigt erscheinen lässt. Auch die Frage nach noch laufenden Straf- oder Ermittlungsverfahren kann – je nach den Umständen – zulässig sein (BAG 6. September 2012 – 2 AZR 270/11 – Rn. 24; 27. Juli 2005 – 7 AZR 508/04 – zu I 1 b bb (1) der Gründe, BAGE 115, 296; 20. Mai 1999 – 2 AZR 320/98 – zu B I 1 b cc der Gründe, BAGE 91, 349). Eine Einschränkung des Fragerechts kann sich insbesondere aus dem allgemeinen Persönlichkeitsrecht des Bewerbers, speziellen datenschutzrechtlichen Bestimmungen und den dabei zu berücksichtigenden Wertentscheidungen des BZRG ergeben (BAG 6. September 2012 – 2 AZR 270/11 – aaO; 21. Februar 1991 – 2 AZR 449/90 – zu II 1 b der Gründe; zur Frage nach eingestellten Ermittlungsverfahren vgl. BAG 15. November 2012 – 6 AZR 339/11 – Rn. 14 ff., BAGE 143, 343). Entsprechendes gilt, soweit dem Arbeitnehmer bei der Einstellung vom künftigen Arbeitgeber vorformulierte Erklärungen abverlangt werden, die sich auf Vorstrafen und/oder staatsanwaltschaftliche Ermittlungsverfahren beziehen (für Erklärungen zur „Verfassungstreue" eines Bewerbers vgl. BAG 12. Mai 2011 – 2 AZR 479/09 – Rn. 45).

cc) Das Verschweigen von Tatsachen, nach denen nicht gefragt wurde, stellt nur dann eine Täuschung dar, wenn hinsichtlich dieser Tatsachen eine Offenbarungspflicht besteht. Eine solche Pflicht ist an die Voraussetzung gebunden, dass die betreffenden Umstände entweder dem Bewerber die Erfüllung seiner vorgesehenen arbeitsvertraglichen Leistungspflicht von vornherein unmöglich machen oder doch seine Eignung für den in Aussicht genommenen Arbeitsplatz entscheidend berühren (BAG 6. September 2012 – 2 AZR 270/11 – Rn. 25; 12. Mai 2011 – 2 AZR 479/09 – Rn. 41; jeweils m.w.N).

dd) Arglistig ist die Täuschung, wenn der Täuschende weiß oder billigend in Kauf nimmt, dass seine Behauptungen nicht der Wahrheit entsprechen und deshalb oder mangels Offenbarung bestimmter Tatsachen irrige Vorstellungen beim (künftigen) Arbeitgeber entstehen oder aufrechterhalten werden. Fahrlässigkeit – auch grobe Fahrlässigkeit – genügt insoweit nicht. Die Beweislast für das Vorliegen von Arglist trägt der Arbeitgeber. Dass es sich hierbei um eine innere Tatsache handelt, steht dem nicht entgegen (BAG 6. September 2012 – 2 AZR 270/11 – Rn. 26; 12. Mai 2011 – 2 AZR 479/09 – Rn. 43; jeweils mwN).

ee) Danach hat der Kläger das beklagte Land nicht arglistig getäuscht, weil er angegeben hat, er sei nicht vorbestraft und nicht „gerichtlich bestraft". Die Verurteilung aus dem Jahr 2003 war im Bundeszentralregister getilgt, als er sich beim beklagten Land bewarb. Der Kläger musste die an ihn gerichteten Fragen und erbetenen Erklärungen nicht so verstehen, dass er Auskunft auch über tilgungsreife oder getilgte Vorstrafen geben sollte. Unabhängig davon hatte das beklagte Land kein berechtigtes Interesse an der Offenbarung entsprechender Verurteilungen.

(1) Nach § 53 Abs. 1 BZRG darf sich der Verurteilte gegenüber Behörden und Privatpersonen als unbestraft bezeichnen und braucht den der Verurteilung zugrunde liegenden Sachverhalt nicht zu offenbaren, wenn die Verurteilung nicht in das Führungszeugnis oder nur in ein Führungszeugnis für Behörden nach § 32 Abs. 3, Abs. 4 BZRG aufzunehmen (§ 53 Abs. 1 Nr. 1 BZRG) oder wenn sie zu tilgen ist (§ 53 Abs. 1 Nr. 2 BZRG).

(2) Gemäß § 53 Abs. 2 BZRG kann sich der Verurteilte zwar – falls er hierüber belehrt wurde – gegenüber Gerichten oder Behörden nicht auf seine Rechte aus § 53 Abs. 1 Nr. 1 BZRG berufen, soweit diese einen Anspruch auf unbeschränkte Auskunft haben. Die Ausnahme vom sog. Verschweigerecht bezieht sich nach der klaren gesetzlichen Vorgabe aber nur auf die von Abs. 1 Nr. 1 der Vorschrift erfassten Sachverhalte, nicht auf Verurteilungen iSv. § 53 Abs. 1 Nr. 2 BZRG, dh. auf tilgungsreife oder bereits getilgte Vorstrafen. Um eine solche Verurteilung handelt es sich hier. Das Amtsgericht Köln hatte gegen den Kläger am 29. Juli 2003 eine Jugendstrafe von sechs Monaten unter Strafaussetzung zur Bewährung verhängt. Die Verurteilung unterlag gemäß § 46 Abs. 1 Nr. 1 Buchst. c BZRG einer Tilgungsfrist von fünf Jahren. Diese Frist war zu Beginn des Bewerbungsverfahrens verstrichen. Die Vorstrafe war überdies bereits aus dem Register entfernt (§ 45 Abs. 2 BZRG). Sie unterlag damit auch nicht mehr einer unbeschränkten Auskunft iSv. § 41 Abs. 1 Nr. 1 BZRG, die Justizvollzugsbehörden für Zwecke des Strafvollzugs einschließlich der Überprüfung aller im Strafvollzug tätigen Personen beanspruchen können (vgl. Hase BZRG § 41 Rn. 1).

(3) Demnach hat der Kläger hinsichtlich der fraglichen Verurteilung selbst dann keine falsche Auskunft erteilt, wenn man die in einigen Fragen des beklagten Landes vorgenommene zeitliche Einschränkung auf die „letzten drei Jahre" unberücksichtigt lässt. Ein Bewerber, der allgemein nach „Vorstrafen" oder „gerichtlichen Bestrafungen" befragt wird, darf regelmäßig davon ausgehen, dass der zukünftige Arbeitgeber das Verschweigerecht achten will und sich die Frage/erbetene Erklärung auf den Umfang der Auskunftspflicht beschränkt. Bezüglich der Bewerbung des Klägers ist davon umso mehr auszugehen, als das beklagte Land ihn im Rahmen der erbetenen Erklärung vom 1. Juni 2010 ausdrücklich auf die Regelungen des BZRG, einschließlich des reklamierten „erweiterten Auskunftsrechts", hingewiesen hat.

(4) Im Übrigen ist ein schutzwürdiges berechtigtes Interesse des beklagten Landes, Auskunft über getilgte oder tilgungsreife Verurteilungen zu erhalten, nicht zu erkennen.

(a) Das sich aus der Vertrags- und Abschlussfreiheit ableitende Fragerecht des Arbeitgebers ist zivilrechtlich durch den Schutz des allgemeinen Persönlichkeitsrechts des Arbeitnehmers begrenzt. Der Ausgleich der widerstreitenden Interessen erfolgt im Rahmen der sich aus § 311 Abs. 2, § 241 Abs. 2 und § 242 BGB ergebenden vorvertraglichen Pflichten (vgl. Riesenhuber NZA 2012, 771, 772 f.).

(b) Datenschutzrechtliche Bestimmungen, wie sie in §§ 179 ff. StVollzG, im BDSG und im DSG NRW normiert sind, konkretisieren und aktualisieren den Schutz des Rechts auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts. Sie regeln, in welchem Umfang im jeweiligen Anwendungsbereich der Gesetze Eingriffe in diese Rechtspositionen zulässig sind (BAG 15. November 2012 – 6 AZR 339/11 – Rn. 16, BAGE 143, 343). Liegt keine Einwilligung des Betroffenen vor, ist die Datenverarbeitung nur zulässig, wenn eine ihrerseits verfassungsgemäße Rechtsvorschrift sie erlaubt. Fehlt es an der erforderlichen Ermächtigungsgrundlage oder liegen deren Voraussetzungen nicht vor, ist die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten verboten. Das gilt für Datenerhebungen nach dem BDSG und DSG NRW ebenso wie für Erhebungen im Bereich des Strafvollzugs (zu Letzterem vgl. Calliess/Müller-Dietz StVollzG 11. Aufl. § 179 Rn. 2). Für Beschäftigte, zu denen nach § 3 Abs. 11 Nr. 1, Nr. 7 BDSG und § 29 Abs. 1 Satz 1 DSG NRW neben Arbeitnehmern auch Bewerber zählen, enthalten § 32 Abs. 1 BDSG und § 29 Abs. 1 DSG NRW einen solchen Erlaubnistatbestand. Danach dürfen personenbezogene Daten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist. Die Regelungen schließen nicht automatisierte Datenerhebungen ein (BAG 20. Juni 2013 – 2 AZR 546/12 – Rn. 24; 15. November 2012 – 6 AZR 339/11 – a.a.O.). Nach § 179 Abs. 1 StVollzG darf die Vollzugsbehörde personenbezogene Daten erheben, soweit deren Kenntnis für den ihr nach dem Gesetz aufgegebenen Vollzug der Freiheitsstrafe erforderlich ist. Gemäß § 179 Abs. 2 Satz 1 StVollzG sind personenbezogene Daten bei dem Betroffenen zu erheben. Daten über Personen, die nicht Gefangene sind, dürfen ohne ihre Mitwirkung bei Personen oder Stellen außerhalb der Vollzugsbehörde nur erhoben werden, wenn sie ua. für die Sicherheit der Anstalt unerlässlich sind und die Art der Erhebung schutzwürdige Interessen der Betroffenen nicht beeinträchtigt.

(c) Es kann dahinstehen, ob die bereichsspezifischen Regelungen in §§ 179 ff. StVollzG auch den Beschäftigtendatenschutz umfassen und in ihrem Anwendungsbereich die allgemeinen Regelungen im BDSG und DSG NRW verdrängen. „Erforderlich" iSv. § 179 Abs. 1 StVollzG und § 32 Abs. 1 BDSG bzw. § 29 Abs. 1 DSG NRW ist die Informationsgewinnung nur, wenn ein berechtigtes, billigenswertes und schutzwürdiges Interesse des Arbeitgebers an der Beantwortung seiner Fragen bzw. der sonstigen Informationsbe-

schaffung besteht und das Interesse des Arbeitnehmers an der Geheimhaltung der Daten das Interesse des Arbeitgebers an ihrer Erhebung nicht überwiegt (BAG 15. November 2012 – 6 AZR 339/11 – Rn. 22, BAGE 143, 343). Davon ist auf der Grundlage sämtlicher hier in Betracht zu ziehenden Ermächtigungsgrundlagen nur dann auszugehen, wenn die nachgefragten Umstände für die Bewertung der Eignung des Beschäftigten von maßgebender Bedeutung sind (vgl. BAG 15. November 2012 – 6 AZR 339/11 – Rn. 28, aaO). Deshalb darf der Arbeitgeber bei der Einstellung in der Regel nur nach „einschlägigen", dh. hinsichtlich der Eignung für einen ins Auge gefassten künftigen Aufgabenbereich relevanten Vorstrafen fragen (BAG 6. September 2012 – 2 AZR 270/11 – Rn. 28).

(d) Handelt es sich um Bewerbungen für Tätigkeiten im öffentlichen Dienst, sind bei der vorzunehmenden Abwägung die Vorgaben aus Art. 33 Abs. 2 GG zu berücksichtigen. Geeignet im Sinne der Bestimmung ist nur, wer dem angestrebten Amt in körperlicher, psychischer und charakterlicher Hinsicht gewachsen ist. Zur Eignung gehören die Fähigkeit und innere Bereitschaft, die dienstlichen Aufgaben nach den Grundsätzen der Verfassung wahrzunehmen, insbesondere die Freiheitsrechte der Bürger zu wahren und rechtsstaatliche Regeln einzuhalten (BAG 15. November 2012 – 6 AZR 339/11 – Rn. 22, BAGE 143, 343; 27. Juli 2005 – 7 AZR 508/04 – zu I 1 b bb (1) der Gründe, BAGE 115, 296).

(e) In Anbetracht dessen erscheint es erwägenswert, den öffentlichen Arbeitgeber als berechtigt anzusehen, Bewerber für eine Tätigkeit im Justizvollzugsdienst ohne gegenständliche Einschränkung nach Vorstrafen zu fragen. Strafrechtliche Verurteilungen sind unabhängig von dem ihnen zugrunde liegenden Delikt geeignet, Zweifel an der Rechtstreue und damit der Eignung des Bewerbers zu begründen. Das gilt allerdings nur für Verurteilungen, die nicht bereits der Tilgung unterliegen. Ein berechtigtes und schutzwürdiges Interesse des beklagten Landes, vom Kläger auch Auskunft über getilgte und zu tilgende Vorstrafen zu erlangen, ist nicht zu erkennen.

(aa) Hinsichtlich getilgter oder tilgungsreifer Verurteilungen steht dem Betroffenen nicht nur das „Verschweigerecht" aus § 53 Abs. 1 Nr. 2 BZRG zu. Er kann sich außerdem auf § 51 Abs. 1 BZRG berufen. Danach darf dem Betroffenen die Tat und die Verurteilung im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden, wenn die Eintragung über die Verurteilung im Strafregister getilgt worden oder zu tilgen ist. Auf diese Weise soll der Verurteilte vom Strafmakel befreit und seine Resozialisierung gefördert oder manifestiert werden (Kuhn JA 2011, 855, 856). Das Verbot erfasst alle Bereiche des Rechtslebens (Hase BZRG § 51 Rn. 2). Es ist auch im privatrechtlichen Bereich zu achten.

(bb) Zwar sieht das Gesetz in § 52 Abs. 1 Nr. 4 BZRG eine Ausnahme vom Vorhalte- und Verwertungsverbot vor, wenn die Einstellung des Betroffenen in den öffentlichen Dienst sonst zu einer erheblichen Gefährdung der Allgemeinheit führen würde. Das erweitert aber nicht dessen Auskunftspflicht. Dem öffentlichen Arbeitgeber wird vielmehr nur die Möglichkeit eingeräumt, die Verurteilung in Fällen zu berücksichtigen, in denen ihm getilgte oder tilgungsreife Verurteilungen auf andere Weise als durch eine Registerauskunft bekannt geworden sind, und auch dies nur wenn schwerwiegende Gründe vorliegen. Die Begrenzung der Offenbarungspflichten des Betroffenen durch das „Verschweigerecht" gemäß § 53 BZRG wird hierdurch nicht berührt (BeckOK StPO/Bücherl BZRG § 52 Rn. 7; Hase BZRG § 52 Rn. 2).

(cc) Eine Verpflichtung, Angaben zu getilgten Strafen zu machen, ergibt sich nicht aus dem Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Landes Nordrhein-Westfalen (SÜG NRW). Im Rahmen einer einfachen Sicherheitsüberprüfung gemäß § 9 SÜG NRW, wie sie beim Kläger offenbar durchgeführt wurde, hat der Beschäftigte lediglich anhängige Straf- und Disziplinarverfahren anzugeben (§ 14 Abs. 1 Nr. 16 SÜG NRW). Das sieht das beklagte Land offenbar selbst nicht anders. Es beruft sich für das reklamierte – weitergehende – Auskunftsrecht nicht auf die fragliche Vorschrift.

(dd) Es spricht einiges dafür, angesichts der in §§ 51 bis 53 BZRG getroffenen Wertentscheidungen des Gesetzgebers ein berechtigtes und schutzwürdiges Interesse auch des öffentlichen Arbeitgebers, beim Stellenbewerber Informationen über getilgte oder tilgungsreife Vorstrafen einzuholen, generell zu verneinen (zur Verpflichtung des öffentlichen Arbeitgebers, ein Strafurteil aus den Personalakten zu entfernen, soweit die Verurteilung im BZRG gelöscht ist vgl. BAG 9. Februar 1977 – 5 AZR 2/76 –). Selbst unterstellt, in den Fällen des § 51 Abs. 1 Nr. 4 BZRG käme ein Fragerecht in Betracht, ist zu berücksichtigen, dass eine Gefährdung der Allgemeinheit nicht allein auf das Vorliegen einer Verurteilung als solche gestützt werden kann (BeckOK StPO/Bücherl BZRG § 52 Rn. 7; Hase BZRG § 52 Rn. 5). Daraus folgt zumindest das Erfordernis, eine Frage oder erbetene Erklärung sachlich auf Taten oder Deliktsbereiche zu begrenzen, die potentiell geeignet erscheinen, eine Ausnahme vom Verbot des § 51 Abs. 1 BZRG zu rechtfertigen. Dem genügt das Ersuchen des beklagten Landes nicht. Es hat seine Frage gegenständlich nicht eingeschränkt. Im Übrigen erscheint es ausgeschlossen, aus einer gegen den Kläger verhängten Jugendstrafe auf eine Gefährdung der Allgemeinheit iSv. § 52 Abs. 1 Nr. 4 BZRG zu schließen.

ff) Eine Verpflichtung des Klägers, die Verurteilung von sich aus zu offenbaren, bestand nicht. Das folgt aus seinem Verschweigerecht und dem zu seinen Gunsten bestehenden Verbot des § 51 Abs. 1 BZRG.

gg) Der Kläger hat das beklagte Land nicht dadurch iSv. § 123 Abs. 1 BGB arglistig getäuscht, dass er die gegen ihn geführten, im Zeitpunkt der Bewerbung bereits eingestellten Ermittlungsverfahren verschwieg.

(1) Soweit dem Arbeitgeber – je nach den Umständen – das Recht zugebilligt wird, Stellenbewerber nach laufenden Ermittlungsverfahren zu fragen, beruht dies auf der Erwägung, dass die Verfahren Zweifel an der Eignung und Zuverlässigkeit des Bewerbers für den konkreten Arbeitsplatz und die Besorgnis begründen können, er werde die in Aussicht genommene Stelle womöglich nicht antreten können, zumindest in seiner Verfügbarkeit eingeschränkt sein (vgl. BAG 6. September 2012 – 2 AZR 270/11 – Rn. 28; 20. Mai 1999 – 2 AZR 320/98 – zu B I 1 b cc der Gründe, BAGE 91, 349; ErfK/Preis 14. Aufl. § 611 Rn. 281; Joussen NZA 2012, 776, 777; Linnenkohl AuR 1983, 129).

(2) Dagegen hat auch der öffentliche Arbeitgeber grundsätzlich kein berechtigtes Interesse, den Bewerber unspezifiziert nach eingestellten strafrechtlichen Ermittlungsverfahren zu fragen (BAG 15. November 2012 – 6 AZR 339/11 – Rn. 17 ff., BAGE 143, 343). Dies folgt aus der in § 53 BZRG iVm. § 41 Abs. 1 BZRG getroffenen Wertentscheidung des Gesetzgebers. Dass die Bestimmungen auf Ermittlungsverfahren nicht unmittelbar anwendbar sind, steht dieser Bewertung nicht entgegen.

(a) Eingestellte Ermittlungsverfahren sind nicht in das Zentralregister einzutragen. Sie zählen demnach nicht zu den Verfahren,

über die Gerichte und Behörden nach § 41 Abs. 1 BZRG uneingeschränkt Auskunft verlangen können. Ohne Schuldnachweis ist es nicht vertretbar, den Betroffenen mit den möglichen nachteiligen Folgen einer Eintragung zu belasten (BAG 15. November 2012 – 6 AZR 339/11 – Rn. 25 mwN, BAGE 143, 343). Besteht ein Verschweigerecht bereits in den von § 53 BZRG ausdrücklich geregelten Fällen, gilt dies umso mehr, wenn nach Vorgängen gefragt wird, die von vornherein nicht in ein Führungszeugnis aufzunehmen sind und über die auch den in § 53 Abs. 2, § 41 Abs. 1 BZRG genannten Stellen keine Auskunft erteilt wird (BAG 15. November 2012 – 6 AZR 339/11 – aaO; Schaub/Linck 15. Aufl. § 26 Rn. 35).

(b) Dabei ist unerheblich, welcher Sachverhalt den Ermittlungen zugrunde lag. Endet ein Strafverfahren durch Einstellung nach §§ 153 ff. StPO, steht der Betroffene weiter unter dem Schutz der Unschuldsvermutung (für eine Einstellung nach § 170 Abs. 2 StPO vgl. BVerfG 19. Dezember 1983 – 2 BvR 1731/82 – zu II 3 b (2) der Gründe; Moldenhauer in Karlsruher Kommentar zur StPO 7. Aufl. § 170 Rn. 18). Diese gilt zwar auch während noch laufender Ermittlungsverfahren. Doch steht für deren Dauer nicht fest, ob dem Arbeitnehmer das Verschweigerecht aus § 53 BZRG auch künftig noch zukommt (BAG 15. Dezember 2012 – 6 AZR 339/11 – Rn. 26, BAGE 143, 343; 27. Juli 2005 – 7 AZR 508/04 – zu I 1 b bb (2) der Gründe, BAGE 115, 296).

(c) Dem Recht, über eingestellte Ermittlungsverfahren zu schweigen, steht nicht entgegen, dass bei Einstellungen nach §§ 153 ff. StPO der Straftatverdacht nicht zwingend ausgeräumt sein muss und deshalb Nachteile durch ein solches Verfahren nicht schlechthin zu unterbleiben haben. Bei Einstellungen nach § 170 Abs. 2 Satz 1 StPO tritt ein Strafklageverbrauch sogar überhaupt nicht ein – das Verfahren kann jederzeit auch bei gleicher Sach- und Rechtslage wieder aufgenommen werden (BAG 29. September 2011 – 2 AZR 674/10 – Rn. 35; 5. April 2001 – 2 AZR 217/00 – zu II 2 c der Gründe; Moldenhauer in Karlsruher Kommentar zur StPO 7. Aufl. § 170 Rn. 23 mwN). Dennoch überwiegt auch in diesem Fall das Recht des Betroffenen, sich nicht offenbaren zu müssen, das Informationsinteresse des Arbeitgebers. Es kommt hinzu, dass Ermittlungsverfahren, die mangels hinreichenden Anlasses zur Erhebung der öffentlichen Klage eingestellt wurden, typischerweise keine geeignete Grundlage für eine Beurteilung der Eignung des Bewerbers bieten. Entsprechendes gilt, wenn die Verfahren auf den Privatklageweg verwiesen wurden. Der Arbeitgeber hat kein schützenswertes Interesse, den Bewerber nach Ermittlungsverfahren zu befragen, in deren Verlauf die Ermittlungsbehörden einen hinreichenden Tatverdacht oder angesichts geringer Schuld ein öffentliches Interesse an einer Strafverfolgung nicht erkannt haben. Für sicherheitsempfindliche Tätigkeiten gilt, wie die Wertungen in § 9 SÜG NRW zeigen, nichts anderes.

c) Das beklagte Land war zur Anfechtung des Arbeitsvertrags nicht wegen des Irrtums über eine verkehrswesentliche Eigenschaft des Klägers nach § 119 Abs. 2 Alt. 1 BGB berechtigt. Zwar kann eine Anfechtung wegen arglistiger Täuschung die Anfechtung wegen Irrtums in sich schließen. Dem Anfechtenden ist es dann grundsätzlich nicht verwehrt, sich nachträglich auf diesen Grund zu berufen (BAG 6. September 2012 – 2 AZR 270/11 – Rn. 38 mwN). Voraussetzung ist aber, dass auch die Frist des § 121 Abs. 1 BGB gewahrt ist. Die Anfechtung muss in den Fällen des § 119 BGB ohne schuldhaftes Zögern (unverzüglich) erfolgen, sobald der Anfechtungsberechtigte von dem Anfechtungsgrund Kenntnis erlangt hat. Das ist hier nicht geschehen. Das beklagte Land hat das Arbeitsverhältnis der Parteien am 17. Dezember 2010 wegen des Verschweigens einer Vorstrafe und mehrerer Ermittlungsverfahren ordentlich gekündigt. Die auf die nämlichen Gründe gestützte Anfechtung des Arbeitsvertrags hat es erst einen Monat später erklärt. Dies war – auch mit Blick auf eine ihm einzuräumende Überlegungsfrist – nicht mehr unverzüglich, ohne dass geklärt werden müsste, zu welchem genauen, allemal aber vor der Kündigung liegenden Zeitpunkt ihm die maßgebenden Tatsachen bekannt geworden waren. Darauf, ob die behauptete Unzuverlässigkeit des Klägers und eine ihm zugeschriebene „Gewalttätigkeit" verkehrswesentliche Eigenschaften einer Person sein können, kommt es nicht an.

2. Die Kündigung vom 17. Dezember 2010 ist sozial ungerechtfertigt iSv. § 1 Abs. 1, Abs. 2 KSchG und deshalb unwirksam.

a) Das Kündigungsschutzgesetz findet auf das Arbeitsverhältnis der Parteien Anwendung. Dieses bestand bei Zugang der Kündigung schon länger als sechs Monate iSv. § 1 Abs. 1 KSchG; der betriebliche Geltungsbereich des Gesetzes nach § 23 Abs. 1 KSchG ist eröffnet.

b) Die Kündigung ist nicht durch Gründe im Verhalten des Klägers bedingt. Dieser hat seine vorvertraglichen Aufklärungspflichten nicht verletzt.

c) Die Kündigung ist ebenso wenig durch Gründe in der Person des Klägers bedingt.

aa) Hat sich der Arbeitnehmer außerdienstlich strafbar gemacht, kann dies Zweifel an seiner Zuverlässigkeit und Vertrauenswürdigkeit begründen. Das außerdienstliche Verhalten kann – abhängig von seiner Funktion – dazu führen, dass dem Arbeitnehmer künftig die Eignung für die Erledigung seiner Aufgaben fehlt. Ob daraus ein in der Person liegender Kündigungsgrund folgt, hängt von der Art des Delikts und der konkreten Aufgabenstellung des Arbeitnehmers ab. So können außerdienstlich begangene Straftaten eines mit hoheitlichen Aufgaben betrauten Arbeitnehmers auch dann zu einem Eignungsmangel führen, wenn es an einem unmittelbaren Bezug zum Arbeitsverhältnis fehlt (BAG 20. Juni 2013 – 2 AZR 583/12 – Rn. 14; 10. September 2009 – 2 AZR 257/08 – Rn. 24, BAGE 132, 72). Das gilt grundsätzlich auch für ein Verhalten vor Begründung des Arbeitsverhältnisses, wenn es die Eignung des Arbeitnehmers tatsächlich (noch) berührt.

bb) Das beklagte Land hat sich für einen Eignungsmangel des Klägers nicht auf die gegen ihn verhängte Jugendstrafe berufen. Sie wäre in der Tat ungeeignet, einen solchen Mangel zu begründen.

cc) Das beklagte Land stützt die Kündigung auf den Gegenstand der gegen den Kläger geführten Ermittlungsverfahren. Sein Vorbringen rechtfertigt die Kündigung nicht. Das gilt auch angesichts seiner Behauptung, der Kläger habe sich in einem Fall selbst angezeigt und dabei angegeben, er habe seine Ehefrau wiederholt körperlich verletzt und sie in der gemeinsamen Wohnung eingesperrt.

(1) Das beklagte Land durfte diese Erkenntnisse zwar verwerten. Sein Vortrag ist aber nicht hinreichend substantiiert. Um darzulegen, der Kläger sei wegen dieses Verhaltens für eine Tätigkeit im Strafvollzugsdienst ungeeignet, reicht es nicht aus, auf einzelne nicht weiter aufgeklärte Umstände zu verweisen und das Verhalten pauschal, ohne konkrete Angaben zur Tatzeit und zum Tathergang zu umschreiben.

(2) Das beklagte Land hat zudem den fraglichen Sachverhalt dem Personalrat nicht unterbreitet. Es hat diesem im Rahmen der schriftlichen Unterrichtung nach § 74 Abs. 1 PersVG NRW lediglich mitgeteilt, der Kläger habe im Verlauf des Bewerbungsverfahrens falsche Angaben gemacht; der Verstoß gegen die Wahrheitspflicht stelle einen schweren Vertrauensbruch dar und sei als arglistige Täuschung zu werten. Zum Gegenstand der Ermittlungsverfahren

hat es – so sein Vorbringen – „in Ergänzung" des Unterrichtungsschreibens „dem Personalrat weitere Einzelheiten (…) mitgeteilt". Um welche „Einzelheiten" es sich dabei handelte, hat es nicht vorgetragen. Dies bedeutet zwar nicht notwendig, dass die Beteiligung des Personalrats fehlerhaft war. Die Mängel in der Unterrichtung verwehren es dem beklagten Land jedoch, sich auf das den Ermittlungsverfahren zugrunde liegende Verhalten des Klägers eigenständig zu berufen (vgl. dazu BAG 21. November 2013 – 2 AZR 797/11 – Rn. 41 mwN).

Manipulation von Akten zur Verschleierung von Pflichtverstößen

(**Bundesarbeitsgericht**, Urteil vom 23. Januar 2014 – 2 AZR 638/13 –)

Wenn ein Arbeitnehmer zur Verschleierung von Pflichtverstößen Akten manipuliert, kann das eine ordentliche Kündigung eines langjährigen Arbeitsverhältnisses auch ohne vorherige Abmahnung rechtfertigen.

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien streiten über die Wirksamkeit einer verhaltensbedingten Kündigung.

Die 1957 geborene Klägerin war seit 1977 bei der Universität des beklagten Landes als Sachbearbeiterin beschäftigt. Zu ihrem Aufgabenbereich gehörten haushälterische, kaufmännische und Sekretariatsaufgaben. Auf das Arbeitsverhältnis fanden die Tarifverträge des öffentlichen Dienstes Anwendung.

Im Jahr 2009 erhielt die Klägerin den Auftrag, die Mülltonnen für zwei Universitätsgebäude bei der Stadt „abzumelden". Ob sie dem nachgekommen ist, ist zwischen den Parteien streitig.

Am 23. Februar 2010 fand ein Mitarbeitergespräch zwischen der Klägerin und ihrer Referatsleiterin statt. Gegenstand war die nicht zufriedenstellende Arbeitsorganisation der Klägerin. Ihr wurde ein Fortbildungsangebot zum Stress- und Zeitmanagement unterbreitet. Dieses nahm sie nicht wahr.

Im Laufe des Jahres erhielt die Universität alle drei Monate Abfallgebührenbescheide und später entsprechende Mahnungen, welche die fraglichen Mülltonnen betrafen. Es handelte sich um insgesamt 16 Schreiben. Diese wurden von der Klägerin nicht bearbeitet. Mit Schreiben vom 31. Januar 2011 übersandte die Stadt der Universität entsprechende Zahlungsaufforderungen über insgesamt 4.936,70 Euro; die Summe wurde aus Kulanz auf 4.632,84 Euro reduziert.

Am 3. Februar 2011 bat die Referatsleiterin die Klägerin zu einem Gespräch. Die Klägerin teilte mit, dass sie die Mülltonnen im November 2009 auftragsgemäß abgemeldet habe. Gegen den ersten Gebührenbescheid habe sie am 5. Februar, gegen den zweiten im Mai 2010 Widerspruch eingelegt. Kopien der Schreiben befanden sich bei den Akten. Es war jedoch weder deren Versand im Postausgangsbuch vermerkt noch ihr Zugang – auf Nachfrage – vom Empfänger bestätigt worden. Die Referatsleiterin äußerte Zweifel am Wahrheitsgehalt der Schilderungen und bat die Klägerin, noch einmal über den Vorgang nachzudenken. Am darauf folgenden Morgen räumte die Klägerin ein, die beiden Widersprüche nicht zu dem darin angegebenen Datum verfasst, sondern nachträglich gefertigt und zu den Unterlagen genommen zu haben. Die Abmeldung der Mülltonnen sei aber tatsächlich erfolgt.

Mit Schreiben vom 20. Februar 2012 kündigte das beklagte Land das Arbeitsverhältnis der Parteien ordentlich zum 30. September 2012.

Die Vorsitzenden haben die gegen die Kündigung gerichtete Klage abgewiesem.

Aus den Gründen:

Die Revision ist unbegründet. Das Landesarbeitsgericht hat die Klage zu Recht abgewiesen. Das Arbeitsverhältnis der Parteien ist durch die ordentliche Kündigung vom 20. Februar 2012 mit Ablauf des 30. September 2012 aufgelöst worden.

I. Die Kündigung ist durch Gründe im Verhalten der Klägerin bedingt.

1. Eine Kündigung ist durch Gründe im Verhalten des Arbeitnehmers iSv. § 1 Abs. 2 Satz 1 KSchG „bedingt", wenn dieser seine vertraglichen Haupt- oder Nebenpflichten erheblich und in der Regel schuldhaft verletzt hat und eine dauerhaft störungsfreie Vertragserfüllung in Zukunft nicht mehr zu erwarten steht. Dann kann dem Risiko künftiger Störungen nur durch die (fristgemäße) Beendigung des Arbeitsverhältnisses begegnet werden. Das wiederum ist nicht der Fall, wenn schon mildere Mittel und Reaktionen von Seiten des Arbeitgebers – etwa eine Abmahnung oder eine Versetzung – geeignet gewesen wären, beim Arbeitnehmer künftige Vertragstreue zu bewirken (BAG 27. September 2012 – 2 AZR 811/11 – Rn. 16 mwN; 9. Juni 2011 – 2 AZR 284/10 – Rn. 34 mwN). Beruht die Vertragspflichtverletzung auf steuerbarem Verhalten des Arbeitnehmers, ist grundsätzlich davon auszugehen, dass sein künftiges Verhalten bereits durch die Androhung von Folgen für den Bestand des Arbeitsverhältnisses positiv beeinflusst werden kann. Einer Abmahnung bedarf es nach Maßgabe des auch in § 314 Abs. 2 i.V.m. § 323 Abs. 2 BGB zum Ausdruck kommenden Verhältnismäßigkeitsgrundsatzes demnach nur dann nicht, wenn eine Verhaltensänderung in Zukunft auch nach Abmahnung nicht zu erwarten steht oder es sich um eine so schwere Pflichtverletzung handelt, dass selbst deren erstmalige Hinnahme dem Arbeitgeber nach objektiven Maßstäben unzumutbar und damit offensichtlich – auch für den Arbeitnehmer erkennbar – ausgeschlossen ist (vgl. BAG 25. Oktober 2012 – 2 AZR 495/11 – Rn. 16; 9. Juni 2011 – 2 AZR 284/10 – Rn. 35).

2. Die Klägerin hat ihre vertraglichen Pflichten – die tatsächliche Abmeldung der Mülltonnen zu ihren Gunsten unterstellt – dadurch erheblich und schuldhaft verletzt, dass sie innerhalb der Zeitspanne von etwa einem Jahr auf insgesamt 16 Schreiben der Stadt nicht reagiert und anschließend zwei in Wahrheit nicht versandte Widerspruchsschreiben unter falschem Datum erstellt und zu den Akten genommen hat. Damit ist sie nicht nur ihren Hauptleistungspflichten nicht ordnungsgemäß nachgekommen. Sie hat darüber hinaus durch Manipulation der Akten versucht, ihre Pflichtverstöße zu verschleiern und eine korrekte Aufgabenerfüllung vorzutäuschen. Auf diese Weise hat sie das in sie gesetzte Vertrauen des beklagten Landes zerstört.

3. Eine auf diese Pflichtverletzungen gestützte ordentliche Kündigung ist nicht unverhältnismäßig. Einer vorherigen Abmahnung bedurfte es nicht.

a) Hätte die Klägerin die Gebührenbescheide und Mahnungen lediglich nicht bearbeitet, wäre zwar auch dies pflichtwidrig gewesen: Gerade auf der Grundlage ihrer Behauptung, sie habe die fraglichen Mülltonnen im November 2009 in Wirklichkeit abgemeldet, hätte sie sich bei der Stadt um Aufklärung des Sachverhalts und ggf. Rücknahme der Bescheide bemühen müssen; auch unter Berücksichtigung eines – behaupteten – hohen Arbeitsaufkommens

ist nicht zu erkennen, dass es ihr unmöglich gewesen wäre, bei Vorgesetzten oder Kollegen Abhilfe zumindest zu initiieren. Der Vorwurf hätte sich dann aber auf bloße Leistungsmängel beschränkt. Selbst wenn sie es – entgegen ihrer Behauptung – versäumt haben sollte, die Mülltonnen bei der Stadt rechtzeitig abzumelden, sie sich dazu aber bei Eingang des ersten oder der späteren Gebührenbescheide bekannt und gegenüber Vorgesetzten offenbart hätte, wäre ihre Pflichtwidrigkeit auf den Leistungsbereich beschränkt und nicht „unverzeihlich" gewesen. In beiden Fällen spräche vieles dafür, dass eine Kündigung mangels Abmahnung als unverhältnismäßig anzusehen wäre. So indessen hat es die Klägerin nicht beim Untätigbleiben bewenden lassen, sondern hat durch ihre manipulative Ergänzung der Akten um zwei vermeintliche Widerspruchsschreiben den Versuch einer aktiven Täuschung ihrer Vorgesetzten unternommen. Darin liegt eine nicht hinnehmbare Grenzüberschreitung. Es ist dem beklagten Land objektiv nicht zuzumuten, eine Mitarbeiterin – wenn es sich dazu denn von sich aus nicht in der Lage sieht – weiterzubeschäftigen, die bereit ist, um der Vertuschung eigener Fehler willen Akten zu manipulieren. (…)

c) Etwas anderes gilt nicht mit Blick auf die Betriebszugehörigkeit der Klägerin von mehr als dreißig Jahren. Die Klägerin hat gezeigt, dass sie bereit ist, ein sich im Laufe von gut einem Jahr im Durchschnitt alle vier bis fünf Wochen bemerkbar machendes, sich dabei insbesondere finanziell ständig verstärkendes Problem vor sich her zu „schieben", um schließlich mit Hilfe von Aktenmanipulationen ein korrektes Verhalten vorzutäuschen und von eigenen Verantwortlichkeiten und Fehlern abzulenken. Ein solcher, mit möglichst großer Heimlichkeit einhergehender Täuschungsversuch wird auch durch jahrzehntelange pflichtgemäße Aufgabenerfüllung nicht aufgewogen. Es kommt hinzu, dass die Klägerin noch im Februar 2010 zum wiederholten Male auf ihre nicht zufriedenstellende Arbeitsorganisation hingewiesen worden war und das ihr unterbreitete Fortbildungsangebot zum Stress- und Zeitmanagement abgelehnt hat.

Videoüberwachung im Eingangsbereich eines Bürogebäudes

(**Oberverwaltungsgericht Lüneburg**, Urteil vom 29. September 2014 – Az.: 11 LC 114/13 –)

1. **Der Eingangsbereich und die Treppenaufgänge zu Geschäftsräumen eines Bürogebäudes sind öffentlich zugängliche Räume im Sinn des § 6b Abs. 1 BDSG.**
2. **Die Videoüberwachung des Eingangsbereichs und der Treppenaufgänge zu den Geschäftsräumen eines Bürogebäudes durch festinstallierte Mini-dome-Kameras ohne Zoom-Funktion und die kurzfristige Speicherung der Aufnahmen im sogenannten black-box-Verfahren kann zur Wahrnehmung berechtigter Interessen – hier zur Verhinderung von Straftaten – nach § 6b Abs. 1 Nr. 3 BDSG erforderlich sein.**

Sachverhalt:

Der beklagte Landesbeauftragte für den Datenschutz Niedersachsen wendet sich mit seiner Berufung dagegen, dass das Verwaltungsgericht die von ihm gegenüber der Klägerin verfügte Ausschaltung der Videokameras der Klägerin sowie die Löschung der auf dem Videoserver gespeicherten Videobilder als rechtswidrig angesehen hat.

Die Klägerin ist Eigentümerin und Verwalterin eines mehrgeschossigen Bürogebäudes (bestehend aus Alt- und Neubau mit jeweils einem Eingang), in in dem sich unter anderem ihr Verwaltungssitz befindet. Die übrigen in dem Gebäude befindlichen Büros sind an Rechtsanwälte, Steuerberater und Wirtschaftsprüfer, Unternehmensberater sowie an eine Förderbank (G.) und andere Unternehmen (insgesamt 13) vermietet. Im Kellergeschoss befinden sich Lagerräume und Räume für Infrastruktur (Serverräume) sowie ein Getränkeautomat; dort befanden sich in der Vergangenheit zeitweise auch mehrere Stühle. Wohnräume gibt es in dem Gebäude nicht.

Nachdem am 16. Dezember 2009 aus dem Büro der im Erdgeschoss des Altbaus befindlichen Steuerberatungskanzlei H. und Partner sechs Notebooks gestohlen worden waren, brachte die Klägerin Anfang 2010 deshalb und wegen vorangegangener drei Fälle von Graffiti-Vandalismus zehn Videokameras an: im Einzelnen in den beiden Eingangsbereichen des Altbaus und des Neubaus (2), in dem ersten und zweiten Obergeschoss (OG) des Altbaus und des Neubaus (jeweils 1, insgesamt 4), in dem dritten Obergeschoss des Neubaus (1), im Vorraum des Treppenhauses im Kellergeschoss (KG) des Altbaus (1) und in den beiden dort befindlichen Serverräumen (jeweils 1). Eine weitere zunächst im Eingangsbereich zu den Büroräumen der G. installierte Kamera wurde auf Verlangen dieser Bank bereits im August 2010 deinstalliert. Die Kameras werden im sogenannten black box-Verfahren als Minidome-Videokameras betrieben, die fest installiert und fest auf einen Sichtbereich ohne Zoom-Funktion ausgerichtet sind. Sie schalten sich (nur) bei Bewegungen im Treppenhaus automatisch ein. Die Aufnahmen werden auf einer Festplatte gespeichert und automatisch überschrieben, d. h. gelöscht, wenn kein Bedarf mehr für Sichtung besteht, spätestens nach 10 Tagen. Die Videoaufnahmen können bei Bedarf auf PC-Monitore übertragen werden. Passwortgesicherten Zugang haben lediglich das Unternehmen, das die Videoanlage installiert hat, und ein von der Klägerin bestellter betrieblicher Datenschutzbeauftragter. Hinweisschilder an den beiden Eingangstüren des Gebäudes weisen in Textform und mittels eines Symbols auf die Videoüberwachung hin und benennen die verantwortliche Stelle.

Nachdem dem Beklagten die Installation der Kameras bekannt geworden war, entwickelte sich zwischen den Beteiligten ein Schriftverkehr zur Funktionsbeschreibung und zur rechtlichen Grundlage für die Videoüberwachung. Im Mai 2011 fand eine Kontrolle durch den Beklagten im Bürogebäude statt, ohne dass eine einvernehmliche Lösung gefunden werden konnte.

Daher forderte der Beklagte die Klägerin mit der streitgegenständlichen Verfügung vom 19. Oktober 2011 auf der Grundlage von § 38 Abs. 5 Satz 1 BDSG unter Androhung eines Zwangsgeldes in Höhe von 1.000 EUR auf, die sieben Videoüberwachungskameras (mit den internen Bezeichnungen: 1. OG Altbau, 2. OG Altbau, Eingang Neubau, 1. OG Neubau, 2. OG Neubau, 3. OG Neubau und KG Treppe) auszuschalten und zu deinstallieren, die im Bereich des Eingangs der Steuerberatungskanzlei betriebene Videoüberwachungskamera (interne Bezeichnung: Eingang Altbau) auszuschalten sowie die auf dem Videoserver gespeicherten Videobilder der vorgenannten Kameras zu löschen. Zur Begründung führte er im Wesentlichen an, die Anlage verstoße gegen § 4 Abs. 1 BDSG, da weder eine Einwilligung der Betroffenen noch die Voraussetzungen des § 6b BDSG gegeben seien. Als Rechtfertigung der Videoüberwachung komme das Hausrecht der Klägerin nicht in Betracht. Es fehle mit Blick auf die vorgetragenen Anlässe des Diebstahls und der Graffitis insgesamt an der Geeignetheit und Erforderlichkeit der Anlage gerade für die Klägerin als Vermieterin des Gebäudes, so dass nur die Abschaltung und Deinstallation der sieben Kameras im Treppenhaus ermessensgerecht und verhältnismäßig sei. Hinsichtlich der Kamera im

Eingangsbereich des Altbaus sei zur Zeit hingegen lediglich der weitere Betrieb zu untersagen, nicht aber die Deinstallation anzuordnen. Denn es könne nicht ausgeschlossen werden, dass angesichts des Diebstahls der Notebooks der Betrieb dieser Kamera durch die Steuerberatungskanzlei als Mieterin datenschutzrechtlich zulässig sei.

Hiergegen hat die Klägerin Klage erhoben, zu deren Begründung sie unter Vorlage der von ihr eingeholten gutachterlichen Stellungnahme von Prof. Dr. J. I. vom 6. Oktober 2011 im Wesentlichen geltend gemacht hat, dass die von dem Beklagten verfügten Maßnahmen nicht von der Ermächtigung des § 38 Abs. 5 Satz 1 BDSG gedeckt seien. Bis auf die G. seien alle Mieter des Bürogebäudes mit der Videoüberwachung einverstanden. Ein Verstoß gegen § 6b BDSG liege nicht vor. Nach Geschäftsschluss sei das gesamte Gebäude nicht mehr öffentlich zugänglich. Auch während der Öffnungszeiten seien keine Persönlichkeitsrechte von Besuchern oder Mitarbeitern verletzt. Von der Videoüberwachung werde nur ein sehr beschränkter Personenkreis betroffen, der sich nur kurz dort aufhalte. Die Videoüberwachung sei zur Wahrnehmung des Hausrechts und zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke erforderlich. Es sei bereits zu Diebstählen gekommen, vor denen die Mieter geschützt werden müssten. Das Kellergeschoss sei nicht öffentlich zugänglich und solle von Besuchern nicht aufgesucht werden. Das black box-Verfahren sei ein sehr schonendes Überwachungsverfahren. Die streitgegenständlichen Maßnahmen des Beklagten seien unverhältnismäßig. Dieser hätte geringere Eingriffe, etwa die zeitliche Beschränkung der Videoüberwachung, wählen können und müssen. Er habe sein Ermessen falsch ausgeübt.

Mit Urteil vom 12. März 2013 (juris), auf das wegen der Einzelheiten verwiesen wird, hat das Verwaltungsgericht den angefochtenen Bescheid des Beklagten aufgehoben und zur Begründung im Wesentlichen ausgeführt, zum einen sei die Beseitigung der Kameras als technische Einrichtung von der allein in Betracht kommenden Rechtsgrundlage des § 38 Abs. 5 Sätze 1 und 2 BDSG nicht als Rechtsfolge vorgesehen. In inaktivem Zustand seien die ausgeschalteten Kameras als sogenannte Dummies nicht rechtswidrig, weil ein „Beobachten" im Sinne des § 6b BDSG nicht gegeben sei und mithin Daten nicht erhoben würden.

Aus den Gründen:

Die Berufung des Beklagten hat keinen Erfolg.

Im Berufungsverfahren sind aufgrund des eingeschränkten Berufungsantrages des Beklagten lediglich die Fragen, ob dieser in seiner streitgegenständlichen Verfügung vom 19. Oktober 2011 zu Recht die Ausschaltung der acht Videokameras und die Löschung der auf dem Videoserver gespeicherten Videobilder dieser Kameras angeordnet hat, zu beantworten. Nicht entscheidungserheblich in der Berufungsinstanz ist demgegenüber die – von dem Verwaltungsgericht in den Vordergrund seiner Ausführungen gerückte – Frage, ob der Beklagte von der Klägerin zu Recht die Deinstallation der Videokameras fordern kann.

Die eingeschränkte Berufung des Beklagten ist unbegründet. Die in der streitgegenständlichen Verfügung angeordnete Ausschaltung der acht Videokameras mit den Bezeichnungen Eingang Altbau, 1. OG Altbau, 2. OG Altbau, Eingang Neubau, 1. OG Neubau, 2. OG Neubau, 3. OG Neubau und KG Treppe sowie die auf diese Kameras bezogene Forderung des Beklagten auf Löschung der gespeicherten Daten sind rechtswidrig und verletzen die Klägerin in ihren Rechten (§ 113 Abs. 1 Satz 1 VwGO).

Rechtsgrundlage für die von dem Beklagten geforderte Ausschaltung der Videokameras in dem Bürogebäude der Klägerin ist § 38 Abs. 5 BDSG. Nach Satz 1 dieser Bestimmung kann die Aufsichtsbehörde zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Gemäß Satz 2 dieser Norm kann sie zudem bei schwerwiegenden Verstößen oder Mängeln die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel nicht in angemessener Zeit beseitigt werden. Diese Voraussetzungen sind hier nicht gegeben. Der Beklagte ist zwar gemäß § 38 Abs. 6 BDSG in Verbindung mit § 22 Abs. 1 Satz 1 NDSG Aufsichtsbehörde, der Betrieb der acht streitgegenständlichen Videokameras in dem Bürogebäude steht aber im Ergebnis in Einklang mit datenschutzrechtlichen Bestimmungen.

Ein Verstoß der Klägerin gegen datenschutzrechtliche Bestimmungen wegen des Betriebs der streitgegenständlichen Kameras und der Speicherung der auf diese Weise gesammelten Daten liegt nicht vor. Das Bundesdatenschutzgesetz ist anwendbar (dazu I.), den Anforderungen des § 6b BDSG ist Genüge getan (dazu II.).

I. Die Videoüberwachung in dem Geschäfts- und Bürogebäude der Klägerin und die Speicherung der dabei gewonnenen Daten unterfällt dem Regelungsregime des Bundesdatenschutzgesetzes.

Das Bundesdatenschutzgesetz ist anwendbar, wenn personenbezogene Daten Gegenstand einer vom Gesetz geregelten Phase der Datenverarbeitung sind. Nach § 1 Abs. 2 Nr. 3 BDSG gilt dieses Gesetz für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person; letztere wird als Betroffener legaldefiniert. Automatisierte Verarbeitung wird in § 3 Abs. 2 BDSG als Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen bezeichnet. Nicht-öffentliche Stellen sind gemäß § 2 Abs. 4 Satz 1 BDSG neben natürlichen auch juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, die nicht hoheitliche Aufgaben wahrnehmen. Diese Voraussetzungen sind hier gegeben.

Fotos und Videoaufnahmen im Rahmen einer Videoüberwachung sind grundsätzlich personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG. Der Personenbezogenheit von Videoaufnahmen steht insbesondere nicht entgegen, dass im Fall der Überwachung öffentlich zugänglicher Räume regelmäßig nur ein ganz geringer Prozentsatz des Bildmaterials tatsächlich zur Identifizierung von Personen genutzt wird. Entscheidend ist, dass der Zweck der Videoüberwachung gerade darin besteht, die auf den Bildern festgehaltenen Personen zu identifizieren, wenn die für die Verarbeitung Verantwortlichen dies für erforderlich halten (Buchner, in: Taeger/Gabel, BDSG, 2. Aufl. 2014, § 3 Rn. 7, 19; Dammann, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 4, 66). Diese personenbezogenen Daten werden mittels einer Datenverarbeitungsanlage von der Klägerin als nicht-öffentliche Stelle im Sinne des § 2 Abs. 4 Satz 1 BDSG erhoben und bei Bedarf verarbeitet und genutzt. Daher ist die Klägerin die für die Videoüberwachung verantwortliche Stelle gemäß § 3 Abs. 7 BDSG.

II. Die Videoüberwachung und die Speicherung des dabei gewonnenen Bildmaterials durch die Klägerin stehen in Einklang mit den datenschutzrechtlichen Bestimmungen.

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Ungeachtet der Frage, ob dieser

„Verarbeitungsrahmen" (so etwa Sokol, in: Simitis, a.a.O., § 4 Rn. 3) im rechtstechnischen Sinn als klassisches „Verbot mit Erlaubnisvorbehalt" charakterisiert werden kann, bedarf die Datenerhebung und -verarbeitung einer besonderen Rechtfertigung entweder in Form einer wirksamen Einwilligung durch den Betroffenen (dazu 1.) oder durch eine Rechtsvorschrift (dazu 2.).

1. Eine wirksame Einwilligung, die den Anforderungen des § 4a Abs. 1 BDSG genügt, durch die von der Videoüberwachung und -speicherung der Klägerin Betroffenen liegt nicht vor.

Von der Videoüberwachung betroffen sind alle diejenigen Personen, die das Büro- und Geschäftsgebäude der Klägerin betreten und allein durch das Betreten des Gebäudes in das Blickfeld der Videokameras gelangen. Art. 2 lit. h) EG-DSRl – deren Umsetzung in nationales Recht § 4a BDSG dient – definiert die Einwilligung der betroffenen Person als jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden. Eine derartige Willensbekundung der Betroffenen ist hier nicht gegeben. Zwar weist die Klägerin in den Eingangsbereichen des Gebäudes auf Schildern auf die Videoüberwachung hin. Daraus kann indes nicht die Schlussfolgerung gezogen werden, dass jeder Betroffene allein durch das Betreten des Gebäudes konkludent in die Datenerhebung und -verarbeitung seiner Bildaufnahme einwilligt. Eine pauschale Einwilligung ist nicht wirksam. Zudem kann es bei Betroffenen an der erforderlichen Einwilligungsfähigkeit fehlen, etwa bei Kindern bis zur Vollendung des 14. Lebensjahres.

Schließlich kommt eine mutmaßliche Einwilligung nur ausnahmsweise dort in Betracht, wo der Gesetzgeber in einer dem Bundesdatenschutzgesetz vorgehenden Regelung diese Möglichkeit ausdrücklich zulässt. Solche auch eine mutmaßliche Einwilligung vorsehenden Vorschriften existieren mitunter für öffentliche Stellen (vgl. etwa § 14 Abs. 2 Nr. 3 BDSG und § 7 Abs. 2 Nr. 2 AsylVfG), sie beziehen sich aber nicht auf den hier vorliegenden Lebenssachverhalt. Daher verbleibt es bei dem allgemeinen Grundsatz, dass eine konkludente, stillschweigende oder mutmaßliche Einwilligung nicht ausreicht (Simitis, in: Simitis, a.a.O., § 4a Rn. 44 m.w.N.).

2. Die von der Klägerin vorgenommene Videoüberwachung mittels der acht Kameras und die gleichzeitige Speicherung der erhobenen Bilddaten ist durch die gesetzliche Norm des § 6b BDSG gerechtfertigt.

§ 6b BDSG verdrängt für die hier vorliegende Videoüberwachung öffentlich zugänglicher Räume als abschließende lex specialis (bereichsspezifische Vorschrift, vgl. hierzu Simitis, in: Simitis, a.a.O., § 28 Rn. 5) die allgemeinere Vorschrift des § 28 BDSG. Die – selbst für Sachkundige schwer verständliche (so Taeger, in: Taeger/Gabel, a.a.O., § 6b Rn. 2 ff. und Simitis, in: Simitis, a.a.O., § 6b Rn. 3, jeweils m.w.N.) – Vorschrift des § 28 Abs. 1 Nr. 2 BDSG betrifft zudem lediglich unter anderem die Erhebung und Speicherung personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke. Die Klägerin als Eigentümerin und Verwalterin des Bürogebäudes und Vermieterin der Büroräume verfolgt mit der Videoüberwachung gegenüber den Betroffenen keine eigenen Geschäftszwecke.

Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) unter näher definierten alternativen Voraussetzungen zulässig (§ 6b Abs. 1 BDSG). Die Verarbeitung und Nutzung derartiger Daten ist dabei unter in Abs. 3 dieser Vorschrift näher bestimmten Bedingungen erlaubt. Ungeachtet der Frage, ob § 6b BDSG systemkonform ist (vgl. hierzu etwa Gola/Schomerus, BDSG, 11. Aufl. 2012, § 6b Rn. 3 m.w.N.), bestimmt diese Vorschrift in Abs. 1 die materiell-rechtlichen Voraussetzungen für eine zulässige Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen und regelt in Abs. 3 unter inhaltlicher Wiederholung dieser Voraussetzungen die Verarbeitung und Nutzung der im Wege dieser Videoüberwachung erhobenen Daten. Die Absätze 2 und 4 dieser Vorschrift ergänzen diese Bestimmungen durch verfahrensrechtliche Regelungen zur Sicherstellung der Transparenz für die von der Videoüberwachung Betroffenen, während Abs. 5 eine gesonderte Regelung zur Löschung derartig gespeicherter Daten enthält.

Diese Norm ist verfassungsrechtlich unbedenklich (dazu a), und die Voraussetzungen im Einzelfall liegen vor (dazu b).

a) Der Senat teilt die einzelnen in der Literatur geäußerten Bedenken an der Verfassungsmäßigkeit des § 6b BDSG nicht. Diese Bedenken werden im Hinblick auf die aus dem Rechtsstaatsprinzip und speziell der verfassungsmäßigen Schranke des Rechts auf informationelle Selbstbestimmung abgeleiteten Gebote der Normenklarheit und Bestimmtheit geäußert (so etwa Scholz, in: Simitis, a.a.O., § 6b Rn. 32 m.w.N.). Der Kritik ist zwar zuzugeben, dass diese Norm insbesondere mit den Begriffsmerkmalen der Wahrnehmung berechtigter Interessen und der Erforderlichkeit sowie des Überwiegens schutzwürdiger Interessen der Betroffenen unbestimmte Rechtsbegriffe enthält. Es reicht aber nach der ständigen Rechtsprechung des Bundesverwaltungsgerichtes aus, wenn die Präzisierung mit Hilfe der üblichen Auslegungsmethoden möglich ist (vgl. hierzu etwa BVerwG, Urt. v. 25.1.2012 – BVerwG 6 C 9.11 –, BVerwGE 141, 329, NordÖR 2012, 413, juris Rn. 38 ff, und vorgehend OVG Hamburg, Urt. v. 22.6.2010 – 4 Bf 276/07 –, NordÖR 2010, 498 m.w.N.). Letzteres ist hier – wie sich aus den nachfolgenden Ausführungen ergibt – der Fall.

b) Die Videoüberwachung der Klägerin unterfällt dem Regelungsgehalt des § 6b BDSG, dessen Anforderungen sie sowohl hinsichtlich der Erhebung der Daten (§ 6b Abs. 1 BDSG) als auch hinsichtlich deren Verarbeitung und Nutzung (§ 6b Abs. 3 BDSG) genügt.

aa) Die Videoüberwachung erfüllt das Merkmal des „Beobachtens" im Sinne des § 6b BDSG.

Unter diesem Merkmal ist die Sichtbarmachung von Geschehnissen und Personen mit Hilfe dazu geeigneter technischer Einrichtungen von einer gewissen Dauer – und damit eine Form des Überwachens – zu verstehen, wobei streitig ist, ob auch bloße Kamera-Monitor-Systeme als „verlängertes Auge" ohne nachfolgende Aufzeichnung oder Auswertung des Bildmaterials hierunter fallen (vgl. bejahend Scholz, in Simitis, a.a.O., § 6b Rn. 63 ff., Zscherpe, in: Taeger/Gabel, a.a.O., § 6b Rn. 17 ff.; zweifelnd Gola/Schomerus, a.a.O., § 6b Rn. 10, jeweils m.w.N). Da im vorliegenden Fall die Bildaufzeichnungen für einen bestimmten Zeitraum in Form des black box-Verfahrens gespeichert werden, um die Möglichkeit der anlassbezogenen nachträglichen Inaugenscheinnahme der gespeicherten Videoaufnahmen zu gewährleisten, liegt ein Beobachten in diesem Sinne unzweifelhaft vor.

Ebenso ist das Merkmal des Erhebens personenbezogener oder zumindest personenbeziehbarer Daten (zu diesem Erfordernis vgl. etwa Scholz, in: Simitis, a.a.O., § 6b Rn. 66 m.w.N.) erfüllt. Denn für die Bestimmbarkeit und spätere Identifizierung einer Person reicht neben den erkennbaren Gesichtszügen auch das sonstige Körperbild, etwa die Körperhaltung, die Kleidung oder mitgeführte Gegenstände aus. Auf eine tatsächlich erfolgreiche Identifizierung in jedem Einzelfall kommt es in diesem Zusammenhang nicht an (Scholz, in: Simitis, a.a.O., § 6b Rn. 67 m.w.N.).

bb) Das Bürogebäude der Klägerin ist als öffentlich zugänglicher Raum im Sinne des § 6b Abs. 1 BDSG anzusehen. Hierunter fallen alle Bereiche, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können und ihrem Zweck nach auch dazu bestimmt sind (Scholz, in: Simitis, a.a.O., § 6b Rn. 42 m.w.N.). Hier ergibt sich die Zweckbestimmung aus dem erkennbaren Willen der Klägerin als Eigentümerin des Gebäudes und ihrer gewerblichen Mieter als Berechtigte, dass sowohl die Beschäftigten als auch die Kunden und Klienten der in dem Bürogebäude befindlichen Betriebe und Kanzleien sowie etwaige Zulieferer freien Zugang zu dem Gebäude erhalten sollen. Daher sind alle Räume, die von der Videoüberwachung betroffen sind, als öffentlich zugänglicher Raum zu betrachten.

Dies gilt neben den Eingangsbereichen und den Treppenhäusern und Obergeschossen auch für den Vorraum des Treppenhauses im Kellergeschoss. Dieser Vorraum befindet sich zwar im Kellergeschoss, in dem keine Büroräume vorhanden sind, so dass zumindest Kunden und Gäste nach dem Willen der Berechtigten keinen freien Zugang hierzu erhalten sollen. Da sich in diesem Vorraum aber unter anderem Lagerräume und ein Getränkeautomat befinden, haben nach den genannten Kriterien jedenfalls die Inhaber der gewerblichen Betriebe und Kanzleien sowie deren Beschäftigte und gegebenenfalls deren Zulieferer freien Zugang in diesen ebenfalls videoüberwachten Bereich. Eine derart eingeschränkte Zugänglichkeit für eine näher bestimmbare Personenzahl reicht für das Merkmal des öffentlich zugänglichen Raums aus. Etwas anderes könnte gelten, wenn der Vorraum im Kellergeschoss nach den objektiven Gegebenheiten eindeutig gegen Publikumsverkehr abgegrenzt ist; hieran fehlt es. Zudem lässt sich aus dem Umstand, dass zumindest in der Vergangenheit neben dem Getränkeautomat mehrere Stühle aufgestellt waren, die Schlussfolgerung ziehen, dass nach dem mutmaßlichen Willen der Berechtigten auch dieser Bereich einer eingeschränkten Öffentlichkeit zugänglich sein soll.

Es ist unerheblich, dass das Geschäfts- und Bürogebäude der Klägerin nur zu den branchenüblichen Sprech- und Öffnungszeiten geöffnet und außerhalb dieser Zeiten verschlossen ist. Aufgrund der Eigenart und Struktur der in dem Gebäude befindlichen Kanzleien und sonstigen Unternehmen kann es durchaus vorkommen, dass auch außerhalb der üblichen Bürozeiten in den Abendstunden oder am Wochenende – wenn auch im eingeschränkten Umfang – Besprechungstermine mit Klienten, Mandanten und Kunden vereinbart werden und mithin Publikumsverkehr stattfinden kann. Das Gebäude ist deshalb auch außerhalb der üblichen Öffnungszeiten als öffentlich zugänglicher Raum anzusehen.

cc) Die Videoüberwachung im öffentlich zugänglichen Teil des Gebäudes der Klägerin ist nach § 6b Abs. 1 Nr. 2 (Wahrnehmung des Hausrechts) und Nr. 3 BDSG (Wahrnehmung berechtigter Interessen) gerechtfertigt und für diese Zwecke erforderlich.

(a) Das Hausrecht, auf das sich auch nicht-öffentliche Stellen wie die Klägerin berufen können, beinhaltet die Befugnis, darüber zu entscheiden, wer ein Gebäude betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen, d. h. Störer zu verweisen und ihnen das Betreten für die Zukunft zu untersagen, mithin ein Hausverbot auszusprechen. Eine Beobachtung zur Wahrnehmung des Hausrechts dient sowohl einem präventiven als auch einem repressiven Zweck, indem zum einen Straftaten durch Abschreckung verhindert und zum anderen die Strafverfolgung durch die Auswertung des aufgenommenen Bildmaterials zum Zweck der Beweissicherung ermöglicht werden. Inhaber des Hausrechts können mehrere Personen sein – etwa der Eigentümer des Objekts und seine Mieter (vgl. hierzu Scholz, in: Simitis, a.a.O., § 6b Rn. 73 ff. m.w.N.).

Im vorliegenden Fall kann sich die Klägerin auf das ihr zustehende Hausrecht in den videoüberwachten Bereichen des Bürogebäudes berufen. Sie hat wegen ihrer Stellung als Eigentümerin und Verwalterin des Gebäudes zum einen ein Interesse daran, ihr (eigenes) Eigentum zu schützen und unberechtigte Personen vom Betreten des Gebäudes fernzuhalten. Zugleich hat sie zum anderen aber auch ein eigenes Interesse daran, dass die Mieter der Büroräume als ihre Vertragspartner in ihrem Gebäude nicht durch unberechtigte Personen zu Schaden kommen. Auf die Fragen, in welchem Verhältnis die Interessen des Eigentümers auf der einen und der obligatorisch berechtigten Mieter auf der anderen Seite zueinander stehen und wie ein etwaiger Interessenkonflikt zwischen diesen Seiten auszugleichen ist, braucht anlässlich des vorliegenden Falles nicht eingegangen zu werden. Denn die Klägerin beschränkt die Videoüberwachung auf die allgemein öffentlich zugänglichen Räumlichkeiten, die von der Vermietung nicht mit umfasst sind, ohne sie auf die Büroräume der Mieter auszudehnen. Zudem hat sie diese vom – wenn auch erst nachträglichen eingeholten – Einverständnis ihrer Mieter abhängig gemacht (vgl. zu diesem Erfordernis etwa AG Tempelhof-Kreuzberg, Urt. v. 6.1.2009 – 12 C 155/08 –, juris). Im Fall fehlenden Einverständnisses – wie bei der G. – hat sie die Videokamera abgebaut.

(b) Zusätzlich kann sich die Klägerin auf den Zulässigkeitstatbestand der Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke berufen. Als derartiges Interesse gilt nicht nur ein rechtliches, sondern jedes tatsächliche Interesse, das auch wirtschaftlicher oder ideeller Art sein kann, wobei es objektiv begründbar sein und sich aus der konkreten Sachlage heraus ergeben muss. Bei dem Einsatz von Videotechnik zum Zweck der Gefahrenabwehr ist regelmäßig von der Wahrnehmung berechtigter Interessen auszugehen (Scholz, in: Simitis, a.a.O., § 6b Rn. 79 m.w.N.).

Die Klägerin kann sich zwar nicht auf eine abstrakte Gefahrenlage berufen, da in ihrem Fall nicht eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist. Ihr Bürogebäude liegt – soweit ersichtlich – nicht in einer Gegend mit potentiell gefährdeten Bereichen, wie dies etwa bei Einkaufszentren, Kaufhäusern und weitläufigen und schwer einsehbaren Geschäftsräumen wie etwa Selbstbedienungsläden der Fall ist. Auch die in dem Bürogebäude befindlichen Kanzleien und Betriebe gehören nicht zu potentiell stark gefährdeten Einrichtungen, die typischerweise Opfer von Straftaten wie Einbruchsdiebstählen oder Überfällen werden, wie dies etwa bei Tankstellen und Juwelierläden angenommen werden kann. Etwas anderes gilt nicht deshalb, weil das Gebäude in der Nähe einer Autobahnauffahrt und in einem Gewerbegebiet liegt. Eine Videoüberwachung mit dem Ziel einer allgemeinen abstrakten Gefahrenvorsorge reicht nicht aus.

Die Klägerin kann sich aber auf eine konkrete Gefährdungslage berufen (zu dieser Alternative vgl. Scholz, in: Simitis, a.a.O., § 6b Rn. 80). Diese konkrete Gefährdungslage ergibt sich zwar nicht mit hinreichender Sicherheit aus dem Gesichtspunkt der Verunstaltung des Gebäudes mit Graffitis. Derartige Schmierereien sind in der Vergangenheit lediglich an der Außenfassade des Gebäudes, nicht aber innerhalb des Gebäudes, in der sich die Videokameras befinden, angebracht worden. Die Klägerin hat aber zutreffend darauf hingewiesen, dass in jüngerer Vergangenheit aus den Büros der in

dem Gebäude befindlichen Steuerberatungsgesellschaft mehrere wertvolle Notebooks und aus dem Kellergeschoss dort lagernde Paletten gestohlen worden sind. Die aufgrund der Abschreckungswirkung mögliche Verhinderung von Straftaten zum Nachteil des Eigentümers des überwachten Objekts und der Vertragspartner und die Sicherung von Beweismaterial zur Aufklärung von begangenen Straftaten stellen ein berechtigtes Interesse dar. Die zu fordernde objektive Begründbarkeit des berechtigten Interesses liegt vor, wenn sie sich auf konkrete Tatsachen stützen kann, aus denen sich der zu erwartende Eintritt einer Gefahr ergibt (Scholz, in: Simitis, a.a.O., § 6b Rn. 79). Ein solcher Fall ist hier gegeben. In diesem Zusammenhang ist zu berücksichtigen, dass sich in den unter anderem an diverse Kanzleien und Steuerberatungsbüros vermieteten Räumen des Bürogebäudes sensible schützenswerte Daten der Kunden dieser Unternehmen befinden. In strafrechtlicher Hinsicht unterliegt die Videoaufnahme, die den Täter beim Diebstahl filmt, keinem Verwertungsverbot (vgl. hierzu etwa BayObLG, Beschl. v. 24.1.2002 – 2 St RR 8/02 –, NJW 2002, 2893). Die Bedenken des Beklagten hinsichtlich des Vorliegens dieser konkreten Gefährdungslage teilt der Senat nicht.

Die Klägerin hat die Zwecke der Videoüberwachung (hier: Verhinderung von Straftaten und Sicherung von Beweismaterial zur Aufklärung begangener Straftaten) in der von dem betrieblichen Datenschutzbeauftragten erstellten Verfahrensübersicht vom 8. September 2011 konkret schriftlich dargelegt und ist dadurch den Anforderungen des § 4e Satz 1 Nr. 4 BDSG hinreichend nachgekommen. Durch dieses Erfordernis soll die verantwortliche Stelle zu einer sorgfältigen Prüfung der Rechtmäßigkeit der Videoüberwachung veranlasst werden (Scholz, in: Simitis, a.a.O., § 6b Rn. 82 ff.).

(c) Die seitens der Klägerin durchgeführte Videoüberwachung in dem Bürogebäude und die Speicherung der Aufnahmen ist für die Erreichung der dargestellten Zwecke der Wahrnehmung ihres Hausrechts und ihrer berechtigten Interessen erforderlich. Dies betrifft sowohl das „Ob" als auch das „Wie" des Einsatzes der Videotechnik.

Die Erforderlichkeit im Sinne des § 6b BDSG setzt voraus, dass das festgelegte Ziel mit der Überwachung tatsächlich erreicht werden kann und es dafür kein anderes, gleich wirksames, aber mit Blick auf das Grundrecht der informationellen Selbstbestimmung der betroffenen Personen weniger einschneidendes, Mittel gibt. Diese Bewertung hat ausgehend von einer objektiven Betrachtungsweise im Rahmen einer Einzelfallprüfung zu erfolgen (Scholz, in: Simitis, a.a.O., § 6b Rn. 86 m.w.N.).

Die Videoüberwachung (Beobachtung und Speicherung) ist zur Abschreckung von Störern und Straftätern (grundsätzlich) geeignet, da der Umstand der Überwachung durch die Hinweisschilder in hinreichendem Umfang erkennbar ist. Sie kann auch im Nachhinein einen hinreichend sicheren Rückschluss auf die verantwortlichen Störer und Täter liefern. Die aufgezeichneten Bilder sind für eine spätere Identifizierung von ausreichender Qualität und werden für einen bestimmten Zeitraum zum Zweck der Auswertung gespeichert. Die Eignung der Bilder für Vorgänge zur Abend- und Nachtzeit mag zwar eingeschränkt sein. Entscheidend ist aber, dass eine Maßnahme nicht nur dann zu einem bestimmten Zweck geeignet ist, wenn dieser mit ihrer Hilfe vollständig erreicht werden kann. Ausreichend ist vielmehr bereits ihre Eignung, diesen Zweck zu fördern (Scholz, in: Simitis, a.a.O., § 6b Rn. 87 m.w.N.). Diese Eignung kommt den Bildern auch bei schlechten Sichtverhältnissen zu.

Mildere, gleich wirksame Mittel zur Zweckerreichung sind nicht erkennbar. Als Alternative zur Videoüberwachung kommt der Einsatz von Wachpersonal in Betracht. Es ist aber bereits fraglich, ob ein derartiger Einsatz in gleicher Weise geeignet ist, die gewünschten Zwecke zu erreichen. Das Wachpersonal kann nicht zu jeder Zeit an allen überwachten Orten zugleich sein. Zudem sähen sich die Bediensteten, Kunden und Mandanten der in dem Bürogebäude ansässigen Kanzleien und Unternehmen einer permanenten Beobachtung durch Wachleute ausgesetzt, die sich gegenüber der Videoüberwachung als ein subjektiv gravierenderer Eingriff darstellt. Schließlich sind die Kosten für den Einsatz von Wachpersonal gegenüber dem Betrieb einer Videoanlage ungleich höher und damit wirtschaftlich nicht vertretbar. Gesichtspunkte, die gegen die Erforderlichkeit der von der Klägerin konkret gewählten Art der Videoüberwachung und damit gegen das „Wie" des Einsatzes der Videotechnik sprechen, sind nicht ersichtlich.

Als milderes Mittel käme zum einen die Beschränkung der Videoüberwachung auf die Zeiträume in Betracht, in denen ein Publikums- und Beschäftigtenverkehr in dem Bürogebäude im Allgemeinen nicht stattfindet. Dies sind vor allem die Abend- und Nachtstunden und die Zeiten der gesetzlichen Feier- und Sonntage. Es ist aber nicht von der Hand zu weisen, dass eine Videoüberwachung zu den genannten Zwecken auch während der Zeiträume, in denen das Gebäude öffentlich zugänglich ist, erforderlich ist. Denn auch während dieser Zeiträume kann es – angesichts der dann freien Zugänglichkeit des Gebäudes sogar mit einer höheren Wahrscheinlichkeit – zu Diebstählen oder anderen Straftaten kommen, so dass in zeitlicher Hinsicht eine Videoüberwachung des Gebäudes „rund um die Uhr" erforderlich ist.

In räumlicher Hinsicht käme zum anderen die Beschränkung der Videoüberwachung allein auf die beiden Eingangsbereiche in Betracht. Da potentielle Störer und Straftäter aber unberechtigterweise auch auf anderen Wegen, beispielsweise über stets verschlossene weitere Türen oder insbesondere durch Fenster, in das Gebäude gelangen können, bedarf es der Überwachung mithilfe der weiteren Videokameras in den übrigen Bereichen. Zudem sind die Aufzeichnungen der weiteren Videokameras geeignet und erforderlich, um den potentiellen Täterkreis weiter einzuengen.

Da die Klägerin mit der Videoüberwachung nicht ausschließlich präventive Zwecke (zur Abschreckung), sondern nach dem oben Gesagten zusätzlich in zulässiger Weise den repressiven Zweck der Aufklärung etwaiger Straftaten verfolgt, bedarf es gemäß § 6b Abs. 3 Satz 1 BDSG nicht nur der Beobachtung, sondern auch der Aufzeichnung und Speicherung der Daten. Ohne Speicherung der Aufnahmen wäre es der Klägerin nicht möglich, im Nachhinein auf das Bildmaterial zuzugreifen, um sich mit dessen Hilfe bei in dem Bürogebäude begangenen Straftaten einen Überblick über mögliche Täter zu verschaffen. Bedenken hinsichtlich des räumlichen Umfangs der Überwachung bestehen nicht, weil die Videoanlage weder über einen Schwenkmechanismus noch über eine Zoomfunktion verfügt und Bereiche außerhalb des Gebäudes und innerhalb der vermieteten Büroräume nicht erfasst werden. Gleiches gilt hinsichtlich der Verfahrensabläufe, da der Zugriff auf die Beobachtungseinrichtungen hinreichend eingeschränkt und gesichert ist.

dd) Anhaltspunkte für das Überwiegen schutzwürdiger Interessen der Betroffenen sind nicht gegeben.

Die Interessenprüfung gemäß § 6b Abs. 1 und 3 BDSG erfordert eine am Verhältnismäßigkeitsgrundsatz orientierte umfassende Abwägung zwischen den durch die Zwecke der Videoüberwachung bestimmten grundrechtlich geschützten Positionen der Anwender von Videotechnik und den Interessen derjenigen, die Objekt der Videoüberwachung und -speicherung sind. Bei der Abwägung sind

auf Seiten der verantwortlichen Stelle insbesondere die Zwecksetzung der Beobachtung sowie die sie begleitenden Umstände (vor allem deren technische Ausgestaltung) zu beachten, während auf Seiten der von der Überwachung betroffenen Personen in erster Linie das allgemeine Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seinen Ausprägungen als Recht der informationellen Selbstbestimmung, des Rechtes am eigenen Bild sowie des Schutzes der Privatsphäre von Bedeutung ist (Zscherpe, in: Taeger/Gabel, a.a.O., § 6b Rn. 53; Scholz, in: Simitis, a.a.O., § 6b Rn. 23 und 92, jeweils m.w.N.). Hierbei sind alle Gesamtumstände des Einzelfalls maßgeblich. Der Frage der Eingriffsintensität kommt eine entscheidende Bedeutung zu. Das Gewicht des Eingriffs wird maßgeblich durch Art und Umfang der erfassten Informationen, durch Anlass und Umstände der Erhebung, den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt. Je stärker das Maß der Beeinträchtigung durch die Überwachungsmaßnahme ist, desto schutzwürdiger sind die Interessen der betroffenen Personen. Hinsichtlich des allgemeinen Persönlichkeitsrechts ist zwischen drei Sphären zu unterscheiden, innerhalb derer das Persönlichkeitsrecht betroffen sein kann: die Individualsphäre, die Privatsphäre und die Intimsphäre (zu dieser Unterscheidung vgl. etwa LG München I, Urt. v. 21.10.2011 – 20 O 19879/10 –, juris, Rn. 27 m.w.N.). Ein Überwiegen der Interessen der Betroffenen muss dabei nicht positiv festgestellt werden, es reicht aus, wenn Anhaltspunkte für ein Überwiegen dieser Interessen nicht ausgeräumt sind (Scholz, in: Simitis, a.a.O., § 6b Rdrn. 92 ff. m.w.N.). Dabei ist zu berücksichtigen, dass nach der Wertung des Gesetzgebers die Videoüberwachung und -speicherung auch durch nichtöffentliche Stellen im öffentlich zugänglichen Bereich zu den genannten – hier gegebenen – Zwecken grundsätzlich zulässig ist und „lediglich" unter dem genannten Vorbehalt steht.

Nach diesen Grundsätzen sind im vorliegenden Fall Anhaltspunkte für ein Überwiegen der schutzwürdigen Interessen der von der Videoüberwachung der Klägerin betroffenen Personen nicht ersichtlich. Hierbei fällt insbesondere ins Gewicht, dass die Klägerin eine Überwachungstechnik einsetzt, die die Persönlichkeitsrechte der Betroffenen nicht tangiert. Die Videokameras werden als sogenannte Mini dome-Kameras betrieben, die fest installiert und auf einen Sichtbereich ohne Zoom-Funktion ausgerichtet sind. Schwenkbewegungen, die die Bewegungen der beobachteten Personen im Raum nachvollziehen, sind nicht möglich. Ebenso wenig ist es möglich, Einzelheiten der beobachteten Personen, insbesondere Gesichtskonturen, näher in den Blick zu nehmen. Daher erfassen die Videokameras weniger als ein aufmerksamer Beobachter (vgl. zu diesem Kriterium XVI. Bericht über die Tätigkeit des Nds. Landesbeauftragten für den Datenschutz, Drs. 14/4000, S. 41 f.). Die von den Kameras überwachten Örtlichkeiten dienen nicht einem längeren Verweilen, etwa zum Zweck einer Kommunikation mit Dritten, sondern die Betroffenen gelangen lediglich für einen sehr kurzen Zeitraum (hierbei dürfte es sich meistens lediglich um Sekunden handeln) in das Blickfeld der Kameras. Bewegungs- und Verhaltensprofile einzelner beobachteter Personen können aufgrund der Videoüberwachung nicht erstellt werden. Es werden keine Einblicke in höchstpersönliche Bereiche der Intim- und Privatsphäre – wie dies etwa bei der Überwachung von Toiletten, Umkleidekabinen, Duschen, Saunen, ärztlichen Behandlungsräumen oder Privaträumen und Gastronomiebetrieben (vgl. zu letzterem etwa AG Hamburg, Urt. v. 22.4.2008 – 4 C 134/08 –, juris) der Fall wäre – und keine Einblicke in Arbeitsbereiche der in dem Bürogebäude der Klägerin tätigen Beschäftigten ermöglicht (zur Frage der <heimlichen> Videoüberwachung am Arbeitsplatz vgl. EGMR, Entscheidung v. 5.10.2010 – 420/07 <Köpke> –, EuGRZ 2011, 471; BAG, Urt. v. 21.6.2012 – 2 AZR 153/11 –, NJW 2012, 3594; ArbG Düsseldorf, Beschl. v. 29.4.2011 – 9 BV 183/10 –, juris). Eine andere Einschätzung ist nicht deshalb gerechtfertigt, weil in der Vergangenheit neben dem Getränkeautomaten im Kellergeschoss einige Stühle aufgestellt waren. Die seinerzeit dort befindlichen Stühle dienten jedenfalls angesichts der wenig einladenden Umgebung im Kellergeschoss offensichtlich nicht einem längeren Verweilen. Die Tatsache der Videoüberwachung wird offengelegt, so dass eine heimliche Vornahme der Überwachungsmaßnahme, die besonders schwerwiegend in die Rechte der betroffenen Personen eingreifen kann, nicht gegeben ist. Es ist deshalb insgesamt nicht ersichtlich, dass durch die Beobachtung ein erhöhter Anpassungsdruck bei den Betroffenen erzeugt wird.

Hinzu kommt, dass die Videoaufnahmen nicht auf einen Monitor übertragen werden, an dem Überwachungspersonen zur ständigen und sofortigen Auswertung der Bilder sitzen. Die Bildaufnahmen werden vielmehr im sogenannten black box-Verfahren auf einen Server geleitet und in der Regel nach einer bestimmten Zeit ohne jede Auswertung durch Überschreiben der digital gespeicherten Daten wieder gelöscht. Lediglich wenn ein Ereignis eintritt, das den oben genannten Zwecken des Hausrechts und der berechtigten Interessen der Klägerin als Hauseigentümerin und ihrer Mieter zuwiderläuft, erfolgt eine Sichtung des aufgenommenen Bildmaterials mit dem Ziel der Auswertung.

ee) Die Klägerin ist den Anforderungen des § 6b Abs. 2 BDSG nach Kenntlichmachung der Beobachtung und der verantwortlichen Stelle hinreichend nachgekommen.

Sinn und Zweck der Verpflichtung der verantwortlichen Stelle zur Kenntlichmachung der Beobachtung ist die Schaffung von Transparenz für den Betroffenen; er soll vor oder bei Betreten des Raumes wissen, dass er beobachtet wird, damit er sein Verhalten danach ausrichten und gegebenenfalls der Beobachtung ausweichen kann (Zscherpe, in: Taeger/Gabel, a.a.O., § 6b Rn. 62 m.w.N.). Diesen Anforderungen genügen die in deutscher Sprache abgefassten und mit einem Symbol versehenen Hinweisschilder an den Türen in den Eingangsbereichen des Gebäudes. Nähere Angaben zur Art und zum Umfang der Videoüberwachung, etwa Angaben über die genaue Anzahl der Kameras einschließlich ihrer Standorte oder über die eingesetzte Technik, verlangt das Gesetz nicht (Scholz, in: Simitis, a.a.O., § 6b Rn. 103). Zudem können die Betroffenen die Identität der verantwortlichen Stelle erkennen.

ff) Die unverzügliche Löschung der erhobenen Daten nach § 6b Abs. 5 BDSG ist gewährleistet.

Nach dieser Vorschrift sind die durch Videoüberwachung gewonnenen Daten unverzüglich zu löschen, wenn sie zur Erreichung des ursprünglich verfolgten Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Nicht mehr erforderlich und daher zu löschen sind nach der – hier allein interessierenden – ersten Alternative des § 6b Abs. 5 BDSG alle Aufzeichnungen, die nicht mehr zur Aufklärung eines relevanten Vorfalls beitragen können, weil sie für eine Gefahrenabwehr oder Rechtsverfolgung nicht mehr benötigt werden. Letzteres ist anzunehmen, wenn die verantwortliche Stelle von einer Verfolgung absieht oder eine weitere Untersuchung der Störung oder Tat eingestellt worden ist (Scholz, in: Simitis, a.a.O., § 6b Rn. 139). Eine zeitliche Grenze ist im Gesetz nicht bestimmt, „unverzüglich" meint hier in entsprechender Anwendung von § 121 BGB ohne schuldhaftes Zögern. Auch wenn die

Gesetzesbegründung von regelmäßig ein bis zwei Arbeitstagen ausgeht (BT-Drs. 14/5793, S. 63, zitiert nach Scholz, in: Simitis, a.a.O., § 6b Rn. 140 in Fn. 296), ist hier die Frist von bis zu zehn Wochentagen noch als angemessen zu betrachten. Diese Frist ist zwar für den verfolgten Zweck der Abschreckung (Prävention) nicht erforderlich, sie ist aber mit Blick auf die Aufklärung etwaiger Rechtsverstöße angemessen. Angesichts der häufigen berufsbedingten Abwesenheit der Mitarbeiter, die in den einzelnen in dem Bürogebäude der Klägerin befindlichen Kanzleien und Praxen beschäftigt sind, und unter Berücksichtigung von mitunter längeren arbeitsfreien Zeiträumen ist die zeitliche Spanne der Speicherung von zehn Wochentagen nicht unverhältnismäßig. Denn oftmals wird erst nach Ablauf dieser Zeitspanne verlässlich feststehen, ob und welche Vorkommnisse eine nähere Untersuchung auch unter Zuhilfenahme der aufgenommenen Videobilder erfordern und rechtfertigen.

Der Einsatz des black box-Verfahrens gewährleistet eine automatische Überschreibung der bisher gespeicherten Bilder und damit eine gesicherte Löschung der gespeicherten Daten (vgl. hierzu Scholz, in: Simitis, a.a.O., § 6b Rn. 151).

Im Ergebnis liegen die Voraussetzungen der „Erlaubnisnorm" des § 6b BDSG insgesamt vor. Die Klägerin nimmt daher die Videoüberwachung ihres Bürogebäudes in Einklang mit den datenschutzrechtlichen Vorgaben vor. Mangels festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel fehlt es bereits an den tatbestandlichen Voraussetzungen der Ermächtigungsnorm des § 38 Abs. 5 BDSG. Auf Fragen der richtigen Ermessensausübung seitens des Beklagten kommt es daher nicht entscheidungserheblich an.

Zur Mitbestimmung des Personalrats bei der Bestellung des Vertreters des behördlichen Datenschutzbeauftragten (Ls)

(**Hessischer Verwaltungsgerichtshof**, Beschluss vom 22. Juli 2014 – 22 A 2226/13 –)

Das Mitbestimmungsrecht des Personalrats nach § 74 Abs. 1 Nr. 3 HPVG erstreckt sich nicht auf die Bestellung des Vertreters des behördlichen Datenschutzbeauftragten gemäß § 5 Abs. 1 Satz 1 HDSG.

Tätowierung im Eignungsauswahlverfahren zum Polizeivollzugsdienst der Bundespolizei (Ls)

(**Hessischer Verwaltungsgerichtshof**, Beschluss vom 9. Juli 2014 – 1 B 1006/14–)

1. **Eine Regelung, die Tätowierungen an Körperstellen verbietet, die beim Tragen der Dienstuniform einschließlich des kurzärmeligen Diensthemdes sichtbar sind (Erlass des Bundesministeriums des Innern vom 12. Mai 2006, B II – 652 100/120, Ziffer II.3.), betrifft auch das Erscheinungsbild der Betroffenen außerhalb der Dienstzeit, so dass die Einschätzung des Dienstherrn, Tätowierungen dürften im Dienst – ausgenommen beim Dienstsport – nicht sichtbar sein, weil dies dem mit dem äußeren Erscheinungsbild der Polizeivollzugskräfte der Bundespolizei verfolgten Zweck zuwider laufe, auf plausible und nachvollziehbare Gründe gestützt sein muss.**
2. **Tätowierungen können auch weiterhin alleine wegen ihres Inhalts als Ausschlussgrund bei einer Bewerbung für den Polizeivollzugsdienst bei der Bundespolizei herangezogen werden, und zwar dann, wenn es sich beispielsweise um gewaltverherrlichende, sexistische oder allgemein die Würde des Menschen verletzende Motive oder verbale Aussagen handelt, aber auch dann, wenn die Tätowierung Symbole aufweist, die einen Bezug zu extremen politischen Auffassungen herstellen.**
3. **Großflächige Tätowierungen, die beim Tragen der vorgeschriebenen Dienstkleidung sichtbar sind, berechtigen den Dienstherrn ungeachtet ihres Inhalts zu einem Ausschluss des eine solche Tätowierung tragenden Bewerbers von der Teilnahme am Eignungsauswahlverfahren für den gehobenen Polizeivollzugsdienst bei der Bundespolizei, weil er in der Tätowierung einen Mangel ader persönlichen Eignung des Bewerbers sieht.**

(Bestätigung von VG Darmstadt, Beschluss vom 27.05.2014 – 1 L 528/14 DA –)

Anspruch auf Löschung intimer Bilder nach Beziehungsende (Ls)

(**Oberlandesgericht Koblenz**, Urteil vom 20. Mai 2014 – 3 U 1288/13 –)

1. **Ein Löschungsanspruch aus dem BDSG (§ 53) erfasst nicht personenbezogene Daten (hier Fotografien), die im Rahmen einer intimen Beziehung für persönliche Zwecke gefertigt wurden.**
2. **Ein Löschungsanspruch aus dem KUG (§ 37) erfasst nur widerrechtlich hergestellte, verbreitete oder vorgeführte Bilder. Eine spätere Rücknahme der Einwilligung in die Herstellung der Bilder ändert an der Rechtmäßigkeit der Herstellung nichts.**
3. **Ein Widerruf des Einverständnisses in die Herstellung der Bilder und ihren damit einhergehenden Besitz ist jedenfalls dann zulässig, wenn sie zur Wahrung des Persönlichkeitsrechts erforderlich ist, weil z.B. das Vorliegen veränderter Umstände, die auf einer gewandelten inneren Einstellung beruhen, eine Fortgeltung der Einwilligung unzumutbar machen.**
4. **Ist eine intime Verbindung beendet, ist das persönliche Interesse der Abgebildeten an der Löschung der in dieser Zeit gefertigten intimen Fotos höher zu bewerten als das**

Eigentumsrecht des Fotoinhabers. Der Löschungsanspruch hinsichtlich der Fotos und ihrer Vervielfältigungsstücke folgt aus §§ 823 Abs. 1, 1004 BGB.

(Nicht amtliche Leitsätze)

Unzulässige Verwendung von Bestandsdaten zu Werbezwecken (Ls)

(**Oberlandesgericht Koblenz**, Urteil vom 26. März 2014 – 9 U 1116/13 –)

1. **Betreibt die Muttergesellschaft im Internet eine Website, auf der Verbraucher Mobilfunkverträge mit der zu 100 % im Eigentum der Mutter befindlichen Tochtergesellschaft abschließen können, kann die Mutter für die Online-Wettbewerbsverstöße ihrer 100%igen Tochtergesellschaft mithaften. Als Inhaberin der Homepage trifft sie bei Kenntnis von konkreten wettbewerbswidrigen Angeboten ihrer Tochter eine Handlungspflicht.**

2. **Keine hinreichende Information über das Widerspruchsrecht enthält folgende Klausel: „Die X-GmbH darf Sie zum Zwecke der Beratung, Werbung und Marktforschung zu eigenen Produkten postalisch oder per E-Mail kontaktieren, sofern Sie nicht gegenüber der X-GmbH widersprechen", da aus ihr nicht eindeutig das Recht des Verbrauchers hervorgeht, jederzeit der Nutzung widersprechen zu können.**

3. **Unwirksam ist folgende Einwilligungsklausel: „Der Vertrag über die Nutzung von Mobilem Internet kommt mit der X-GmbH, einer 100%igen Tochtergesellschaft der Y-AG, unter Einbeziehung der AGB sowie der Leistungsbeschreibung zustande. Die anfallenden Entgelte werden von meinem Bankkonto eingezogen.**

   ☐ Ja ich stimme zu

   und möchte zu den Produkten der X-GmbH und der mit ihr verbundenen Unternehmen, die zur Y-Gruppe gehören, beraten werden. Meine Bestandsdaten dürfen während der Vertragslaufzeit zum Zwecke der Beratung, Werbung und Marktforschung verarbeitet und genutzt werden. Hierzu darf ich auch telefonisch kontaktiert werden. Ich kann diese Einwilligung jederzeit ganz oder teilweise widerrufen", einmal weil die Regelung, obwohl sie mit anderen Vereinbarungen verbunden ist, von diesen nicht durch besondere Gestaltung deutlich vorgehoben wurde, und zum anderen, da sie die weiteren Unternehmen nicht namentlich bezeichnet, sondern lediglich von „verbundenen Unternehmen" spricht, so dass für den Verbraucher nicht ersichtlich ist, welche Firmen genau damit gemeint sind.

(Nicht amtliche Leitsätze)

Keine Bereitstellung eines separaten Telefon- und Internetanschlusses für den Betriebsrat

(**Landesarbeitsgericht Niedersachsen**, Beschluss vom 30. Juli 2014, 16 TaBV 92/13–)

1. **Der Möglichkeit der Überwachung und Kontrolle des Telefon- und Internetverkehrs des Betriebsrats kann durch entsprechende Vereinbarung zwischen Arbeitgeber und Betriebsrat begegnet werden. Dies erfordert keinen separaten Telefon- und Internetanschluss des Betriebsrats.**

2. **Dem Verlangen des Betriebsrats nach einem uneingeschränkten Internetzugang steht das Interesse des Arbeitgebers entgegen, den Zugriff auf Seiten mit strafbarem und/oder sittenwidrigem Inhalt zu unterbinden.**

Sachverhalt:

Die Beteiligten streiten über einen separaten Telefon- und Internetanschluss für den Betriebsrat, hilfsweise über einen uneingeschränkten Internetzugang.

Der Arbeitgeber, der zum Konzern der M. AG, W-Stadt gehört, unterhält neben seinem Betrieb an seinem Sitz in X-Stadt mit circa 165 Arbeitnehmern einen Betrieb in A-Stadt mit circa 65 Arbeitnehmern, in dem der antragstellende fünfköpfige Betriebsrat gewählt ist.

In den Konzerngesellschaften werden Telefonanlagen des Typs Hipath 3000 eingesetzt, die so eingestellt werden können, dass die Verkehrsdaten mit vollständigen Zielnummern gespeichert und personenbezogen ausgewertet werden können. Die einzelnen Anlagen können gekoppelt und zentral konfiguriert und verwaltet werden. Das Betriebsratsbüro in A-Stadt ist mit einem Nebenstellenanschluss ausgestattet. Zudem steht dem Betriebsrat ein mobiles Telefongerät zur Verfügung, das auf diese Nebenstelle geschaltet ist. Weiter ist das Betriebsratsbüro mit einem PC und einem Laptop ausgestattet. Der Internetzugang ist dem Betriebsratsgremium zugeordnet. PC und Laptop laufen über dasselbe Passwort. Der Internetzugang wird konzernweit über einen Proxyserver bei der M. AG vermittelt. Von dort kann der Zugang verwaltet und überwacht werden. Es ist möglich, User- und zumindest IP-Adressen und alle URLs der Browserzugriffe zu protokollieren und personenbezogen auszuwerten. Die Emailpostspeicher können von Administratoren gelesen werden, auf Grund von backups auch gelöschte Email. Es werden Emailfilter eingesetzt, um Spam dem Fach Junkmail zuzuordnen. Über Filter werden unerwünschte Internetadressen gesperrt. Deshalb konnte der Betriebsrat nicht auf die Seiten von „youtube" und „eRecht24" zugreifen.

Der Betriebsrat hat die Auffassung vertreten, dass ihm wegen dieser Gegebenheiten ein separater Telefon- und Internetzugang zur Verfügung zu stellen sei.

Aus den Gründen:

Der Betriebsrat kann keinen separaten Telefonanspruch beanspruchen.

Nach § 40 Abs. 2 BetrVG hat der Arbeitgeber dem Betriebsrat für die laufende Geschäftsführung in erforderlichem Umfang Informations- und Kommunikationstechnik zur Verfügung zu stellen. Vorliegend hat der Arbeitgeber dem Betriebsrat einen eigenen Nebenstellenanschluss zur Verfügung gestellt. Einen separaten eigenen Amtsanschluss kann der Betriebsrat nicht beanspruchen.

Dem Betriebsrat obliegt im Rahmen der § 40 Abs. 2 BetrVG die Prüfung, ob ihm ein eigener Amtsanschluss als erforderliches

Sachmittel zur Verfügung zu stellen ist. Die Entscheidung hierfür darf er nicht allein an seinen subjektiven Bedürfnissen ausrichten. Er muss vielmehr die betrieblichen Verhältnisse und die sich ihm stellenden Aufgaben berücksichtigen. Dabei sind die Interessen der Belegschaft an einer sachgerechten Ausübung des Betriebsratsamts und die berechtigten Interessen des Arbeitgebers, auch soweit sie auf eine Begrenzung der Kostentragungspflicht gerichtet sind, gegeneinander abzuwägen. Die Entscheidung des Betriebsrats über die Erforderlichkeit des verlangten Sachmittels unterliegt der arbeitsgerichtlichen Kontrolle. Diese ist auf die Prüfung beschränkt, ob das verlangte Sachmittel auf Grund der konkreten betrieblichen Situation der Erledigung der gesetzlichen Aufgaben des Betriebsrats dient und der Betriebsrat bei seiner Entscheidung nicht nur die Interessen der Belegschaft berücksichtigt, sondern auch berechtigte Interessen des Arbeitgebers Rechnung getragen hat. Dient das jeweilige Sachmittel der Erledigung betriebsverfassungsrechtlicher Aufgaben und hält sich die Interessenabwägung des Betriebsrats im Rahmen seines Beurteilungsspielraums, kann das Gericht die Entscheidung des Betriebsrats nicht durch seine eigene ersetzen (BAG, 18.07.2012 – 7 ABR 23/11 – Rn. 20).

Unter Berücksichtigung dieser Grundsätze überschreitet die Entscheidung des Betriebsrats seinen Beurteilungsspielraum.

Dem Betriebsrat steht zur Erledigung seiner Aufgaben der betriebsübliche Telefonanschluss zur Verfügung. Dieser ist für die Erledigung seiner Aufgaben ausreichend. Das Verlangen nach einem eigenen separaten Amtsanschluss verursacht zusätzliche Kosten, ohne dass ein eigener Amtsanschluss zur Vermeidung der abstrakten Möglichkeit der Überwachung und Kontrolle seines Telefonverkehrs notwendig ist. Ausreichend ist, dass der Betriebsrat von dem Arbeitgeber verlangen kann, dass sein Telefonanschluss unkontrolliert bleibt, indem die Aufzeichnung der Verkehrsdaten seines Nebenstellenanschlusses unterdrückt und deren Auswertung verboten werden, zumal der Arbeitgeber, wie in der Beschwerdeanhörung erklärt, zum Abschluss einer entsprechenden Vereinbarung bereit ist.

Der Betriebsrat kann auch keinen separaten Internetzugang beanspruchen.

Unter Berücksichtigung der oben dargelegten Grundsätze zu § 40 Abs. 2 BetrVG überschreitet das Verlangen des Betriebsrats seinen Beurteilungsspielraum. Es lässt berechtigte Sicherheitsinteressen des Arbeitgebers außer Acht.

Die Kommunikation zwischen Arbeitgeber und Betriebsrat erfolgt im Intranet über Email. Diese enthalten mitunter vertrauliche Informationen. Bei einer Übermittlung per Email über das Internet an einen separaten also externen Internetanschluss des Betriebsrates entstünde eine nicht notwendige Sicherheitslücke. Diese braucht der Arbeitgeber nicht hinzunehmen, zumal dem berechtigten Verlangen des Betriebsrats nach einem unkontrollierten Emailverkehr gleichfalls durch eine Vereinbarung entsprochen werden kann, die eine mögliche Kontrolle des Emailverkehrs des Betriebsrates verbietet, wozu der Arbeitgeber nach seiner Erklärung bereit ist.

Der Hilfsantrag des Betriebsrats ist gleichfalls unbegründet.

Das Verlangen nach einem uneingeschränkten Internetzugang berücksichtigt nicht das berechtigte Interesse des Arbeitgebers, einen Zugriff auf Seiten mit strafbarem und/oder sittenwidrigem Inhalt durch die Installierung entsprechender Firewalls auf dem Proxyserver zu unterbinden. Das berechtigte Interesse, sich über betriebsratsrelevante Themen im Internet zu unterrichten, kann der Betriebsrat durch die Beantragung der Freistellung der von ihm benötigten Seiten erreichen. Er hat zum Beispiel nicht dargelegt, dass er die Freischaltung der Seite „E-Recht 24“ beantragt hätte, diese ihm aber verweigert worden wäre.

Pflicht zur Vorlage eines erweiterten Führungszeugnisses (Ls)

(**Arbeitsgericht Gelsenkirchen**, Urteil vom 4. Juli 2014, 2 Ca 1310/13 –)

1. **Aus § 241 Abs. 2 BGB kann sich die Verpflichtung eines Arbeitnehmers ergeben, seinem Arbeitgeber ein erweitertes Führungszeugnis nach § 30a BRZG vorzulegen.**
2. **Bei der Frage, ob ein erweitertes Führungszeugnis durch den Arbeitnehmer vorzulegen ist, sind die Informationsinteressen des Arbeitgebers und die Schutzinteressen des Arbeitnehmers bezogen auf seine persönlichen Daten gegeneinander abzuwägen.**
3. **Soweit die Voraussetzungen des § 30a Abs. 1 Ziffer 1 oder 2 BRZG erfüllt sind, ergibt sich regelmäßig ein Recht des Arbeitgebers auf Vorlage eines erweiterten Führungszeugnisses durch den Arbeitnehmer. Soweit die Voraussetzungen des § 30a BRZG dagegen nicht erfüllt sind, wird der Arbeitgeber in der Regel die Vorlage eines erweiterten Führungszeugnisses nicht verlangen können.**
4. **Eine Vorlageverpflichtung auf der Grundlage des § 30a Abs. 1 Ziffer 2c BRZG erfordert einen Kontakt des Arbeitnehmers zu Minderjährigen, der zu einer besonderen Gefahrensituation werden kann.**
5. **Bei der Einschätzung der Frage, ob eine besondere Gefahrensituation entstehen kann, steht dem Arbeitgeber ein Beurteilungsspielraum zu.**
6. **Die bloße Möglichkeit, dass ein Arbeitnehmer zukünftig mit minderjährigen Klienten, Praktikanten oder Auszubildenden in Kontakt treten könnte, rechtfertigt die Vorlage eines erweiterten Führungszeugnisses regelmäßig nicht.**
7. **Die Tätigkeit in einer Mitarbeitervertretung oder einem Betriebsrat führt auch dann, wenn in einem Betrieb minderjährige Mitarbeiter beschäftigt werden, in aller Regel nicht zu einer besonderen Gefahrensituation, die die Vorlage eines erweiterten Führungszeugnisses rechtfertigen könnte.**

Private Aufnahmen mit einer Dash-Cam unterliegen einem Beweisverwertungsverbot

(**Amtsgericht München**, Beschluss vom 13. August 2014 – 345 C 5551/14–)

Gegenüber dem Interesse zur Sicherung von Beweismitteln durch Dash-Cam-Aufnahmen im Falle möglicher Verkehrsunfälle überwiegen die schutzwürdigen Interessen der betroffenen Verkehrsteilnehmer an der Wahrung ihrer Allgemeinen Persönlichkeitsrechte. Deshalb unterliegen

private Videoaufnahmen mit einer Dash-Cam einem Verwertungsverbot im Zivilprozess.

(Nicht amtlicher Leitsatz)

Aus den Gründen:

Nach ständiger Rechtsprechung hängt die Verwertbarkeit solcher Aufnahmen von den jeweils schutzwürdigen Interessen der Parteien ab, die gegeneinander abzuwägen sind (vgl. AG München, Urteil vom 06. 06. 2013, Az. 343 C 4445/13, Ziffer 13; BVerfG NJW 2002, 3619; vgl. Thomas/Putzo/Reichold, ZPO, § 371, Vorbemerkung, Rn 6). Indizwirkung hat dabei auch der Verstoß gegen einfachgesetzliche Normen. Verbotswidrig erlangte Beweismittel sind nur ausnahmsweise verwertbar, nämlich wenn der geschützten Eigensphäre überwiegende berechtigte Interessen gegenüberstehen.

Die permanente, anlasslose Überwachung des Straßenverkehrs durch eine in einem PKW installierte Autokamera („Car-Cam" bzw. „Dash-Cam") verstößt gegen § 6b Abs. 1 Nr. 3 BDSG sowie gegen § 22 S. 1 KunstUrhG und verletzt den Beklagten in seinem Recht auf Informationelle Selbstbestimmung als Ausfluss seines Allgemeinen Persönlichkeitsrechts, Art. 2 Abs. 1, 1 Abs. 1 GG. Es liegen auch keine überwiegenden Interessen des Beweisführers vor, die die Verwertung dieser rechtswidrig erlangten Beweismittel erlauben würden.

1. Verstoß gegen § 6b Abs. 1 Nr. 3 BDSG

Die anlasslose Verwendung der Autokamera verstößt gegen § 6b Abs. 1 Nr. 3 BDSG.

Das Bundesdatenschutzgesetz bezweckt gem. § 1 Abs. 1 BDSG den Schutz des Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechts. Nach § 1 Abs. 2 Nr. 3 BDSG gilt das BDSG dabei auch für nicht-öffentliche Stellen, insbesondere für natürliche Personen, vgl. § 2 Abs. 4 S. 1 BDSG.

Gem. § 6b Abs. 1 Nr. 3 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (vgl. Erfurter Kommentar zum Arbeitsrecht/Franzen, BDSG, § 6b, Rn 4 ff.).

Zwar ist der Zweck der Autokamera, die Sicherung von Beweismitteln im Falle möglicher Verkehrsunfälle, hinreichend konkret, es überwiegen allerdings die schutzwürdigen Interessen des Betroffenen an der Wahrung seines Allgemeinen Persönlichkeitsrechts (dazu Nr. 3). Die Zulassung solcher Videos als Beweismittel durch die Zivilgerichte würde zweifellos zu einer weiten Verbreitung oder sogar standardmäßigen Ausstattung mit Carcams führen. Was mit den so gefertigten Aufzeichnungen geschieht und wem diese zum Beispiel über eine Cloud zugänglich gemacht werden, wäre jeglicher Kontrolle insbesondere durch die aufgezeichneten Personen entzogen. Ebenso wäre eine Auswertung durch eine entsprechende Gesichtserkennungssoftware jeder Kontrolle entzogen. Damit wäre eine privat organisierte dauerhafte und flächendeckende Überwachung sämtlicher Personen, welche am öffentlichen Verkehr teilnehmen, denkbar. Im Gegensatz zur dauerhaften Offenbarung privater Daten in Diensten wie Facebook, wo dies von den Teilnehmern freiwillig geschieht, wäre dieser Datensammlung jedermann ausgesetzt, der sich in die Öffentlichkeit begibt.

2. Verstoß gegen § 22 S. 1 KunstUrhG

Die anlasslose Verwendung der Autokamera verstößt ferner gegen § 22 S. 1 KunstUrhG.

Danach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Eine Ausnahme besteht nach § 23 Abs. 1 Nr. 2 KunstUrhG für Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen.

Der permanente Einsatz der Autokamera führt auch zur Erstellung von Fotografien derjenigen Personen, die außerhalb des KFZ des Verwenders am Straßenverkehr beteiligt sind, sei es als Insassen eines anderen KFZ, sei es etwa als Fußgänger. Sinn und Zweck der Erstellung dieser Bildnisse ist die Beweisführung in einer möglichen Gerichtsverhandlung, die gem. § 169 S. 1 GVG öffentlich ist.

Ein Ausnahmetatbestand liegt nicht vor, insbesondere sind die abgebildeten Personen nicht bloßes „Beiwerk", sondern ihre Aufzeichnung ist im Gegenteil gerade das Ziel des Verwenders (vgl. OLG Frankfurt a. M. MMR 2004, 683 f.; Beck´scher Online-Kommentar Urheberrecht/Engels, KunstUrhG, § 23, Rn 13 „Hauptmotiv"). Zwar haftet gem. § 7 StVG der Halter eines KFZ ohne Rücksicht auf seine Person, so dass sich das Interesse insoweit auf ein Fotografieren des KFZ-Kennzeichens reduzieren dürfte. Allerdings hat der Verwender regelmäßig auch ein Interesse daran, die Person des Fahrzeugführers ausfindig zu machen, etwa um Ansprüche gem. § 18 StVG oder § 823 BGB geltend zu machen. Insbesondere bei Radfahrern und Fußgängern ist § 823 BGB alleinige Anspruchsgrundlage.

Jedenfalls aber erstreckt sich die Befugnis nach § 23 Abs. 1 Nr. 2 KunstUrhG nicht auf eine Verbreitung und Zurschaustellung, durch die ein berechtigtes Interesse des Abgebildeten verletzt wird, Abs. 2. Die permanente, anlasslose Überwachung des Straßenverkehrs und der an ihm beteiligten oder sogar unbeteiligten Personen verletzt die Betroffenen jedoch in ihrem Allgemeinen Persönlichkeitsrecht (dazu sogleich Nr. 3).

3. Verletzung des Betroffenen in seinem Grundrecht auf Informationelle Selbstbestimmung, Art. 2 Abs. 1, 1 Abs. 1 GG

a. Schutzbereich

Das Recht auf Informationelle Selbstbestimmung als Ausfluss des Allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1, 1 Abs. 1 GG) umfasst das Recht am eigenen Bild (BVerfGE 87, 334 ff.; 97, 228 ff.; 120, 180 ff.; Jarass/Pieroth, GG, Art. 2, Rn 45).

Grundrechtsträger sind Inländer wie Ausländer (Jarass/Pieroth, GG, Art. 2, Rn 6 ff.).

b. Eingriff

Durch die unbefugte Erstellung von Fotoaufnahmen wird in dieses Grundrecht eingegriffen. Zwar binden die Grundrechte primär die staatliche Gewalt (Art. 1 Abs. 3 GG), allerdings strahlen die Grundrechte über die Figur der „mittelbaren Drittwirkung" in das Privatrecht ein und sind hier insbesondere für die Auslegung unbestimmter Rechtsbegriffe heranzuziehen (BVerfGE 7, 198 ff. „Lüth-Urteil" BVerfGE 39, 67 ff.; BVerfGE 89, 214 ff. (st. Rspr.); Maunz/Dürig/Herdegen, GG, Art. 1 Abs. 3, Rn 52 ff.). Das Recht auf Informationelle Selbstbestimmung ist daher insbesondere im Rahmen der Prüfung von § 6b Abs. 1 Nr. 3 BDSG und § 22 S. 1, 23 Abs. 2 KunstUrhG in die Abwägung mit einzustellen.

c. Verfassungsrechtliche Rechtfertigung

Der Eingriff kann nicht verfassungsrechtlich gerechtfertigt werden. Die Interessen des Verwenders der Autokamera überwiegen nicht diejenigen des Betroffenen.

Das Recht auf Informationelle Selbstbestimmung kann insbesondere durch konkurrierende Grundrechte Dritter eingeschränkt werden (Jarass/Pieroth, GG, Art. 2, Rn 58 ff.; 60 ff.). Als ein solches Grundrecht kommt hier das Interesse des Verwenders an einer fairen Handhabung des Beweisrechts in Betracht (Art. 20 Abs. 3

GG vgl. BVerfG NJW 2011, 2783 ff., 2785: „Aus dem Rechtsstaatsprinzip folgt die Verpflichtung zu einer fairen Handhabung des Beweisrechts, insbesondere der Beweislastregeln (...)." vgl. Bachmeier, DAR 2014, 21; vgl. auch Art. 6 Abs. 1 S. 1 EMRK).

Dieses Interesse ist in seinem Grundsatz auch legitim, da sich gerade im Verkehrsrecht mitunter erhebliche Beweisprobleme und -schwierigkeiten ergeben können, wenn etwa Mitfahrer als Zeugen zu vernehmen sind etc.

Gleichwohl vermag es nicht generell das Informationelle Selbstbestimmungsrecht des Betroffenen zu überwiegen (vgl. BVerfG NJW 2009, 3279: „Allein das allgemeine Interesse an einer funktionstüchtigen Straf- und Zivilrechtspflege reicht aber nicht, um im Rahmen der Abwägung stets von einem gleichen oder gar höheren Gewicht ausgehen zu können, als es dem allgemeinen Persönlichkeitsrecht zukommt. Vielmehr müssen weitere Aspekte hinzutreten, die ergeben, dass das Interesse an der Beweiserhebung trotz der Persönlichkeitsbeeinträchtigung schutzbedürftig ist").

Das Beweiserhebungsinteresse überwiegt jedenfalls dann nicht die Beeinträchtigung des Persönlichkeitsrechts des Betroffenen, wenn nicht konkrete Anhaltspunkte dafür bestehen, dass eine gerichtliche Beweisführung wegen einer erheblichen Beeinträchtigung in naher Zukunft unmittelbar erforderlich wird.

So hat der BGH entschieden, dass die permanente, verdachtslose Überwachung des Zugangs zu einem Wohnhaus das Persönlichkeitsrecht der Betroffenen selbst dann verletzt, wenn die Aufzeichnungen nicht verbreitet werden sollen (BGH NJW 1995, 1955 ff., 1957: „Gegenüber (...) gänzlich unbeteiligten Dritten könnte ein derartiger Eingriff in das allgemeine Persönlichkeitsrecht aber höchstens dann zulässig sein, wenn schwerwiegenden Beeinträchtigungen (...), etwa Angriffen auf ihre Person oder ihre unmittelbare Wohnsphäre, nicht in anderer Weise zumutbar begegnet werden könnte"; vgl. auch Bachmeier, DAR 2014, 18). Eine Videoüberwachung in der Tiefgarage einer WEG kann nicht mehrheitlich beschlossen werden, da diese gegen das Persönlichkeitsrecht der Wohnungseigentümer verstößt (LG Müchen I, Urteil vom 11. 11. 2011, Az. 1 S 12752/11).

Entsprechend verfährt die Rechtsprechung zur Problematik der Videoüberwachung am Arbeitsplatz (vgl. nur BAG, Urteil vom 21. 06. 2012, Az. 2 AZR 153/11 Ziffer 30: „Danach ist die heimliche Videoüberwachung eines Arbeitnehmers zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit praktisch das einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist (...)"; vgl. ferner LAG Hamm, Urteil vom 30. 10. 2012, Az. 9 Sa 158/12; LAG Mainz, Urteil vom 23. 05. 2013, Az. 2 Sa 540/12).

Die bloße Möglichkeit des Notwendigwerdens einer Beweisführung aufgrund der generellen Gefährlichkeit des Straßenverkehrs genügt diesen Anforderungen nicht.

4. Ergebnis

Auch wenn die Verwendung von Autokameras immer beliebter wird, können die durch sie erlangten Fotografien nicht als zivilprozessuales Beweismittel verwertet werden, da diese Aufnahmen in aller Regel unter Verletzung des Grundrechts der Betroffenen auf Informationelle Selbstbestimmung gewonnen wurden, Art. 2 Abs. 1, 1 Abs. 1 GG. Selbst wenn man davon ausgeht, manche Bürger seien in Zeiten sozialer Netzwerke ohnehin mit der Preisgabe persönlicher Informationsgehalte einverstanden bzw. sie hätten sich in Ermangelung einer Alternative hiermit abgefunden, vermag dieser „(...) Verzicht auf Persönlichkeitsrechte jene Bürger, die sie weiterhin schützen wollen, nicht zu binden" (Bachmeier, DAR 2014, 21).

Die Alternative zu dieser Ansicht der Gerichts würde konsequenterweise bedeuten, dass jeder Bürger Kameras ohne jeden Anlass nicht nur in seinem PKW, sondern etwa auch an seiner Kleidung befestigen könnte, jedermann permanent gefilmt und überwacht würde und so das Recht auf Informationelle Selbstbestimmung praktisch aufgegeben würde.

Keine mutmaßliche Einwilligung für E-Mail-Fortbildungsangebot an Rechtsanwälte

(**Amtsgericht Leipzig**, Urteil vom 18. Juli 2014 – 107 C 2154/14 –)

1. **Auch wenn Rechtsanwälte berufsrechtlich zur Fortbildung verpflichtet sind, kann hieraus auf keine vermutliche Einwilligung zur Zusendung von E-Mail-Werbung für Fortbildungen hergeleitet werden.**
2. **Ein datenschutzrechtlicher Auskunftsanspruch ist hinsichtlich des Inhalts, der Herkunft und der Empfänger erfüllt, wenn auf die Entnahme der Adressdaten aus dem Internet hingewiesen wurde und sich konkludent ergibt, dass diese nicht an Dritte weitergegeben wurden.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Beklagte übersandte an den Kläger am 18.10.2013 um 14.01 Uhr an die Adresse eine Einladung zum Hessischen Medizinrechtstag. Die Beklagte war Veranstalter der Veranstaltung. Inhalt der Veranstaltung war das Patientenrechtsgesetz. Hinzu kamen weitere medizinrechtlich relevante Fragestellungen, wie z.B. die Patientenverfügung, weitere Vorsorgemöglichkeiten, Fragen aus dem Vertragsarztrecht sowie das Thema Europarecht und deren Einflüsse auf das Deutsche Medizinrecht. Der Kläger teilte der Beklagten mit E-Mail vom 20.10.2013 mit, dass jegliche Werbung per Mail, Telefax, Brief oder Anruf zu unterlassen sei, der Nutzung der Daten gern. § 28 Abs. 4 BDSG widersprochen und eine Auskunft sowie eine strafbewährte Unterlassungsklärung bis zum 07.11.2013 erwartet werde. Bezüglich der Auskunft wurde aufgefordert, darüber Auskunft zu geben, welche Daten bei der Beklagten gespeichert sind, auch soweit sie sich auf Herkunft und Empfänger beziehen, welcher Zweck mit der Speicherung dieser Daten verfolgt wird und an welche Personen oder Stellen diese Daten regelmäßig übermittelt werden. Die Beklagte erklärte mit E-Mail am 22.10.2013, dass der Kläger aus dem Verteiler für künftige Veranstaltungen entfernt worden ist. Mit Schreiben vom 02.12.2013 wurde dem Kläger mitgeteilt, dass die Beklagtenseite im Rahmen ihrer Geschäftstätigkeit u.a. seit vielen Jahren in den verschiedenen Bundesländern Kongressveranstaltungen organisiert und hierüber Anwälte und Anwältinnen unter Übermittlung des Tagungsprogrammes informiert werden. Es wurde darauf hingewiesen, dass Name und Anschrift dabei aus den veröffentlichten Angaben im Internet entnommen werden. Der Kläger ist der Ansicht, dass ihm ein Unterlassungsanspruch und ein Auskunftsanspruch zustehe.

Aus den Gründen:

Die Klage ist zulässig. Sie hat bezüglich des Unterlassungsanspruches Erfolg.

Der Kläger hat einen Anspruch aus §§ 1004 Abs. 1 Satz 2, 823 Abs. 1 BGB.

Nach ständiger Rechtsprechung stellt die Werbung mittels E-rv-tail, Telefax oder Werbeanrufe eine unzulässige Belästigung im Sinne von §§ 823, 1004 BGB dar, da sie die Aufmerksamkeit des Betroffenen über Gebühr hinaus in Anspruch nimmt und zu einer unzumutbaren Belästigung des privaten oder beruflichen Bereichs führt, wobei auch die einmalige Zusendung einen rechtswidrigen Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb bzw. in das Persönlichkeitsrecht darstellt. Die Zusendung von E-Mail mit werbendem Inhalt an einen Rechtsanwalt, der aus berufsrechtlichen Gründen seine E-Mail sorgfältig lesen muss, ist als Eingriff in dessen eingerichteten und ausgeübten Gewerbebetrieb unzulässig. Die zugesandte E-Mail der Beklagten hinsichtlich der Teilnahmemöglichkeit am Hessischen Medizinrechtstag ist als Werbung zu qualifizieren. Als Werbung ist jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerkes oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen zu fördern, zu verstehen. Die E-Mail der Beklagten enthält ein Angebot zur Teilnahme an einer Fachtagung. Dabei bietet die Beklagte innerhalb der Ausübung ihres Gewerbes eine Erbringung von Dienstleistungen an. Die Beklagte beabsichtigte mit der Zusendung der Einladung, den Kläger zur Teilnahme an der Tagung zu gewinnen und daher den Absatz zu fördern. Eine Einwilligung des Klägers lag nicht vor. Es gab zwischen den Parteien weder einen vorherigen Kontakt noch eine anderweitige ausdrückliche Einwilligung. Der Kläger hat auch explizit auf seiner Internetseite der Kontaktierung per Werbe-E-Mail widersprochen. Eine mutmaßliche Einwilligung ergibt sich auch nicht aus der von der Beklagten angesprochenen Berufspflicht der Fortbildung gern. § 43a Abs. 6 BRAGO. Es ist jedem Rechtsanwalt unbenommen, wie und auf welcher Weise er sich fortbildet. Ein mittelbarer Drittschutz für Anbieter von Fortbildungsveranstaltungen kann daraus nicht abgeleitet werden. Auch ist die Wiederholungsgefahr nicht ausgeräumt worden. Der Unterlassungsanspruch und die hierfür erforderliche Wiederholungsgefahr, also die ernstliche, sich auf Tatsachen begründende Besorgnis, dass in Zukunft weiterer Verstoß droht, werden nach der ständigen Rechtsprechung bereits durch den zweifelsfrei festgestellten Rechtsverstoß begründet. Es besteht grundsätzlich eine tatsächliche Vermutung für das Vorliegen einer Wiederholungsgefahr, wenn bereits ein rechtswidriger Eingriff, hier in Form der Übersendung einer E-Mail, in das allgemeine Persönlichkeitsrecht, das Eigentum bzw. den eingerichteten und ausgeübten Gewerbebetriebs des Klägers vorgenommen wurde. An den Wegfall dieser Vermutung werden strenge Anforderungen gestellt. Im Wettbewerbsrecht wurden in ständiger Rechtsprechung diese Anforderungen konkretisiert. So kann der Störer die tatsächliche Vermutung nur durch die Abgabe einer unbedingten, unwiderruflichen und strafbewährten Unterlassungsklärung widerlegen. Die Rechtsprechung, die diesen Grundsatz für den Bereich des Wettbewerbsrechts entwickelt hat, hat jedoch auch eingeräumt, dass auch ohne eine solche Erklärung die Verneinung der Wiederholungsgefahr in Ausnahmefällen denkbar ist (vgl. BGH NJW 1994, S. 1281). Der Grundsatz, dass die Wiederholungsgefahr nur dann entfällt, wenn der Störer dem Beeinträchtigten eine strafbewährte Unterlassungserklärung abgibt, gilt auch für den deliktischen Unterlassungsanspruch, jedoch nicht in gleicher Strenge (vgl. LG Leipzig, Urteil vom 12.03.2004, Az..: 16 S 4165/03). Im Deliktsrecht kann der Schwere des Eingriffs, den Umständen der Verletzungshandlung, der fallbezogenen Wahrscheinlichkeit und vor allem der Motivation des Störers für die Entkräftung der Vermutung der Wiederholungsgefahr durchaus ein erhebliches Gewicht zukommen.

Die Anwendung dieser Grundsätze führt jedoch vorliegend nicht dazu, dass die Vermutung der Wiederholungsgefahr entkräftet ist. Die Beklagtenseite hat keine Unterlassungserklärung abgegeben. An den Fortfall der Wiederholungsgefahr werden strenge Anforderungen gestellt. Ein bloßes Unterlassen oder Ändern der beanstandeten Handlung beseitigt die Wiederholungsgefahr grundsätzlich nicht. Zwar hat die Beklagtenseite mitgeteilt, dass der Kläger aus dem Verteiler gelöscht wurde. Es ist jedoch nicht ausgeschlossen, dass die Aufnahme des Klägers in den Verteiler erneut erfolgt. Da die Internetadresse des Klägers für die Beklagte jederzeit erneut abrufbar ist, ist die Wiederholungsgefahr aus Sicht des Gerichtes nicht ausgeräumt.

Ein Anspruch des Klägers aus § 34 Bundesdatenschutzgesetz besteht nicht, da die Beklagtenseite den Anspruch bereits erfüllt hat. Gemäß § 34 Bundesdatenschutzgesetz kann jeder Betroffene Auskunft darüber verlangen, welche personenbezogenen Daten über ihn bei einem bestimmten Unternehmen vorliegen. Auch wenn keine Daten vorliegen, besteht ein Auskunftsanspruch.

Die Auskunft ist jedoch durch das Schreiben des Beklagtenvertreter vom 02.12.2013 erteilt worden. Die Beklagtenseite hat mitgeteilt, dass die Daten aus den veröffentlichten Angaben im Internet entnommen werden. Der Kläger hat selbst eingeräumt, dass seine E-Mailanschrift unproblematisch dem Internet entnommen werden kann. Die Beklagtenseite hat auch den Zweck mitgeteilt, nämlich, dass die Beklagte im Rahmen ihrer Geschäftstätigkeit Kongressveranstaltungen abhält. Der Kläger konnte daher der Information entnehmen, woher die Beklagte seine E-Mailadresse hat und warum Interesse an der E-Mailanschrift bestanden hat. Aus dem Schreiben des Beklagtenvertreters vom 02.12.2013 ist nach Ansicht des Gerichtes auch konkludent zu entnehmen, dass eine Übermittlung an Dritte nicht stattgefunden hat. Im Übrigen wäre dies auch unerheblich, da sich jederzeit dritte Personen die E-Mailanschrift des Klägers über das Internet besorgen können und somit kein Fall vorliegt in dem vertrauliche personenbezogene Daten an Dritte weitergegeben werden. Es stellt sich daher bereits die Frage, ob dem Kläger überhaupt ein Anspruch aus § 34 BDSG zusteht, da der Kläger selbst durch die öffentliche Bekanntmachung seiner E-Mailanschrift im Internet einen Zugriff auf diese Daten ermöglicht hat und ihm daher bekannt ist, woher die Beklagte seine E-Mailanschrift kennt.

Berichte, Informationen, Sonstiges

Marktmacht und informationelleSelbstbestimmung

(Beschluss der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2014 in Hamburg)

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen Double-Click. Die Übernahme wurde sowohl von den Kartellbehörden in den USA als auch in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist darauf hin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

(Beschluss der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2014 in Hamburg)

Der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.
- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.
- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.
- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.
- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Eu-DS-GVO: Datenschutzneuregelung in Europa

In Europa wird z.Zt., ohne dass dies eine besondere Aufmerksamkeit in der Öffentlichkeit erfährt, über eine umfassende Neuregelung des Datenschutzrechts beraten. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat die bislang in deutscher Sprache vorliegenden wesentlichen Dokumente, den Vorschlag der Europäischen Kommission und die Änderungsvorschläge des Europäischen Parlaments in einer Synopse zusammengestellt und bietet diese interessierten Lesern zum Download an.

(Pressemitteilung vom 08.09.2014)

9 Millionen Deutsche haben Partner im Internet gesucht

Nach einer repräsentativen Umfrage, die Bitkom Research im Zusammenhang mit Aris durchgeführt hat, wurden im September 2014 1.014 Internetnutzer ab 14 Jahren befragt. Hochgerechnet ergabe sich folgendes Ergebnis:

- 4 Millionen Deutsche sind derzeit im Online-Dating aktiv
- Jeder dritte Nutzer hat einen festen Partner kennengelernt

Bei der Suche nach einem Partner greifen viele Menschen auf Online-Dating zurück. Jeder sechste Internetnutzer ab 14 Jahren (16 Prozent) hat schon in Internet-Singlebörsen oder per Dating-App nach Partnern gesucht. Das entspricht rund neun Millionen Bundesbürgern.

Vor allem Jüngere suchen gerne nach möglichen Partnern im Netz: Fast jeder Vierte der 14- bis 29-jährigen (23 Prozent) hat einschlägige Erfahrungen. Bei den 30- bis 49-jährigen ist es jeder sechste Internetnutzer (16 Prozent). Von den 50- bis 64-jährigen hat schon jeder Siebte (14 Prozent) Dating-Dienste im Internet genutzt. Aber nicht jeder, der schon einmal auf Dating-Dienste zurückgegriffen hat, ist heute noch aktiver Nutzer. Insgesamt sagt jeder achte Internetnutzer (12 Prozent), dass er aktuell bei einem Online-Dating-Dienst oder einer Dating-App angemeldet ist. Aber nur 8 Prozent bestätigen, dass sie die jeweiligen Dienste momentan auch aktiv nutzen. Das entspricht gut vier Millionen Bundesbürgern, die momentan über Online-Dienste oder Apps nach Partnern suchen.

Für viele Nutzer war die Partnersuche über das Internet erfolgreich. Mehr als jeder Dritte (36 Prozent) hat dadurch einen festen Partner kennengelernt. Beim Online-Dating sind vor allem kostenlose Angebote beliebt. Nur ein Viertel der Dienste-Nutzer (25 Prozent) gibt dafür Geld aus, 69 Prozent entscheiden sich für kostenlose Dating-Möglichkeiten.

(Bitkom Pressemitteilung vom 15.10.2014)

Bundesinnenministerium legt am 19.8.2014 Entwurf für IT-Sicherheitsgesetz vor

Das Vorhaben sei ein wesentlicher Baustein der Digitalen Agenda der Bundesregierung, so das BMI.

Die Sicherheit der Informationstechnik sei Grundlage jeder Form von Digitalisierung und damit zentrales Querschnittsthema der Digitalen Agenda, mit der die Bundesregierung die Digitalisierung von Wirtschaft, Gesellschaft und Staat begleiten und voranbringen will.

Für den in der Digitalen Agenda verankerten präventiven Ansatz solle der nunmehr vorliegende Entwurf für ein neues IT-Sicherheitsgesetz den nötigen Rahmen schaffen. Das Bundesministerium des Innern habe den Referentenentwurf am 19.08.2014 den beteiligten Ressorts der Bundesregierung zur weiteren Abstimmung zugeleitet.

Der Entwurf nehme – über die im Koalitionsvertrag vereinbarten Mindestanforderungen an die IT-Sicherheit für Kritische Infrastrukturen hinaus – die Sicherheit der Systeme und den Schutz der Bürgerinnen und Bürger generell in den Blick. Die IT-Systeme und digitalen Infrastrukturen Deutschlands sollten die sichersten weltweit werden.

Der vorgelegte Gesetzentwurf enthält Regelungen zu folgenden Themenfeldern:

- Verbesserung der IT-Sicherheit bei Unternehmen – insbesondere bei kritischen Infrastrukturen;
- Schutz der Bürgerinnen und Bürger in einem sicheren Netz;
- Schutz der IT des Bundes;
- Stärkung des Bundesamtes für Sicherheit in der Informationstechnik;

- Erweiterung der Ermittlungszuständigkeiten des Bundeskriminalamtes im Bereich Cybercrime.

„Wir müssen sicherer werden als bisher. Wer ein Risiko setzt für andere, trägt dafür auch die Verantwortung. Wer Kritische Infrastrukturen betreibt, der muss sie sicher betreiben," erklärte Bundesinnenminister Dr. Thomas de Maizière zum Gesetzentwurf.

Nach der Ressortabstimmung solle das Vorhaben im Rahmen einer breiten öffentlichen Debatte intensiv mit den beteiligten Kreisen aus Wirtschaft und Gesellschaft erörtert werden.

(Pressemitteilung des BMI vom 19.8.2014)

DSRI Herbstakademie 2014

In diesem Jahr fand vom 10.9. bis 13.9.2014 die 15. Herbstakademie der Deutschen Stiftung für Recht und Informatik (DSRI) unter der Überschrift „BIG DATA & Co – Neue Herausforderungen für das Informationsrecht" an der Johannes Gutenberg-Universität Mainz statt. Die auch in diesem Jahr sehr gut besuchte Veranstaltung bot einen breit gefächerten Überblick über die neuesten Entwicklungen unter Berücksichtigung der aktuellen Rechtsprechung auf dem Gebiet des Informationstechnologierechts.

Bei der diesjährigen Herbstakademie, bestand für jeden Teilnehmer die Möglichkeit, sich sein eigenes Programm aus insgesamt 58 Vorträgen zusammenzustellen, eingeteilt in Panels mit den Oberbegriffen „Big Data", „Gewerblicher Rechtsschutz", „Immaterialgüterrecht", „Datenschutzrecht", „Internetrecht" und „IT-Recht".

Eine der Auftaktveranstaltungen brachte einen allgemeinen Überblick über den Rechtsschutz von Datenbanken. Um die Relevanz des Datenbankrechts für Big Data herauszustellen, wurde durch RA Götz zunächst die Begrifflichkeit „Big Data", welche vielfältig interpretiert wird und zu einem bunten Potpourri an Beiträgen führt, erörtert sowie die Entwicklung des Datenbankrechts in der EU und Deutschland aufgezeigt. Sodann konnten unter Berücksichtigung der maßgeblichen

Rechtsprechung die Voraussetzungen des Datenbankschutzes in Deutschland dargestellt werden. Weitere spannende und durch den technischen Fortschritt geförderte Fragen zu Big Data finden sich vor allem im Gesundheitswesen. Denn dabei werden regelmäßig besondere personenbezogene Daten i.S.d. § 3 Abs. 9 BDSG tangiert, die nach den Wertungen des Gesetzgebers besonderen Schutz genießen. Gleichwohl können gerade hier durch die Verknüpfung von großen Datenmengen Patientengruppen gebildet und abgeglichen werden, was zu einer gezielten und schnellen Diagnose führt. Dass hierbei zahlreiche datenschutzrechtliche Herausforderungen entstehen, liegt auf der Hand, hat doch schon das Bundesverfassungsgericht frühzeitig das Prinzip der Datensparsamkeit und das Prinzip der Zweckbindung verankert. Ausgehend davon lassen sich, auch aufgrund bereichsspezifischer Sonderregelungen, die konkreten datenschutzrechtlichen Bewertungen nur für die Einzelfälle treffen. Einen Einstieg in diese Thematik mit anschaulichen Fallbeispielen, etwa zu der soeben beschriebenen Ähnlichkeitsanalyse, lieferte der Vortrag von RA'in Brus und RA Schwab.

Big Data steht für die Wahrscheinlichkeitsberechnung aus einer Masse an Daten, was positive wie negative Entwicklungen mit sich bringen kann. RA Piltz diskutierte in seinem Vortrag daher die Notwendigkeit einer Big Data-Kommission. Ziel einer solchen sollte es sein, insbesondere ethische oder gesellschaftliche Gesichtspunkte in die Datenanalyse im Rahmen von Big Data mit einfließen zu lassen. Der Einsatz von Big Data-Kommissionen könne jedoch allenfalls dann wertvoll sein, wenn diese mit den nötigen Befugnissen ausgestattet sind, ohne dabei die freie Forschungs- und Entwicklungsmöglichkeit unnötig zu unterdrücken.

Dass sich bei der diesjährigen Herbstakademie mehrere Vorträge mit „Connected-Cars" im engeren oder weiteren Sinne befasst haben (Rammo/Holzgräfe; Reiter/Methner; Kraus; Hinzpeter), zeigt die rasant wachsende Bedeutung. Was noch vor Jahren nach Science-Fiction klang, ist schon heute greifbare Realität und in zahlreichen Fahrzeugen verbaut. Betrachtet man andere Bereiche, etwa die bereits bekannte Verschmelzung von TV und Internet (Smart-TV), ist die Erstreckung auf Fahrzeuge als logischer Schritt einer stetigen Medienkonvergenz zu bewerten. Fahrzeuge werden mit einer Internetverbindung ausgestattet, um mit anderen Fahrzeugen oder der Umwelt zu kommunizieren. Mit Einführung des für Neuwagen künftig verbindlichen sog. eCall Systems, welches bei einem Verkehrsunfall automatisch eine Verbindung zu der zuständigen Unfallleitstelle herstellt und relevante Daten (z.B. Position und Fahrtrichtung) an diese übermittelt, werden die Fahrzeuge die entsprechende Technik ohnehin eingebaut haben. Aus dem Geflecht der im Fahrzeug verfügbaren Sensoren resultiert eine Menge an Daten, die sich in Echtzeit übermitteln lassen. Dabei stehen eigentumsrechtliche Probleme (Stichwort: kein Eigentum an Daten) ebenso im Fokus der juristischen Betrachtung wie der Datenschutz. Daraus entspringen aber auch zahlreiche Folgeprobleme, etwa der Anwendbarkeit des TKG, die der Klärung bedürfen. Bei den datenschutzrechtlichen Anforderungen wird man de lege lata nicht umhinkommen, sich eine Einwilligung nach § 4a Abs. 1 BDSG beim Betroffenen einzuholen. Um hier mehr Planungssicherheit zu erhalten, wurde im Rahmen der Herbstakademie deshalb der Vorschlag für einen gesetzlichen Rahmen zur Stärkung von Datenschutz und Datensicherheit bei Fahrdaten und Fahrzeugzustandsdaten geäußert.

Natürlich konnte die mit Wirkung zum 13.6.2014 vollzogene Umsetzung der Richtlinie über die Rechte der Verbraucher (VR-RL) nicht verschwiegen werden, womit sich der kritische Vortrag von RA Vander auseinandersetzte. Einen erheblichen Änderungsbedarf brachte die VR-RL insbesondere bei der Bestimmung der Widerrufsfrist sowie der Kostentragungspflicht bei der Ausübung des Widerrufsrechts durch den Verbraucher. Trotz eines intensiven und langwierigen Gesetzgebungsverfahrens bis zur Verabschiedung der VR-RL krankt das endgültige Dokument an inhaltlichen Schwächen, so dass es nicht gelungen ist, dem Rechtsanwender ein praxisgerechtes Regelwerk an die Hand zu geben.

Wer sich einen persönlichen Eindruck von der Veranstaltung machen möchte, sollte sich bereits jetzt den 9 bis. 12.9.2015 für die Herbstakademie 2015 im Kalender mit einem Rotstift markieren. Alle Vorträge als Aufzeichnung samt Präsentationsfolien können auf der Webseite der DSRI (http://www.dsri.de) angeschaut werden. Die schriftlichen Beiträge können zudem im „Tagungsband Herbstakademie 2014" (Jürgen Taeger Hrsg., OlWIR Verlag für Wirtschaft, Informatik und Recht, ISBN-13978-3-95599-006-0) nachgelesen werden.

RA'in Barbara Buchalik,
LLR LegerlotzLaschet Rechtsanwälte

Literaturhinweise

Buchbesprechungen

Michael Wächter, **Datenschutz im Unternehmen**, Verlag C.H. Beck, 4. neue bearbeitete Aufl., 2014, 611 S., 59,00 €

Datenschutz hat sich von einer rechtlichen Spezialmaterie hin zu einer Basismaterie für Unternehmen entwickelt. Das Werk wurde deshalb neu geschrieben. Konzeption, Aufbau und Titel wurden beibehalten. Sie sind für die Neubearbeitung tragfähig. Um die Nutzung des Werkes als produktivem Text für Praktiker zu verbessern, wurden Ausführungen zu klassischen Fragestellungen gestrafft. Rechtlichen Fragestellungen zu neuen Sachverhalten im Unternehmensdatenschutz wurde mehr Raum zur Erläuterung eingeräumt. Denn Datenschutz muss im Rahmen seiner normativen Vorgaben im jeweils spezifischen Kontext zutreffend umgesetzt werden. Hierbei geht es um den richtigen Umgang mit Datenschutz im Unternehmen. Bei der Umsetzung helfen aktuelle gesetzliche Vorschriften und Rechtsprechungsgrundsätze. Sie wurden eingearbeitet. Schwerpunkt des Werkes ist es aber, die Zielsetzung gesetzlicher Regelungsvorgaben an Hand von Praxisbeispielen „auf den Punkt" zu bringen. Das abstrakte BDSG wird auf diese Weise fallbezogenen konkretisiert.

Der Umfang der einzelnen Kapitel hat sich zur Vorauflage – orientiert an der jeweiligen Praxisrelevanz – verändert. Manche Fragestellungen haben sich weitgehend erledigt. Sie sind nicht mehr aktuell oder es herrscht weitgehende Klarheit. Dem Thema Datensicherheit wurde ein sehr viel breiterer Raum eingeräumt. Datenschutz muss heute in erster Linie durch Maßnahmen zur Datensicherung für Datenbestände und zur Sicherheit der IT, Kommunikation gewährleistet werden. Hinzu kommt die Handhabung von Unterlagen und Dokumenten. Durch die heute umfassende Nutzung der IT in vielen Unternehmen durch eine hohe Anzahl von Personen wurde im Werk der Perspektive der Nutzer und Betroffenen größerer Raum eingeräumt. Das Selbstverständnis zum Datenschutz variiert heute sehr stark. Für Unternehmen ist Datenschutz allerdings trotz einer Vielfalt von Meinungen zu dem Thema zum unabdingbaren Bestandteil zur Gewährleistung von Compliance geworden. Er ist damit auf allen Ebenen im Unternehmen betrieblich-organisatorisch zu implementieren.

Die überarbeitung der Neuauflage konzentriert sich auf drei Schwerpunkte:

- personenbezogene Datenverarbeitung zur Unterstützung primärer Vertragszwecke
- neue Phänomene intensiver Datenverarbeitung, wie z.B. Vernetzung, Business Anatics und Cloud Computing
- moderne Sachverhalte des Arbeitnehmerdatenschutzes. Hierzu werden im Werk betrieblich-organisatorische Konzepte entwickelt.

Das Werk wendet sich an Personal- und EDV-Abteilungen, Datenschutzbeauftragte, Betriebsräte, Rechtsanwälte sowie an Justiziare und Richter.

(Redaktion)

Utz Schliesky/Christian Hoffmann/Anika D. Luch/Sönke E. Schulz/Kim Corinna Borchers, **Schutzpflichten und Drittwirkung im Internet –** Das Grundgesetz im digitalen Zeitalter, DIVSI-Perspektiven Band I, Nomos Verlagsgesellschaft Baden-Baden, 2014, 184 S., 48,00 €

Die Schrift ist der erste Band einer vom Deutschen Institut für Vertrauen und Sicherheit im Internet konzipierten neuen Schriftenreihe. Die stattfindende Diskussion um die Frage, ob der Staat die umfassende Sicherheit der Bürger im Netz, die Vertraulichkeit ihrer Daten und die Integrität ihrer informationstechnischen Systeme garantieren muss bzw. kann, wird eingeleitet durch ein Geleitwort von Roman Herzog. Ausgangspunkt sind die Debatten um die umfangreichen Ausspähaktivitäten der NSA und zum problematischen Umgang privater Internet-Dienste mit den personenbezogenen Daten der Nutzer auf, durch welche neue Bedrohungsszenarien offenbart und daraus resultierende Schutzdefizite im globalen digitalen Raum aufgedeckt wurden. Infolgedessen wird häufig das Grundgesetz herangezogen und kritisiert, dass es nur defizitären Schutz im Rahmen internationaler Kommunikation und Interaktion gewährleiste. Daher erscheint es folgerichtig zu analysieren, inwiefern es sinnvoll ist, die grundrechtlichen Wirkungsdimensionen fortzuentwickeln. Schutzpflichten und mittelbare Drittwirkung sind anerkannte Argumentationsmuster, die sich jedoch auch im digitalen Raum bewähren müssen. Darüber hinaus werden weitere denkbare Reaktionsmöglichkeiten des Staates untersucht, damit dieser seinem verfassungsrechtlichen Schutzauftrag möglichst vollumfänglich nachkommen kann, wobei sich diese in rechtliche und tatsächliche Reaktionsmöglichkeiten einteilen lassen.

Dort, wo das Grundgesetz anwendbar ist und Geltung beansprucht, vermittelt es effektiven Schutz, dort wo es nicht gilt, handelt es sich um das falsche Regelungsinstrument, so dass auch eine Fortentwicklung nicht zielführend ist. Eine nationalstaatliche Verfassung und ihre Grundrechte, auch in einer erweiterten Wirkungsperspektive, sind nicht geeignet, internationale Sachverhalte zu reglementieren. Ob und wie sich diese „Lücke" zeitnah schließen lässt, kann hier nicht weiter vertieft werden. Es ist jedoch an der Zeit, eine gesellschaftliche Diskussion über die Rolle des Staates in der digitalen, kaum noch nationalstaatlich steuerbaren Welt zu führen. Es bleibt zu hoffen, dass die ernüchternde Einschätzung zur Frage, ob die Politik und Gesellschaft bereit wären, die Herausforderungen von Big Data zu bewältigen, nicht ganz allgemein für die hier beschriebenen aktuellen Konfliktlinien der digitalen Welt gilt.

(Redaktion)

Stefan Strohmeier, Franca Piazza (Hrsg.), **Human Resource Intelligence und Analytics – Grundlagen, Anbieter, Erfahrungen und Trends**, Springer Gabler, Wiesbaden 2015, 378 S., 49,99 €

Das Buch beschäftigt sich umfassend mit der Bereitstellung und Verwendung entscheidungsunterstützender Informationen im Human Resource Management. Dazu wird der Themenbereich Human Resource Intelligence und Analytics (HRIA) aus den unterschiedlichen Perspektiven der Wissenschaft, der Anbieter und der Anwender durch jeweils einschlägige Spezialisten beleuchtet. Leser erhalten so ein umfassendes und facettenreiches Portfolio an Beiträgen mit zahlreichen Informationen zu zentralen Fragestellungen der HRIA. Ein erster Teil geht auf Grundlagen ein und führt in die Analysen, die Prozesse, die Systeme und die rechtliche Regelungen der HRIA ein, wozu auch der von Gola behandelte Datenschutz gehört. In einem zweiten Teil stellen mit ROC, SAP und SAS bedeutende Anbieter ihre Lösungen und Dienstleistungen im Bereich der HRIA vor. In einem dritten Teil berichten Allianz, F. Hoffman-La Roche und Kromberg & Schubert von ihren Erfahrungen mit der Einführung und Anwendung der HRIA. Abschließend werden in einem vierten Teil zentrale Trends der HRIA vorgestellt.

(Schriftleitung)

Spiros Simitis (Hrsg.), **Bundesdatenschutzgesetz**, 8. neu bearbeitete Aufl., Nomos, Baden-Baden, 2014, 2072 S., 198,00 €

Nur einige wenige Kommentare haben das BDSG bereits seit seinem Erscheinen begleitet. Der Simitis gehört hierzu und hat für Rechtsprechung und Literatur von Anfang an bei der Interpretation der Rechtsnormen wesentliche Wegzeichen gesetzt. In jüngerer Zeit kamen neue Kommentare hinzu, wobei keiner die Auffassungen im Simitis außen vor lassen konnte. Das Datenschutzrecht in Deutschland hat durch den Simitis wesentlich seine Gestalt erhalten. Der Verlag bezeichnet das Buch als Großkommentar und das in zweifacher Hinsicht zu Recht. Mit seinen nunmehr 2072 Seiten (rund 200 mehr als in der Vorauflage) ist er nicht nur bezogen auf das äußere Bild des Buches „gewichtig" und damit die wohl umfangreichste Kommentierung des BDSG. Gewichtig ist vor allem seine wissenschaftliche Durchdringung der Materie, die jedoch den notwendigen Praxisbezug nicht zurückstehen lässt. Ein u.a. besonders hervor zu hebendes Beispiel ist die von Seifert vorgenommene Kommentierung des § 32 BDSG, die umfangmäßig um 50 Prozent zugenommen hat und mit ihren rund 90 eng bedruckten Seiten gesondert auch als eigenes kleines „Handbuch" zum Beschäftigtendatenschutz fungieren könnte. Eine detaillierte Historie des nationalen und internationalen Datenschutzrechts in Gesetzgebung und Rechtsprechung gibt die über 100 Seiten ausmachende Einleitung wieder, wobei die Beurteilung der derzeitig bekannten Regelungen der EU-DS-GVO durch Simitis natürlich von aktuellem Interesse ist. Ein Fazit für den Kommissionsvorschlag fällt dahin aus, dass er allein schon wegen der für die Betroffenen ebenso wie für die verantwortlichen Stellen eigentlich nicht erkennbaren Folgen vieler seiner wichtigsten Vorschriften unhaltbar sei.

Insgesamt betrachtet gilt: Die 8. Auflage bringt das Werk auf den neuesten Stand und berücksichtigt auch als Blick in die Zukunft die aktuelle Diskussion um die EU-DS-GVO, die insbesondere der Globalisierung der Verarbeitung von Daten und dem Internet als Kommunikationsmittel Rechnung zu tragen hat. Ein Schwerpunkt ist der Ausbau der informationellen Selbstbestimmung insbesondere im Hinblick der Datenverarbeitungen durch in- und ausländische Sicherheitsbehörden.

Das bisherige namhafte 10köpfige Autorenteam ist beisammen geblieben und gewährleistet die Kontinuität der Überarbeitung. Für alle, die sich etwas grundlegender mit Fragen des Datenschutzes zu befassen haben, gehört der aktuelle Simitis mit zur Grundausrüstung. Das gilt für die, die das Werk bisher nicht hatten genauso wie für Besitzer der 7. Auflage.

Prof. Peter Gola, Königswinter

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.

Lennart Elkin/Cay Fürsen,
Unternehmenszugehörigkeit im Internet, NZA 2014, S. 1111 ff.
Sind Mitarbeiter in beruflichen Netzwerken unkündbar? lautet der Untertitel des Beitrags, mit dem auf die Problematik hingewiesen wird, dass in selbstveröffentlichten Lebensläufen Angaben zur aktuellen Beschäftigungssituation ggf. überholt sind, da das Profil nach der Beendigung der Beschäftigung nicht geändert wurde. Dem ehemaligen Arbeitgeber werden allein schon in Bezug auf Haftung, Marketing und Reputation Wege aufgezeigt, um auch die virtuelle Unternehmenszugehörigkeit auf der Basis des § 241 Abs. 2.2 BGB herbeizuführen. Angezeigt sei es, vor der Unterlassungsklage bzw. der entsprechenden einstweiligen Verfügung per Abmahnung eine strafbewehrte Unterlassungserklärung einzufordern.

Bernd Liedke, **BIG DATA – small information: Muss der datenschutzrechtliche Auskunftsanspruch reformiert werden?, K&R 2014, S. 709 ff.**
Der Autor beantwortet die gestellte Frage mit positivem Ergebnis.

Wulf Kamlah/Oliver Hornung, **Zur Übermittlung sogenannter Negativdaten an Auskunfteien, PinG 2014, S. 265 ff.**
Die Autoren zeigen an Hand der zu § 28a BDSG ergangenen Rechtsprechung die Reichweite dieser Erlaubnisnorm auf und bewerten die Norm als den beteiligten Interessen ausgewogen gerecht werdende Regelung.

Rainer Knyrim/Gerald Trieb, **Videokameras in Autos – vom Teufelszeug zum Beweismittel, ZD 2014, S. 547 ff.**
Der Beitrag äußert sich zur Vereinbarkeit von Dash-Cams mit datenschutzrechtlichen Grundsätzen und kommt zu dem Ergebnis, dass je nach den technischen Spezifikationen der Aufzeichnungstechnik, insbesondere wenn die Kameras erst im Unfallzeitpunkt als „Crash-Cam“ fungieren, die Zulässigkeit zu bejahen ist.

Alexander Koch, **Rechtliche und ethische Verschlüsselungspflichten?, DuD 2014, S. 691 ff.**
Am Beispiel der Anwaltschaft untersucht der Autor der Frage, ob bereits heute für Berufsgeheimnisträger eine rechtliche Verpflichtung zur Verschlüsselung bei der Übermittlung von Berufsgeheimnissen besteht oder sich aus standesrechtlichen Grundsätzen ableiten lässt. Während er eine allgemeine rechtliche Verschlüsselungspflicht negiert, bejaht er sie aus berufsethischen Gesichtspunkten und aus Haftungsgründen.

Bruno Schierbaum, **Zulässige Verarbeitung von Beschäftigtendaten. Die zentralen Vorgaben der Landesdatenschutzgesetze, CuA 10/2014, S. 14 ff.**
Erläutert werden die in den Landesdatenschutzgesetzen enthaltenen, aber im Detail nicht übereinstimmenden Vorschriften für die Datenverarbeitungen in Dienst- und Arbeitsverhältnissen, die jedoch nur für Arbeitnehmer des jeweiligen öffentlichen Dienstes gelten, da das Beamtenrecht bereits seit Langem ein speziell geregeltes „Personalaktenrecht“ hat.

Sylle Schreier-Bestmann/Martin John, **Datenschutz- und wettbewerbsrechtliche Anforderungen an Werbemaßnahmen während „Inbound“-Telefonaten mit Verbrauchern unter Berücksichtigung der Anwendungshinweise des Düsseldorfer Kreises, PinG 2014, S. 258 ff.**
An Fallbeispielen wird belegt, dass im Rahmen von Inbound-Telefonaten platzierte Werbeangebote, sofern sie die Grenze einer unzumutbaren Belästigung nicht tangieren, zulässig sind. Gleiches gilt für die Einholung der zu dokumentierenden und nachträglich zu bestätigenden Einwilligung des Kunden in nachfolgende werbliche Telefon- und E-Mail-Kontakte.

Aus den Anfängen von Datenschutz und Datensicherheit

Gestufte Sicherheit

Als der Datenschutz noch in den Kinderschuhen steckte und die erste RDV noch nicht erschienen war, befasste sich die Gesellschaft noch nicht mit Datenschutzfragen sondern mit Verkehrserziehung. Der 7. Sinn wurde von 1966 bis 2005 ausgestrahlt. Es war eine Fernsehsendung mit Tipps zur Sicherheit im Straßenverkehr. Anhand von eindringlichen Darstellungen von gefährlichen Verkehrssituationen wurde man für Gefahren sensibilisiert. Man konnte lernen, dass man sich mit einem Cabriolet – selbst mit Überrollbügel – weniger sicher überschlägt, als mit einem geschlossenen Fahrzeug. Oder dass man auf feuchter, laubbedeckter Fahrbahn im Herbst leichter aus der Kurve fliegt, als bei trockener und freier Fahrbahn. Es ging in der Sendung nicht darum, den Menschen das Autofahren im Herbst oder mit dem Cabriolet madig zu machen. Vielmehr lernte man dort – so drückte es der Bundesinnenminister auf dem nationalen IT-Gipfel 2014 aus – was gestufte Sicherheit bedeutet, nämlich dass von mehreren möglichen Verhaltensweisen manche sicherer sind als andere. Mit diesem Wissen kann man die Verantwortung für mehr oder weniger sicheres Verhalten übernehmen und sein Handeln in freier Entscheidung sicherer oder weniger sicher gestalten. Man trägt dann das Risiko der Freiheit bewusst.

Eine Aufklärung über gestufte Sicherheit und die Folgen weniger sicheren Verhaltens tut auch für die Nutzung des Internets Not. Sich im Internet zu bewegen ist nicht nur sinnvoll und in vielen Bereichen des modernen Lebens unabdingbar. Jedem sollte klar sein, dass Online-Banking am heimischen Computer und Online-Shopping im Netz weniger sicher sind, als seine Zahlungsvorgänge in bar oder unter persönlicher Vorsprache am Bankschalter. Ebenso wichtig ist es, dass sich die Menschen mit der Frage auseinander setzen, wie sie ihren Online-Verkehr so sicher gestalten, dass er ihnen sicher genug ist. Das fängt beim aktuellen Virenscanner und regelmäßigen Softwareupdates der Computer und Smartphones an und hört noch lange nicht beim verantwortungsbewussten Einsatz von Passwörtern auf. Niemand sollte sich grundsätzlich von der Nutzung des Netzes abschrecken lassen. Es ist aber fahrlässig und falsch zu glauben, man könne seine Sicherheit im Netz Anderen oder gar dem Staat überlassen. Auch im Straßenverkehr muss er nur Straßen bauen, Verkehrsregeln schaffen und deren Einhaltung durchsetzen. Für die Entscheidung, ob man ein Cabrio oder einen sicheren Wagen fährt oder mit welcher Geschwindigkeit man in eine Kurve fährt ist jeder selbst verantwortlich. Einen siebten Sinn benötigen wir jedenfalls nicht nur, um die Gefahren im Verkehr einzuschätzen, sondern auch, um moderne Online-Dienste möglichst sicher zu nutzen.