ISSN 0178-8930

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

2/2014

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

SCHWARTMANN / THEODOROU – Aktuelle Rechtsprechung des EuGH zum Datenschutzrecht

KREMER – Datenschutzerklärungen von Social Media Diensten: Anwendbares Recht und AGB-Kontrolle

KIPKER / VOSKAMP – PRISM und staatliche Schutzpflichten – ein politisches Märchen?

Kurzbeiträge

GOLA – Aus den aktuellen Berichten der Aufsichtsbehörden (12)

KLUG – Die Position des EU-Parlaments zur zukünftigen Rolle von Datenschutzbeauftragten – ein kommentierter Überblick

WRONKA – Anmerkungen zu den Verhaltensregeln der Deutschen Versicherungswirtschaft

Rechtsprechung

Aus dem Inhalt

BAG, Entlassung wegen HIV-Infektion ist diskriminierend (Ls)

BAG, Beweisverwertungsverbot heimlicher Videoüberwachung am Arbeitsplatz

BAG, Verpflichtung zur Nutzung einer elektronischen Signaturkarte und der dazu erforderlichen Datenweitergabe an den Zertifizierungsdiensteanbieter

BAG, Verwertung von Beweismitteln aus heimlicher Schrankkontrolle

BAG, Keine AGG-Entschädigungsansprüche gegenüber Personalvermittler (Ls)

30. Jahrgang
April 2014
Seiten 59–116

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

BLUE COAT®

SIE HABEN MEHR ALS EINE SANDBOX VERDIENT: Advanced Threat Protection

Advanced Threat Protection:

- **Phase 1: Blockieren bekannter Bedrohungen**
- **Phase 2: Analysieren unbekannter Bedrohungen und Gefahren eingrenzen**
- **Phase 3: Ermitteln und Beseitigen der Bedrohung**

ERKENNEN SIE UNBEKANNTE MALWARE IN IHRER INFRASTRUKTUR RECHTZEITIG

Hier können Sie wertvolle Whitepaper und Reports* u.a. zum Thema Sandbox herunterladen >

*powered by KASPERSKY

http://dc.bluecoat.com/ATPLifecycleDefenseAd

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

30. Jahrgang 2014
Heft 2
Seiten 59–116

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 59

Veranstaltungen 60

Aufsätze

Rolf SCHWARTMANN / Elissavet THEODOROU
Aktuelle Rechtsprechung des EuGH zum Datenschutzrecht **61**

Sascha KREMER
Datenschutzerklärungen von Social Media Diensten: Anwendbares Recht und AGB-Kontrolle **73**

Dennis-Kenji KIPKER / Friederike VOSKAMP
PRISM und staatliche Schutzpflichten – ein politisches Märchen? **84**

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten der Aufsichtsbehörden (12) **88**

RA Christoph KLUG
Die Position des EU-Parlaments zur zukünftigen Rolle von Datenschutzbeauftragten – ein kommentierter Überblick **90**

RA Dr. Georg WRONKA
Anmerkungen zu den Verhaltensregeln der Deutschen Versicherungswirtschaft **93**

Rechtsprechung

Entlassung wegen HIV-Infektion ist diskriminierend (Ls)
(BAG, Urteil vom 19.12.2013) **96**

Beweisverwertungsverbot heimlicher Videoüberwachung am Arbeitsplatz
(BAG, Urteil vom 21.11.2013) **96**

Verpflichtung zur Nutzung einer elektronischen Signaturkarte und der dazu erforderlichen Datenweitergabe an den Zertifizierungsdiensteanbieter
(BAG, Urteil vom 25.09.2013) **98**

Verwertung von Beweismitteln aus heimlicher Schrankkontrolle
(BAG, Urteil vom 20.06.2013) **103**

Keine AGG-Entschädigungsansprüche gegenüber Personalvermittler (Ls)
(BAG, Urteil vom 23.01.2013) **108**

Unzulässige Androhung einer Datenübermittlung an die Schufa
(OLG Celle, Urteil vom 19.12.2013) **108**

Unzumutbare Belästigung durch trotz Widerspruch, „An die Bewohner des Hauses" gerichtete Werbepost
(OLG München, Urteil vom 05.12.2013) **110**

Kein Anspruch auf Medienöffentlichkeit von Gemeinderatssitzungen (Ls)
(HessVGH, Urteil vom 31.10.13) **110**

BR-Zuständigkeit bei Regelung der angestrebten unternehmensweiten Vorlagepflicht von Arbeitsunfähigkeitsbescheinigungen (Ls)
(LAG Köln, Beschluss vom 21.08.2013) **111**

Zur Zulässigkeit der Anordnung eines Drogentests durch die Agentur für Arbeit (Ls)
(LG Heidelberg, Urteil vom 22.08.2013) **111**

Diskriminierung bei Ablehnung einer Bewerberin mit 7-jährigem Kind (Ls)
(LAG Hamm, Urteil vom 06.06.2013) **111**

Berichte, Informationen, Sonstiges

BMJV: „Mailen, Surfen, Chatten – wie ist die Privatsphäre zu retten?" **112**

EU-Datenschutz-Konföderation CEDPO im Aufwind **113**

Zur Auskunft über Scorewertberechnung **113**

Literaturhinweise

Buchbesprechungen

Däubler / Klebe / Wedde / Weichert, Bundesdatenschutzgesetz (WRONKA) **114**

Neuerscheinungen

Aufsätze **115**

Nachgefasst **116**

Beilagenhinweis GDD-Mitteilungen 2/2014, Tagungsbericht 37. DAFTA; DATAKONTEXT, Frechen

Manuskripte
Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an die Schriftleitung erbeten. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Sie können nur zurückgesandt werden, wenn Rückporto beigefügt ist. Beiträge werden grundsätzlich nur angenommen, wenn sie nicht einer anderen Zeitschrift zur Veröffentlichung angeboten wurden. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Autor alle Rechte, insbesondere das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken mit Hilfe fotomechanischer oder anderer Verfahren.

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

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

Erscheinungsweise
6 x jährlich

Bezugspreis
Jahresabonnement € 139,–
Einzelheft € 25,–
MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Bestellungen
DATAKONTEXT
Verlagsgruppe Hüthig Jehle Rehm GmbH
Standort Frechen
Jürgen Weiß
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-71
Telefax: (0 22 34) 9 89 49-32
E-Mail: weiss@datakontext.com
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Abbestellungen
Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Verlag
DATAKONTEXT
Verlagsgruppe Hüthig Jehle Rehm GmbH
Standort Frechen
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-30
Telefax: (0 22 34) 9 89 49-32
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Satz
alka mediengestaltung gmbh
Ottostraße 6, 53332 Bornheim-Sechtem

Druck
AZ Druck und Datentechnik GmbH
Heisinger Straße 16, 87437 Kempten

Anzeigenverwaltung
DATAKONTEXT
Verlagsgruppe Hüthig Jehle Rehm GmbH
Thomas Reinhard-Rief
Hultschiner Straße 8
D-81677 München
Telefon: (089) 21 83-89 35
Fax: (089) 21 83-96 02 33
E-Mail: reinhard@datakontext.com
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Zeitschrift für
Datenschutz-, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
30. Jahrgang 2014 Heft 2
Seiten 59–116

RDV
Recht der Datenverarbeitung

30. Jahrgang · April 2014 · Seiten 59–116

Editorial

Datenschutz in der Warteschleife

In diesen Tagen wartet Europa auf wichtige Weichenstellungen des Europäischen Gerichtshofs. Er wird bald die Richtung für die Frage der Vorratsdatenspeicherung ebenso vorgeben, wie er einen rechtlichen Rahmen für den Einsatz von Suchmaschinen stecken wird. Unabhängig davon steht die Datenschutz-Grundverordnung aus. Obwohl das Europäische Parlament sich im März 2014 fast einstimmig für sie ausgesprochen hat, ist das Schicksal ihrer konkreten Ausgestaltung mit Blick auf die in diesem Sommer neu beginnende europäische Legislaturperiode und die schwierigen Verhandlungen im Europäischen Rat ein wenig ungewisser geworden. Ungeachtet dessen warten die Mitgliedstaaten und insbesondere auch Deutschland auf die Vorgaben aus Brüssel und Luxemburg. Das ist unbefriedigend, denn es stehen ausweislich des Koalitionsvertrages von 2013 bedeutende innerstaatliche Regelungen an, die der Gesetzgeber nicht ohne europäischen Rahmen angehen will. Sie reichen von der Vorratsdatenspeicherung bis zum Beschäftigtendatenschutz.

Auch über Europa hinausgehend drängt der Datenschutz zunehmend in den Fokus der Diskussion. Er bestimmt den Fortgang der Verhandlungen über das Freihandelsabkommen zwischen Europa und den Vereinigten Staaten, ebenso die Frage nach der Aussetzung oder Kündigung etwa des Safe Harbour Abkommens. Daneben befassen nationale Gerichte sich etwa mit der Frage der Anwendbarkeit deutschen Rechts bei der Benutzung amerikanischer Dienste auf innerstaatlichem Territorium.

Die wachsende Bedeutung des europäischen und internationalen Datenschutzes haben die Herausgeber der RDV veranlasst, sich diesem Thema einmal im Jahr mit einem Schwerpunktheft zu widmen. Die Hauptbeiträge dieser Ausgabe befassen sich dementsprechend zum einem mit einem Überblick über aktuelle Entscheidungen des Europäischen Gerichtshofs zum Datenschutzrecht. Sie sollen einen Eindruck von der aktuellen Entscheidungslage sowie von anstehenden Entscheidungen geben, zu denen die Generalanwälte bereits votiert haben. Nach diesem Überblick soll das für die Praxis zentrale Thema der Datenschutzerklärungen von Social Media Diensten und das darauf anwendbare Recht erörtert werden. Schließlich geht es im dritten Beitrag um staatliche Schutzpflichten gegen das Ausspähen von Daten durch ausländische Geheimdienste.

Zugleich liegt diesem Heft erstmals eine Sonderveröffentlichung bei, die eine Niederschrift des Eröffnungsvormittages der Datenschutzfachtagung des Jahres 2013 enthält. Sie stand unter der Überschrift „Big Data – Big Responsibility“. Die Beilage enthält neben dem Beitrag von Johannes Masing zum Datenschutz als unterentwickeltes Grundrecht auch alle anderen Vorträge und Wortbeiträge der Kölner Veranstaltung. Die Qualität der Beiträge machte diesen Schritt erforderlich und wir freuen uns, Ihnen diesen Service mit Unterstützung von LLR Rechtsanwälte und der LLR Data Security and Consulting GmbH anbieten zu können. Zugleich danke ich allen Beteiligten für ihre Mitwirkung bei der Umsetzung dieses Projekts.

Rolf Schwartmann

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

Termin	Thema	Ort	Kontakt
29.04.2014	7. KommunalerDatenschutzkongress in Nordrhein-Westfalen	Duisburg	KommunalAgentur-NRW GmbH, Tel.: 0211/43077-0 info@Kommunal-AgenturNRW.de www.Kommunal-AgenturNRW.de
06.-07.05.2014	Datenschutz-Management – Teil 3	Köln	GDD e.V. und DATAKONTEXT
07.05.2014	Datenschutzprüfungen der Aufsichtsbehörden	Düsseldorf	GDD e.V. und DATAKONTEXT
08.05.2014	Audit Technisch-organisatorischer Datenschutz	Köln	GDD e.V. und DATAKONTEXT
12.05.2014	Rechtssichere Personaldatenverarbeitung und Prozesse	Stuttgart	GDD e.V. und DATAKONTEXT
12.05.2014	Die 30 häufigsten Datenschutz-Schwachstellen und deren Lösung	Frankfurt/M.	GDD e.V. und DATAKONTEXT
19.05.2014	Datenschutz und IT-Sicherheit beim Einsatz mobiler Endgeräte	Düsseldorf	GDD e.V. und DATAKONTEXT
20.05.2014	Cloud Computing: Datenschutz und IT-Sicherheit	Düsseldorf	GDD e.V. und DATAKONTEXT
21.05.2014	Repetitorium GDDcert.	Köln	GDD e.V. und DATAKONTEXT
22.05.2014	Auftragsdatenverarbeitung	Düsseldorf	GDD e.V. und DATAKONTEXT
26.05.2014	Prüfung von SAP-Systemen durch Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
26.05.2014	Datenschutz im Personalwesen – Transparenz bei Personal-prozessen	Köln	GDD e.V. und DATAKONTEXT
03.06.2014	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert.)	Köln	GDD e.V. und DATAKONTEXT
04.06.2014	Datenschutz im Unternehmen richtig positionieren	Köln	GDD e.V. und DATAKONTEXT
17.06.2014	„DIN 66399" – Die neue Norm zur Datenträgervernichtung	Köln	GDD e.V. und DATAKONTEXT
25.06.2014	Social Media im Unternehmen	Köln	GDD e.V. und DATAKONTEXT
26.06.2014	Herausforderung: Internationaler Datenverkehr	Stuttgart	GDD e.V. und DATAKONTEXT
23.-27.06.2014	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Potsdam	GDD e.V. und DATAKONTEXT
27.06.2014	Die Datenpanne! Ein Albtraum jedes Unternehmens	Frankfurt/M.	GDD e.V. und DATAKONTEXT
15.09.2014	Rechtssichere Personaldatenverarbeitung und Prozesse	Düsseldorf	GDD e.V. und DATAKONTEXT
16.09.2014	Praxisfragen beim betrieblichen Internet- und E-Mail-Einsatz	Düsseldorf	GDD e.V. und DATAKONTEXT
22.-26.09.2014	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
29.-30.09.2014	Datenschutz Kompakt	Frankfurt/M.	GDD e.V. und DATAKONTEXT

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

Aufsätze

Rolf Schwartmann / Elissavet Theodorou

Aktuelle Rechtsprechung des EuGH zum Datenschutzrecht

Datenschutz ist seit langem nicht mehr nur von nationalen Vorschriften geprägt. Das europäische Recht in der Auslegung des Europäischen Gerichtshofs hat längst auch den Wirkungskreis der betrieblichen Datenschutzbeauftragten erreicht. Der Beitrag stellt die wichtigsten aktuellen Entscheidungen vor.

I. Einleitung

Dass Daten als digitalisierte Privatheit ein kostbares Gut sind, hat längst die Grenzen des Wirkungsbereichs des betrieblichen Datenschutzbeauftragten überschritten. Daten sind gleicher maßen Objekt des Zugriffs von Geheimdiensten wie von Milliardengeschäften unter Kommunikationsdiensten. In allen Fällen geht es um die Speicherung, Auswertung und Löschung von Daten, die in Europa in der Regel eine Einwilligung des Nutzers oder eine gesetzliche Ermächtigung voraussetzen. Die Reichweiten dieser Vorgänge und deren rechtliche Bewertung beschäftigen zunehmend auch die nationalen und internationalen Gerichte. Im nationalen deutschen Recht ist Datenschutz seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 als „Recht auf informationelle Selbstbestimmung“ ausgestaltet[1]. Es beschreibt das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Im Zuge der Anpassung an die technologischen Gegebenheiten ist 2008 als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts[2] das Recht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ hinzugetreten. Es dient dem Schutz personenbezogener Daten, die in informationstechnischen Systemen gespeichert oder verarbeitet werden. Ein explizites Datenschutzgrundrecht ist im Grundgesetz allerdings nicht normiert[3].

Im Zuge der Europäisierung wird das deutsche Datenschutzrecht durch europäisches Recht überformt. Dies gilt bereits jetzt, wobei die Harmonisierung des Datenschutzrechts in Europa durch die Verabschiedung der EU-Datenschutzgrundverordnung voranschreiten wird. Dieser Beitrag soll im Vorfeld der Verordnung einen Überblick über die Entscheidungen des Europäischen Gerichtshofs zum Datenschutzrecht geben.

Grundlegend für das Verständnis des Datenschutzes im Internet – und deshalb vorab zu benennen – ist die Entscheidung „Lindqvist“ aus dem Jahre 2003[4]. Hier hatte eine schwedische Katechetin persönliche Informationen aus ihrer Kirchengemeinde im Internet veröffentlicht, und es ging um die dortige Zulässigkeit der Verwendung von personenbezogenen Daten. Der EuGH setzte sich hier mit grundlegenden datenschutzrechtlichen Begriffen wie dem der personenbezogenen Daten, der automatisierten Datenverarbeitung sowie der Übermittlung personenbezogener Daten in ein Drittland auseinander. Die Nennung des Namens einer Person in Verbindung mit ihrer Telefonnummer oder mit Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigungen falle ebenso unter den Begriff der personenbezogenen Daten wie Informationen über den Gesundheitszustand einer Person[5]. Personenbezogene Daten auf einer Homepage zu veröffentlichen, sei als automatisierte Verarbeitung anzusehen[6]. Allerdings stelle die Aufnahme und Zugänglichmachung dieser Daten im Netz für jede Person, die eine Verbindung zum Internet herstellt, noch keine Übermittlung in ein Drittland dar[7]. Schließlich, so der EuGH, sei es Sache der Mitgliedsstaaten, ein angemessenes Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Meinungsfreiheit sicher zustellen[8].

II. Datenschutz im europäischen Rechtssystem

Die Europäischen Gerichte, namentlich der Europäische Gerichtshof für Menschenrechte (EGMR) für den Bereich des Europarats[9] und - seit der Geltung des Vertrages von Lissabon - auch der EuGH für die Staaten im Geltungsbereich der Europäischen Union, können, anders als die deutsche Rechtsprechung, auf explizite Datenschutzgrundrechte zurückgreifen. Für die Mitgliedsstaaten des Europarats wird in Art. 8 EMRK das

1 BVerfGE 65, 1; dazu Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, S. 53-63.

2 BVerfG, 27.02.2008 – Az. 1 BvR 370/07, 1 BvR 595/07; dazu Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, S. 53-63.

3 Masing, Datenschutz – ein unterentwickeltes Grundrecht? In Schwartmann/Jaspers, Big Data – Big Responsibility, Sonderveröffentlichung zur RDV 02/2014, S. 3-9 (3).

4 EuGH, Urteil vom 06.11.2003, C-101/01 – „Lindqvist“; s. hierzu Anm. Roßnagel, EuGH: Personenbezogene Daten im Internet, MMR 2004, 95; Dammann, Der EuGH im Internet – Ende des internationalen Datenschutzes?, RDV 2004, 19-21.

5 EuGH, Urt. v. 06. 11.2003, C–101/01, Lindquist, Rn 24, 50, 51.

6 EuGH, Urt. v. 06. 11.2003, C–101/01, Lindquist, Rn 25, 26.

7 EuGH, Urt. v. 06. 11.2003, C–101/01, Lindquist, Rn 68-71.

8 EuGH, Urt. v. 06. 11.2003, C–101/01, Lindquist, Rn 90.

9 Im Rahmen dieses Beitrages bleibt die Rechtsprechung des EGMR unberücksichtigt. Vgl. dazu z.B. EGMR, Urt. v. 04.12.2008 – 30562/04, 30566/04; Urt. v. 03.04.2007 – 62617/00; Urt. v. 03.04.2012 – 41723/06; Entsch. v. 05.10.2010 – 420/07; Urt. v. 14.04.2009 – 37374/05; Entsch. v. 29.06.2006 – 54934/00.

Recht auf Achtung des Privat- und Familienlebens gewährt, das auch den Datenschutz umfasst[10].

Im Recht der Europäischen Union enthält die Charta der Europäischen Grundrechte (GRC) ein ausdrückliches Datenschutzgrundrecht, das in Art. 8 Abs. 1 GRC unter der Überschrift „Schutz personenbezogener Daten" einer jeden Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten gewährt. In Art. 8 Abs. 2 GRC sind die Grundsätze einer zulässigen Datenverarbeitung sowie das Auskunftsrecht jeder Person über die sie betreffenden erhobenen Daten und der Anspruch auf Berichtigung dieser normiert. Zudem ist der Schutz personenbezogener Daten in Art. 16 Abs. 1 AEUV in wortgleicher Übereinstimmung mit Art. 8 Abs. 1 GRC geregelt.

Auf sekundärrechtlicher Ebene finden sich konkrete datenschutzrechtliche Vorgaben in der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (RL 1995/46/EG) sowie in der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (RL 2002/58/EG). Letztere wurde durch die sog. „Cookie-Richtlinie"[11] geändert. Die Änderungen betreffen insbesondere die Nutzung von Cookies, also Textdateien, die vom Webserver im Computer des Web-Clients platziert werden, auf Webseiten und sollen mehr Transparenz und Sicherheit für die Verbraucher schaffen. So enthält die „Cookie-Richtlinie" Vorgaben zur benutzerfreundlichen Gestaltung der Verwendung von Cookies sowie zum Erfordernis einer Einwilligung beim Einsatz von Cookies. Obwohl die Umsetzungsfrist ebenfalls abgelaufen ist, ist diese Richtlinie in Deutschland mit Verweis auf bestehende nationale Regelungen sowie auf das Erfordernis der Klärung praktischer Fragen bislang nicht umgesetzt worden.

Weitere sekundärrechtliche Vorgaben speziell in Bezug auf die Vorratsspeicherung von Daten waren in der „Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden," (RL 2006/24/EG) enthalten. Der EuGH hat jüngst diese Richtlinie aufgrund einer Unvereinbarkeit mit der EU-Grundrechte-Charta für ungültig erklärt[12].

Ebenfalls auf sekundärrechtlicher Ebene sind datenschutzrechtliche Bestimmungen mit Verbindlichkeit für die Organe der EU in der Verordnung VO (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, die sog. Datenschutzverordnung, enthalten.

Die Luxemburger Richter werden bei der Auslegung sowie bei der Überprüfung der Einhaltung der europäischen datenschutzrechtlichen Vorgaben auf unterschiedliche Veranlassung aktiv. So hat der Europäische Gerichtshof im Rahmen von Vorabentscheidungsverfahren nach Art. 267 AEUV auf Ersuchen eines nationalen Gerichts über die Auslegung der sekundär rechtlichen datenschutzrechtlichen Vorgaben und deren Vereinbarkeit mit nationalen Bestimmungen zu entscheiden. Er wird auch dann eingeschaltet, wenn die Vorgaben der Datenschutzrichtlinien von den Mitgliedstaaten nach Ansicht der Kommission nicht, unvollständig oder verspätet in nationales Recht umgesetzt werden, so dass es zu einem Vertragsverletzungsverfahren nach Art. 258 AEUV kommt. Darüber hinaus kann der Gerichtshof im Rahmen einer Nichtigkeitsklage auch europäische Gesetzgebungsakte und Handlungen europäischer Organe auf deren Vereinbarkeit mit den europäischen Datenschutzregelungen nach Art. 263 AEUV überprüfen. Hierbei geht es um die Verletzung von Bestimmungen, welche die Organe bei der Ausübung ihrer Tätigkeiten binden.

Der EuGH hat im Datenschutzrecht einen umfassenden Regelungsanspruch. Wenn das Europäische Recht Datenschutzstandards setzt, so dürfen diese durch innerstaatliche Regeln weder unter noch überschritten werden[13]. Es geht nicht bloß darum, einen Mindeststandard für den Datenschutz der EU zu schaffen, sondern um eine Vollharmonisierung des Datenschutzrechts. Nationale Regelungen dürfen die Vorgaben der Datenschutzrichtlinie danach nur konkretisieren, nicht aber weitergehende Regelungen einführen. Die Mitgliedstaaten dürfen weder neue Grundsätze in Bezug auf die Zulässigkeit der Datenverarbeitung einführen noch zusätzliche Bedingungen aufstellen, die über die Vorgaben der Datenschutzrichtlinie hinausgehen.

III. Ausgewählte aktuelle Rechtsprechung des EuGH

Die hier referierte Rechtsprechung des EuGH zum Datenschutz beschränkt sich im Wesentlichen auf die Jahre 2012 bis 2014. Themen waren das Verhältnis von Datenschutz und Urheberrecht, die Unabhängigkeit der Datenschutzkontrolle, die datenschutzrechtliche Zulässigkeit der Erfassung und Verarbeitung von Arbeitszeiten, die Zulässigkeit biometrischer Fingerabdrücke in Pässen sowie die Vorratsdatenspeicherung. In einem weiteren Themenbereich, nämlich der Verantwortung von Internetsuchmaschinenanbietern, steht die richterliche Entscheidung kurz bevor, so dass hier der Standpunkt des Generalanwaltes vorgestellt wird.

1. Datenschutz und Geistiges Eigentum

Das Spannungsverhältnis zwischen Datenschutz und Urheber recht zeigt sich bei der Bekämpfung von Internetpiraterie deutlich, und es hat den EuGH in mehreren Entscheidungen beschäftigt.

10 S. dazu das Beschwerdeverfahren vor dem EGMR der britischen Bürger rechtsgruppen Big Brother Watch, Open Rights Group, des britischen Schriftstellerverbandes PEN und der Sprecherin des Chaos Computer Clubs Constanze Kurz gegen den britischen Geheimdienst Government Communications Headquarters (GCHQ) wegen Verstoßes durch unkontrollierte Überwachung gegen Artikel 8 EMRK und das dort allen EU-Bür gern eingeräumte Menschenrecht auf Privatsphäre, s. dazu http://www. ccc.de/de/updates/2014/gchq-egmr.

11 Richtlinie 2009/136/EG zur Änderung der RL 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der RL 2002/58/EG über die Verarbeitung perso nenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der VO (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

12 EuGH, Urteil vom 08.04.2014, C-293/12 und C-594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung".

13 EuGH, Urteil vom 24.11.2011, C-468/10, C-469/10 – „ASNEF/FECEMD", s. hierzu Bongers, Verbot der Datenverarbeitung muss durch Interessenabwägung abwendbar sein, GWR 2012, 45.

1.1 Promusicae

Im Jahr 2008 befasste sich der EuGH in der Entscheidung *„Promusicae/Telefónica"*[14] mit dem Verhältnis von Datenschutz und dem Schutz des geistigen Eigentums im Internet. Er hielt fest, dass sich aus dem Gemeinschaftsrecht zwar kein Anspruch zur Mitteilung personenbezogener Daten durch den Access-Provider ergebe, um Urheberrechtsverstöße im Zivilprozess verfolgen zu können. Das Gemeinschaftsrecht hindere die Mitgliedstaaten gleichwohl nicht daran, eine Verpflichtung der Access-Provider zur Weitergabe personenbezogener Daten an Privatpersonen zu schaffen, um die Verfolgung von Urheberrechtsverstößen vor den Zivilgerichten zu ermöglichen. Es sei deren Sache, ein angemessenes Gleichgewicht zwischen dem Recht auf Schutz personenbezogener Daten und auf Achtung des Privatlebens zum einen und dem Recht auf Schutz des geistigen Eigentums, insbesondere des Urheberrechts, und dem Recht auf einen wirksamen Rechtsbehelf zum anderen sicherzustellen.

1.2 LSG/Tele 2

Mit der datenschutzrechtlichen Beurteilung von urheberrechtlichen Auskunftsansprüchen gegen Access-Provider nach EU-Recht befasste sich der EuGH auch im Fall *„LSG/Tele2"*[15]. Hier stellte er in Übereinstimmung mit „Promusicae/Telefónica" fest, dass eine Verpflichtung zur Weitergabe personenbezogener Verkehrsdaten an private Dritte zum Zweck der zivilgerichtlichen Verfolgung von Urheberrechtsverstößen mit dem Gemeinschaftsrecht vereinbar sei und dass nationale Regelung es erlauben müssten, die verschiedenen beteiligten Grundrechte miteinander in Ausgleich zu bringen.

1.3 Scarlet Extended

In *„Scarlet Extended"*[16] stellte der EuGH darüber hinaus präzisierend fest, dass der Schutz des Urheberrechts keinen Anspruch gegen Betreiber von Internet-Tauschbörsen begründe, ein Filtersystem zur Kontrolle aller Aktivitäten einzurichten. Die Verpflichtung eines Providers zur systematischen Prüfung aller Kommunikationsinhalte sowie zur Sammlung und Identifizierung von IP-Adressen bedeute die Auferlegung einer generellen Überwachungspflicht und verletze neben der unternehmerischen Freiheit des Unternehmens das Recht der Kunden auf den Schutz personenbezogener Daten und auf freien Empfang oder freie Sendung von Informationen.

1.4 Bonnier Audio

„Bonnier Audio u.a./Perfect Communication"[17] ist die jüngste Entscheidung zu diesem Bereich. Auch hier geht es um die Vereinbarkeit von Auskunftsansprüchen gegen Provider zur Verfolgung von Urheberrechtsverstößen in Zivilverfahren (sog. Filesharing-Verfahren) mit dem Gemeinschaftsrecht. In einem schwedischen Zivilrechtsstreit klagten verschiedene Hörbuch-Verlage gegen einen Internet-Provider auf Herausgabe der Daten eines Kunden des Providers, weil dieser Hörbücher der Verlage ohne deren Zustimmung über Tauschbörsen im Netz verbreitet hatte. Der Provider weigerte sich jedoch unter Berufung auf die Vorratsdatenspeicherungsrichtlinie, die von den Verlagen ermittelten IP-Adressen der Nutzer (Kunden) herauszugeben. Nachdem dem Auskunftsersuchen in erster Instanz stattgegeben wurde, legte das Berufungsgericht dem EuGH die Frage nach der Vereinbarkeit der nationalen Regelungen mit EU-Recht vor, die den Provider zur Herausgabe von Kundendaten potentieller Urheberrechtsverletzer verpflichteten.

a. Unanwendbarkeit der Vorratsdatenspeicherungsrichtlinie

Der EuGH stellte zunächst fest, dass hier kein Anwendungsfall der Vorratsdatenspeicherungsrichtlinie vorliegt, da die betreffenden nationalen Regelungen die Weitergabe von Daten in einem Zivilverfahren zur Feststellung einer Urheberrechtsverletzung betreffen[18]. Die Richtlinie 2006/24/EG betreffe hingegen ausschließlich die Verarbeitung und Vorratsspeicherung von Daten, die von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten erzeugt oder verarbeitet werden[19].

b. Konflikt Datenschutz und Urheberrecht

Er prüfte sodann die Vereinbarkeit der betroffenen schwedischen Regelungen anhand der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (RL 2002/58/EG)sowie der Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums (RL 2004/48/EG)[20]. Unter Berufung auf Promusicae[21] hielt er fest, dass die einschlägigen Richtlinien die EU-Mitgliedstaaten nicht daran hindern würden, eine Verpflichtung zur Weitergabe personenbezogener Daten an Privatpersonen zu schaffen, um die Verfolgung von Urheberrechtsverstößen vor den Zivilgerichten zu ermöglichen. Allerdings zwängen sie sie europarechtlich auch nicht dazu, eine derartige Verpflichtung vorzusehen[22]. Sähe ein Mitgliedstaat aber eine solche

14 EuGH, Urteil vom 29.01.2008, C-275/06 – „Promusicae/Telefónica".; s. hierzu Anm. Schoene, in: FD-GewRS 2008, 252938; Kahlert, Urheberrecht kontra Datenschutz: EuGH bremst Forderungen nach einem zivilrechtlichen Auskunftsanspruch gegen Internet-Provider über die Identität von Tauschbörsen-Benutzern, ELR 2008, 78-82.

15 EuGH, Urteil vom 19.02.2009, C-557/07 – „LSG/Tele2", s. hierzu Anm. Nordemann/Schaefer, EuGH: Vermittlereigenschaft eines Access-Providers, GRUR 2009, 579.

16 EuGH, Urteil vom 24.11.2011, C-70/10 – „Scarlet Extended"; s. hierzu Maaßen, Pflicht zur präventiven Filterung des gesamten Datenverkehrs zur Bekämpfung von Urheberrechtsverletzungen nicht mit europäischem Recht vereinbar – „Scarlet Extended" in: GRUR-Prax 2011, 535.

17 EuGH, Urteil vom 19.04.2012, C-461/10 – „Bonnier Audio u.a/Perfect Communication", s. hierzu Ohst, Urheberrechtlicher Auskunftsanspruch mit EU-Recht vereinbar, in: GRUR-Prax 2012, 235.

18 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a./Perfect Communication, Rn. 45.

19 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a./Perfect Communication, Rn 40.

20 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a/Perfect Communication, Rn. 52, 54.

21 EuGH, Urteil vom 29.01.2008, C-275/06 – Promusicae, Rn. 54, 55.

22 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a/Perfect Communication, Rn. 55.

Verpflichtung vor, so müsse er dafür sorgen, dass die jeweilige Regelung eine Einzelfallabwägung[23] ermögliche, die ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Unionsrechtsordnung geschützten Grundrechten aus den Bereichen Datenschutz und Schutz des geistigen Eigentums[24] sicherstelle [25]. Im konkreten Fall sah der EuGH diese Anforderungen als erfüllt an, zumal für die Anordnung der Weitergabe von personenbezogenen Daten im Rahmen eines Zivilverfahrens nach der betreffenden schwedischen Regelung klare Beweise für die Verletzung des Urheberrechts vorliegen müssten. Zudem müssten die begehrten Auskünfte dazu geeignet sein, die Untersuchung der Urheberrechtsverletzung oder -beeinträchtigung zu erleichtern, und verhältnismäßig sein[26].

c. Zwischenfazit

Die Entscheidung schließt an vorherige Entscheidungen des EuGH an, wonach eine Weitergabe personenbezogener Daten im Rahmen von Zivilverfahren zur Verfolgung von Urheberrechtsverstößen europarechtlich grundsätzlich zulässig ist. Deren Verhältnismäßigkeit verlangt, dass vor Herausgabe der Daten klare Beweise für eine Urheberrechtsverletzung vorliegen müssen, die zur Verfolgung der Urheberrechtsverletzung geeignet sein müssen. Ein besonderes Problem stellt hier die Einbindung der Access-Provider dar, die Kundendaten zwar zur Vertragspflege vorhalten, sich aber nicht für die Rechteverfolgung von Urheberrechtsinhabern in die Plicht nehmen lassen wollen[27]. Dennoch kann eine zielgerichtete Durchsetzung von verletzten Urheberrechten, jedenfalls wenn Tauschbörsen betroffen sind, in der Praxis regelmäßig nur über einen Auskunftsanspruch gegenüber einem Provider gewährleistet werden[28]. Die grundsätzliche Zulässigkeit der Identifizierung eines Rechtsverletzers durch einen Abgleich der beim Internetaccessprovider gespeicherten Verbindungsdaten (insbes. IP-Adresse) hatte der EuGH bereits im Fall LSG/Tele2 bejaht[29].

In Bonnier gibt der EuGH nun eine Prüfungsreihenfolge für eine Verhältnismäßigkeitsprüfung vor[30]. Danach müssen zunächst eindeutige Beweise für die Verletzung des Urheberrechts an einem Werk vorliegen. Zudem müssen die begehrten Auskünfte geeignet sein, die Untersuchung der Urheberrechtsverletzung oder -beeinträchtigung zu erleichtern, und die Gründe für die Anordnung müssen die Nachteile für Provider und Nutzer sowie sonstige betroffene Dritte aufwiegen. Erfüllt eine nationale Regelung diese Voraussetzungen, so ist sie europarechtskonform[31].

2. Unabhängigkeit der Datenschutzaufsicht

Die Unabhängigkeit ihrer Aufgabenwahrnehmung gegenüber dem Staat ist für die Datenschutzaufsicht zentral und war bislang Gegenstand von zwei Entscheidungen des EuGH.

2.1 Deutschland/Kommission

Zur Unabhängigkeit der Datenschutzaufsicht entschied der EuGH 2010 im Fall *„Kommission/Deutschland“*[32]. Hier befasste er sich mit dem Erfordernis der Unabhängigkeit der Datenschutzbehörden und verlangte zur Kontrolle des Datenschutzes institutionelle Unabhängigkeit, die garantiere, dass die Datenschutzbehörden ihre Aufgaben völlig frei von jeglicher Einflussnahme von außen effektiv wahrnehmen können. Die staatliche Aufsicht der deutschen Datenschutzbehörden wurde mit diesem Unabhängigkeitserfordernis für nicht vereinbar erklärt und nach der Entscheidung teilweise neu organisiert[33].

2.2 Kommission/Österreich

In der Folge dieser Entscheidung erging 2012 ein Urteil in der Rechtssache *„Kommission/Österreich“*[34]. Auch dieses betrifft ein Vertragsverletzungsverfahren, in dem es um die Umsetzung der Verpflichtung der Datenschutzrichtlinie 95/46/EG zur Gewährleistung der völligen Unabhängigkeit der österreichischen Datenaufsichtsbehörde geht. Die EU-Kommission leitete nach der Beschwerde einer Bürgerrechtsorganisation ein Vertragsverletzungsverfahren gegen Österreich ein, das die dortige Datenschutzkommission (im Folgenden: DSK) betrifft.

a. Bedeutung der Unabhängigkeit

Der EuGH erklärt in seiner Entscheidung zunächst die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten zum wesentlichen Element des Datenschutzes[35] und betont das

23 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a/Perfect Communication, Rn. 59.

24 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a/Perfect Communication, Rn. 60.

25 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a/Perfect Communication, Rn. 56.

26 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a/Perfect Communication, Rn. 58.

27 Siehe dazu Anm. von Nordemann/Schaefer zum EuGH, Beschluss vom 19.02.2009 – C-557/07 – LSG/Tele2, in: GRUR 2009, 579.

28 Möller, Urheber-/Datenschutzrecht: Herausgabe gespeicherter Verkehrsdaten zur zivilrechtlichen Verfolgung von Urheberrechtsverletzungen, EuZW 2012, 517-520(520).

29 EuGH, C- 557/07, LSG/Tele2, Urteil vom 19.02.2009, Rn. 29.

30 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a/Perfect Communication, Rn. 58.

31 EuGH, Urteil vom 19.04.2012, C-461/10 – Bonnier Audio u.a/Perfect Communication, Rn. 59. Nach deutschem Recht ist der Auskunftsanspruch gegen den Access-Provider in § 101 UrhG normiert, der diesen Anforderungen genügen dürfte, weil er eine offensichtliche Rechtsverletzung voraussetzt und Maßnahmen von einer Verhältnismäßigkeitsprüfung abhängig macht. Dazu Ohst, Urheberrechtlicher Auskunftsanspruch mit EU-Recht vereinbar, GRUR-Prax 2012, 235. Es muss aber durch Richtervorbehalt für eine grundrechtliche Absicherung der Rechte der Betroffenen gesorgt sein. Dazu Baum, Anmerkung zu einer Entscheidung des EuGH, Urteil vom 19.04.2012 (C-461/10; MR-Int 2012, 29) – Zur Frage der Abwägung der widerstreitenden Interessen der Rechteinhaber zur Verfolgung von Urheberrechtsverstößen im Internet gegenüber den datenschutzrechtlichen Belangen der Nutzer.

32 EuGH, Urteil vom 09.03.2010, C-518/07 – “Kommission/Deutschland”; s. hierzu Anm. Roßnagel, EuGH: Verurteilung Deutschlands zur Neuorganisation seiner Datenschützer EuZW 2010, 296.

33 Seit dem Urteil des EuGH haben alle Bundesländer neue Gesetze verabschiedet, um die geforderte Unabhängigkeit der Datenschutzbehörden zu gewährleisten, siehe Übersicht unter: http://www.daten-speicherung.de/data/BMI_Unabhaengigkeit_20-05-2011.pdf. Allerdings sollen nach Ansicht der EU-Kommission auch die neuen Gesetze keine vollständige Unabhängigkeit der Datenschutz-Aufsichtsbehörden gewährleisten, weil die Datenschutzbehörden weiterhin einer Dienstaufsicht der Landesregierung oder des Landtags unterworfen werden, s. dazu unter: http://www.daten-speicherung.de/index.php/eu-kommission-deutsche-datenschutzaufsicht-ist-weiterhin-nicht-unabhaengig/.

34 EuGH, Urteil vom 16.10.2012, C-614/10 – „Kommission/Österreich“. Siehe dazu unten unter II.3.3.

35 EuGH, Urteil vom 16.10.2012, C-614/10 – Kommission/Österreich, Rn. 7.

Erfordernis der völligen Unabhängigkeit[36]. Dabei reiche eine funktionelle Unabhängigkeit, wie im Falle der DSK, allein nicht aus, um äußere Einflussnahmen zu verhindern[37]. Drei Punkte seien dabei von Bedeutung. Erstens sei das geschäftsführende Mitglied der Datenschutzkommission in Österreich ein der Dienstaufsicht unterliegender Bundesbediensteter, dessen Überwachungsbefugnis mit der Unabhängigkeitsanforderung unvereinbar sei[38]. Zweitens sei die Geschäftsstelle der DSK in das österreichische Bundeskanzleramt eingegliedert, da dieses die Sach- und Personalausstattung für die Geschäftsstelle der DSK bereitstelle, so dass das Personal der Geschäftsstelle der DSK der Dienstaufsicht des Bundeskanzleramts unterstehe[39]. Durch diese Verzahnung sei die DSK nicht über jeden Verdacht der Parteilichkeit erhaben und könne ihre Aufgaben nicht frei von jedem Einfluss des Bundeskanzleramts wahrnehmen[40]. Drittens sei der Bundeskanzler befugt, sich über alle Gegenstände der Geschäftsführung der DSK zu unterrichten, wodurch die DSK einem mittelbaren und datenschutzrechtlich unzulässigen Einfluss des Bundeskanzlers ausgesetzt sein könne[41].

In Österreich wurde die DSK in April 2013 gesetzlich[42] als unabhängige Behörde eingerichtet und ihre völlige Unabhängigkeit im Sinne der Datenschutz-Richtlinie verankert[43]. Sie unterstand nicht mehr der Dienstaufsicht des Bundeskanzleramts, sondern der des Vorsitzenden der DSK, und das Unterrichtungsrecht des Bundeskanzlers wurde eingeschränkt[44]. Anfang 2014 wurde die Datenschutzkommission durch die österreichische Datenschutzbehörde ersetzt[45], deren Zuständigkeiten und Befugnisse denen der ehemaligen Datenschutzkommission entsprechen[46].

b. Organisatorische oder institutionelle Unabhängigkeit

Der EuGH betont auch in dieser Entscheidung die besondere Bedeutung der völligen Unabhängigkeit der nationalen Datenschutzbehörden in Übereinstimmung mit Art. 28 Abs. 1 der Datenschutzrichtlinie. Sie ist für eine effektive Aufgabenwahrnehmung der Datenschutzbehörden essenziell. Datenschutzbehörden müssen bereits wegen ihres Status als grundrechtlich gebotene Kontrollinstanzen dem Erfordernis der Unabhängigkeit entsprechen[47], das auf europäischer Ebene mehrfach ausdrücklich fixiert ist. So legt Art. 8 Abs. 3 EGRC fest, dass die Einhaltung von Datenverarbeitungsregeln durch eine unabhängige Stelle überwacht wird. Gemäß Art. 44 Abs. 1 VO 45/2001/EG übt auch der Europäische Datenschutzbeauftragte sein Amt in völliger Unabhängigkeit aus. Eine entsprechende Regelung findet sich in der Datenschutzrichtlinie. Dieses Gebot enthält allerdings keine Vorgaben zum genauen Umfang der geforderten Unabhängigkeit der Datenschutzbehörden. Das Adjektiv „völlig" war nicht im Richtlinienvorschlag der Kommission enthalten und wurde im Gesetzgebungsprozess eingefügt, so dass es an den entsprechenden Erwägungsgründen zu dem Kriterium der „völligen Unabhängigkeit" fehlt. Damit liefert die Rechtsprechung des EuGH den einzigen Anhaltspunkt für dessen Auslegung[48]. Dabei dürfte das Erfordernis der Freiheit der Kontrollstelle von der Einflussnahme durch kontrollierte Stellen unstreitig sein[49]. Im Gegensatz zur Auffassung der Bundesregierung, die eine funktionelle Unabhängigkeit für ausreichend hält[50], hält der EuGH eine lediglich funktionelle Unabhängigkeit für unzureichend und verlangt institutionelle Unabhängigkeit, um eine Kontrollstelle vor jeder äußeren Einflussnahme bewahren zu können[51]. Schließlich müssten auch solche Einflussmöglichkeiten, die aus organisatorischen Zusammenhängen resultieren, ausgeschlossen werden[52]. Weder die österreichische noch die deutsche Datenschutzbehörde wiesen für den EuGH die erforderliche institutionelle Unabhängigkeit auf.

c. Problem der innerstaatlichen Umsetzung

Es ist indes nicht von der Hand zu weisen, dass sich mit Blick auf die Anbindung der Datenschutzaufsicht Spannungen aus dem Recht der Mitgliedstaaten zum Unionsrecht ergeben. Das Demokratieprinzip verlangt nämlich, dass auch unabhängige Behörden durch Aufsichts- und Informationsrechte der obersten Organe eine Rückbindung an die unmittelbar demokratisch legitimierten Organe erfahren[53]. Im Fall Kommission/Deutschland sollte das staatliche Aufsichtsrecht über Datenschutzbehörden und im Fall Kommission/Österreich das Unterrichtungsrecht des Bundeskanzlers gegenüber der DSK für eine solche demokratische Rückbindung sorgen. Der EuGH hat diese Einwände in beiden Verfahren zurückgewiesen. Die Einrichtung von völlig unabhängigen Behörden sei mit dem Demokratieprinzip vereinbar, zumal diese an das Gesetz gebunden blieben und der gerichtlichen Kontrolle unterworfen seien. Schließlich müssten

36 EuGH, Urteil vom 16.10.2012, C-614/10 – Kommission/Österreich, Rn. 41; Verweis auf EuGH, Urteil vom 09.03.2010, C-518/07 – Kommission/Deutschland, Rn. 19, 25, 30 und 50.

37 EuGH, Urteil vom 16.10.2012 C-614/10, Kommission/Österreich, Rn. 42.

38 EuGH, Urteil vom 16.10.2012 C-614/10, Kommission/Österreich, Rn. 50.

39 EuGH, Urteil vom 16.10.2012 C-614/10, Kommission/Österreich, Rn. 56.

40 EuGH, Urteil vom 16.10.2012C-614/10, Kommission/Österreich, Rn. 57, 61.

41 EuGH, Urteil vom 16.10.2012, C-614/10 – Kommission/Österreich, Rn. 63.

42 (Österreich) Bundesgesetzblatt I Nr. 57/2013, 17.04.2013, abrufbar unter: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2013_I_57/BGBLA_2013_I_57.html (letzter Abruf: 06.01.2014).

43 S. hierzu Vorblatt und Erläuterungen zur Regierungsvorlage, abrufbar unter: http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_02131/fname_281037.pdf (letzter Abruf: 06.01.2014); Pabel, Ungenügende Unabhängigkeit der Datenschutzkommission, Österreichische Zeitschrift für Wirtschaftsrecht 2013, S. 25-28 (27).

44 S. hierzu Fieseler/Ritter, „Nach EuGH-Urteil: Datenschutzkommission wird unabhängig", 26.04. 2013 im BehördenSpiegel.at, abrufbar unter: http://www.behoerdenspiegel.at/?p=1400 (letzter Abruf: 06.01.2014).

45 http://www.dsb.gv.at/ (letzter Abruf: 06.01.2014).

46 http://www.dsb.gv.at/DocView.axd?CobId=53385 (letzter Abruf: 06.01.2014).

47 S. dazu Petri/Tinnefeld, Völlige Unabhängigkeit der Datenschutzkontrolle. Demokratische Legitimation und unabhängige parlamentarische Kontrolle als moderne Konzeption der Gewaltenteilung, MMR 2010, S. 157 (158).

48 Siehe dazu: Schmidl, Die österreichische Datenschutzkommission erfüllt nach Ansicht des Gerichtshofes der Europäischen Union nicht das Kriterium der «völligen» Unabhängigkeit, European Law Reporter 2012 p. 292-294, ELR 2012, 291-293.

49 Petri/Tinnefeld (s. Fn. 47), S. 157(159).

50 EuGH, Urteil vom 09.03.2010, C-518/07, Rn. 16, 19.

51 EuGH, Urteil vom 09.03.2010, C-518/07, Rn. 18, 19, 30; s. dazu Petri in Simitis, BDSG, § 38, Rn. 11.

52 Siehe dazu: Pabel, Ungenügende Unabhängigkeit der Datenschutzkommission, Österreichische Zeitschrift für Wirtschaftsrecht 2013, S. 25-28 (27).

53 Pabel, Ungenügende Unabhängigkeit der Datenschutzkommission, Österreichische Zeitschrift für Wirtschaftsrecht 2013, S. 25-28 (27); siehe dazu auch Ziebarth, Demokratische Legitimation und Unabhängigkeit der deutschen Datenschutzbehörden, Computer und Recht 201, S. 60-68.

Datenschutzbehörden ihre Aufgaben so ausüben können, dass sie der politischen Einflussnahme entzogen seien[54].

3. Aufzeichnungen über Arbeitszeiten

Eine weitere aktuelle Entscheidung befasst sich mit einer arbeitsrechtlichen Problematik. In der Entscheidung *„Worten"*[55] geht es um die datenschutzrechtlich veranlasste Verpflichtung eines Unternehmens zur unmittelbaren Vorlage von Aufzeichnungen über Arbeitszeiten. Die portugiesische Behörde für die Überwachung der Arbeitsbedingungen (ACT) bemängelte in einem Betrieb das Fehlen unmittelbar einsehbarer Aufzeichnungen über Arbeits- und Ruhezeiten sowie deren Berechnung. Dies verstieß gegen eine Regelung des portugiesischen Arbeitsgesetzbuchs über die Vorlagepflicht derartiger Aufzeichnungen. Ein Unternehmer klagte gegen die Herausgabepflicht, und das zuständige Arbeitsgericht legte dem EuGH die Frage nach der Gemeinschaftsrechtskonformität der entsprechenden portugiesischen Regelungen vor.

3.1 Datenschutzrechtliche Einordnung von Arbeitszeiten

Der EuGH klassifizierte die entsprechenden Aufzeichnungen über Arbeits- und Ruhezeiten der einzelnen Arbeitnehmer als personenbezogene Daten[56]. Deren Erhebung, Speicherung, Aufbewahrung, Nutzung und Übermittlung an die Behörden sei dementsprechend eine „Verarbeitung personenbezogener Daten". Diese sei nach den Vorgaben der Datenschutzrichtlinie entweder dann zulässig, wenn sie für die Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt (Art. 7 c RL 95/46/EG), oder wenn sie für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde (Art. 7 e RL 95/46/EG), erforderlich ist. Der EuGH sah die entsprechenden Vorgaben im konkreten Fall als erfüllt an[57]. Das Erfordernis der unverzüglichen Einsicht sei gerechtfertigt, weil so jegliche Möglichkeit der Manipulation der Daten zwischen Kontrollbesuch und tatsächlicher Überprüfung ausgeschlossen werden könne[58].

3.2 Interessenabwägung

Die Legitimation der Arbeitszeiterfassung zur Kontrolle der Arbeitnehmer steht grundsätzlich, insbesondere auch im deutschen Datenschutzrecht (vgl. § 32 Abs. 1 S. 1 BDSG) außer Frage. Die geleistete Arbeitszeit bildet – jedenfalls bei den Zeitlohnsystemen – die Grundlage für die Bemessung des Arbeitsentgelts, so dass deren Erfassung für die Durchführung des Arbeitsverhältnisses erforderlich ist[59]. Im Fall *„Worten"* kommt der Aufzeichnung der Arbeitszeiten aber eine besondere Funktion zu, nämlich die der Kontrolle der Einhaltung der gesetzlich vorgegebenen Anforderungen an die Arbeitszeiten. Der Eingriff in die datenschutzrechtliche Sphäre dient also der Sicherheit und dem Gesundheitsschutz der Arbeitnehmer. In der bei jedem Eingriff in die Persönlichkeitsrechte bzw. in die Privatsphäre vorzunehmenden Abwägung der betroffenen Rechtsgüter steht hier der Schutz der personenbezogenen Daten auf der einen Seite und der Schutz der Gesundheit und der Sicherheit der betroffenen Personen auf der anderen Seite. Dabei ist zu berücksichtigen, dass der Eingriff in der unverzüglichen Zurverfügungstellung der ohnehin schon erfassten personenbezogenen Daten besteht. Lediglich die Schutzrichtung der Arbeitszeiterfassung wird geändert. Es wird dabei den nationalen Gerichten überlassen festzustellen, ob im Einzelfall die unverzügliche Übermittlung notwendig ist, damit die zuständige Behörde ihre Überwachungsaufgaben hinsichtlich der Anwendung der Regelungen über die Arbeitsbedingungen, insbesondere in Bezug auf die Arbeitszeit, wahrnehmen kann. Ist das der Fall, so dürfte im Hinblick auf die geringe Intensität des „erneuten" Eingriffes, der in der unverzüglichen Zurverfügungstellung bzw. Übermittlung der betroffenen Daten besteht, und den mit dieser Übermittlung verfolgten legitimen Zweck, nämlich den Gesundheitsschutz der Arbeitnehmer, also ein dem Persönlichkeitsrecht ähnlich wichtiges Schutzobjekt[60], dieser erneute Eingriff als verhältnismäßig anzusehen sein.

4. Digitaler Fingerabdruck im Reisepass

Ein anderes Spezialproblem war Gegenstand des Vorabentscheidungsverfahrens Schwarz gegen die Stadt Bochum[61]. Hier ging es um die Vereinbarkeit der Erfassung und Speicherung von biometrischen Fingerabdrücken in Reisepässen und Reisedokumenten mit europäischen Grundrechten. Konkret ging es um das Recht auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten aus Art. 7 und 8 der Europäischen Grundrechtecharta (im Folgenden: GRC).

Der Kläger beantragte bei der Stadt Bochum einen Reisepass, verweigerte jedoch die Erfassung seiner Fingerabdrücke. Nachdem sein Antrag abgelehnt wurde, erhob er eine verwaltungsgerichtliche Klage auf Erstellung eines Reisepasses ohne Fingerabdrücke. Er stellte dabei die Verordnung Nr. 2252/2004[62], durch die die entsprechende Verpflichtung eingeführt worden war, wegen der Verletzung von Verfahrensvorschriften sowie des Rechts auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, in Frage. Die Regelung[63] sieht vor, dass Pässe und Reisedokumente mit einem Speichermedium versehen sind, das ein Gesichtsbild und Fingerabdrücke enthält. Das Speichermedium muss hohen Sicherheitsstandards entsprechen und geeignet sein, die Integrität, die Authentizität und die Vertraulichkeit der Daten sicherzustellen. Die gespeicherten biometrischen Daten dürfen nur zu dem Zweck verwendet werden, die Authentizität des Passes und die Identität seines Inhabers zu überprüfen. Das Verwaltungsgericht legte dem EuGH die Frage

54 EuGH, Urteil vom 09.03.2010, C-518/07 – Kommission/Deutschland, Rn. 42.

55 EuGH, C-342/12 – Worten (30.05.2013).

56 EuGH, Urteil vom 30.05.2013 C-342/12, Worten, Rn. 19.

57 EuGH, Urteil vom 30.05.2013C-342/12, Worten, Rn. 35.

58 EuGH, Urteil vom 30.05.2013 C-342/12, Worten, Rn. 41.

59 S. dazu Seifert in Simitis, BDSG Kommentar, 7. Aufl., § 32, Rn. 72.

60 Riesenhuber, Die Einwilligung des Arbeitnehmers im Datenschutzrecht, RdA 2011, 257(265).

61 EuGH, C-291/12 – Michael Schwarz/Stadt Bochum (17.10.2013).

62 ABl. L 385, S. 1, geändert durch die Verordnung (EG) Nr. 444/2009 des Europäischen Parlaments und des Rates vom 6. Mai 2009, ABl. L 142, S. 1, Berichtigung in ABl. L 188, S. 127.

63 Art. 1 Abs. 2 VO 2252/2004.

vor, ob die Verordnung Nr. 2252/2004 ungültig sei, weil sie die Speicherung von Fingerabrücken in Pässen und Reisedokumenten vorsehe und hierdurch das Grundrecht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten verletze.

4.1 Eingriff

Der EuGH begreift die Erfassung und Speicherung von Fingerabdrücken durch die nationalen Behörden zunächst als gerechtfertigten Eingriff in die Rechte des Betroffenen auf Achtung des Privatlebens und auf Schutz personenbezogener Daten[64]. Er diene dem Gemeinwohlbelang des Schutzes vor betrügerischer Verwendung von Reisepässen[65].

4.2 Verhältnismäßigkeit

Die Rechte aus Art. 7 und 8 GRC unterlägen gesetzlich vorzusehenden Einschränkungen. Der Schutz vor Fälschung sowie die Verhinderung einer betrügerischen Verwendung von Pässen rechtfertigen die Eingriffe[66], da hierdurch die illegale Einreise von Personen in das Unionsgebiet verhindert werden könne[67]. Die Erfassung von Fingerabdrücken sei erforderlich. Andere geeignete Vornehmungen als die obligatorische Erfassung von Fingerabdrücken[68] seien ebenso wenig ersichtlich wie mildere Maßnahmen[69]. Insbesondere sei das Verfahren der *Iris-Erkennung* technisch nicht derart ausgereift wie die Erfassung von Fingerabdrücken und sei wegen der höheren Kosten für eine allgemeine Anwendung weniger geeignet[70], um illegale Einreisen in das Unionsgebiet zu verhindern[71]. Auch insgesamt sei das Verfahren geeignet[72]. Fingerabdrücke enthielten objektiv unverwechselbare Informationen und ermöglichten eine genaue Identifizierung von Personen[73], ferner sei ihre Erfassung und Speicherung in Reisepässen zur Bekämpfung illegaler Einreisen erforderlich und nach Art. 8 Abs. 2 der GRC zulässig, wenn sie mit Einwilligung oder auf Basis gesetzlicher Ermächtigung erhoben würden. Da es vorliegend an einer freiwilligen Einwilligung fehle, könne der Eingriff nur durch eine „sonstige gesetzlich geregelte legitime Grundlage" gerechtfertigt werden (52 Abs. 1 GRC).

4.3 Abwägung

In der Abwägung verneint der EuGH eine besondere Sensibilität der Fingerabdrücke mit der Begründung, dass diese auch normalerweise den Blicken Dritter ausgesetzt seien, so dass deren Erfassung nichts Intimes zeige. Er setzt sie mit der Aufnahme eines Gesichtsbilds gleich, das ebenfalls öffentlichen Blicken ausgesetzt ist und dessen Aufnahme dem Betroffenen nicht über Gebühr körperlich oder psychisch Unannehmlichkeiten bereite[74]. Das überzeugt insofern nicht, als zwar die Finger, nicht aber die in der Fingerkuppenhaut codierten biometrischen Merkmale den Blicken anderer Personen ausgesetzt sind[75]. Das Iris-Erkennungsverfahren, das der EuGH zur allgemeinen Anwendung mit Verweis auf dessen Kostspieligkeit und die fehlende technische Reife für ungeeignet hält, dürfte tatsächlich nicht weniger in die Persönlichkeitsrechte der Betroffenen eingreifen als eine Erfassung von Fingerabrücken. Die Gefahr der zentralen Speicherung der Fingerabdrücke und das Risiko, sie zu anderen Zwecken als den in der Verordnung vorgesehenen verwenden zu können, sieht der EuGH nicht. Nicht von der Hand zu weisen ist aber, dass die Verordnung ein erster Schritt in Richtung einer künftigen Zentralisierung sein kann, und dass eine digitale Speicherung von Fingerabdrücken in Reisepässen künftigen Missbrauch ermöglichen kann. Mit Blick auf die mit einer zentralen Speicherung in Datenbanken verbundenen Gefahren spricht vieles dafür, die konkrete Maßnahme als unverhältnismäßig einzustufen[76].

5. Verantwortung von Internetsuchmaschinen

Eines der vergleichsweise neuen Probleme betrifft die Verantwortung von Internetsuchmaschinenbetreibern. Der EuGH ist hier mit einer Reihe von Rechtsproblemen konfrontiert, die in einem Rechtsstreit gegen Google zur Entscheidung anstehen. Derzeit liegt der Standpunkt des Generalanwalts vor, der hier vorgestellt werden soll[77].

5.1 Der Ausgangsfall

Im Rahmen eines spanischen Vorabentscheidungsverfahrens geht es um die Verantwortlichkeit des Suchmaschinenbetreibers Google für personenbezogene Daten, die auf den von diesem Unternehmen verarbeiteten Webseiten aufgefunden werden können. Ausgangspunkt des Verfahrens[78] war eine Veröffentlichung von zwei Bekanntmachungen Anfang 1998 in der Druckausgabe einer spanischen Zeitung, in denen es um eine Immobilienversteigerung nach einer Pfändung ging. In der auch in der Folgezeit noch in der Onlineausgabe verfügbaren Bekanntmachung war der Eigentümer der Immobilie namentlich genannt. Dieser wandte sich Ende 2009 an den Zeitungsverlag und beanstandete, dass bei Eingabe seines Namens in die Suchmaschine von Google eine Verlinkung zu den Seiten der Zeitung mit diesen Bekanntmachungen erscheine. Das Pfändungsverfahren sei seit Jahren erledigt und zwischenzeitlich ohne aktuelle Relevanz. Der Verlag lehnte die Löschung der Daten ab, da die Veröffentlichung auf Basis einer staatlichen Anordnung erfolgt war. Im Februar 2010 forderte der Betroffene von Google Spain, die Verbindung der Eingabe seines Namens in die Internetsuchmaschine mit dem Inhalt aus dem Jahre 1998 aufzulösen. Die spanische Google-Nieder-

64 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 30.

65 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 64.

66 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 36.

67 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 37.

68 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 47.

69 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 53.

70 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 52.

71 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 61.

72 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 64.

73 EGMR, Urteil vom 04.12.2008, S. and Marper/the United Kingdom, Applications nos. 30562/04 and 30566/04, Rn. 84.

74 EuGH, Urteil vom 17.10.2013, C-291/12, Schwarz/Stadt Bochum, Rn. 48.

75 Siehe dazu: Steinbeis, Der maschinenlesbare Mensch: EuGH kann kein Problem erkennen, unter: http://www.verfassungsblog.de/de/der-maschinenlesbare-mensch-eugh-kann-kein-problem-erkennen/.

76 Bamberger, in: Beck'scher Online-Kommentar BGB, Hrsg: Bamberger/Roth, § 12 BGB Rn. 161.

77 Schlussanträge des Generalanwaltes Jääskinen, Fall Google (C-131/12-25.06.2013).

78 Pressemitteilung Nr. 77/13 vom 25.06.2013.

lassung leitete das Ersuchen an die Mutter Google Inc. in die USA weiter. Die Beschwerde des Betroffenen gegen den Verlag und Google bei der spanischen Datenschutzbehörde (Agencia Española de Protección de Datos, AEPD) wurde mit Blick auf den Verlag zurückgewiesen, weil dieser auf Basis einer gesetzlichen Verpflichtung handelte. Allerdings gab sie der Beschwerde gegen Google statt und forderte Google Spain und Google Inc. auf, die Daten aus dem Jahr 1998 zu löschen und einen künftigen Zugriff darauf unmöglich zu machen. Daraufhin klagten sowohl Google Inc. also auch Google Spain auf Aufhebung der Entscheidung.

5.2 Anwendbarkeit nationalen Datenschutzrechts für internationale Anbieter

Seit Juni 2013 liegen die Schlussanträge des Generalanwaltes Jääskinen vor. Er beschäftigte sich zunächst mit der räumlichen Anwendbarkeit der nationalen Datenschutzvorschriften. Als maßgeblichen Anknüpfungspunkt für die Datenverarbeitung eines Internetsuchmaschinenbetreiber stellt er nicht auf den Ort des technischen Vorganges der Datenverarbeitung ab. Diese erfolge jedenfalls dann in der Niederlassung des Internetsuchmaschinenbetreibers im jeweiligen Gaststaat, wenn dieser für die Vermarktung der Suchmaschine zuständig sei und die Werbung sich an die Einwohner des Mitgliedstaats richte. Dann seien die Datenschutzbestimmungen des Staates, in dem sich die Niederlassung befindet, anwendbar; vorliegend gelte also spanisches Recht[79]. Der Generalanwalt stellt nicht auf den physischen Ort der Datenverarbeitung ab, sondern auf den werblichen Wirkungskreis des Internetsuchmaschinenbetreibers, und er stimmt insoweit mit der Art. 29 Datenschutzgruppe zu Datenschutzfragen zu Suchmaschinen überein[80]. Auch das Gremium stellt für die Anwendung nationalen Datenschutzrechts auf eine bestimmte Suchmaschine, deren Hauptsitz sich außerhalb des EWR befindet, darauf ab, ob Niederlassungen im Hoheitsgebiet eines Mitgliedstaats an der Verarbeitung von Benutzerdaten beteiligt sind. Sie bejaht eine Anwendung nationalen Datenschutzrechts nach Art. 4 Abs. 1 lit a der Datenschutz-RL konkret dann, wenn ein Suchmaschinenbetreiber ein Büro in einem Mitgliedstaat (EWR) einrichtet, das am Verkauf zielgruppenspezifischer Werbeanzeigen an die Einwohner dieses Staates beteiligt ist[81]. Teilweise wird die Anwendung nationaler Datenschutzbestimmungen auch mit Art. 4 Abs. 1 lit c der Datenschutz-RL und der Nutzung spanischer Googlebots in Spanien begründet. Googlebots ist ein Computerprogramm, das automatisiert Dokumente im Web durchsucht und sie über die Suchfunktion von Google auffindbar macht. Sein Sinn ist es, Informationen von – in diesem Fall – spanischsprachigen Webseiten zu sammeln und das Angebot für spanische Werbeanwender zu optimieren, worin eine „Nutzung von Mitteln" im Sinne von Art. 4 Abs. 1 lit c der Datenschutz-RL gesehen wird[82].

5.3 Keine generelle Verantwortlichkeit des Suchmaschinenbetreibers

Google sei indes nicht generell für personenbezogene Daten verantwortlich, die auf Webseiten Dritter veröffentlicht werden und durch die Suchmaschinen zugänglich würden. Als für die Verarbeitung Verantwortlicher im Hinblick auf die über die Suchmaschine lokalisierten Daten sei der Anbieter der Quellenwebseite anzusehen. Er habe in dieser Eigenschaft für die auf seiner Website veröffentlichten personenbezogenen Daten einzustehen. Google stelle lediglich ein Instrument zur Lokalisierung der Informationen bereit. Eine Kontrolle über die auf Webseiten Dritter vorhandenen Inhalte habe das Unternehmen nicht. Daher könne der Internetsuchmaschinenbetreiber grundsätzlich nicht zur Entfernung von Informationen aus seinem Index verpflichtet werden. Hier nicht einschlägige Ausnahmen würden gelten, wenn der Suchmaschinenbetreiber sog. exclusion codes nicht beachtet hätte[83], die ihn verpflichten, bestimmte Inhalte aus der Suchfunktion auszuschließen, oder er einer Aufforderung des Webseitenbetreibers zur Aktualisierung des Cache nicht nachgekommen wäre.

5.4 Das Recht auf Vergessenwerden

Der Generalanwalt nimmt in seinen Schlussanträgen auch zu einem möglichen „Recht auf Vergessenwerden" Stellung, das in Art. 17 des Entwurfs der DS-GVO beschrieben ist. Dieses würde zwar jedermann das Recht gewähren, aus überwiegenden schutzwürdigen, sich aus seiner besonderen Situation ergebenden Gründen der Verarbeitung von ihn betreffenden Daten zu widersprechen. Ein bloßes subjektives Verlangen stellt aber für den GA noch keinen derartigen Schutzgrund dar. Die Richtlinie berechtige also nicht dazu, die Verbreitung personenbezogener Daten zu beschränken oder unterbinden zu lassen, weil die betroffene Person sie für abträglich oder ihren Interessen zuwiderlaufend halte. Würde man von Suchmaschinenbetreibern verlangen können, Informationen zu unterdrücken, die rechtmäßig öffentlich geworden sind, so stelle dies eine nicht gerechtfertigte Einschränkung der Meinungsäußerungsfreiheit des Betreibers der Webseite dar.

Das in Art. 7 des Entwurfs der DS-GVO vorgesehene „Recht auf Vergessenwerden" gewährt insbesondere kein Recht des Betroffenen, selbst darüber entscheiden zu können, welche Informationen über ihn aus dem Internet gelöscht werden sollen[84]. Vorgesehen ist vielmehr ein Löschungsanspruch, der nur eine geringfügige Erweiterung des im deutschen Datenschutzrecht bereits bestehenden Löschungsanspruchs (§ 35 Abs. 2 BDSG) darstellt. Er verpflichtet den zur Löschung Verantwortlichen, datenverarbeitende Dritte über das Löschungsverlangen

79 Eingehend zur Frage des anwendbaren Rechts Kremer, in diesem Heft.

80 Stellungnahme 1/2008 der Artikel 29-Datenschutzgruppe zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, 04.04.2008, WP 148, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf.

81 Stellungnahme 1/2008 der Artikel 29-Datenschutzgruppe, WP 148 (s.o.), S.11.

82 Arenas Ramiro/Yankova, Spanische Datenschutzbehörde (AEPD) vs. Google: „Das Recht auf Vergessen" in ZD-Aktuell 2012, 02845.

83 Der Urheber von Quellenwebseiten kann „exclusion codes" für die Operation der Internetsuchmaschinen verwenden. Damit wird den Suchmaschinen der Befehl erteilt, eine Quellenwebseite nicht zu indexieren, zu speichern oder im Rahmen ihrer Suchergebnisse anzuzeigen, und auf diese Weise der Schutz personenbezogener Daten verstärkt, Schussanträge des Generalanwalts, Rn. 41, 42.

84 Hornung/Hofmann, Ein „Recht auf Vergessenwerden"?, JZ 2013, 163 (170).

des Betroffenen durch Querverweise auf die betroffenen Daten oder Vervielfältigungen dieser Daten, zu informieren[85].

Im Fall Google geht es um das Recht auf Löschung von Daten, die rechtmäßig und korrekt an die Öffentlichkeit gelangt sind und durch die Suchmaschine indexiert wurden[86]. Sofern es um unrichtige oder unvollständige Daten geht, ergibt sich bereits aus der Datenschutzrichtlinie das Recht der Betroffenen auf Berichtigung, Löschung oder Sperrung dieser Daten[87]. Fraglich ist aber, ob ein Betroffener unter Berufung auf sein Persönlichkeitsrecht die Löschung von Daten verlangen kann, die legal in das Netz gelangt sind. Konkret geht es darum, ob allein die dauerhafte digitale Verfügbarkeit der Informationen sowie ihre einfache Zugänglichkeit und Auffindbarkeit dieses Recht gewähren[88]. Würde man bei Abwägung von Persönlichkeitsrecht und Informationsfreiheit das „Recht auf Vergessenwerden" anerkennen, so würde die Entscheidung, welche persönlichen Informationen im Internet verbreitet werden dürfen, in den Händen des Betroffenen liegen. Das Recht, Inhalte zu entfernen, würde deutlichen Einfluss auf die Zuverlässigkeit und Objektivität der Informationen im Internet nehmen[89].

Der Generalanwalt sieht in einem solchen Löschungsanspruch eine unzulässige Beschneidung der im Netz veröffentlichten Inhalte durch Private und damit einen Eingriff in die Meinungsäußerungsfreiheit des Betreibers der Seite[90].

Schließt sich der EuGH ihm etwa auch unter Berufung auf die Informationsfreiheit an, so wird es nicht zulässig sein, dass Betroffene sich an Suchmaschinenbetreiber mit dem Anliegen der Indexierung sie betreffender Informationen wenden dürfen. Dies erscheint gerade bei einem Vergleich digitaler und körperlicher Archive plausibel, denn es wäre nicht vertretbar, körperliche Zeitungsarchive nach Ablauf einer bestimmten Frist zu bereinigen. Da auch das Recht auf Veröffentlichung von Daten im Internet auch bei Online-Pressearchiven anerkannt ist, reduziert sich die Frage auf das Recht von Betroffenen, Suchmaschinenbetreibern das Verlinken auf personenbezogene Informationen zu untersagen. Dabei sind die möglichen Gefahren des nicht vergessenden Internets evident. Die dauerhafte Speicherung von Informationen über eine Vielzahl von Vorgängen kann nicht zuletzt dazu führen, dass Menschen ihr Verhalten vor dem Hintergrund der Verfestigung von Informationen langfristig selbst zensieren[91]. Jedenfalls käme es neben der technischen Machbarkeit bei einer Umsetzung des Rechts auf Vergessenwerden darauf an, inwieweit Suchmaschinen vom Schutzbereich der Pressefreiheit erfasst sind, und ob das Haftungsrisiko des Suchmaschinenbetreibers nach einer Verlinkung zu hoch werden kann[92]. Der Nutzer ist für Generalanwalt Jääskinen jedenfalls nicht in der Verantwortung. Der EuGH dürfe keiner Auslegung folgen, „die praktisch jede Person, die ein Smartphone, ein Tablet oder einen Laptop besitzt, zu einem für die Verarbeitung von im Internet veröffentlichten personenbezogenen Daten Verantwortlichen macht."[93] Bei natürlicher Betrachtung ist es aber durchaus auch der Nutzer, der Daten verarbeitet und verbreitet.

5.5 Wer trägt die Verantwortung?

Der EuGH wird sich auch mit der Frage befassen müssen, ob der Suchmaschinenbetreiber als „für die Verarbeitung Verantwortlicher" hinsichtlich personenbezogener Daten Dritter auf fremden Webseiten ist. Der Generalanwalt lehnt diese unter Verweis auf die fehlende Kontrolle des Suchmaschinenbetreibers über die personenbezogenen Daten auf fremden Seiten ab. Er liegt auch in dieser Frage auf der Linie der Art. 29-Datenschutzgruppe. Nach deren Auffassung handeln Suchmaschinenbetreiber ausschließlich als Vermittler und können aus Gründen der Verhältnismäßigkeit nicht als Hauptverantwortliche für Persönlichkeitsrechtsverletzungen bei Datenverarbeitungen angesehen werden[94]. Die Hauptverantwortung liege beim Informationsanbieter[95].

Die anstehende Entscheidung des EuGH dürfte eine Weiche für die Einordnung der Verantwortung von Suchmaschinenbetreibern sein. Die mangelnde Verantwortlichkeit der Suchmaschinenbetreiber wird mit der Passivität der Vermittlungsfunktion und der rein technischen Leistung zurückgeführt[96]. Kann ein Suchmaschinenbetreiber in den Fällen, in denen seine Funktion über die Erbringung von rein technischen Leistungen hinausgeht, zur Verantwortung gezogen werden, weil nur er die Funktionsweise seiner Suchfunktion kennt und sie verändern kann? Steuert er damit auch den Meinungsbildungsprozess, wenn er eingreift, oder muss er Verantwortung für den Schutz von Persönlichkeitsrechten übernehmen? Das dahinter stehende Rechtsproblem besteht in der Beantwortung der Frage, wie die Haftung für das nachhaltige Auffinden von Inhalten im Netz mit Zurechnungsmodellen und dem Ausbau der deliktsrechtlichen Störerhaftung gelöst werden kann. Kann man Betreibern von Diensten das Wirken der von ihnen betriebenen Technik zurechnen? Wer Youtube darauf hinweist, dass sein geistiges Eigentum dort ohne Lizenz verfügbar ist, hat einen Anspruch darauf, dass

85 Tscherwinka, Gibt es ein (Datenschutz-) Recht auf Vergessenwerden? unter: http://www.marktforschung.de/information/marktforschung-recht/gibt-es-ein-datenschutz-recht-auf-vergessenwerden/.

86 Arenas Ramiro, Yankova (s.o.) ZD-Aktuell 2012, 02845.

87 Art. 12 Richtlinie 95/46/EG (des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr).

88 Arenas Ramiro/Yankova, (s.o.) ZD-Aktuell 2012, 02845.

89 Arenas Ramiro/Yankova, (s.o.) ZD-Aktuell 2012, 02845.

90 Schussanträge – 25.06.2013, Rs. C-131/12, Generalanwalt, Jääskinen, Rn. 134.

91 Hornung/Hofmann, Ein „Recht auf Vergessenwerden"?, JZ 2013, 163 (164).

92 Hornung/Hofmann, Ein „Recht auf Vergessenwerden"?, JZ 2013, 163 (165).

93 Schussanträge – 25.06.2013, Rs. C-131/12, Generalanwalt, Jääskinen, Rn. 81.

94 Auf das Merkmal der Kontrolle über die Verarbeitung personenbezogener Daten stellt auch das VG Schleswig-Holstein allerdings betreffend die datenschutzrechtliche Verantwortlichkeit des Betreibers einer Facebookfanpage ab und lehnt diese im Hinblick auf den fehlenden tatsächlichen und/oder rechtlichen Einfluss des Fanpage-Betreibers in Bezug auf die mit der Nutzung einer Fanpage ausgelöste Verarbeitung personenbezogener Daten ab. Dazu VG Schleswig-Holstein, Urteil vom 09.10.2013, – 8 A 218/11 –, Rn. 87; s. dazu auch Anm. 6 v. Albrecht, jurisPR-ITR 24/2013. Der Nutzer einer Fanpage rufe unmittelbar eine Seite des Dienstes auf, so dass personenbezogene Daten ausschließlich vom Nutzer direkt zu Facebook gelangen würden. So komme der Betreiber der Fanpage mit seinem operativen Instrumentarium nicht in direkten Kontakt zu deren Nutzer und dessen personenbezogenen Daten. Seine datenschutzrechtliche Verantwortlichkeit sei dadurch ausgeschlossen. VG Schleswig-Holstein, Urteil vom 09.10.2013, – 8 A 218/11 –, Rn. 72,73.

95 Stellungnahme 1/2008 der Artikel 29-Datenschutzgruppe, WP 148 (s.o,), S.15.

96 Nolte/Wimmers (s.o.) GRUR 2014, 16 (25).

es beseitigt und dauerhaft vom Dienst ferngehalten wird. Das führt in der Praxis zu billigen Ergebnissen, wenn sich eine Rechtsverletzung wie im Falle eines illegalen Videos mit der Beseitigung beheben lässt. Bei dem Zusammenwirken von Suchanfragen und Algorithmus ist das aber anders. Kann oder muss einem Suchdienst ein Verursachungsbeitrag für die gesuchten Inhalte oder das Wirken der Autosuchfunktion zugerechnet werden? Obwohl sowohl das Betreiben des Suchdienstes durch Google als auch das Stellen von Suchanfragen durch die Nutzer sowie deren Ordnung nach Prioritäten weit davon entfernt sind, rechtswidrig zu sein, entstehen in der Praxis Schäden. Dies zeigen Fälle, die derzeit auch deutsche Gerichte mit Blick auf die Haftung von Google für die Suchfunktion befassen. Das LG Hamburg hatte die Entscheidung über die Unterlassungsklage von Bettina Wulff gegen die Ergänzungsvorschläge „Escort" und „Rotlicht" zu ihrem Namen in der Autovervollständigungsfunktion mit Blick auf eine anstehende Entscheidung des BGH ausgesetzt. Dieser hat im Mai 2013 Google als Diensteanbieter im Sinne des TMG (§ 2 S. 1 Nr. 1 TMG) angesehen und eine Haftung (§ 7 Abs. 1 TMG) bejaht[97]. Im entschiedenen Fall wurde ein Unternehmer von der Autocompletefunktion mit den Begriffen „Scientology" und „Betrug" in Verbindung gebracht. Der BGH nahm eine Haftung von Google an, da eigene Informationen (Suchwortergänzungsvorschlage als Ergebnis der Autocomplete-Funktion) zur Nutzung bereitgehalten wurden. Demnach erkannte der BGH einen Unterlassungsanspruch (§§ 1004 Abs. 1 analog i.V.m. 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, Art. 2 Abs 1 GG, allg. Gesetze)[98]. Eine Verletzung des Persönlichkeitsrechts liege, so der BGH, wegen des unwahren Aussagegehalts der Ergänzungsvorschläge vor, denn es bestehe keine Verbindung des Klägers zu Betrug oder Scientology. Der BGH geht also von einer Störerhaftung bei Google aus, die eine Verletzung von – im Einzelfall zumutbaren – Prüfpflichten voraussetzt. Es soll also keine präventive Prüfungspflicht für Suchergänzungsvorschläge geben, es sei denn, bei Vorliegen besonders schutzwürdiger Belange, z.B. bei Kinderpornographie. Die Prüfungspflicht für Google entsteht erst ab Kenntnis von Persönlichkeitsrechtsverletzungen[99]. Der BGH wird wegen dieser Rechtsprechung kritisiert, weil er die Suchvorschläge als eigenen Inhalt von Google begreift und den Suchmaschinenbetreiber als Täter behandelt, im Ergebnis aber nur eine Störerhaftung annimmt[100]. Das mag pragmatische Gründe haben, denn anderenfalls käme es zu einer untragbaren Einschränkung der Informationsfreiheit.

Das LG Köln hatte die Klage gegen Google zuvor etwa mit der Begründung abgewiesen, dass von dem Dienst keine eigenen Informationen zur Nutzung bereitgehalten würden und deshalb eine Haftung (§ 7 Abs. 1 TMG) ausscheide. Mit der automatisierten Ergänzungsfunktion würden weder eigene Aussagen von Google wiedergegeben, die nach bestimmten sinnhaften Kriterien geordnet worden wären, noch Aussagen Dritter, die Google innerhalb der Suchergänzungsfunktion wiedergebe. Die Berufungsinstanz beim OLG Köln hatte die Verantwortlichkeit (§ 7 Abs. 1 TMG) zwar grds. bejaht, da Google mit den Suchvorschlägen eigene Inhalte bereithalte. Die Suchvorschläge hätten aber keinen persönlichkeitsverletzenden Aussagegehalt[101]. Aus Sicht eines Durchschnittsrezipienten lasse sich der Anzeige der Ergänzungssuchbegriffe lediglich die eigene Aussage der Suchmaschine entnehmen, dass andere vorherige Nutzer die gewählten Begriffskombinationen zur Recherche als womöglich wahre Tatsachenbehauptung ohne verletzenden Aussagegehalt eingegeben hätten.

Das OLG München verneinte in einem anderen Fall die Haftung von Google auch mit der Begründung, dass die Autocomplete-Funktion als Ergebnis fremden Suchverhaltens und Resultat eines vollständig automatisierten Vorgangs Google nicht zugerechnet werden könne. Durch die Autocomplete-Funktion würden nicht eigene Inhalte des Suchmaschinenbetreibers, sondern fremde Inhalte, nämlich Suchanfragen zeitlich vorangehender Nutzer der Suchmaschine, angezeigt. Für den verständigen und angemessen aufmerksamen Durchschnittsnutzer der Suchmaschine sei bereits aufgrund des maschinellen Charakters des in Anspruch genommenen Dienstes klar, dass der Suchmaschinenbetreiber lediglich das Ergebnis fremden Suchverhaltens als Resultat eines vollständig automatisierten Vorgangs wiedergebe[102].

6. Vorratsdatenspeicherung

In zwei Vorabentscheidungsersuchen ging es schließlich um die Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG). Der EuGH folgte im Wesentlichen einem zuvor veröffentlichten Gutachten des Generalanwalts Cruz Villalón[103] und erklärte die Richtlinie in ihrer bisherigen Form für unvereinbar mit dem Gemeinschaftsrecht.

6.1 Ausgangsverfahren aus Irland und Österreich

Im Ausgangsverfahren hatte eine Nichtregierungsorganisation gegen zwei Minister der irischen Regierung geklagt und geltend gemacht, dass irische Behörden Daten rechtswidrig verarbeitet sowie auf Vorrat gespeichert und kontrolliert hätten. Sie beantragte zum einen die Nichtigerklärung der innerstaatlichen Rechtsakte, die die Anbieter von Telekommunikationsdiensten zur Vorratsspeicherung von Telekommunikationsdaten verpflichten, da diese mit der irischen Verfassung und dem Unionsrecht unvereinbar wären. Zum anderen stellte sie die Gültigkeit der Richtlinie 2006/24/EG im Hinblick auf die Charta und/oder die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten in Frage. In einem zweiten Verfahren klagten neben der Kärntner Landesregierung Privatpersonen beim österreichischen Verfassungsgerichtshof auf Nichtigerklärung der österreichischen Vorschriften zur Umsetzung der Vorratsdatenspeicherungsrichtlinie. Sie sahen in der Verpflichtung von Kommunikationsnetzbetreibern zur

97 BGH, Urteil vom 14.05.2013 – VI ZR 269/12 –, BGHZ 197, 213-224.

98 BGH, Urteil vom 14.05.2013 – VI ZR 269/12 –, BGHZ 197, 213-224, Rn. 16-17.

99 BGH, Urteil vom 14.05.2013 – VI ZR 269/12 –, BGHZ 197, 213-224, Rn. 30.

100 Hoeren, ZD 2013, 407-408 (Anmerkung zum BGH Urteil VI ZR 269/12).

101 OLG Köln, Urteil vom 10.5.2012 – I-15 U 199/11.

102 OLG München, Urteil vom 29.09.2011 – 29 U 1747/11, Rn. 67.

103 Generalanwalt beim EuGH Cruz Villalón – C- 293/12, C- 594/12, Digital Rights Ireland u.a. (12.12.2013).

anlasslosen Datenspeicherung gegen den Willen der Betroffenen einen Verstoß gegen Art. 8 GRC.

6.2 Inhalte der Vorratsdatenspeicherungsrichtlinie

Die streitgegenständliche Richtlinie 2006/24/EG legte den Mitgliedstaaten die Verpflichtung auf, bestimmte Daten, die im Rahmen der elektronischen Kommunikation der Unionsbürger erzeugt und/oder verarbeitet werden, zu erheben und für einen bestimmten Zeitraum anlasslos auf Vorrat zu speichern. Dadurch sollte ihre Verfügbarkeit zum Zweck der Ermittlung und Verfolgung schwerer Straftaten gewährleistet und das reibungslose Funktionieren des Binnenmarkts sichergestellt werden. Ziel der Richtlinie war in erster Linie die Harmonisierung der teilweise bereits vorhandenen mitgliedstaatlichen Regelungen, die Telekommunikationsdiensteanbieter zur Vorratsdatenspeicherung verpflichten[104], die bereits auf Basis der Richtlinie 2002/58/EG erlassen wurden. Art. 15 Abs. 1 dieser Richtlinie ermächtigt die Mitgliedstaaten, durch Rechtsvorschriften vorzusehen, dass Daten für eine begrenzte Dauer zu Sicherheitszwecken und zu Strafverfolgung und Verbrechensprävention gespeichert werden. Auf diese Weise sollte die Richtlinie 2006/24/EG teilweise auf Grundlage von Art. 15 Abs. 1 der Richtlinie 2002/58 erlassene Vorschriften harmonisieren. Mit dem Ziel der Harmonisierung wurden aber auch Mitgliedstaaten, die nicht über eine entsprechende Regelung verfügen, zur Erhebung und Vorratsspeicherung der genannten Daten verpflichtet. Konkret verlangte die Richtlinie von den Mitgliedstaaten, die Vorratsspeicherung von Daten sicherzustellen, die die Identifizierung einer Person sowie die räumliche und zeitliche Situation dieser Person ermöglichen oder ermöglichen können[105]. Die genannten Daten sollten dabei für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden[106].

6.3 Entscheidung des EuGH

Für den EuGH ist die Vorratsdatenspeicherung nicht generell unzulässig. Er moniert aber deren Umsetzung in der Richtlinie und erklärt diese daher für ungültig.

a. Schaffung von Überwachungsvoraussetzungen

So greife die Richtlinie 2006/24/EG auf unzulässige Weise in das Recht auf Achtung des Privatlebens der Unionsbürger aus Art. 7 und 8 GRC ein[107]. Die Erhebung von Kommunikationsdaten schaffe Voraussetzungen für eine Überwachung, die die Wahrung des Privatlebens während der gesamten Dauer der Vorratsspeicherung permanent bedrohe[108]. Verstärkt würden die Wirkungen des Eingriffs durch die Bedeutung elektronischer Kommunikationsmittel in Zeiten der Digitalisierung bei massiver und intensiver Nutzung durch die Unionsbürger in allen Bereichen ihrer privaten oder beruflichen Tätigkeiten[109]. Die in der Richtlinie vorgesehene Vorratsspeicherung von Daten stelle zwar einen besonders schwerwiegenden Eingriff dar, gleichwohl werde der Wesensgehalt von Art. 7 GRC nicht angetastet, da die Kenntnisnahme des Inhalts elektronischer Kommunikation gerade nicht gestattet werde[110]. Die Möglichkeit zum Missbrauch der auf Vorrat gespeicherten Daten zu rechtswidrigen, potenziell die Privatsphäre verletzenden und betrügerischen oder heimtückischen Zwecken verstärke die Eingriffsintensität[111]. Verschärfend komme hinzu, dass Diensteanbieter nicht verpflichtet seien, die Daten auf dem Gebiet der EU zu speichern, so dass missbräuchliche Erhebung und Verbreitung im EU-Ausland zu befürchten seien[112].

b. Fehlende Voraussetzungen einer Rechtfertigung

Ein verhältnismäßiger Eingriff ergebe sich nicht allein aus seiner gesetzlichen Fixierung. Dazu müssten der Zugang zu den betroffenen Daten und die Möglichkeit ihrer Auswertung – zumindest in Grundsätzen – durch hinreichende Garantien eingeschränkt sein[113]. So müsse der Unionsgesetzgeber Grundprinzipien für den Datenzugang definieren[114]. Die Voraussetzungen zum Zugriff auf die im Rahmen der Vorratsdatenspeicherung erhobenen Daten seien im Hinblick auf den zeitlichen und räumlichen Zusammenhang des Personenkreises und der Straftat zu fassen[115] und die Zugriffsberechtigung sei auf unabhängige Stellen zu begrenzen[116]. In der bisherigen Form stehe die Sicherstellung der Verfügbarkeit der auf Vorrat gespeicherten Daten zum Zweck der Verfolgung schwerer Straftaten außer Verhältnis zum Recht auf Achtung des Privatlebens[117]. Dabei handele es sich bei der Sicherstellung der Verfügbarkeit der erhobenen und auf Vorrat gespeicherten Daten zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten durchaus um ein legitimes Anliegen[118]. Eine Mindestspeicherdauer von sechs Monaten lasse sich ohne Unterscheidung von konkreten Datenkategorien und deren Nutzen für das verfolgte Ziel nicht rechtfertigen[119]. Nach Art. 52 Abs. GRC müsse jede Einschränkung anerkannter Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Nur unter Beachtung des

104 Siehe Art. 1 RL 2006/24/EG.

105 Art. 5 RL 2006/24/EG.

106 Art. 6 RL 2006/24/EG.

107 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 37.

108 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 37.

109 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 56.

110 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 39.

111 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 54, 66.

112 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 68.

113 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 60, 66.

114 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 61, 65.

115 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 59.

116 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 62.

117 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 63 ff.

118 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 49.

119 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 63.

Verhältnismäßigkeitsgrundsatzes dürften Einschränkungen vorgenommen werden[120].

c. Ausblick

Nachdem das Bundesverfassungsgericht die Vorschriften zur Vorratsdatenspeicherung im „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der RL 2006/24/EG", das zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung am 1. Januar 2008 in Kraft getreten war, im Jahr 2010 wegen der Verletzung des Fernmeldegeheimnisses sowie wegen Verstoßes gegen den Grundsatz der Verhältnismäßigkeit bei der Speicherung der Daten für verfassungswidrig und nichtig erklärt hatte[121], hat nun auch der EuGH enge Vorgaben für die Einführung einer Vorratsdatenspeicherung formuliert.

Nach dem Karlsruher Votum zu den damaligen Regelungen[122] erlaubten diese einen „besonders schweren Eingriff in das Fernmeldegeheimnis mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt"[123]. Sie eröffneten den Behörden Einblicke „bis in die Intimsphäre" der Bürger[124]. Zudem sei das Gesetz nicht hinreichend transparent und enthalte keine Angaben über den Umfang der Nutzung der gesammelten Daten[125].

Wie das Bundesverfassungsgericht lehnt allerdings auch der EuGH eine anlasslose Vorratsdatenspeicherung nicht schlechthin ab. Eine verfassungsrechtlich haltbare Regelung muss konkrete Maßgaben zur Datensicherheit, zur Begrenzung der Datenverwendung, zur Begrenzung des Datenzugriffs, zur Speicherdauer, zur Transparenz und zum Rechtsschutz enthalten. Der Koalitionsvertrag von 2013 sieht noch die Umsetzung der Richtlinie vor. Der Zugriff auf die gespeicherten Daten soll danach nur bei schweren Straftaten und nach richterlicher Genehmigung sowie zur Abwehr akuter Gefahren für Leib und Leben zulässig sein. Zudem soll die Speicherung der deutschen Telekommunikationsverbindungsdaten auf Servern in Deutschland vorgenommen werden, und die Speicherfrist soll auf EU-Ebene auf drei Monate verkürzt werden[126]. Während das Innenministerium nach der Entscheidung des EuGH weiterhin auf eine rasche Einführung drängt, sieht man im Justizministerium mit dem Wegfall der Umsetzungsverpflichtung keinen Grund mehr zur Eile[127].

IV. Fazit

Dieser Überblick über die aktuelle Rechtsprechung des EuGH zum Datenschutz stellt einen Ausschnitt der bereits jetzt vorhandenen Bandbreite der Entscheidungen dar. Sie erfassen grundsätzliche Fragen des Umgangs mit sensiblen Daten ebenso wie Details wie die Behandlung von Arbeitszeiten oder digitale Fingerabdrücke in Reisepässen. Auch vor dem Inkrafttreten der Datenschutzgrundverordnung ist klar, dass der EuGH eine immer wichtiger werdende Rolle im Datenschutzrecht spielt, und man wird sehen, wie er seiner Verantwortung für ein ausgewogenes Verhältnis zwischen Privatheit des Unionsbürgers auf der einen Seite und den Sicherheitsinteressen der Mitgliedsstaaten sowie der Verwendung von Daten zu privaten Wirtschaftszwecken auf der anderen Seite gerecht wird. Dabei kommt es insbesondere darauf an, die nationalen Bedürfnisse der Mitgliedstaaten zu erkennen und auf einen gemeinsamen Nenner zu bringen, der einerseits ein akzeptiertes Privatheitskonzept für Europa enthält und auf der anderen Seite eine hinreichende Abgrenzung zu den teilweise deutlich gegenläufigen Privatheitskonzepten, insbesondere in den USA und dem asiatischen Raum, beinhaltet[128]. Das stellt die Luxemburger Richter in einer Welt, in der Daten längst als neue Währung angekommen sind, vor eine beträchtliche Herausforderung. Sie müssen sich ihr mit Blick für den Welthandel ebenso stellen wie mit Bedacht auf die Eigenheiten der Mitgliedstaaten[129].

Rolf Schwartmann
Rolf Schwartmann lehrt Medienrecht an der Fachhochschule Köln und ist Leiter der Kölner Forschungsstelle für Medienrecht (www.medienrecht.fh-koeln.de). Er ist Mitherausgeber der RDV und Vorsitzender der GDD.

Elissavet Theodorou
Ass. iur. Elissavet Theodorou ist wissenschaftliche Mitarbeiterin an der Forschungsstelle.

120 EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C594/12 – „Digital Rights Ireland Ltd/Irland und Kärntner Landesregierung", Rn. 38.

121 BVerfG, 02.03.2010 – 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08.

122 § 113a TKG verpflichtete alle öffentlich zugänglichen Telekommunikationsdiensteanbieter dazu, von ihnen bei der Nutzung ihrer Dienste (Telefon-, E-Mail- und Internetdienste) erzeugte oder verarbeitete Verkehrsdaten vorsorglich und anlasslos zu speichern. Nach sechs Monaten sollten die Daten innerhalb eines Monats gelöscht werden. § 113b TKG regelte die möglichen Zwecke, für die diese Daten verwendet werden dürfen (nämlich die Verfolgung von Straftaten, die Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und die Erfüllung von nachrichtendienstlichen Aufgaben). § 113 a und § 113 b TKG wurden für nichtig erklärt.

123 BVerfG, 02.03.2010 – 1 BvR 256/08; 1BvR 263/08 und 1 BvR 586/08, Rn. 210.

124 BVerfG, 02.03.2010 – 1 BVR 256/08; 1 BvR 263/08 und 1 BvR 586/08, Rn 211.

125 Siehe dazu Beukelmann, Vorratsdatenspeicherung so nicht verfassungsgemäß, NJW-Spezial 2010, 184.

126 Siehe „Koalitionsvertrag zwischen CDU, CSU und SPD, 18. Legislaturperiode, S. 103, abrufbar unter https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf (letzter Abruf: 08.04.2014).

127 http://www.tagesschau.de/inland/vorratsdaten-inland100.html (letzter Abruf 08.04.2014).

128 Dazu Schwartmann, Freies Surfen, F.A.Z. vom 12.07.2013, http://www.faz.net/aktuell/politik/datenschutz-freies-surfen-12279103.html.

129 Dazu Schwartmann, in: Schwartmann/Jaspers, Big Data – Big Responsibility, Sonderveröffentlichung zur RDV 02/2014, S. 20.

Sascha Kremer

Datenschutzerklärungen von Social Media Diensten: Anwendbares Recht und AGB-Kontrolle

Social Media Dienste verarbeiten fortlaufend personenbezogene Nutzerdaten. Ihre Betreiber bedienen sich zur steuerlichen, haftungs- und datenschutzrechtlichen Optimierung ihrer Geschäftsmodelle komplexer, weltweit verteilter Konzernstrukturen. Die Frage nach dem anwendbaren Datenschutzrecht drängt sich auf und wird hier behandelt.

I. Überblick

Social Media Dienste verarbeiten über ihre Websites und Apps fortlaufend personenbezogene Daten ihrer Nutzer (Ziff. 1.1). Dabei bedienen sich die Betreiber der Social Media Dienste zur steuerlichen, haftungs- und datenschutzrechtlichen Optimierung ihres Geschäftsmodells komplexer, weltweit verteilter Konzernstrukturen. Die Bestimmung des anwendbaren Datenschutzrechts bedarf deshalb einer sorgfältigen Feststellung des Sachverhalts (Ziff. 1.2).

Bei der Bestimmung des anwendbaren Datenschutzrechts ist von der Kollisionsnorm in § 1 Abs. 5 BDSG auszugehen, die wegen der umfassenden Harmonisierungswirkung der Datenschutzrichtlinie (DSRL) von Art. 4 Abs. 1 DSRL überlagert wird (Ziff. 2.1). § 1 Abs. 5 BDSG und Art. 4 Abs. 1 DSRL konkurrieren mit den Kollisionsnormen der Verordnung über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I), so dass das Verhältnis der datenschutzrechtlichen Kollisionsnormen zu den allgemeinen Kollisionsnormen (Ziff. 2.2 und 2.4) und die Vorgehensweise des Gerichts im Streitfall (Ziff. 2.3) zu klären sind.

Die gefundenen Ergebnisse sind auf den Sachverhalt zu übertragen. Dies verlangt zunächst die Ermittlung des Regelungsgehalts von Art. 4 Abs. 1 DSRL (Ziff. 3.1), sowohl bezogen auf das Erfordernis einer Niederlassung innerhalb von EU/EWR i.S.v. Art. 4 Abs. 1 lit. a) DSRL (Ziff. 3.2) als auch auf das Erfordernis des Rückgriffs auf innerhalb von EU/EWR belegener Mittel durch den für die Verarbeitung Verantwortlichen i.S.v. Art. 4 Abs. 1 lit. c) DSRL (Ziff. 3.3). Anschließend erfolgt die Anwendung auf typische Konstellationen bei Social Media Diensten (Ziff. 3.4).

Wird die Datenschutzerklärung des Social Media Dienstes zum Bestandteil des Vertrags mit dem Nutzer gemacht, kann es sich bei den dort enthaltenen Bestimmungen um Allgemeine Geschäftsbedingungen handeln (Ziff. 4.1). Für die dann erforderliche Inhaltskontrolle bedarf es wiederum der Feststellung des anwendbaren Rechts (Ziff. 4.2).

Die wesentlichen Ergebnisse werden im Fazit (Ziff. 5) festgehalten.

II. Sachverhalt

1. Datenverarbeitung durch Betreiber von Social Media Diensten

Nutzer von Social Media Diensten unterliegen einer Dauerüberwachung durch deren Betreiber. Die Verarbeitung[1] personenbezogener Daten ist allgegenwärtig:

a) Die Apps der Social Media Dienste zeichnen für die Betreiber über Sensoren in den Endgeräten oder die im Umfeld des Endgeräts verfügbaren WLAN-Basisstationen Lokalisierungsdaten auf, um nach Ermittlung des Standorts oder Erstellung eines Bewegungsprofils dem Nutzer standortbasierte Inhalte oder Werbung anzubieten.

b) Über Funktionen der Apps oder Websites der Social Media Dienste wie den „Freundefinder“[2] von Facebook werden die Kontakte oder Fotos des Nutzers im Speicher des Endgeräts oder aus anderen Anwendungen durch die Betreiber ausgelesen, um Beziehungen des Nutzers zu anderen Nutzern der Dienste herstellen und die Nutzer virtuell zusammenzuführen.

c) In Cookies[3] oder mittels Browser Fingerprinting[4] werden vom Betreiber die vom Nutzer in Social Media Diensten und auf anderen Websites abgerufenen Inhalte und deren Nutzungsdauer protokolliert, um die so gewonnenen Angaben zur Erstellung von Nutzungsprofilen[5] zu nutzen und zur Grundlage der dem Nutzer angebotenen weiteren Inhalte oder nutzerspezifischer Werbung zu machen.

d) Durch die Auswertung von auf den Servern der Betreiber gespeicherten Inhalten in Social Media Diensten sowie dem Handeln des Nutzers in diesen Diensten und auf Websites Dritter über Statistikdienste wie Facebook Insights[6] und Social-Plugins ermitteln Betreiber unabhängig vom konkreten Verhalten des Nutzers, z.B. über Gesichtserkennung in Fotos oder vom Nutzer vorgenommene „Likes“, dessen Beziehungen zu anderen Nutzern, Unternehmen oder Marken, um den Nutzer damit in Verbindung zu bringen oder nutzerspezifische Werbung zu unterbreiten.

1 Der Begriff der Verarbeitung oder Datenverarbeitung wird in diesem Beitrag entsprechend Art. 2 lit. b) DSRL (Richtlinie 95/46/EG) als Oberbegriff für das Erheben, Verarbeiten und Nutzen personenbezogener Daten i.S.v. § 3 Abs. 3 bis 5 BDSG verwendet.

2 Facebook Freundefinder: https://de-de.facebook.com/find-friends (Alle Links in diesem Beitrag wurden am 20.2.2014 geprüft).

3 Zur sog. „Cookie-Richtlinie“ Schleipfer, RDV 2011, 170; zur angeblichen Umsetzung in Deutschland siehe Telemedicus: http://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html.

4 Zum Browser Fingerprinting: http://heise.de/-1982976; zur datenschutzrechtlichen Bewer-tung Alich/Voigt, CR 2012, 344.

5 Zu Technik und Anwendungsgebieten von Nutzungsprofilen Schleipfer, RDV 2008, 143 ff.

6 Facebook Insights: http://www.facebook.com/help/399262596797358/.

Die Datenverarbeitung durch die Betreiber der Social Media Dienste erfolgt damit zunächst automatisiert auf den Endgeräten der Nutzer, wenn dort deren personenbezogene Daten erhoben und gespeichert werden. Sie setzt sich aber auf den von den Betreibern der Social Media Dienste selbst oder durch Dritte betriebenen Servern fort, weil dort personenbezogene Daten der Nutzer wiederum gespeichert, zu den vorbezeichneten oder anderen Zwecken genutzt und ggf. an Dritte übermittelt werden. Dies kann für Big Data Analysen geschehen, aber auch zur Anmeldung bei einer App eines Dritten auf dem Endgerät des Nutzers mit seinen Zugangsdaten zu einem Social Media Dienst, etwa mittels Facebook Login[7] oder Sign in with Twitter[8].

Ob die Datenverarbeitungen durch einen gesetzlichen Erlaubnistatbestand gerechtfertigt sind oder einer Einwilligung der Nutzer bedürfen, bestimmt sich nach dem für den jeweiligen Datenverarbeitungsvorgang anwendbaren Datenschutzrecht. Dies gilt ebenso für die Notwendigkeit einer Datenschutzerklärung für Social Media Dienste und deren ggf. notwendiger Inhaltskontrolle als Allgemeine Geschäftsbedingungen (dazu unten Ziff. 4)[9].

2. Konzernstrukturen bei Betreibern von Social Media Diensten

Als Betreiber eines Social Media Dienstes tritt zumeist ein Unternehmen auf. Dieses ist Diensteanbieter i.S.v. § 2 Nr. 1 TMG, denn Social Media Dienste sind Telemedien i.S.v. § 1 Abs. 1 S. 1 TMG. Dabei ist das Unternehmen regelmäßig Teil einer komplexen, weltweit verteilten Konzernstruktur, die der steuerlichen, haftungs- und datenschutzrechtlichen Optimierung des eigenen Geschäftsmodells dient[10]. Welches Konzernunternehmen in welchem Teilbereich eines Social Media Dienstes in welcher konzerninternen Organisationsmatrix tätig wird und damit an Verarbeitungen personenbezogener Daten der Nutzer des Dienstes beteiligt ist, erschließt sich nach außen meist nicht.

Kommt es für die Bestimmung des anwendbaren Rechts auf den Ort der Datenverarbeitung an (siehe unten Ziff. 3), kann das Ergebnis der insoweit vorzunehmenden rechtlichen Prüfung ausschließlich vom Sachverhalt abhängen, welcher dem Prüfenden bekannt ist, gleich ob es sich hierbei um ein Gericht oder eine Aufsichtsbehörde handelt. Das kann zu widersprüchlichen Feststellungen bei einem vermeintlich einheitlichen Geschehen führen, die ihre Ursachen nicht in unterschiedlichen Rechtsansichten, sondern anderen Tatsachengrundlagen finden.

Das zeigen die Gerichtsverfahren um Facebook.

Im u.a. um den „Freundefinder" von Facebook (siehe oben Ziff. 1.1 lit. b)) geführten Rechtsstreit vor dem LG Berlin[11] und dem KG[12] war nach dem KG als Sachverhalt zugrunde zu legen, dass die Facebook Ireland Limited „in Europa das soziale Internet-Netzwerk ‚Facebook' betreibt"[13]. Die Datenverarbeitung erfolge tatsächlich aber durch die Facebook Inc. in den USA, deren 100prozentige Tochtergesellschaft die Facebook Ireland Limited sei. Selbst wenn sich die Facebook Inc. als Auftragsverarbeiter der Facebook Ireland Limited vertraglich unterworfen habe, liege wegen der gesellschaftsrechtlichen Befugnisse „de facto die Verantwortung" für die Datenverarbeitung bei der Facebook Inc., so dass für die Bestimmung des anwendbaren Rechts nicht auf die Facebook Ireland Limited abgestellt werden könne[14].

Anders stellte sich der Sachverhalt in dem vor dem VG Schleswig[15] und OVG Schleswig[16] durch die Facebook Inc. um die Weigerung zur Führung pseudonymer Nutzerkonten[17] geführten verwaltungsgerichtlichen Eilverfahren dar. Nach dem dort von VG und OVG zugrunde zu legenden Sachverhalt stand fest, „dass seit dem 28.8.2009 für deutsche Nutzer [Facebook] von der Facebook Ireland Limited [...] angeboten [wird] und [diese] und die Facebook Inc. mit Wirkung vom 15.12.2010 das ‚Data Transfer and Processing Agreement' geschlossen haben." Aus dem vorgenannten Agreement ergebe sich, „dass die Facebook Ireland Limited hinsichtlich ‚bestimmter' Datenkategorien [...] die verantwortliche Stelle ist." Zudem sei „der irische Datenschutzbeauftragte [...] zu dem Ergebnis gelangt, dass Facebook Ireland Limited die einzige Stelle und rechtlich das Unternehmen innerhalb der Facebook Gruppe ist, das Nutzerdaten von nicht nordamerikanischen Nutzern kontrolliert". Deshalb bestünden „keine durchgreifenden Bedenken dagegen [...], dass zum Tätigkeitsbereich der Facebook Ireland Ltd. die hier relevante Verarbeitung personenbezogener Daten gehört." Hiernach war für die Bestimmung des anwendbaren Rechts auf die Facebook Ireland Limited abzustellen, ohne dass gesellschaftsrechtliche Überlegungen seitens des Gerichts angestrengt wurden[18].

Die Feststellung des Sachverhalts, sei es ausgehend vom Vortrag der Parteien oder der Amtsermittlung im Verwaltungsverfahren nach den § 24 Abs. 1 S. 1 VwVfG, § 68 Abs. 1 S. 1 VwGO, ist deshalb mit Blick auf die Bestimmung des anwendbaren Datenschutzrechts von herausragender Bedeutung und mit entsprechender Sorgfalt zu betreiben. Dies gilt nicht nur für die Ermittlung des für die Verarbeitung Verantwortlichen i.S.v. Art. 2 lit. d) DSRL bzw. § 3 Abs. 7 BDSG und seiner ggf. vorhandenen Niederlassungen, sondern auch für die Ermitt-

7 Facebook Login: https://developers.facebook.com/docs/facebook-login.

8 Sign in with Twitter: https://dev.twitter.com/docs/auth/sign-twitter.

9 Ob die Datenverarbeitungen durch Social Media Dienste und deren Datenschutzerklärungen im Einzelfall mit dem (deutschen) Datenschutzrecht in Einklang stehen, ist nicht Gegenstand dieses Beitrags.

10 Zu Steuersparmodellen bei Google und Apple siehe Merten, Steueroasen Ausgabe 2014, S. 35 ff., 43 f.

11 LG Berlin, Urt. v. 6.3.2012 – 16 O 551/10 = CR 2012, 270.

12 KG, Urt. v. 24.1.2014 – 5 U 42/12 (unveröffentlicht).

13 Impressum Facebook: https://www.facebook.com/legal/terms (18.2.2014).

14 KG, Urt. v. 24.1.2014 – 5 U 42/12 unter B.III.3. lit. a) lit. bb) lit. ccc) (unveröffentlicht).

15 VG Schleswig, Beschlüsse v. 14.2.2013 – 8 B 60/12 und 8 B 61/12, CR 2013, 254.

16 OVG Schleswig, Beschlüsse v. 22.4.2013 – 4 MB 10/13 und 4 MB 11/13 = CR 2013, 536.

17 Facebook Nutzungsbedingungen, Ziff. 4.1: https://de-de.facebook.com/legal/terms; zur pseudonymen Nutzung von Telemedien Schleipfer, RDV 2008, 143, 146 ff.

18 OVG Schleswig, Beschlüsse v. 22.4.2013 – 4 MB 10/13 und 4 MB 11/13, Rn 16 f. = CR 2013, 536, 537.

lung der zu beurteilenden Verarbeitungsvorgänge i.S.v. Art. 2 lit. b) DSRL bzw. § 3 Abs. 3 bis 5 BDSG einschließlich der hierfür i.S.v. Art. 4 Abs. 1 lit. c) DSRL verwendeten Mittel (dazu unten Ziff. 3.3) sowie deren Zuordnung für dem für die Verarbeitung Verantwortlichen bzw. dessen Niederlassungen.

III. Bestimmung des anwendbaren Datenschutzrechts

Die Bestimmung des anwendbaren Datenschutzrechts richtet sich vorrangig nach § 1 Abs. 5 BDSG oder Art. 4 DSRL. Zu klären ist deren Verhältnis zu den Vorschriften über das auf vertragliche Schuldverhältnisse anzuwendende Recht nach Rom I (Verordnung EG Nr. 593/2008) einschließlich der Frage, ob das anzuwendende Datenschutzrecht der freien Rechtswahl durch die Parteien obliegt.

1. § 1 Abs. 5 BDSG und Art. 4 Abs. 1 DSRL als Kollisionsnormen

1.1 Einführung des § 1 Abs. 5 BDSG durch das BDSG 2001

Die DSRL bedurfte als Richtlinie i.S.v. Art. 249 S. 3 EGV (entspricht Art. 288 S. 3 AEUV) einer durch Art. 32 Abs. 1 DSRL ausdrücklich angeordneten Umsetzung in nationales Recht. Erwägungsgrund 8 DSRL formulierte dabei das Ziel eines unerlässlichen, gleichwertigen Schutzniveaus „hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung [ihrer] Daten in allen Mitgliedstaaten". Trotz dieses angestrebten gleichmäßigen Schutzniveaus sollten die Mitgliedsstaaten nach Erwägungsgrund 9 DSRL bei der Umsetzung einen Spielraum haben, innerhalb dessen „unter Beachtung des Gemeinschaftsrechts Unterschiede bei der Durchführung der Richtlinie auftreten [können]".

In Deutschland wurde die DSRL mit dem BDSG 2001 in nationales Recht überführt[19]. Soweit für diesen Beitrag relevant, ist mit dem BDSG 2001 als Kollisionsnorm (oder Kollisionsvermeidungsnorm[20]) § 1 Abs. 5 BDSG in Umsetzung von Art. 4 DSRL ergänzt worden. Dabei hat der Gesetzgeber von dem ihm nach Erwägungsgrund 9 DSRL vermeintlich zustehenden Spielraum Gebrauch gemacht und Art. 4 DSRL nicht unverändert übernommen. So wird etwa in § 1 Abs. 5 S. 2 BDSG als Bezugspunkt für die Anwendbarkeit des BDSG auf einen Umgang mit personenbezogenen Daten[21] im Inland durch eine nicht in EU/EWR belegene verantwortliche Stelle abgestellt, während das in Art. 4 Abs. 1 lit. c) DSRL vorgesehene Erfordernis des Rückgriffs auf „automatisierte oder nicht automatisierte Mittel" (dazu unten Ziff. 3.3) zum Zweck der Datenverarbeitung vollständig entfallen ist[22].

§ 1 Abs. 5 BDSG findet mangels eigener Regelung im TMG auch Anwendung, wenn es um die Bestimmung der Anwendbarkeit der §§ 11 ff. TMG, als i.S.v. § 1 Abs. 3 S. 1 BDSG vorrangigen telemedienrechtlichen Spezialregelungen zum Schutz personenbezogener Daten, geht[23]. Das Herkunftslandsprinzip in § 3 Abs. 1, Abs. 2 TMG ist gem. § 3 Abs. 3 Nr. 4 TMG ohne Bedeutung[24].

1.2 Harmonisierungswirkung der DSRL nach dem EuGH

Der EuGH hat bereits 2003 entschieden, dass sich die DSRL nicht auf eine Mindestharmonisierung beschränke, sondern grundsätzlich zu einer „umfassenden Harmonisierung" führe[25]. Diese weithin ignorierte Rechtsprechung[26] stützte der EuGH u.a. auf Erwägungsgrund 7 DSRL, der ein unterschiedliches Schutzniveau bei der Verarbeitung personenbezogener Daten als „Hemmnis [...] für Wirtschaftstätigkeiten auf Gemeinschaftsebene [...]" einordnet, und Erwägungsgrund 10 DSRL, wonach Ziel der DSRL die Sicherstellung eines „hohen Schutzniveaus" in der Gemeinschaft sei. In der Folge hat der EuGH 2011 Art. 7 lit. f) DSRL als in den Mitgliedsstaaten unmittelbar anwendbares Recht eingeordnet, welches strengeren nationalen Regelungen entgegensteht[27].

Die vom EuGH befürwortete „umfassende Harmonisierung" durch die DSRL ist nicht mit einer Vollharmonisierung gleichzusetzen[28]. Der EuGH weist selbst darauf hin, dass die DSRL sehr wohl Vorschriften kenne, „die durch eine gewisse Flexibilität gekennzeichnet sind", ebenso, dass die DSRL „den Mitgliedsstaaten unbestreitbar ein mehr oder weniger großes Ermessen bei der Umsetzung einiger ihrer Bestimmungen einräumt."[29] Es ist deshalb in jedem Einzelfall zu entscheiden, ob nationale Regelungen sich auf die nähere Bestimmung von in der DSRL bereits enthaltenen Grundsätzen bei ein entsprechendes Ermessen einräumenden Vorschriften beschränken oder die nationalen Regelungen solche Vorschriften der DSRL ändern, die keinerlei Flexibilität zu Gunsten des nationalen Gesetzgebers kennen.

In Art. 4 Abs. 1 DSRL heißt es insoweit, jeder Mitgliedsstaat „wendet [...] auf alle Verarbeitungen [...] an", nämlich die von ihm in Umsetzung der DSRL erlassenen gesetzlichen Regelungen; Art. 4 Abs. 2 DSRL spricht davon, dass der für die Verarbeitung Verantwortliche einen Vertreter „zu benennen" hat. Ermessenspielraum oder Flexibilität kennt Art. 4 DSRL nicht. Dazu passt, dass erst Art. 5 DSRL den Mitgliedsstaaten für die nachfolgenden Vorschriften im Kapitel II der DSRL ein Bestimmungsrecht einräumt. Nachdem Art. 4 DSRL auch aus sich heraus so verständlich ist, „dass sich ein Einzelner darauf berufen

19 Gola/Schomerus, BDSG 11. Aufl. 2012, Einl. Rn. 10 f.

20 Simitis/Dammann, BDSG 7. Aufl. 2011, § 1 Rn. 197.

21 Aus dem Zusammenspiel von § 1 Abs. 1, Abs. 2 BDSG ergibt sich, dass der Umgang mit personenbezogenen Daten i.S.d. BDSG der Oberbegriff für das Erheben, Verarbeiten und Nutzen i.S.v. § 3 Abs. 3 bis 5 BDSG ist.

22 Simitis/Dammann, BDSG 7. Aufl. 2011, § 1 Rn. 217.

23 Kremer/Laoutoumai, jurisPR-ITR 5/2013 Anm. 6; Gabel in: Taeger/Gabel, BDSG Kommentar, 2010, § 1 Rn. 53; Jotzo, MMR 2009, 232, 234; Jandt, DuD 2008, 664, 668.

24 Dietrich/Ziegelmayer, CR 2013, 104, 105.

25 EuGH, Urt. v. 6.11.2003 – C-101/01, Lindqvist, Rn. 96 = RDV 2004, 16; ebenso EuGH, Urt. v. 16.12.2008 – C-524/06, Huber, Rn. 51 = RDV 2009, 65.

26 Freund, Anm. EuGH, Urt. v. 24.11.2011 – C-468/10, ASNEF/FECEMD, CR 2012, 29, 32.

27 EuGH, Urt. v. 24.11.2011 – C-468/10, ASNEF/FECEMD, Rn. 39, 55 = RDV 2012, 22; da-zu Kahler, RDV 2012, 167, 169 f.

28 Ebenso Kahler, RDV 2012, 167, 172; Lang, K&R 2012, 43, 44.

29 EuGH, Urt. v. 24.11.2011 – C-468/10, ASNEF/FECEMD, Rn. 35, 52 = RDV 2012, 22.

und ein nationales Gericht ihn anwenden kann“[30], fällt er ebenfalls unter diejenigen Vorschriften der DSRL, die im Sinne der Rechtsprechung des EuGH unmittelbare Wirkung in jedem Mitgliedsstaat entfalten[31].

Einer richtlinienkonformen Auslegung des § 1 Abs. 5 BDSG bedarf es nicht (mehr), weil zur Bestimmung des anwendbaren Datenschutzrechts Art. 4 DSRL[32] unmittelbar angewendet werden kann[33].

2. Verhältnis von Art. 4 Abs. 1 DSRL zu Art. 3, Art. 4 und Art. 6 Rom I

Durch die Inanspruchnahme von Social Media Diensten kommt es zu einem Vertragsschluss zwischen dem jeweiligen Betreiber und Nutzer[34]. Mangels Eingreifens eines der Ausnahmetatbestände in Art. 1 S. 2, Abs. 2 Rom I ist der Anwendungsbereich der „Verordnung über das auf vertragliche Schuldverhältnisse anzuwendende Recht“ nach Art. 1 S. 1 Rom I eröffnet, wenn Nutzer und Betreiber des Social Media Dienstes ihren gewöhnlichen Aufenthalt in verschiedenen Staaten innerhalb von EU/EWR haben und der Vertrag gem. Art. 28 Rom I nach dem 17.12.2009 geschlossen worden ist. Damit stellt sich die Frage, wie sich die Bestimmung des anwendbaren Rechts nach Art. 4 Abs. 1 DSRL zur Bestimmung des anwendbaren Rechts nach Rom I verhält.

Mit Blick auf Rom I tritt das EGBGB wegen der dort zum Internationalen Privatrecht (IPR) getroffenen Regelungen gem. Art. 3 Nr. 1 lit. b) EGBGB Rom I zurück[35]. Im Übrigen ist das anwendbare Recht unabhängig von der internationalen Zuständigkeit der ggf. zur Entscheidung berufenen nationalen Gerichte zu bestimmen[36].

2.1 Social Media Dienste als Dienstleistung i.S.v. Art. 4 Abs. 1 lit. b) Rom I

Haben die Parteien eine Rechtswahl nicht getroffen (dazu unten Ziff. 2.3) könnte sich über Art. 4 Abs. 1 lit. b) Rom I eine Anwendbarkeit des Datenschutzrechts in demjenigen Staat ergeben, in dem der Dienstleister seinen gewöhnlichen Aufenthalt hat.

Der Begriff des Dienstleistungsvertrags wird in Rom I nicht definiert. Er ist als Auffangtatbestand zu verstehen und deshalb weit auszulegen[37], so dass er jeden auf die Erbringung einer Tätigkeit gerichteten Vertrag erfasst[38], ohne dass es zwingend einer entgeltlichen Tätigkeit bedarf[39]. Die Bereitstellung von Social Media Diensten ist ein Handeln des Betreibers und eine Tätigkeit, deren Entgeltlichkeit für den Nutzer sich aus der Kommerzialisierung seiner personenbezogenen Daten als Gegenleistung an den Betreiber ergibt[40]. Der Anwendungsbereich von Art. 4 Abs. 1 lit. b) Rom I wäre mithin eröffnet.

Die anderen Tatbestände in Art. 4 Abs. 1 lit. a), lit. c) bis lit. h) Rom I sind ersichtlich nicht einschlägig.

2.2 Social Media Dienste als Verbrauchervertrag i.S.v. Art. 6 Abs. 1 Rom I

Art. 4 Rom I fungiert als Generalklausel, welche durch die spezielleren Vorschriften der Art. 5 bis Art. 8 Rom I verdrängt wird[41]. Art. 5, Art. 7 und Art. 8 Rom I über Beförderungs-, Versicherungs- und Individualarbeitsverträge sind auf die Nutzung von Social Media Diensten unanwendbar.

In Betracht kommt als speziellere Vorschrift allein Art. 6 Abs. 1 Rom I für Verbraucherverträge. Hiernach unterliegt ein zwischen einem Verbraucher und einem Unternehmer[42] abgeschlossener Vertrag dem Recht des Staates, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat, sofern der Unternehmer entweder

a) seine berufliche oder gewerbliche Tätigkeit in dem Staat ausübt, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat, oder
b) eine solche Tätigkeit in irgendeiner Weise auf diesen Staat oder auf mehrere Staaten, einschließlich dieses Staates, ausrichtet,

und der Vertrag in den Bereich dieser Tätigkeit fällt.

Art. 6 Abs. 1 Rom I beschränkt sich nicht auf Ansprüche der am Verbrauchervertrag beteiligten Parteien, sondern erfasst auch mittelbar auf die Vertragsbeziehung einwirkende Ansprüche, etwa an die Unwirksamkeit von Allgemeinen Geschäftsbedingungen anknüpfende Unterlassungsansprüche gem. § 1 UKlaG[43] (zu Datenschutzerklärungen als Allgemeine Geschäftsbedingungen siehe unten Ziff. 4).

Auf dieser Grundlage hat das LG Berlin 2013 in dem von einem Verbraucherverband gegen die Apple Distribution International Limited als die den europäischen Apple Store im Internet betreibende Tochter der Apple Inc. geführten und zwischenzeitlich rechtskräftig abgeschlossenem Rechtsstreit über die Wirksamkeit bestimmter Klauseln in der dort verwendeten Datenschutzerklärung angenommen, dass der Rechtsstreit

30 EuGH, Urt. v. 24.11.2011 – C-468/10, ASNEF/FECEMD, Rn. 52 = RDV 2012, 22.

31 Ebenso KG, Urt. v. 24.1.2014 – 5 U 42/12 unter B.III.3. lit. a) lit. aa) lit. aaa) (unveröffentlicht); offen gelassen für die Art. 2 bis 12 DSRL von Freund, Anm. EuGH, Urt. v. 24.11.2011 – C-468/10, ASNEF/FECEMD, CR 2012, 29, 33.

32 Für die weiteren Betrachtungen wird Art. 4 Abs. 2 DSRL nicht berücksichtigt.

33 Anderer Ansicht Simitis/Dammann, BDSG 7. Aufl. 2011, § 1 Rn. 218; Piltz, K&R 2013, 292, 295.

34 Zur Rechtsnatur des Nutzungsvertrags Bräutigam, MMR 2012, 635, 636 ff.; Geis/Geis, CR 2007, 721.

35 Vorrangige, für den in diesem Beitrag zu betrachtenden Sachverhalt zu berücksichtigende völkerrechtliche Vereinbarungen i.S.v. Art. 3 Nr. 2 EGBGB, die unmittelbar anwendbares na-tionales Recht geworden sind, sind nicht ersichtlich.

36 Piltz, K&R 2013, 414; zur internationalen gerichtlichen Zuständigkeit Kremer/Buchalik, CR 2013, 789, 790 f.

37 Martiny, in: Münchener Kommentar BGB, 5. Aufl. 2010, Art. 4 Rom I Rn. 17.

38 Martiny, in: Münchener Kommentar BGB, 5. Aufl. 2010, Art. 4 Rom I Rn. 22.

39 Offen gelassen von Martiny, in: Münchener Kommentar BGB, 5. Aufl. 2010, Art. 4 Rom I Rn. 24.

40 Die Preisgabe personenbezogener Daten als Entgelt ebenfalls für möglich hält Bräutigam, MMR 2012, 635, 639.

41 Martiny, in: Münchener Kommentar BGB, 5. Aufl. 2010, Art 4. Rom I Rn. 5.

42 Die Definitionen der Begriffe Verbraucher und Unternehmer in Art. 6 Abs. 1 Rom I ähneln denjenigen in §§ 13, 14 BGB. Zum Verbraucher- und Unternehmerbegriff i.S.v. Art. 6 Abs. 1 Rom I siehe Martiny in: Münchener Kommentar BGB, 5. Aufl. 2010, Art. 6 Rom I Rn. 6 ff.

43 Plath, in: Plath, BDSG Kommentar, 2012, § 1 Rn. 4; a.A. für eine Anwendbarkeit von Rom II Piltz, K&R 2013, 414; Steinrötter, MMR 2013, 691, 692; Micklitz in: Münchener Kommentar ZPO, 4. Aufl. 2013, § 1 UklaG Rn. 55.

vollständig nach deutschem Recht zu entscheiden sei[44]. Dabei hat das LG Berlin allerdings § 1 Abs. 5 BDSG und Art. 4 Abs. 1 DSRL übersehen und sich deshalb mit dem Verhältnis dieser datenschutzrechtlichen Kollisionsnormen zu Rom I fälschlicherweise nicht auseinandergesetzt[45].

Ob bei einem Verbraucher bei Nutzung eines Social Media Dienstes Art. 6 Abs. 1 lit. a) Rom I erfüllt ist, lässt sich über einen Blick in die nach Art. 5 Abs. 1 ECRL (Richtlinie 2000/31/EG) oder § 5 Abs. 1 TMG erforderliche Anbieterkennzeichnung („Impressum") des Betreibers leicht feststellen.

Alternativ verlangt Art. 6 Abs. 1 lit. b) Rom I die Ausrichtung des Social Media Dienstes durch den Betreiber „in irgend einer Weise" auf den Staat, in dem der Verbraucher-Nutzer seinen gewöhnlichen Aufenthalt hat. Der EuGH hat zur Feststellung einer solchen Ausrichtung eine nicht abschließende Liste von Indizien entwickelt[46]. Demnach soll eine solche Ausrichtung nicht bereits aus der technisch kaum zu unterbindenden Abrufbarkeit eines Internet-Dienstes folgen. Vielmehr muss der Unternehmer mit seinem Dienst den Willen zum Ausdruck bringen, seine Leistungen auch Verbrauchern aus anderen Staaten anzubieten. Ein solcher Wille sei etwa bei einer Anpassung des Portals an die jeweils im anderen Staat geltende Sprache und Währung, die Angabe von Telefonnummern mit internationaler Vorwahl oder die von Anfahrtsbeschreibungen aus dem anderen Staat anzunehmen. Derartige Umstände lassen sich bei nahezu jedem Social Media Dienst festmachen[47].

Nutzt mithin ein Verbraucher einen Social Media Dienst, wird Art. 4 Abs. 1 lit. b) Rom I durch Art. 6 Abs. 1 Rom I verdrängt. Bei einem Nicht-Verbraucher als Nutzer eines Social Media Dienstes wäre demnach gem. Art. 4 Abs. 1 lit. b) Rom I das Recht des Staates anwendbar, in dem der Betreiber seinen gewöhnlichen Aufenthalt hat, während bei einem Verbraucher als Nutzer gem. Art. 6 Abs. 1 Rom I das Recht des Staates anwendbar ist, in dem entweder Nutzer und Betreiber gemeinsam ihren gewöhnlichen Aufenthalt haben oder das Recht des Staates, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat. Das anwendbare Recht kann deshalb für Nicht-Verbraucher und Verbraucher nach Rom I nicht einheitlich bestimmt werden.

2.3 Art. 4 Abs. 1 DSRL als vorrangige Eingriffsnorm i.S.d. Art. 9 Abs. 1 Rom I

Art. 4 Abs. 1 DSRL stellt zur Bestimmung des anwendbaren Rechts vorrangig auf das Niederlassungsprinzip oder eingeschränkte Sitzprinzip ab[48].

Ausschlaggebend ist nach Art. 4 Abs. 1 lit. a) S. 1 DSRL der Belegungsort des für die Verarbeitung Verantwortlichen in einem Mitgliedsstaat. Hat der für die Verarbeitung Verantwortliche auch eine mit der Datenverarbeitung befasste Niederlassung in einen anderen Mitgliedsstaat, findet gem. Art. 4 Abs. 1 lit. a) S. 2 DSRL auch das Recht dieses Mitgliedstaates Anwendung[49]. Nur bei einem außerhalb von EU/EWR belegenen für die Verarbeitung Verantwortlichen kommt es zur Anwendung des Territorialprinzips gem. Art. 4 Abs. 1 lit. c) DSRL mit der Folge, dass das Datenschutzrecht desjenigen Mitgliedsstaates Anwendung findet, in dem die vom für die Verarbeitung Verantwortlichen zum Zweck der Datenverarbeitung verwendeten Mittel[50] belegen sind[51].

Insbesondere, wenn Betreiber des Social Media Dienstes und der für die Verarbeitung Verantwortliche sachlich und räumlich auseinanderfallen, was bei den Konzernstrukturen der Betreiber von Social Media Diensten (siehe oben Ziff. 1.2) eher Regel als Ausnahme ist, ist das nach Rom I anwendbare Recht nicht zwingend das nach Art. 4 Abs. 1 DSRL anwendbare Recht. Damit stellt sich die Frage nach dem Verhältnis von Art. 4 DSRL zu Art. 4 und Art. 6 Rom I.

Ein Vorrang von Art. 4 Abs. 1 DSRL gem. Art. 23 Rom I scheidet aus, da es sich bei Art. 4 Abs. 1 DSRL nicht um eine besondere Kollisionsnorm für vertragliche Schuldverhältnisse handelt[52]. Denn ausweislich Art. 1 Abs. 1 DSRL gewährleistet diese „den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten". Dieser Schutz wird nicht über die Regelung von Schuldverhältnissen erreicht, sondern durch die Festlegung von Vorgaben für die Verarbeitung personenbezogener Daten einschließlich deren Kontrolle durch betroffene Person und Aufsichtsbehörde[53].

Das Verhältnis der datenschutzrechtlichen Kollisionsnorm zu Rom I könnte jedoch durch Art. 9 Abs. 2 Rom I geklärt werden, wenn es sich bei Art. 4 Abs. 1 DSRL respektive der nationalen Umsetzung in § 1 Abs. 5 BDSG (zum Verhältnis siehe oben Ziff. 2.1.2) um eine Eingriffsnorm i.S.d. Art. 9 Abs. 1 Rom I handelt.

a. Eingriffsnormen i.S.d. Art. 9 Rom I und deren Wirkung

Art. 9 Abs. 2 Rom I führt zu einem zwingenden, keinerlei Ermessen zulassendem[54] Anwendungsvorrang einer Eingriffsnorm i.S.d. Art. 9 Abs. 1 Rom I gegenüber den Vorschriften des Vertragsstatuts in Rom I[55]. Im Anwendungsbereich einer

44 LG Berlin, Urt. v. 30.4.2013 – 15 O 92/12 = CR 2013, 402 ff.

45 Kremer/Buchalik, CR 2013, 789, 791 f.

46 EuGH, Urt. v. 7.12.2010 – C-585/08 = CR 2011, 108; EuGH, Urt. v. 7.12.2010 – C-144/09 = K&R 2011, 33.

47 Siehe nur die deutschsprachigen Portale von Facebook, Twitter, Google+, Pinterest, Foursquare und LinkedIn.

48 Plath in: Plath, BDSG Kommentar, 2012, § 1 Abs. 5 Rn. 49. Am Niederlassungsprinzip soll unter der Datenschutz-Grundverordnung [DS-GVO, Kom(2012) 11 endgültig: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:HTML; überarbeiteter LIEBE-Entwurf: http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.doc] als Ausdruck der Niederlassungsfreiheit aus Art. 52 AEUV festgehalten werden, vgl. Schröder, ZD 2013, 454; zur DS-GVO insgesamt Gola/Schulz, RDV 2013, 1; Schwartmann, RDV 2012, 55; Eckhardt, CR 2012, 195; Schneider, ITRB 2012, 180.

49 Art. 4 Abs. 1 lit. b) DSRL ist für diesen Beitrag nicht von Bedeutung.

50 Der durch Art. 4 Abs. 1 lit. c) DSRL und § 1 Abs. 5 S. 4 BDSG geregelte Ausnahmefall ei-ner bloßen Durchfuhr der Mittel durch EU/EWR bedarf für diesen Beitrag keiner Betrach-tung.

51 Gola/Schomerus, BDSG Kommentar, 11. Aufl. 2012, § 1 Rn. 29.

52 Schröder, ZD 2013, 453, 454; a.A. ohne Begründung Kümmel, ITRB 2013, 130.

53 Im Einzelnen Simitis, NJW 1997, 281, 286 f.

54 Martiny, in: Münchener Kommentar BGB, 5. Aufl. 2010, Art. 9 Rom I Rn. 109.

55 Martiny, in: Münchener Kommentar BGB, 5. Aufl. 2010, Art. 9 Rom I Rn. 104.

Eingriffsnorm muss Rom I, das ein einheitliches Kollisionsrecht mit dem Ziel rechtssicherer und vorhersehbarer Entscheidungen innerhalb des Binnenmarktes garantieren soll, zurücktreten[56].

Art. 9 Abs. 1 Rom I enthält die Legaldefinition einer Eingriffsnorm.

Bei einer Eingriffsnorm handelt es sich um eine „zwingende Vorschrift, deren Einhaltung von einem Staat als so entscheidend für die Wahrung seines öffentlichen Interesses [...] angesehen wird, dass sie ungeachtet [der Vorschriften von Rom I] auf alle Sachverhalte anzuwenden ist, die in ihren Anwendungsbereich fallen." In jedem Einzelfall ist damit ungeachtet des privat- oder öffentlich-rechtlichen Charakters eines materiellen Gesetzes zu prüfen, ob die jeweilige Regelung zwingend wirken soll, weil sie ihrem Normzweck nach[57] nicht nur im Individualinteresse, sondern auch im Gemeinwohlinteresse geschaffen wurde, gleich ob dieses wirtschaftspolitischer oder sozialpolitischer Natur ist[58]. Sofern die Regelung auf der Umsetzung einer EU-Richtlinie beruht ist zu prüfen, ob und inwieweit der nationalen Regelung explizit oder versteckt ein Eingriffsbefehl beigemessen wird[59].

b. Art. 4 Abs. 1 DSRL als Eingriffsnorm i.S.d. Art. 9 Abs. 1 Rom I

Art. 4 Abs. 1 DSRL ist in Deutschland unmittelbar anwendbar. Die Vorschrift gewährt dem nationalen Gesetzgeber keinerlei Flexibilität oder Ermessen in ihrer Umsetzung (siehe oben Ziff. 2.1.2).

Zweck von Art. 4 Abs. 1 DSRL und der Umsetzungsregelung in § 1 Abs. 5 BDSG ist es, ein abhängig vom Belegungsort des für die Verarbeitung Verantwortlichen (Art. 4 Abs. 1 lit. a) DSRL) oder des für die Verarbeitung verwendeten Mittels (Art. 4 Abs. 1 lit. c) DSRL) einheitliches Datenschutzregime für die von der Verarbeitung betroffenen Personen herzustellen[60]. Zugleich wird den in EU/EWR belegenen, für die Verarbeitung Verantwortlichen ohne Berücksichtigung anderer Rechtsordnungen der Export ihres „eigenes Datenschutzrechts" in andere Mitgliedsstaaten ermöglicht[61], um i.S.v. Art. 1 Abs. 2 DSRL eine Beschränkung oder gar Untersagung für „den freien Verkehr personenbezogener Daten zwischen Mitgliedsstaaten" zu unterbinden[62].

Die mit Art. 4 Abs. 1 DSRL und § 1 Abs. 5 BDSG verfolgten Zwecke dienen ausweislich der schon oben (siehe Ziff. 2.1.2) erwähnten Erwägungsgründe 7 und 8 DSRL Gemeinwohlinteressen. Dort wird das Erreichen eines gemeinsamen „Schutzniveaus hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung [personenbezogener] Daten" als Ziel vorgegeben und von der Beseitigung von einem „Hemmnis für die Ausübung einer Reihe von Wirtschaftstätigkeiten auf Gemeinschaftsebene" gesprochen, welches zuvor „die Erfüllung des Auftrages der in dem Anwendungsbereich des Gemeinschaftsrechts tätigen Behörden" verhindert hat.

Mit der durch § 3 Abs. 3 Nr. 4 TMG angeordneten Ausnahme vom Herkunftslandsprinzip, die auf Art. 1 Abs. 5 lit. b) ECRL zurückgeht[63], zeigt der nationale Gesetzgeber zudem, dass er Art. 4 Abs. 1 DSRL bzw. § 1 Abs. 5 BDSG als mit einem zwingenden Eingriffsbefehl ausgestattet betrachtet. Die datenschutzrechtliche Kollisionsnorm in § 1 Abs. 5 BDSG, der wegen seiner unmittelbaren Anwendbarkeit durch Art. 4 Abs. 1 DSRL überlagert wird, soll von jeglichen Vorschriften in anderen Gesetzen zur Bestimmung des anwendbaren Rechts unberührt bleiben.

§ 1 Abs. 5 BDSG und damit Art. 4 Abs. 1 DSRL als unmittelbar anwendbares Recht erfüllen mithin alle Voraussetzungen einer Eingriffsnorm i.S.d. Art 9 Abs. 1 Rom I[64]. In Übereinstimmung mit dem VG Schleswig[65] und dem OVG Schleswig[66] ist deshalb davon auszugehen, dass es sich hierbei um gegenüber Art. 4 und Art. 6 Abs. 1 Rom I vorrangige Eingriffsnormen i.S.d. Art. 9 Abs. 1 Rom I handelt[67]. Erst nach Prüfung der tatbestandlichen Voraussetzungen aus Art. 4 Abs. 1 DSRL kann ein Gericht demnach eine Entscheidung darüber treffen, welches materielle Datenschutzrecht bei seiner Entscheidungsfindung anzuwenden ist. Dies gilt auch, wenn das Datenschutzrecht nur mittelbar Prüfungsgegenstand ist, etwa bei einer Inhaltskontrolle von Bestimmungen in Datenschutzerklärungen nach den §§ 307 ff. BGB (dazu unten Ziff. 4)[68].

3. Rechtswahl der Parteien nach Art. 3 und Art. 6 Abs. 2 Rom I

Art. 3 Abs. 1 S. 1 Rom I gibt der Rechtswahl durch die Parteien stets den Vorrang. Dies gilt gem. Art. 6 Abs. 2 S. 1 Rom I auch bei Verbraucherverträgen, solange hierdurch dem Verbraucher nicht ein durch Regelungen des nach Art. 6 Abs. 1 Rom I anwendbaren Rechts (dazu oben Ziff. 2.2.2) gewährter zwingender Schutz entzogen wird.

Der Vorrang von Eingriffsnormen gem. Art. 9 Abs. 2 Rom I gilt jedoch nicht nur gegenüber dem gem. Art. 4 bis Art. 8 Rom I ermittelten Vertragsstatut, sondern insbesondere auch gegenüber einem durch Rechtswahl der Parteien bestimmten Vertragsstatut[69]. Anderenfalls würde die zwingende Wirkung einer Eingriffsnorm (dazu oben Ziff. 2.2.3.1) allein durch den Parteiwillen ausgehebelt werden. Rechtswahlklauseln in Nutzungsbedingungen oder Datenschutzerklärungen der Betreiber von Social Media Diensten, die zu einer Beeinflussung des an-

56 Martiny, in: Münchener Kommentar BGB, 5. Aufl. 2010, Art. 9 Rom I, Rn. 12.

57 Piltz, K&R 2012, 640, 643.

58 BAG, Urt. v. 9.10.2002 – 5 AZR 307/01 = NZA 2003, 339; Martiny in: Münchener Kom-mentar BGB, 5. Aufl. 2010, Art. 9 Rom I Rn. 12 f.

59 Ferrari, in: Internationales Vertragsrecht, 2. Aufl. 2011, Art. 9 Rom I Rn. 14.

60 Dammann, in: Simitis, BDSG Kommentar, 7. Aufl. 2011, § 1 Rn. 199.

61 Plath, in: Plath, BDSG Kommentar, 2012, § 1 Rn. 46.

62 Dazu Simitis, NJW 1997, 281, 282.

63 Weller, in: Beck'scher Online Kommentar Informations- und Medienrecht, Edition 2 Nov. 2013, § 3 TMG Rn. 20.

64 Anderer Ansicht Steinrötter, MMR 2013, 691, 693.

65 VG Schleswig, Beschlüsse v. 14.2.2013 – 8 B 60/12 und 8 B 61/12, CR 2013, 254.

66 OVG Schleswig, Beschlüsse v. 22.4.2013 – 4 MB 10/13 und 4 MB 11/13 = CR 2013, 536.

67 Ebenso Piltz, K&R 2013, 292, 296.

68 Ebenso Piltz, K&R 2013, 413, 414; a.A. Steinrötter, MMR 2013, 691, 693.

69 Martiny, in: Münchener Kommentar BGB, 5. Aufl. 2010, Art. 9 Rom I Rn. 104.

wendbaren Datenschutzrechts führen sollen, laufen deshalb wegen des zwingenden Vorrangs von Art. 4 Abs. 1 DSRL ins Leere[70]. Dies verkennt das KG[71], wenn es eine Rechtswahl im Vertrag zwischen Betreiber und Nutzer eines Social Media Dienstes unter Hinweis auf den privatrechtlichen Charakter einzelner Normen im BDSG zulässt.

4. Ermittlung des anwendbaren Rechts durch das Gericht

Im Umkehrschluss aus § 293 S. 1 ZPO folgt, dass das Gericht deutsches Recht einschließlich des IPR und des Rechts der Europäischen Gemeinschaft zu kennen hat[72]. Dies gilt jedoch nicht für das in einem anderen Staat in EU/EWR geltende Recht, mag dieses auch auf europäischen Verordnungen oder Richtlinien beruhen[73].

Die Ermittlung des anwendbaren Rechts erfolgt bei einem Sachverhalt wie hier die Nutzung von Social Media Diensten mit dem BDSG, Rom I und DSRL ausschließlich über die Anwendung deutschen Rechts. Erst wenn sich hieraus ergibt, dass ein ausländisches Sachrecht anzuwenden ist, greift § 293 ZPO mit der Folge, dass das Gericht dessen Regelungsgehalt von Amts wegen zu ermitteln hat[74].

IV. Anwendung des Art. 4 Abs. 1 DSRL auf den Sachverhalt

1. Regelungsgehalt des Art. 4 Abs. 1 DSRL

Wie oben bereits ausgeführt (siehe Ziff. 2.2.3) knüpft Art. 4 Abs. 1 DSRL für die Bestimmung des anwendbaren Rechts zunächst gem. Art. 4 Abs. 1 lit. a) DSRL an den Belegungsort der Niederlassung des für die Verarbeitung Verantwortlichen in einem Mitgliedsstaat oder mehreren Mitgliedsstaaten an. Fehlt es an einer solchen Niederlassung innerhalb von EU/EWR, kann über Art. 4 Abs. 1 lit. c) DSRL gleichwohl das Recht eines Mitgliedsstaates anwendbar sein, wenn dort anstelle einer Niederlassung die automatisierten oder nicht automatisierten Mittel belegen sind, auf welche der für die Verarbeitung Verantwortliche zum Zweck der Verarbeitung zurückgreift.

2. Vorhandensein einer Niederlassung innerhalb von EU/EWR

2.1 Begriff der Niederlassung i.S.d. DSRL

Der Begriff der Niederlassung wird anders als der Begriff des für die Verarbeitung Verantwortlichen in Art. 3 DSRL nicht definiert. Auch § 3 Abs. 7, Abs. 8 BDSG kennt nur Definitionen von verantwortlicher Stelle, Empfänger und Dritten. Aus Erwägungsgrund 19 S. 1 DSRL lässt sich entnehmen, dass eine Niederlassung eine feste Einrichtung voraussetzt, von der die jeweilige Tätigkeit [...] effektiv und tatsächlich ausgeübt wird[75].

Auf die Rechtsform der Niederlassung kommt es nach Erwägungsgrund 19 S. 2 DSRL nicht an, ebenso wenig auf den Sitz der verantwortlichen Stelle[76]. Dabei macht das Kriterium der effektiven und tatsächlichen Ausübung in Übereinstimmung mit dem Wortlaut von Art. 4 Abs. 1 lit. a) BDSG deutlich, dass die Verarbeitung personenbezogener Daten durch die Niederlassung erfolgen und beherrscht werden muss[77]. Auftragsverarbeiter i.S.v. Art. 2 lit. e) DSRL scheiden damit als Niederlassung aus[78].

2.2 Erweiterung des Niederlassungsbegriffs durch Konzernbetrachtungen

Abweichend von Erwägungsgrund 19 S. 1 DSRL will der Generalanwalt beim EuGH den Begriff der Niederlassung mit Blick auf die Ubiquität des Internet und der dort erfolgenden Verarbeitungen neu fassen[79]. Er geht dabei vom Geschäftsmodell der Suchmaschinenbetreiber aus, die nationale Märkte durch einen global verfügbaren Dienst bedienen, ohne dass die in den nationalen Märkten ihren Sitz nehmenden Konzerngesellschaften (zu Konzernstrukturen bei Betreibern von Social Media Diensten oben Ziff. 1.2) selbst noch i.S.d. Erwägungsgrund 19 S. 1 DSRL „effektiv und tatsächlich" Tätigkeiten ausüben. Es soll genügen, wenn diese als Bindeglied zwischen nationalem Markt und global verfügbarem Dienst fungieren, selbst wenn „der technische Datenverarbeitungsvorgang in anderen Mitgliedsstaaten oder Drittländern erfolgt"[80]. Im Fokus des Generalanwalts stehen damit die Vertriebsniederlassungen der global agierenden „Online-Konzerne" in den Mitgliedstaaten[81].

Mit dieser Definition der Niederlassung liest der Generalanwalt Art. 3 DS-GVO[82] (siehe Fußnote 48) in Art. 4 Abs. 1 DSRL hinein, was jedoch mit der Systematik von Art. 4 Abs. 1 DSRL unvereinbar ist. Bereits Art. 4 Abs. 1 lit. c) DSRL erlaubt die Erstreckung des europäischen Datenschutzrechts auf für die Verarbeitung Verantwortliche außerhalb von EU/EWR, wenn diese auf in EU/EWR belegene Mittel zu Zwecken der Verarbeitung zurückgreifen. Mit der vom Generalanwalt vorgeschlagenen Erweiterung des Begriffs der Niederlassung würde Art. 4 Abs. 1 lit. c) DSRL überflüssig werden, weil in dem vom Generalanwalt skizzierten Sachverhalt stets Art. 4 Abs. 1 lit. a) DSRL greifen würde und für Art. 4 Abs. 1 lit. c) DSRL kein Anwendungsbereich mehr verbliebe.

70 Ebenso Piltz, K&R 2013, 292, 296.

71 KG, Urt. v. 24.1.2014 – 5 U 42/12 unter B.III.3. lit. a) lit. cc) lit. bbb) (unveröffentlicht).

72 Huber, in: Musielak, ZPO Kommentar, 10. Aufl. 2013, § 293 Rn. 2.

73 Huber, in: Musielak, ZPO Kommentar, 10. Aufl. 2013, § 293 Rn. 3.

74 BGH, Urt. v. 21.9.1995 – VII ZR 248/94 = NJW 1996, 54, 55; Huber in: Musielak, ZPO Kommentar, 10. Aufl. 2013, § 293 Rn. 6; zum Verfahren der Amtsermittlung Kremer/Buchalik, CR 2013, 789, 793.

75 Ausführlich Piltz, K&R 2013, 292, 294 f.

76 Dammann, in: Simitis, BDSG Kommentar, 7. Aufl. 2011, § 1 Rn. 203.

77 Gabel, in: Taeger/Gabel, BDSG Kommentar, 2010, § 1 Rn. 59; kritisch zu extensiven Auslegungen des Begriffs Niederlassung Ott, MMR 2009, 158, 160.

78 Alich/Sagalov, CR 2013, 783, 789; einschränkend Dammann in Simitis, BDSG Kommentar, 7. Aufl. 2011, § 1 Rn. 203.

79 Dazu Kremer/Buchalik, CR 2013, 789, 792 f.

80 Schlussanträge v. 25.6.2013 – C-131/12, Rn. 60 ff. = EWS 2013, 493, 494.

81 Alich/Sagalov, CR 2013, 783, 784.

82 Zu Art. 3 DS-GVO Piltz, K&R 2013, 292, 296 f.

Auch der Wortlaut von Art. 4 Abs. 1 lit. a) BDSG steht einem solchen Verständnis einer Niederlassung entgegen. Hiernach wird das anwendbare Recht nur insoweit durch Art. 4 Abs. 1 lit. a) BDSG bestimmt, wie die Verarbeitungen „im Rahmen der Tätigkeit der Niederlassung ausgeführt werden". Nach den Vorstellungen des Generalanwalts muss die Niederlassung aber überhaupt keine Verarbeitung mehr ausführen, womit die Wortlautgrenze deutlich überschritten wird [83].

Das im Schlussantrag des Generalanwalts formulierte Niederlassungsverständnis läuft auf eine Gesamtbetrachtung rechtlich selbständiger Konzernunternehmen wegen der von ihnen an welchem Ort auch immer vorgenommenen Verarbeitungen hinaus, solange diese nur in mindestens einen nationalen Markt hineinwirken[84]. Damit konstruiert der Generalanwalt eine Konzerndiskriminierung, obwohl die DSRL im Übrigen ein Konzernprivileg nicht kennt. Es bleibt zu hoffen, dass der EuGH diese Überlegungen nicht aufgreift und es beim vom Wortlaut des Erwägungsgrunds 19 S. 1 DSRL ausgehenden Begriff der Niederlassung belässt.

3. Rückgriff auf innerhalb von EU/EWR belegenen Mitteln

§ 1 Abs. 5 S. 2 BDSG ist eine unvollständige Umsetzung von Art. 4 Abs. 1 lit. c) DSRL (dazu oben Ziff. 2.1.2). Entscheidend ist entgegen § 1 Abs. 5 S. 2 BDSG nicht, ob die Verarbeitung in einem Mitgliedsstaat erfolgt. Ausreichend ist gem. § 4 Abs. 1 lit. c) DSRL, wenn der für die Verarbeitung Verantwortliche auf im Mitgliedsstaat belegene „automatisierte oder nicht automatisierte Mittel" zu Zwecken der Verarbeitung zurückgreift.

Das BDSG kennt den Begriff des Mittels nicht. In Art. 2 DSRL fehlt eine Definition des Mittels. Aus Art. 4 Abs. 1 lit. a) DSRL lässt sich lediglich ableiten, dass eine Niederlassung kein Mittel ist. Vielmehr sind damit technische Einrichtungen gemeint, durch welche die Verarbeitung personenbezogener Daten erfolgt und die von dem für die Verarbeitung Verantwortlichen gesteuert werden, die mithin eine Verarbeitung „auf Distanz" ermöglichen[85], gleich ob es sich dabei um Hardware oder Software handelt[86].

Ob die technischen Einrichtungen durch den für die Verarbeitung Verantwortlichen betrieben werden oder in dessen Eigentum stehen, ist für Art. 4 Abs. 1 lit. c) DSRL bedeutungslos. Art 4 Abs. 1 lit. c) verlangt nur einen Rückgriff auf die Mittel und damit die ggf. nur mittelbare Möglichkeit des für die Verarbeitung Verantwortlichen zur Einflussnahme auf die Nutzung der Mittel zur Datenverarbeitung[87]. Damit sind auch die vom Auftragsverarbeiter für den für die Verarbeitung Verantwortlichen bei einer Auftragsdatenverarbeitung eingesetzten Mittel solche i.S.d. Art. 4 Abs. 1 lit. c) DSRL[88]. Anderenfalls könnte Art. 4 Abs. 1 lit. c) DSRL durch die „richtige" Vertragsgestaltung entkernt werden.

Wenn für die Erhebung personenbezogener Daten ein Rückgriff auf Mittel i.S.v. Art. 4 Abs. 1 lit. c) DSRL verneint wird, solange die betroffene Person selbst in hierfür von dem für die Verarbeitung Verantwortlichen gestellten Eingabemasken auf einer Website oder in einer Anwendung (App) auf einem mobilen Endgerät personenbezogene Daten eingibt[89], ist dies zutreffend. Zwar handelt es sich bei von dem für die Verarbeitung Verantwortlichen gestellten Eingabemasken um Mittel i.S.v. Art. 4 Abs. 1 lit. c) DSRL. Von diesen macht der für die Verarbeitung Verantwortliche jedoch keinen Gebrauch[90]. Denn die Eingaben in solchen Masken werden nicht als Erhebung von dem für die Verarbeitung Verantwortlichen i.S.v. Art. 4 Abs. 1 lit. c) DSRL ausgeführt, sondern von der betroffenen Person selbst[91].

4. Anwendbares Recht bei Social Media Diensten

Überträgt man die obigen Ausführungen zu Art. 4 Abs. 1 DSRL auf Social Media Dienste und den oben geschilderten Sachverhalt (siehe Ziff. 1.1), ergibt sich die nachfolgend beschriebene Rechtslage.

4.1 Niederlassung innerhalb von EU/EWR

Erfolgt die Verarbeitung personenbezogener Daten durch eine Niederlassung des für die Verarbeitung verantwortlichen Betreibers innerhalb von EU/EWR, findet über Art. 4 Abs. 1 lit. a) S. 1 DSRL das Datenschutzrecht desjenigen Staates Anwendung, in dem die Niederlassung belegen ist, also ihren Sitz hat[92]. Dies bedingt allerdings, dass die Niederlassung die Verarbeitung tatsächlich beherrscht (siehe oben Ziff. 3.2.1).

In dem oben geschilderten Fall von Facebook (siehe Ziff. 1.2) scheint zwar nach den Feststellungen des OVG Schleswig[93] und des KG[94] festzustehen, dass die Facebook Ireland Limited mit Sitz in Irland als 100prozentige Tochter der Facebook Inc. mit Sitz in den USA Vertragspartnerin der Nutzer von Facebook in Europa wird und insoweit Betreiberin dieses Social Media Dienstes ist. Unklar ist aber, wer die Verarbeitungen der Daten betroffener Personen beherrscht, ob also die Facebook Ireland Limited „effektiv und tatsächlich" i.S.v. Erwägungsgrund 19 S. 1 DSRL diese Tätigkeit ausübt.

83 Alich/Sagalov, CR 2013, 783, 786, 788.

84 Alich/Sagalov, CR 2013, 783, 787.

85 Gusy, in: Beck'scher Online-Kommentar Datenschutzrecht, Edition 6 November 2013, § 1 BDSG Rn. 113; von „an einen Datenträger gebundenen Vorgängen" spricht Dammann in: Simitis, BDSG Kommentar, 7. Aufl. 2011, § 1 Rn. 220; siehe auch WP 56 Art. 29 Gruppe über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU, S. 9 ff.: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_de.pdf; ferner WP 179 der Art. 29 Gruppe mit der Stellungnahme 8/2010 zum anwendbaren Recht, S. 25 ff.: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf.

86 Jandt, DuD 2008, 664, 669.

87 Gusy, in: Beck'scher Online-Kommentar Datenschutzrecht, Edition 6 November 2013, § 1 BDSG Rn. 112; KG, Urt. v. 24.1.2014 – 5 U 42/12 unter B.III.3 lit. a) lit. aa) lit. bbb) (unveröf-fentlicht).

88 Gabel, in: Taeger/Gabel, BDSG Kommentar, 2010, § 1 Rn. 58; a.A. Dammann, in: Simitis, BDSG Kommentar, 7. Aufl. 2011, § 1 Rn. 230.

89 Dammann, in: Simitis, BDSG Kommentar, 7. Aufl. 2011, § 1 Rn. 223.

90 Piltz, K&R 2013, 292, 295; a.A. nach normativer Auslegung Jotzo, MMR 2009, 232, 236.

91 Ebenso Klar, ZD 2013, 109, 114; Alich/Nolte, CR 2011, 741, 742.

92 Dammann, in: Simitis, BDSG Kommentar, 7. Aufl. 2011, § 1 Rn. 204.

93 OVG Schleswig, Beschlüsse v. 22.4.2013 – 4 MB 10/13 und 4 MB 11/13 = CR 2013, 536.

94 KG, Urt. v. 24.1.2014 – 5 U 42/12 (unveröffentlicht).

Klar ist, dass sich die Facebook Ireland Limited auf der Grundlage eines „Data Transfer and Processing Agreement" der Facebook Inc. als Auftragsverarbeiter in den USA bedient. Diese Konstruktion erscheint gem. Art. 25 Abs. 1, Abs. 5 DSRL in Verbindung mit den Safe Harbor Grundsätzen[95] grundsätzlich als zulässig, hat sich doch Facebook der Safe Harbor Zertifizierung unterworfen[96].

Allerdings stellt sich die vom KG aufgeworfene Frage, welche Auswirkungen es hat, dass es sich bei der für die Verarbeitung verantwortlichen Facebook Ireland Ltd. um eine 100prozentige Tochtergesellschaft der Facebook Inc. handelt, wie es mithin um die tatsächliche Herrschaft über die bei der Facebook Inc. als Auftragsverarbeiter liegenden personenbezogenen Daten bestellt ist[97]. Dieser vom OVG Schleswig[98] außer Acht gelassene Aspekt kommt auch im Working Paper 169 der Art. 29 Gruppe vom 16.10.2010[99] zum Ausdruck, wenn dort für die Frage nach der Entscheidungsbefugnis des für die Verarbeitung Verantwortlichen auf die Analyse faktischer Elemente oder Umstände eines Falles und nicht auf rechtliche Erwägungen abgestellt wird[100]. Dabei wird ausdrücklich die Kategorie der Verantwortung für die Verarbeitung auf Grund eines tatsächlichen Einflusses gebildet[101].

Legt man diesen Maßstab zu Grunde sind die Erwägungen des KG valide.

Insbesondere in den USA wird der Social Media Dienst Facebook nicht von der Facebook Ireland Limited, sondern unmittelbar von der Facebook Inc. betrieben. Ob diese Teilung des Betriebs von Facebook dazu führt, dass auch die personenbezogenen Daten der Nutzer in unterschiedlichen Datenbanken landen, die zur Ermöglichung einer weltweiten Kommunikation über Schnittstellen miteinander verbunden sind, ist nicht bekannt, erscheint aber lebensfremd. Wenn sich die Facebook Ireland Limited der Facebook Inc. als Auftragsverarbeiter bedient, dürfte dies gerade zu dem Zweck geschehen, eine weltweit einheitliche Datenhaltung zu ermöglichen. Insoweit erweckt der Sachverhalt bezogen auf den europäischen Teil von Facebook den Eindruck, als diene die Einschaltung der Facebook Ireland Inc. als Betreiberin für Facebook in Europa und der Abschluss des „Data Transfer and Processing Agreement" nur dazu, über Art. 4 Abs. 1 lit. a) DSRL die Anwendbarkeit irischen Datenschutzrechts zu erzwingen. Bereits das Vorhandensein einer einheitlichen Datenbank über alle Nutzer hinweg würde dafür sprechen, dass die Facebook Inc. den tatsächlichen Einfluss auf diese Datenbank hat, während die Facebook Ireland Limited ungeachtet der im „Data Transfer and Processing Agreement" getroffenen Vereinbarungen der verlängerte Arm der Facebook Inc. in Europa und nicht umgekehrt ist.

Aber auch aus den vom KG angeführten gesellschaftsrechtlichen Aspekten heraus hat die Facebook Inc. die tatsächliche Herrschaft über die bei ihr befindlichen Daten. Denn als alleinige Gesellschafterin kann sie jederzeit, wie es das KG formuliert, „die Entscheidungsprozesse an sich ziehen".[102] Die dem Auftragsverarbeiter gegenüber gem. Art. 17 Abs. 3, 1. Spiegelstrich DSRL und § 11 Abs. 3 S. 1 BDSG bestehende jederzeitige Weisungsbefugnis des für die Verarbeitung Verantwortlichen bleibt wirkungslos, wenn der Auftragsverarbeiter durch gesellschaftsrechtliche Einflussnahme die Erteilung von Weisungen inhaltlich beeinflussen oder vollständig verhindern kann[103].

Die Facebook Ireland Limited führt demnach im Tatsächlichen keine Verarbeitungen personenbezogener Daten als eine Niederlassung der Facebook Inc. in einem Mitgliedsstaat aus. Art. 4 Abs. 1 lit. a) DSRL kann deshalb zur Bestimmung des anwendbaren Rechts für Facebook nach dem derzeit bekannten Sachverhalt (siehe oben Ziff. 1.2) nicht herangezogen werden.

Anders wäre dies bei denjenigen Betreibern von Social Media Diensten, die entweder selbst als der für die Verarbeitung Verantwortliche ihren Sitz innerhalb von EU/EWR haben oder dort eine tatsächlich im Sinne eines beherrschenden Einflusses mit der Verarbeitung befasste Niederlassung unterhalten. Dann fände über Art. 4 Abs. 1 lit. a) DSRL bzw. § 1 Abs. 5 S. 1, 1. Halbsatz BDSG das Datenschutzrecht des jeweiligen Sitzlandes Anwendung.

4.2 Mittel innerhalb von EU/EWR

Scheidet Art. 4 Abs. 1 lit. a) DSRL als Anknüpfungspunkt für eine Bestimmung des anwendbaren Datenschutzrechts aus und hat der Betreiber eines Social Media Dienstes als der für die Verarbeitung Verantwortliche seinen Sitz außerhalb von EU/EWR, kann die Bestimmung des anwendbaren Rechts über Art. 4 Abs. 1 lit. c) DSRL geschehen, wenn der Betreiber zum Zweck der Verarbeitung auf innerhalb von EU/EWR belegene Mittel (zum Begriff oben Ziff. 3.3) zurückgreift.

Das ist in der Regel der Fall, wenn der Social Media Dienst über Nutzer innerhalb von EU/EWR verfügt. Nicht ausreichend hierfür ist zwar, wenn sich der Nutzer der vom Betreiber auf einer Website oder in einer App[104] zur Erfassung von Inhalten bereitgestellten Eingabemasken bedient (dazu oben Ziff.

95 Safe Harbor Grundsätze: http://www.export.gov/safeharbor/; dazu: Entscheidung der Kommission vom 26.7.2000 – 2000/520/EG: http://tinyurl.com/mqh23zk; Beschluss des Düsseldorfer Kreises am 28./29. April 2010 in Hannover (überarbeitete Fassung vom 23.8.2010): http://tinyurl.com/k2kkb4v; zur Entwicklung von Safe Harbor Weichert, RDV 2012, 113, 117; Wybitul/Patzak, RDV 2011, 11, 13.

96 Facebook Safe Harbor Zertifizierung: https://www.facebook.com/safeharbor.php.

97 KG, Urt. v. 24.1.2014 – 5 U 42/12 unter B.III.3. lit. a) lit. bb) lit. ccc) (unveröffentlicht).

98 OVG Schleswig, Beschlüsse v. 22.4.2013 – 4 MB 10/13 und 4 MB 11/13 = CR 2013, 536.

99 WP 169 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter": http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf.

100 Art. 29 Gruppe, WP 169 (Fußnote 99), S. 11.

101 Art. 29 Gruppe, WP 169 (Fußnote 99), S. 14.

102 KG, Urt. v. 24.1.2014 – 5 U 42/12 unter B.III.3. lit. a) lit. bb) lit. ccc) (unveröffentlicht).

103 Zur Rolle der Facebook Germany GmbH siehe OVG Schleswig, Beschlüsse v. 22.4.2013 – 4 MB 10/13 und 4 MB 11/13, Rn. 16 = CR 2013, 536, 537.

104 Zum Datenschutz bei Entwicklung, Vertrieb und Nutzung von Apps Lober, K&R 2013, 357; Kremer, CR 2012, 438; zur Vertragsgestaltung Kremer, CR 2011, 769.

3.4.2). In dem Moment aber, in dem der Betreiber als für die Verarbeitung Verantwortlicher die Verarbeitung selbständig steuert, wird die Website oder App zum Mittel i.S.v. Art. 4 Abs. 1 lit. c) DSRL. Dazu genügt es, wenn über Cookies oder Browser Fingerprinting personenbezogene Daten über den Nutzer im Social Media Dienst oder auf Websites Dritter erhoben werden. Die Erfassung von Lokalisierungsdaten über Sensoren in den Endgeräten oder im Umfeld des Endgeräts verfügbare WLAN-Basisstationen fällt ebenso hierunter wie das Auslesen von Kontakten, Fotos oder anderen Inhalten auf dem Endgerät. Der Nutzer hat mangels Einblick in die Verarbeitung trotz einer etwaig von ihm erteilten Einwilligung in diese Vorgänge keinen Einblick in die konkreten Abläufe und kann diese auch nicht steuern.

Über Art. 4 Abs. 1 lit. c) DSRL gelangt man in den hier bezeichneten Fällen stets zur Anwendung des nationalen Datenschutzrechts in allen Mitgliedsstaaten, in denen Nutzer des jeweiligen Social Media Dienstes ihren gewöhnlichen Aufenthalt haben.

V. AGB-Kontrolle von Datenschutzerklärungen

1. Datenschutzerklärungen als Allgemeine Geschäftsbedingungen

Auch die Anwendbarkeit des bereichsspezifischen Datenschutzrechts für Telemedien in den §§ 11 ff. TMG richtet sich nach § 1 Abs. 5 BDSG bzw. Art. 4 Abs. 1 DSRL (siehe oben Ziff. 2.1.1).

§ 13 Abs. 1 S. 1 TMG legt den Betreibern von Social Media Diensten (bei denen es sich um Telemedien handelt, siehe oben Ziff. 1.2), so denn deutsches Datenschutzrecht Anwendung findet (siehe oben Ziff. 3.4), die Verpflichtung auf, Nutzer vor der erstmaligen Inanspruchnahme des Dienstes „zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb [von EU/EWR] in allgemein verständlicher Form zu unterrichten“ und diese Unterrichtung sodann gem. § 13 Abs. 1 S. 3 TMG „jederzeit abrufbar“ für den Nutzer zu halten.

Bei der häufig als Datenschutzerklärung bezeichneten Unterrichtung nach § 13 Abs. 1 S. 1 TMG handelt es sich um eine Wissenserklärung[105] des Betreibers. Die Datenschutzerklärung dient allein der Schaffung von Transparenz durch Information des Nutzers[106], ohne dass hieran wie bei einer Willenserklärung oder geschäftsähnlichen Handlung der Eintritt einer Rechtsfolge geknüpft ist, die kraft Parteiwillens gewollt oder unabhängig hiervon vom Gesetzgeber angeordnet ist.

Bezieht der Betreiber eines Social Media Dienstes die Bestimmungen der Datenschutzerklärung jedoch in den mit dem Nutzer geschlossenen Vertrag (dazu oben Ziff. 2.2) ein, wird aus der Wissenserklärung des Betreibers eine von diesem für eine Vielzahl von Fällen vorformulierte Vertragsbedingung i.S.v. § 305 Abs. 1 S. 1 BGB. Unabhängig vom tatsächlichen Regelungsgehalt einer Datenschutzerklärung ist für das Vorliegen einer Vertragsbedingung ausreichend, wenn der Erklärungsempfänger den Eindruck gewinnt, diese begründe eine „irgendwie geartete Verbindlichkeit“[107]. Bei der Datenschutzerklärung handelt es sich dann um Allgemeine Geschäftsbedingungen[108].

Bei Social Media Diensten erfolgt die Einbeziehung der Datenschutzerklärung in den Nutzungsvertrag regelmäßig mittels Aktivierung einer Checkbox durch den Nutzer vor einem Text wie „Mit Geltung der Allgemeinen Geschäftsbedingungen [als Link ausgeführt] und der Datenschutzerklärung [als Link ausgeführt] bin ich einverstanden.“ im Prozess der Anmeldung für den Social Media Dienst. Eine derartige Einbeziehung ist wirksam, wenn sie gegenüber Verbrauchern den Anforderungen gem. § 305 Abs. 2 BGB genügt[109]. Bei Unternehmern ist demgegenüber jede Einbeziehungsvereinbarung ausreichend. Allein die Branchenüblichkeit der Verwendung von AGB kann deren Einbeziehung jedoch nicht begründen[110].

2. Bestimmung des für die Inhaltskontrolle anzuwendenden Rechts

Mit der Inhaltskontrolle Allgemeiner Geschäftsbedingungen wird deren Wirksamkeit als Bestandteil eines Vertrags festgelegt. Es geht nicht um materielles Datenschutzrecht, sodass § 1 Abs. 5 BDSG und Art. 4 Abs. 1 DSRL als Kollisionsnormen ausscheiden. Stattdessen richtet sich die Bestimmung des anwendbaren Rechts bei grenzüberschreitenden Sachverhalten nach Rom I (zu Rom I oben Ziff. 2.2). Art. 10 Abs. 1 Rom I legt insoweit ausdrücklich fest, dass sich die Wirksamkeit von Vertragsbestimmungen nach dem Recht richtet, welches anzuwenden wäre, wenn die Vertragsbestimmungen wirksam sind. Dies gilt auch für die Inhaltskontrolle Allgemeiner Geschäftsbedingungen[111].

In Betracht kommt wiederum eine Bestimmung des anwendbaren Rechts durch Rechtswahl der Parteien gem. Art. 3 Abs. 1 S. 1 Rom I und Art. 6 Abs. 2 Rom I (dazu oben Ziff. 2.3), gem. Art. 6 Abs. 1 Rom I bei Verbraucherverträgen (dazu oben Ziff. 2.2.2) oder gem. Art. 4 Abs. 1 lit. b) Rom I bei Nutzungsverträgen über Social Media Dienste mit Nichtverbrauchern (dazu oben Ziff. 2.2.1). Handelt es sich bei Nutzern von Social

105 Zum Begriff Armbrüster, in: Münchner Kommentar BGB, 6. Aufl. 2012, Vor § 116 Rn. 16.

106 Müller-Broich, TMG Kommentar, 2012, § 13 Rn. 1.

107 Basedow, in: Münchener Kommentar BGB, 6. Aufl. 2012, § 305 Rn. 12.

108 Ebenso Schröder, ZD 2013, 453, 454; LG Hamburg, Urt. v. 7.8.2009 – 324 O 650/08 = CR 2010, 53, 56 f.; vom BGH bislang nur bejaht für einseitig zu Lasten des Empfängers wirkende datenschutzrechtliche Einwilligungserklärungen, siehe BGH, Urt. v. 11.11.2009 – VIII ZR 12/08 – HappyDigits = RDV 2010, 77; Urt. v. 16.7.2008 – VIII ZR 348/06 – Payback = RDV 2008, 201.

109 Zu den Erleichterungen gegenüber Verbrauchern bei AGB beachte § 310 Abs. 3 BGB.

110 BGH, Urt. v. 15.1.2004 – VIII ZR 111/13, Rn. 17 = BeckRS 2014, 03240.

111 Spellenberg, in: Münchener Kommentar BGB, 5. Aufl. 2010, Art. 10 Rom I Rn. 150.

Media Diensten um Verbraucher mit gewöhnlichem Aufenthalt in Deutschland, ist selbst bei einer abweichenden Rechtswahl durch den Betreiber des Social Media Dienstes gem. Art. 6 Abs. 2 S. 2 Rom I regelmäßig deutsches Recht für die Inhaltskontrolle anwendbar, also die §§ 305 ff. BGB. Diese enthalten z.B. in den §§ 308, 309, 310 Abs. 3 BGB zwingendes Recht zu Gunsten des Verbrauchers, von dem durch Rechtswahl nicht abgewichen werden darf.

Welche gesetzliche Regelung im Datenschutz wiederum der Prüfungsmaßstab i.S.d. § 307 Abs. 2 Nr. 1 BGB für eine als Allgemeine Geschäftsbedingungen geltende Datenschutzerklärung ist, mit deren wesentlichen Grundgedanken die dort niederlegten Bestimmungen für eine wirksame Einbeziehung in den Nutzungsvertrag übereinstimmen müssen, bemisst sich wegen der Bezugnahme auf materielles Datenschutzrecht als Prüfungsmaßstab wiederum nach Art. 4 Abs. 1 DSRL (dazu oben Ziff. 2.2.3).

VI. Fazit

Bei der Bestimmung des anwendbaren Datenschutzrechts hat Art. 4 Abs. 1 DSRL, der wegen seiner ungenügenden Umsetzung in § 1 Abs. 5 BDSG in Deutschland unmittelbar anzuwenden ist, als Eingriffsnorm i.S.d. Art. 9 Abs. 1 Rom I über Art. 9 Abs. 2 Rom I Vorrang gegenüber dem sich nach Rom I ergebenden Vertragsstatut.

Bei Social Media Diensten ist das anwendbare Datenschutzrecht nach Art. 4 Abs. 1 lit. a) DSRL und Art. 4 Abs. 1 lit. c) DSRL zu bestimmen.

Art. 4 Abs. 1 lit. a) DSRL verlangt das Vorhandensein einer innerhalb von EU/EWR belegenen Niederlassung des für die Verarbeitung Verantwortlichen. Diese muss i.S.d. Erwägungsgrund 19 S. 1 DSRL tatsächlich den Verarbeitungsvorgang beherrschen. Handelt es sich bei der Niederlassung um ein Konzernunternehmen, welches zwar gegenüber seinen Nutzern innerhalb von EU/EWR als Diensteanbieter i.S.d. § 2 Nr. 1 TMG auftritt, die Verarbeitung der personenbezogener Daten der Nutzer jedoch der beherrschenden Konzernmutter als Auftragsverarbeiter überlasst, wird die tatsächliche Kontrolle über die Verarbeitung nicht von der Konzerntochter, sondern von der Konzernmutter ausgeübt. In diesem Fall scheidet die Konzerntochter als eine die Verarbeitung ausführende Niederlassung i.S.v. Art. 4 Abs. 1 lit. a) DSRL aus.

Die für Art. 4 Abs. 1 lit. c) DSRL erforderlichen, innerhalb von EU/EWR belegenen Mittel sind insbesondere Websites und Apps. Erhebt der Betreiber eines Social Media Dienstes über seine Website oder Apps personenbezogene Daten seiner Nutzer, etwa durch die automatisierte Erfassung von Lokalisierungsdaten oder das Verfolgen der Handlungen des Nutzers innerhalb oder außerhalb des Dienstes mittels Cookies oder Browser-Fingerprinting, greift er auf diese Mittel bei der Verarbeitung zurück, so dass der Anwendungsbereich von Art. 4 Abs. 1 lit. c) DSRL eröffnet ist. Hat der Nutzer seinen Sitz in Deutschland, führt dies zur Anwendbarkeit deutschen Datenschutzrechts.

Bezieht der Betreiber eines Social Media Dienstes seine Datenschutzerklärung in den Vertrag mit dem Nutzer ein, sind die in der Datenschutzerklärung enthaltenen Regelungen Allgemeine Geschäftsbedingungen i.S.v. § 305 Abs. 1 S. 1 BGB. Das auf die Bestimmung der Wirksamkeit solcher Allgemeiner Geschäftsbedingungen anwendbare Recht bemisst sich gem. Art. 10 Abs. 1 Rom I nach Rom I, soweit es um Social Media Dienste geht insbesondere nach Art. 3 Abs. 1 S. 1, Art. 4 Abs. 1 lit. b) und Art. 6 Abs. 1 Rom I. Handelt es sich beim Nutzer um einen Verbraucher i.S.v. Art. 6 Abs. 1 Rom I mit Sitz in Deutschland, bleibt es auch bei einer abweichenden Rechtswahl im Vertrag gem. Art. 6 Abs. 2 S. 2 Rom I bei der Anwendbarkeit der §§ 305 ff. BGB auf die Inhaltskontrolle. Prüfungsmaßstab bei der Inhaltskontrolle nach § 307 Abs. 2 Nr. 1 BGB ist dann wiederum das zuvor über Art. 4 Abs. 1 DSRL ermittelte materielle Datenschutzrecht.

Sascha Kremer

Sascha Kremer ist Fachanwalt für IT-Recht und Partner bei LLR LegerlotzLaschet Rechtsanwälte in Köln (www.llr.de). Zugleich ist er Geschäftsführer der LLR Data Security and Consulting GmbH (www.llrdsc.de) und als externer Datenschutzbeauftragter tätig. Er unterrichtet als Lehrbeauftragter an der Heinrich-Heine-Universität Düsseldorf und der Hochschule Bonn-Rhein-Sieg. Spezialisiert ist er auf das Informationstechnologie-Recht nebst den Bezügen zum Gewerblichen Rechtsschutz (insb. Urheberrecht, Wettbewerbsrecht) und das Datenschutzrecht, ebenso auf die praktische Umsetzung des Datenschutzes und der IT-Sicherheit in Unternehmen.

Dennis-Kenji Kipker / Friederike Voskamp

PRISM und staatliche Schutzpflichten – ein politisches Märchen?

Die Datenströme machen an den nationalstaatlichen Grenzen nicht halt. Besonders deutlich wurde die globale Vernetzung des Datenverkehrs an dem zur Jahresmitte 2013 vom amerikanischen Whistleblower Edward Snowden bekannt gemachten NSA-Skandal, in dessen Rahmen auch die personenbezogenen Daten deutscher Bürger zu Zwecken der öffentlichen Sicherheit von amerikanischen Regierungsbehörden ausgewertet wurden. Folglich bedeutet für die Zukunft die Interessenabwägung zwischen informationeller Freiheit und staatlicher Sicherheit nicht nur, sich auf die Kontrollrechte und Abwehrmöglichkeiten gegenüber nationalen, deutschen Behörden zu beschränken. Darüber hinaus stellt sich die Frage, ob die informationellen Grundrechte in Deutschland über ihre Abwehrfunktion hinaus Geltung beanspruchen können, indem der einzelne Betroffene auch eine Schutzfunktion des deutschen Staates in Bezug auf seine Privatsphäre gegenüber fremden Staaten einfordern kann, die in seine informationelle Freiheit zu Zwecken der Aufrechterhaltung der öffentlichen Sicherheit eingreifen.

I. Einleitung

Wie die Datenströme nicht vor Nationalgrenzen halt machen – im Gegenteil, sogar ein Großteil des globalen Datenverkehrs wird über die USA abgewickelt – so haben auch die Bedrohungen für die öffentliche Sicherheit einen zunehmend globalen Charakter. Man kann insoweit auch von einer Globalisierung des Sicherheitsbegriffes sprechen, infolgedessen jeder Staat zu einem möglichen Betroffenen werden kann. Indem die Aufrechterhaltung der öffentlichen Sicherheit somit gezwungenermaßen auch eine staatenübergreifende Aufgabe wird, stellt sich die Frage, ob infolge des daraus resultierenden globalen Datenaustausches auch der Grundrechtsschutz zu einer staatenübergreifenden Aufgabe wird. Für den einzelnen Nationalstaat, hier Deutschland, könnte eine solche grenzüberschreitende Aufgabe nur begründet werden, wenn ihn eine verfassungsrechtliche Schutzpflicht hinsichtlich der informationellen Selbstbestimmung träfe.

II. Nationalstaatliche Schutzpflichten vor internationalen Datenschutzbedrohungen?

Bei der rechtlichen Begründung von Schutzpflichten gilt es aber zu bedenken, dass die Grundrechte primär als Abwehrrechte gegenüber dem Staat ausgestaltet sind[1]. Die Freiheitsrechte trifft die Aufgabe sicherzustellen, dass der Einzelne in seiner Grundrechtsausübung nicht in ungebührlichem, sprich unverhältnismäßigem Umfang eingeschränkt wird. Nur in Einzelfällen kann darüber hinaus eine weitere Grundrechtsfunktion in Form einer staatlichen Schutzpflicht hergeleitet werden[2]. Die informationelle Selbstbestimmung stellt ihrem Wesen nach ein solches Freiheitsrecht dar. Berücksichtigt man bereits seine Entstehung aus dem sogenannten „Volkszählungsurteil" des Bundesverfassungsgerichts im Jahre 1983 heraus, so wird dies in besonderer Weise deutlich, da es in dem Fall um die zwangsweise Erhebung personenbezogener Daten zur Durchführung einer Volkszählung ging[3]. In gleichem Maße ist der Bürger auch heute betroffen, wenn der Staat durch seine eigenen Behörden zu Zwecken der Aufrechterhaltung der öffentlichen Sicherheit personenbezogene Daten erhebt und automatisiert verarbeitet. Wenn jedoch, wie beim NSA-Skandal geschehen, ausländische Behörden fremder Staaten deutsche Bürger ausspionieren, so stellt sich die Frage, ob in einem solchen Fall über die bloße Abwehrfunktion hinaus, welche hier im Regelfall mangels Tätigwerden nationaler Organe keine grundrechtlichen Gewährleistungen bietet, eine Schutzpflicht des deutschen Staates für das Grundrecht der informationellen Selbstbestimmung begründet werden kann. Ausgangspunkt für die Annahme einer derartigen Schutzpflicht ist die Erkenntnis, dass das einzelne Grundrecht nicht lediglich ein subjektives Abwehrrecht ist, sondern darüber hinaus auch einen objektivrechtlichen Charakter aufweist, welcher dafür sorgt, dass sowohl die Gesetzgebung wie auch die Verwaltung und Rechtsprechung Richtlinien und Impulse von den Grundrechten erhalten. Diese Wertentscheidung beruht auf der sich frei entfaltenden menschlichen Persönlichkeit und der ihr damit zukommenden Würde[4].

Zumindest für den Bereich privater Übergriffe ist das Bestehen gesetzgeberischer Schutzpflichten zur Sicherung des Rechts auf informationelle Selbstbestimmung anerkannt, soweit eine Schutzpflichtlage besteht[5]. Die Annahme einer solchen steht in Abhängigkeit zur Verfassungsinterpretation, insbesondere auch, ob gesetzgeberische Schutzpflichten über Private hinaus auch gegenüber ausländischen Staaten gelten können. Berücksichtigt werden muss dabei, dass der Kern der informationellen Selbstbestimmung darin liegt, eigenständig

1 Klein, NJW 1989, 1633 (1633).

2 Siehe weitergehend zur umfänglichen grundrechtsdogmatischen Herleitung von Schutzpflichten auch Klein, NJW 1989, 1633.

3 Vgl. auch Gola/Schomerus, BDSG, 11. Aufl. 2012, § 1 Rn. 11.

4 BVerfG, Urt. v. 15.1.1958 – 1 BvR 400/57, NJW 1958, 257.

5 Di Fabio, in: Maunz/Dürig, GG, 39. Ergänzungslieferung 2001, Art. 2 Rn. 189.

darüber zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Eine solche freie Entscheidung erfordert auch, dass mit hinreichender Sicherheit überschaubar ist, welche die eigene Person betreffende Informationen in bestimmten Bereichen ihrer sozialen Umwelt bekannt sind. Wer dabei das Wissen anderer Stellen nicht abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt sein, aus eigener Selbstbestimmung heraus zu planen oder eigene Entscheidungen zu treffen[6]. Bereits für die Datenerhebungs- und Datenverarbeitungsmaßnahmen nationaler Behörden im Sicherheitsbereich ist diese hinreichende Transparenz zur Ausübung der informationellen Selbstbestimmung nicht unproblematisch. Wenn sich darüber hinaus ausländische Behörden Zugriff auf personenbezogene Daten Einzelner verschaffen, sind im Regelfall deren Legitimation und die einzelnen Verarbeitungsvorgänge unbekannt und nicht mit den Mitteln des deutschen Rechtsstaats überprüfbar. Auch ist nicht ersichtlich, an welche Stellen oder Länder einmal erhobene Daten weiter übermittelt werden. Im Rahmen der globalen Informationsgesellschaft verflüchtigen sich aufgrund der unbegrenzten Weitergabe- und Replizierungsmöglichkeiten die Grenzen zwischen dem öffentlichen und dem privaten Sektor[7]. Für Datenbestände, die einmal an die Öffentlichkeit gelangt sind, lässt sich nicht mehr bestimmen, welcher weiteren Nutzung durch welche Institutionen sie unterliegen. Daher ist zu fordern, dass sich auch der Schutz der informationellen Selbstbestimmung über rein nationale Grenzen hinweg an die Gefahren der heutigen Informationsgesellschaft anpasst, um den Grundrechtsschutz infolge der vernetzten Globalisierung nicht in den kommenden Jahren erodieren zu lassen[8]. Dies muss umso mehr gelten, je höher der Rang des in Frage stehenden Rechtsgutes innerhalb der Wertordnung des Grundgesetzes anzusetzen ist[9]. Insbesondere für die informationelle Selbstbestimmung gilt hier, dass jetzt und auch in den zukünftigen Jahren immer mehr sensitive personenbezogene Daten in informationstechnische Systeme eingepflegt und unter Umständen auch dezentral über Cloud-Dienste gespeichert werden. Für die eigene Persönlichkeitsentwicklung wird das Grundrecht auf informationelle Selbstbestimmung folglich einen immer größeren Stellenwert besitzen. Somit besteht auch eine diesbezügliche nationalstaatliche Schutzpflicht vor internationalen Datenschutzbedrohungen.

III. Realisierbarkeit der Schutzpflichten durch technische Maßnahmen

Soweit den deutschen Staat eine Schutzpflicht für die informationelle Selbstbestimmung gegenüber den Eingriffsmaßnahmen fremder Staaten trifft, stellt sich die Frage, wie weit eine solche reicht und wo im Zweifelsfall ihre Grenzen zu setzen sind. Bei der Umsetzung von Schutzpflichten, welche einen ausländischen Bezug vorweisen, wird insbesondere der Exekutive ein weites Ermessen zugestanden, da die Gestaltung auswärtiger Verhältnisse und Geschehensabläufe nicht allein von deutschen Interessen abhängig ist, sondern auch vielfach Umstände betrifft, die sich der Gestaltungsmacht eines Einzelstaates entziehen[10]. Wo zu früheren Zeiten in den allermeisten Fällen die Gestaltungsmacht des Einzelstaates durch politische Umstände beschränkt war, könnte es heute, zumindest bezogen auf die Gewährleistung der informationellen Selbstbestimmung, durch technische Mittel möglich sein, staatliche Maßnahmen fremder Mächte abzuwehren. Dies gilt umso mehr, als sich der materielle Inhalt der Schutzpflicht am möglichst effektiven Schutz des jeweiligen Rechtsguts zu orientieren hat[11]. Fraglich ist dabei jedoch, ob es dem Staat tatsächlich möglich ist, die personenbezogenen Daten seiner Bürger vollständig zu schützen, und wichtiger noch, ob er jedwede technische Maßnahme ergreifen muss, die ihm potenziell zur Verfügung steht, oder ob sich nicht vielmehr, ausgehend vom Untermaßverbot, die Schwelle des staatlichen Tätigwerdens am Verhältnismäßigkeitsgrundsatz orientieren muss. Aus der Eigenart der Computertechnik und der damit verbundenen nur begrenzten Kontrollierbarkeit von Datenströmen ergibt sich für die informationelle Selbstbestimmung, dass der Staat nur solche Maßnahmen zu ihrem Schutz zu treffen hat, die nach dem Stand der Technik die wesentlichsten Risiken für die Grundrechtsausübung ausschließen. Es kann jedoch keine Verpflichtung dahingehend bestehen, sämtliche personenbezogenen Daten durch technische Mittel zur Gänze vor dem Zugriff ausländischer Behörden zu schützen, wo sich bereits die Frage der Realisierbarkeit stellt. Unmögliches kann auch im Rahmen staatlicher Schutzpflichtgewährleistungen nicht verlangt werden[12].

Darüber hinaus stellt die Datenausspähung durch andere Staaten, in Anlehnung an die verfassungsrechtlichen Probleme im Umweltrecht (z.B. bei Immissionen und ihren weitergehenden Auswirkungen), aufgrund ihrer oftmals fehlenden Offensichtlichkeit, der Geheimhaltung und den Schwierigkeiten des Einzelnen, eine kausale Betroffenheit nachzuweisen, eine Grundrechtsbeeinträchtigung mit einem diffusen Charakter dar[13]. Soweit bei Schutzmaßnahmen unklar ist, ob und wie sie den Grundrechtsschutz gewährleisten sollen, können sie nicht eingreifen[14]. Auch aus diesem Grunde heraus stellt sich die Frage, wie technische Schutzmaßnahmen im Konkreten auszugestalten wären, um einen effektiven Grundrechtsschutz zu

6 Vgl. BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419 (421).

7 Hoffmann-Riem, AöR 123 (1998), 513 (514).

8 So auch Di Fabio, in: Maunz/Dürig, GG, 39. Ergänzungslieferung 2001, Art. 2 Rn. 190.

9 BVerfG, Urt. v. 25.2.1975 – 1 BvF 1 – 6/74, NJW 1975, 573 (575).

10 BVerfG, Beschl. v. 16.12.1980 – 2 BvR 419/80, NJW 1981, 1499.

11 Vgl. BVerfG, Urt. v. 16.10.1977 – 1 BvQ 5/77, NJW 1977, 2255.

12 So auch Hans-Jürgen Papier im Interview mit der „Welt": „Der Staat hat die grundsätzliche Pflicht, seine Bürger vor Zugriffen ausländischer Mächte zu schützen. Aber der Staat kann nur zu etwas verpflichtet sein, das er rechtlich und tatsächlich auch zu leisten vermag. Wo die Unmöglichkeit anfängt, endet die Schutzpflicht. Das rechtlich und tatsächlich Mögliche und Geeignete muss er aber zum Schutz seiner Bürger auch tun.", in: Gaugele, „Die Welt" vom 05.08.2013, „Die Freiheitsrechte dürfen nicht geopfert werden", abrufbar unter: http://www.welt.de/politik/deutschland/article118684465/Die-Freiheitsrechte-duerfen-nicht-geopfert-werden.html (Stand: 12.03.2014).

13 Vgl. Schmidt-Aßmann, AöR 106 (1981), 205, 216.

14 Vgl. Klein, NJW 1989, 1633 (1638).

gewährleisten. Mangels genauer Kenntnis der Bedrohungslage und eines verhältnismäßig schlechten Informationsstandes seitens der parlamentarischen Öffentlichkeit kann es zum jetzigen Zeitpunkt keine Antwort auf diese Frage geben. Auch wenn grundsätzlich eine nationale Schutzpflicht vor internationalen Datenschutzbedrohungen besteht, so scheitert diese in ihrer Umsetzung – zumindest vorerst – letztlich an ihrer eigenen technischen Realisierbarkeit.

IV. Realisierbarkeit der Schutzpflichten durch Internationale Datenschutzabkommen

Dennoch stellt sich für den Schutz des Bürgers vor globalen Datenschutzbedrohungen die Frage, inwieweit, um zumindest teilweise der begründeten staatlichen Schutzpflicht nachzukommen, politische Regelungen geschaffen werden können, die einer Ausspähung durch ausländische Behörden entgegenwirken. In erster Linie ist hier an Instrumentarien des Völkerrechts zu denken, insbesondere auch an bilaterale Abkommen zwischen den „Big Players", also jenen Staaten, zwischen denen die höchste Transferdichte von Computerdaten vorherrscht. Auch mit Blick auf die technische Entwicklung könnten solche Regelungsansätze die einzige Lösungsmöglichkeit sein, um dafür Sorge zu tragen, dass die zwar national und somit lediglich für nationale Behörden gewährleisteten Datenschutzregelungen nicht auf Dauer durch ausländische Behörden unterminiert werden.

1. Safe Harbor-Abkommen

So schlossen die USA und die EU im Jahr 2000 das so genannte Safe Harbor-Abkommen[15] zur Regelung datenschutzrechtlicher Fragen. Im Safe Harbor-Abkommen werden durch das US-Handelsministerium in Zusammenarbeit mit der EU-Kommission entwickelte Grundsätze[16] festgehalten, die Vorgaben zur Verarbeitung erhobener Daten, zur Datensicherheit sowie zu durch den Datenverarbeiter zu beachtende Betroffenenrechte enthalten, denen sich Unternehmen freiwillig unterwerfen können. Mit diesem freiwilligen Beitritt entsteht eine rechtliche Bindung des Unternehmens, den Prinzipien auch tatsächlich zu genügen. Die Durchsetzung ist dem US-Handelsministerium, der Federal Trade Commission, übertragen. In der Folge eines Beitritts wird der Datentransfer von der EU in die USA gestattet. Hintergrund des Abkommens ist, dass ein Datentransfer in Drittstaaten wie die USA nach EU-Recht zu unterbleiben hat, wenn in diesem Drittland kein angemessenes Datenschutzniveau gewährleistet ist[17], und ein solches Datenschutzniveau hinsichtlich der USA von Seiten der EU bisher nicht festgestellt wurde. Das Safe Harbor-Abkommen soll den praktisch sehr wichtigen Datenexport in die USA erleichtern und einen dem Kriterium des angemessenen Datenschutzniveaus entsprechenden Zustand herstellen. Damit aber dient das Safe Harbor-Abkommen gerade nicht primär dem Ziel, der Ausspähung durch ausländische Staaten entgegenzuwirken, sondern vielmehr einen Datentransfer über staatliche Grenzen hinweg überhaupt erst zu ermöglichen. Seinen Schutzpflichten gegenüber seiner Bürger kommt der Staat durch das Safe Harbor-Abkommen mithin schon aufgrund der Zwecksetzung des Abkommens nicht nach.

2. Abkommen Internationaler Organisationen

Neben dem Safe Harbor-Abkommen, das lediglich für die USA und die EU Wirkung entfaltet, bestehen verschiedene Datenschutzabkommen Internationaler Organisationen.

Als international prägend haben sich insbesondere die bereits 1980 erlassenen „Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten" der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) erwiesen, die zu einer gewissen internationalen Einigkeit in den allgemeinen Grundsätzen des Datenschutzes führen konnten. Sie richten sich sowohl an den öffentlichen als auch an den nicht-öffentlichen Bereich und enthalten Verarbeitungsgrundsätze, bestimmen Betroffenenrechte und appellieren an die Mitgliedsstaaten, den freien grenzüberschreitenden Datentransfer zu gewährleisten. Aufgrund der Fortentwicklung der Technik wurde 2013 ihre Überarbeitung vorgenommen. Die Leitlinien entfalten jedoch lediglich unverbindliche Wirkung gegenüber den Mitgliedsstaaten und stellen ihnen ihre Umsetzung frei[18]. Weiterhin sind sie zu allgemein gehalten, um auf konkrete Gefahren stets adäquate Antworten zu finden.

Auch die Vereinten Nationen (UN) haben sich im Bereich des Datenschutzes bereits engagiert und 1990 die „Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien" verabschiedet. Ebenso wie die Leitlinien der OECD gelten die UN-Richtlinien für den öffentlichen und nicht-öffentlichen Bereich und entfalten lediglich Empfehlungswirkung. Verglichen mit den Datenschutzleitlinien der OECD haben sie nur äußerst geringe praktische Bedeutung und können zu einem effektiven Betroffenenschutz nur unzureichend beitragen.

Von praktischer Relevanz ist neben den Leitlinien der OECD die Europäische Datenschutzkonvention des Europarats aus dem Jahr 1981, die insbesondere allgemeine Datenschutzgrundsätze und Bestimmungen zum grenzüberschreitenden Datenverkehr und zur gegenseitigen Hilfeleistung der Vertragsparteien bei der Durchführung des Abkommens enthält. Sie wurde 2001 durch das „Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr", das sogenannte Zusatzprotokoll, ergänzt, das die Zulässigkeit einer Datenübermittlung in einen Nicht-Vertragsstaat an

15 Vgl. Europäische Kommission, Entscheidung der Kommission gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (2000/520/EG) vom 25.08.2000.

16 Abrufbar unter: http://export.gov/safeharbor/eu/eg_main_018475.asp (Stand: 12.03.2014).

17 Vgl. Art. 25 Abs. 1 DSRL 95/46/EG.

18 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, (München) 2012, S. 71.

die Feststellung eines angemessenen Datenschutzniveaus knüpft[19]. Bei der Datenschutzkonvention handelt es sich um das erste gegenüber den Vertragsstaaten verbindliche internationale Datenschutzabkommen; auch durch diese Bindungswirkung hat sie das Datenschutzrecht insbesondere in Europa stark geprägt[20]. Jedoch stammt die Datenschutzkonvention aus einer Zeit vor der allgemeinen Verbreitung des Internets, so dass derzeit ebenfalls an einer Novellierung gearbeitet wird.

Vereinzelt wird zwar von verschiedenen Autoren[21] und zuletzt auch dem Europarat selbst[22] eine Eignung der Datenschutzkonvention des Europarates als Grundlage für globale Datenschutzregeln erwogen; jedoch ist insofern bereits zu beachten, dass die USA als wohl entscheidender Staat für ein durchsetzungsstarkes internationales Datenschutzabkommen nicht zu den Vertragsstaaten der Datenschutzkonvention gehören. Auch wenn eine Teilnahme als Nicht-Mitgliedsstaat des Europarates grundsätzlich möglich ist, wird eine solche Entwicklung bezüglich der USA nicht in nächster Zeit zu erwarten sein, da diese nicht das notwendige Datenschutzniveau aufweisen, das für eine Teilnahme vorausgesetzt wird[23]. Damit aber kann den Gefahren, die sich insbesondere in der PRISM-Affäre offenbart haben, auch nicht durch die Datenschutzkonvention des Europarates zufriedenstellend begegnet werden.

V. Fazit

Es wurde gezeigt, dass sich durchaus staatliche Pflichten zur Wahrung der Integrität der informationellen Selbstbestimmung des einzelnen Bürgers aus dem Schutzpflichtcharakter der Grundrechte herleiten lassen. In Betracht kommen als Realisierungswerkzeuge insbesondere technische Maßnahmen wie auch internationale Datenschutzabkommen. Diese Mittel erweisen sich in der Praxis jedoch derzeit als nicht realisierbar, was auch auf die unzureichende staatliche Aufklärungsarbeit und fehlende Transparenz gegenüber der parlamentarischen Öffentlichkeit im Falle von sicherheitsbehördlichen Eingriffen in die informationellen Grundrechte zurückzuführen ist. Zu berücksichtigen ist dabei aber, wie eingangs bereits erwähnt, auch, dass dem deutschen Staat bei der Umsetzung von Schutzpflichten, die einen Auslandsbezug aufweisen, ein weites Ermessen zugestanden wird, da die Gestaltung auswärtiger Verhältnisse und Geschehensabläufe nicht allein von deutschen Interessen abhängig ist, sondern vielfach Umstände betrifft, die sich der Gestaltungsmacht eines Einzelstaates entziehen.[24]

Darüber hinaus kommt internationalen Datenschutzabkommen nur eine begrenzte praktische Bedeutung zu. Sie sind alle vor der Verbreitung des Internets entstanden, was u.a. dazu geführt hat, dass die Regelungen des Europarats und der OECD momentan überarbeitet werden bzw. wurden. Jedoch wird auch eine solche Überarbeitung nichts an ihrem politischen Kompromisscharakter und der daraus folgenden Beschränkung auf allgemeine datenschutzrechtliche Grundsätze ändern können, so dass die bestehenden Abkommen auf internationaler Ebene keinen ausreichenden Schutz der Bürger garantieren. Auch die Entwicklung eines neuen Datenschutzabkommens auf internationaler Ebene oder gegebenenfalls bilateral mit den USA, das nicht die Schwächen der bestehenden internationalen Datenschutzabkommen aufwiese und u.U. verbindlicher Natur wäre, scheint auf nationaler Ebene politisch derzeit kaum durchsetzbar und damit nur schwer erreichbar[25]*. Zwar plant die EU als Folge des NSA-Skandals im vergangenen Jahr, bis Mitte 2014 ein Datenschutz-Rahmenabkommen mit den USA in den Bereichen Polizei und Justiz umzusetzen, ob ihr dies aber gelingt, erscheint, unter der Prämisse des alten Grundsatzes von Spinoza „Jeder hat nur soviel Recht, wie er auch Macht hat" fraglich.*

Die praktische Erreichbarkeit eines ausreichenden Schutzes der Bürger vor Ausspähung durch ausländische Stellen im Wege internationaler Datenschutzabkommen ist damit momentan bedauerlicherweise zu verneinen. Dennoch bleibt zu hoffen, dass sich in der Zukunft neue Wege der Kooperation auf überstaatlicher Ebene finden, um auf die Gefahren, die sich insbesondere infolge des Internets für den Datenschutz auftun, sachgerecht reagieren zu können.

Dennis-Kenji Kipker
Seit 2012 Wissenschaftlicher Mitarbeiter und Doktorand am Institut für Informations-, Gesundheits- und Medizinrecht an der rechtswissenschaftlichen Fakultät der Universität Bremen mit den Forschungsschwerpunkten Polizei- und Nachrichtendienstrecht, Informationsrecht und Medizininformationsrecht.

Friederike Voskamp
Seit 2012 Wissenschaftliche Mitarbeiterin und Doktorandin am Institut für Informations-, Gesundheits- und Medizinrecht an der rechtswissenschaftlichen Fakultät der Universität Bremen mit den Forschungsschwerpunkten internationales Datenschutz- und IT-Recht.

19 Vgl. Art. 2 Abs. 1 des Zusatzprotokolls.

20 Greenleaf, International Data Privacy Law 2012 (Vol. 2, Issue 2), 7.

21 Greenleaf, The Influence of European Data Privacy Standards outside Europe, S. 31; Bygrave, Scandinavian Studies of Law 2010, 165 (181); Greenleaf/Clarke/Water, UNSW Law Research Paper 2013-62, 3.

22 Europarat, Council of Europe points to the Data Protection Convention as global standard, Ref. DC 113 (2011), abrufbar unter: http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp (Stand: 12.03.2014).

23 Vgl. Ermert, Europarat will Datenschutzkonvention zum globalen Minimalstandard machen, abrufbar unter: http://www.heise.de/newsticker/meldung/Europarat-will-Datenschutzkonvention-zum-globalen-Minimialstandard-machen-1389776.html (Stand: 27.02.2014).

24 BVerfG, Beschl. v. 16.12.1980 – 2 BvR 419/80, NJW 1981, 1499.

25 Vgl. Kuner, Computer Law & Security Review 2009, 307 (310).

Kurzbeiträge

Aus den aktuellen Berichten der Aufsichtsbehörden (12)

Zusammengestellt und kommentiert von Prof. Peter Gola, Königswinter*

Beschäftigtendatenschutz

Alkoholtest am Arbeitsplatz

Ein Unternehmen mag Anlass haben, durch ein Alkoholverbot jeglichem Alkoholmissbrauch am Arbeitsplatz vorzubeugen, wobei dem Arbeitnehmer auch ohne ausdrückliches Verbot klar sein muss, dass jeder Alkoholgenuss, der seine Arbeitsfähigkeit beeinträchtigt, pflichtwidrig ist. Insofern kann auch ein Interesse des Arbeitgebers nicht verneint werden, Verstöße gegen das Alkoholverbot beweiskräftig festzustellen. Zutreffend weist der LfD Baden Württemberg (31. TB, 2012/2013, Ziff. 9.1) unter Bezugnahme auf die Rechtsprechung des BAG darauf hin, dass Arbeitnehmer wegen ihres verfassungsmäßigen garantierten Grundrechts auf körperliche Integrität vom Arbeitgeber weder zu einer Untersuchung ihres Blutalkoholwertes noch zur Mitwirkung an einer Atemalkoholanalyse gezwungen werden können. Zulässig wäre der Test nur, falls der Betroffene einwilligt (BAG vom 26.01.1995 – 2 AZR 649/94 –), was er freiwillig wohl nur tun würde, falls er annimmt, damit die Unbegründetheit des Verdachts beweisen zu können.

Auch bei Abgabe einer unbefristeten, bindenden und damit nicht widerrufbaren arbeitsvertraglichen Zustimmung, im konkreten Verdachtsfall an einer Atemalkoholanalyse teilzunehmen, kann die Freiwilligkeit der Einwilligung des Mitarbeiters zu dem Zeitpunkt, an dem die Untersuchung tatsächlich stattfinden soll, in Frage stehen. Um dem Arbeitnehmer Gelegenheit zu geben, den Verdacht einer Alkoholisierung auszuräumen, sollte der Arbeitgeber die Möglichkeit der freiwilligen Mitwirkung an objektiven Tests (z.B. mittels „Alkomat“ oder einer von einem Arzt entnommenen Blutprobe) anbieten. Verpflichtet ist er hierzu, wenn der Arbeitnehmer den Test verlangt (BAG vom 16.09.1999 – 2 AZR 123/99 –)

Urlaubsanträge nur mit Begründung?

Das BUrlG trifft keine Regelung, dass ein Arbeitnehmer bei der Beantragung von Urlaub auch Angaben zu den Gründen oder zu der Gestaltung des Urlaubs zu machen habe. Will der Arbeitgeber gleichwohl solchen Angaben erheben, so hängt es von den konkreten Gegebenheiten ab, ob diese zusätzliche Information für die Durchführung des Arbeitsverhältnisses objektiv erforderlich ist (§ 32 Abs. 1 S. 1 BDSG).

Dies kann sich nach dem Sächsischen Landesbeauftragten (6. TB Datenschutz im nicht öffentl. Bereich, 2011/3, 2013, Ziff. 8.3.1) aus mehren Gründen ergeben. Und zwar u.a., wenn mehrere Urlaubsanträge für den gleichen Zeitraum vorliegen, aber aus betrieblichen Gründen nicht alle genehmigt werden können. Auch wenn der Arbeitnehmer von der gesetzlichen Regel, den Urlaub in der Weise zeitlich zusammenhängend zu nehmen (§ 7 Abs. 2 BUrlG), damit der mit dem Urlaub verfolgte Erholungszweck gewährleistet ist, abweicht und wiederholt Kurzurlaube beantragt, kann ein Grund bestehen, Angaben zur Verwendung des Urlaubs zu verlangen. Andererseits bedeutet das, dass der der Arbeitgeber nicht befugt wäre, z.B. pauschal in Urlaubsantragsformularen die Urlaubsverwendung abzufragen. Dem stände das Recht des Arbeitnehmers, seine Freizeit frei gestalten zu dürfen, sowie sein Recht auf Privatsphäre bzw. informationelle Selbstbestimmung entgegen.

Fingerabdruck zur Identifizierung bei Gleitzeiterfassung

Bedenken meldet der Sächsische LfD (6. TB für den nicht öffentl. Bereich, 2011/3, 2013 Ziff. 8.3.2) gegenüber dem zunehmenden Einsatz von fingerabdruckbasierten Zeiterfassungssystemen an

Angesichts der besonderen Sensibilität solcher körperbezogenen Daten sei eine Nutzung für Zwecke der Zutrittskontrolle aus Verhältnismäßigkeitsgründen auf besondere Ausnahmefälle zu beschränken. Dazu gehörten in erster Linie Anwendungsfälle mit besonderen Sicherheitsanforderungen. Hier sollten dann vorzugweise besonders datenschutzfreundliche Verfahren zum Einsatz kommen, bei denen etwa beim Arbeitgeber selbst keine Daten gespeichert werden, weil die Fingerabdrücke stattdessen ausschließlich auf einem im Besitz des Betroffenen befindlichen und unter seiner Kontrolle stehenden Chip gespeichert sind und die Authentifizierung durch Vergleich des tatsächlichen biometrischen Musters mit dem gespeicherten Muster direkt auf der Karte (Comparison on Card) erfolgt.

Die Erforderlichkeit biometrischer Systeme wird in jedem Falle zutreffend verneint bei dem bloßen Zweck der Zeiterfassung;, zumal dafür wesentlich weniger in das Persönlichkeitsrecht der Arbeitnehmer eingreifende Verfahren zur Verfügung stehen. Der LfD verweist auch auf Literaturstimmen, nach denen eine Erforderlichkeit dann nicht besteht, wenn von mehreren gleichermaßen wirksamen Maßnahmen die den Arbeitnehmer stärker belastende gewählt wird (vgl. Gola/Schomerus, BDSG, 11 Aufl., Rdn. 12 zu § 32; Seifert in Simitis (Hrsg.), BDSG, 7 Aufl., Rdn. 97 zu § 32). Auch nach Däubler in Däubler/Klebe /Wedde/Weichert, BDSG, 3. Aufl. § 32 Rdn. 86) könne der Zweck „Erfassung der Arbeitszeit“ keinen so weitreichenden Eingriff gestatten.

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

Führerscheinprüfung durch externe Dienstleister

§ 21 Abs. 1 Nr. 2 StVG verpflichtet den Arbeitgeber, wenn Arbeitnehmer Firmenfahrzeuge nutzen dürfen bzw. müssen, sich der gültigen Fahrerlaubnis des Fahrers zu vergewissern. Erforderlich ist auch eine in Zeitabständen erfolgende Nachprüfung, für die – sofern kein besonderer Anlass vorliegt – nach dem datenschutzrechtlichen Erforderlichkeitsgrundsatz der Quartalszeitraum genügt. Der LfD Sachsen, (6. TB für den nichtöffentlichen Bereich, 2011/3, 2013, Ziff 8.3.3) hatte zu beurteilen, unter welchen Gegebenheiten der Arbeitgeber die Kontrolle einem externen Dienstleister übertragen könne. Die Kontrolle durch den Dienstleister erfolgte unter Einschaltung eines bundesweit tätigen Tankstellenunternehmens, das den mit einem Barcode versehenen Führerschein scannt und dem Dienstleister zuleitet. Die individuelle Aufforderung zur Führerscheinvorlage erfolgt über eine im System des Dienstleisters gespeicherte Rufnummer bzw. E-Mail-Adresse.

Dazu hält der LfD zunächst fest, dass insoweit das Verlangen nach einer privaten Rufnummer oder E-Mail-Adresse nicht gerechtfertigt sei. Die Kontrolle selbst ist aber im Rahmen der Durchführung des Beschäftigungsverhältnisses erforderlich bzw. geboten. Keine Bedenken bestehen, wenn die betriebliche Rufnummer und andere notwendige betriebsbezogene Daten im Rahmen eines Vertrages nach § 11 BDSG durch den Dienstleister verarbeitet werden und in den Vertrag auch der Kooperationspartner, der die Sichtprüfung vornimmt, wirksam einbezogen ist.

Arbeitgeberauskünfte und Referenzen

Keine neue Erkenntnis ist es, dass ein Arbeitgeber Auskünfte über einen Bewerber bei dessen früheren oder derzeitigen Arbeitgeber nur mit Zustimmung des Betroffenen einholen darf. Erstrecken dürfen sich die Auskünfte nur auf Angaben, die für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich sind. Gleiches gilt für die Befragung von Referenzpersonen, wobei in deren selbstverständlich freiwilligen Benennung durch den Bewerber eine konkludente Zustimmung in die Einholung entsprechender Auskünfte liegen kann (LfD Baden-Württemberg, 31. TB, 2012/2013, Ziff. 9.2). Die Auskunft macht nur Sinn, wenn sie die Angaben im Zeugnis des Bewerbers insbesondere um aktuelle Angaben ergänzt, die nach dem Zeugnisrecht nicht vermerkt werden dürfen.

Due-Diligence-Prüfung

Die Zulässigkeit der Übermittlung von Beschäftigtendaten an einen potentiellen Unternehmenskäufer beschäftigten die Aufsichtsbehörden immer wieder (vgl. Bericht 7, RDV 3/2013, S. 140). Datenschutzrechtliche Fragen tauchen nicht auf, wenn Angaben zu Geschlecht, Qualifikation, Bezahlung, Altersstruktur, Dauer der Betriebszugehörigkeit oder zum Krankenstand anonymisiert und aggregiert erfolgen. Anders ist es, wenn – was auch der Fall sein kann, wenn die Angaben pseudonymisiert erfolgen – Einzelpersonen, z.B. aus der Funktionsbezeichnung (Prokurist; Leiter Forschungsabteilung etc.), identifiziert werden können. Hier ist § 28 Abs. 1 S. 1 Nr. 2 bzw. Abs. 2 Nr. 2a BDSG als Rechtfertigungsnorm zu prüfen und zumindest bei für das Unternehmen wichtigen Personen zu bejahen. Einer Übermittlung besonderer Arten personenbezogener Daten, wie z.B. Angaben über Krankheitszeiten, würde jedoch durch die insoweit maßgebende Zulässigkeitsnorm des § 28 Abs. 6 Nr. 3 und Abs. 7 S. 1 BDSG nicht gerechtfertigt (LfD Sachsen, 6. TB Datenschutz im nicht öffentl. Bereich, 2011/3, 2013, 8.3.6.).

Eine Auskunft zu viel

Unbefugt erfolgte dagegen eine Auskunft, die ein Arbeitgeber einem besorgten Vater erteilte. Dieser wollte erfahren, warum der Arbeitgeber das Ausbildungsverhältnis der Tochter beendet habe. Der Arbeitgeber korrigierte – wohl zur Überraschung des Vaters – den Sachverhalt und teilte mit, dass die Kündigung von der Tochter selbst ausgesprochen worden sei (LfD Sachsen-Anhalt, 11. TB, 4, 2011/3, 2013, Ziff. 11.4), worüber sich die Tochter bei dem LfD beschwerte.

Der betriebliche Datenschutzbeauftragte

Der DSB geht als letzter

Im Falle der Insolvenz eines Unternehmens erlischt die Pflicht des Unternehmens zur Bestellung eines Datenschutzbeauftragten erst dann, wenn – nach Abschluss des Insolvenzverfahrens – der Betrieb eingestellt wird bzw. im Rahmen der Abwicklung des Unternehmens die Mitarbeiterzahl i.S.d. § 4f Abs. 1 BDSG unter die gesetzlich Bestellgrenze fällt (LfD Baden Württemberg, 31. TB, 2012/2013, Ziff. 10.1). Mit Wegfall der Bestellpflicht verliert der DSB sein Amt. Ein Widerruf der Bestellung erübrigt sich. Der Eintritt der Insolvenz ist jedoch kein wichtiger Grund, der zum Widerruf oder zur Kündigung berechtigt. Ggf. geht der DSB somit als letzter.

Auch die andere Seite kann es treffen

Geht ein externer betrieblicher Datenschutzbeauftragter in Konkurs, so muss nach Auffassung des LfD Sachsen (6. TB für den nicht-öffentl. Bereich, 2011/3, 2013, Ziff 8.13.4) der Insolvenzverwalter die Daten, die der Datenschutzbeauftragte in Wahrnehmung seiner Aufgabe erhalten hatte, aus der Insolvenzmasse aussondern (§§ 667, 1. Alt., 675 BGB i.V.m. § 47 InsO) und (nach Anbieten) auf Verlangen den Auftraggebern herausgeben. Keine Aussage trifft er dazu, ob mit der Eröffnung der Insolvenz die Bestellung als Datenschutzbeauftragter endet.

Unwirksame Bestellung eines Mitinhabers und Finanzleiters

Die gesetzlich geforderte Zuverlässigkeit des betrieblichen Datenschutzbeauftragten (§ 4f Abs. 2 S. 1 BDSG) ist in Frage gestellt, wenn der Finanzleiter eines Unternehmens, an dem er gleichzeitig als Mitgesellschafter beteiligt ist, zum Datenschutzbeauftragten bestellt wird. Es muss die nahe liegende Gefahr ausgeschlossen werden, dass von dem Betroffenen – auch im höchsteigenen Interesse – zu berücksichtigende Finanzinteressen des Unternehmens der Wahrnehmung der unabhängigen Rolle des DSB entgegenstehen (vgl. LfD

Sachsen, 6. TB für den nicht öffentl. Bereich 2011/3/2013, Ziff. 8.13.3).

DSB bei Arztpraxen

Der LfD Baden-Württemberg (31. TB, 2012/2013, Ziff. 7.10) hält fest, dass in Arztpraxen die Bestellpflicht für einen DSB regelmäßig erst bei Überschreiten der in § 4 f Abs. 1 BDSG genannten Zahl der bei der Verarbeitung personenbezogener Daten Beschäftigten eintritt. Auch wenn es hier vornehmlich um die Verarbeitung von Patienten- und Gesundheitsdaten, also um besonders sensible Daten i.S.d. § 3 Abs. 9 BDSG, gehe, bestehe nicht die ansonsten eine Bestellpflicht auslösende Pflicht zur Vorabkontrolle nach § 4d Abs. 5 BDSG, da im Regelfall ein Behandlungsvertrag nach § 630a BGB vorliege, d.h. die Erhebung und Verarbeitung zur Durchführung eines Rechtsgeschäftes bzw. teilweise sogar auf Grund einer Einwilligung des Patienten erfolge. Somit obliegt in kleineren Praxen die Erfüllung der BDSG-Pflichten dem Praxisinhaber selbst (§ 4g Abs. 2a BDSG).

Die Position des EU-Parlaments zur zukünftigen Rolle von Datenschutzbeauftragten – ein kommentierter Überblick

RA Christoph Klug, Köln*

Nach seinem ursprünglichen Zeitplan um einige Monate verspätet hat der LIBE-Ausschuss[1] des Europäischen Parlaments am 21.10.2013 mit breiter Mehrheit[2] einen Kompromisstext zur geplanten EU-Datenschutz-Grundverordnung (EU-DS-GVO) verabschiedet, der am 12.03.2014 durch ein deutliches Votum[2a] des EU-Parlaments bestätigt worden ist. Das EU-Parlament hat damit ein offizielles Mandat zur Führung von Verhandlungen mit dem Rat und der Kommission im Rahmen des sog. Trilogs[3]. Basierend auf der bisherigen Parlamentsarbeit[4] stellt der Beitrag wesentliche Neuerungen der nunmehr abgestimmten Position des EU-Parlaments zur Rolle von Datenschutzbeauftragten vor.

I. Bestellungspflicht

1. Zahlenmäßiger Schwellenwert

Sollte hinsichtlich der Bestellung von Datenschutzbeauftragten nach dem ursprünglichen Entwurf der EU-Kommission noch auf die Anzahl der im Unternehmen *Beschäftigten* abgestellt werden, so sah bereits der nachfolgende Berichtsentwurf des parlamentarischen Berichterstatters Jan Philipp Albrecht[5] – offensichtlich mit Blick auf das Risikopotenzial der Datenverarbeitung – stattdessen eine Orientierung an der Anzahl der *Betroffenen* vor. Dieser Orientierung folgend, allerdings unter Zugrundelegung eines erheblich erhöhten Schwellenwerts, wird nach dem nunmehr vorliegenden Kompromisspapier des LIBE-Ausschusses eine Bestellungspflicht von Unternehmen vorgeschlagen, wenn die Datenverarbeitung innerhalb von 12 Monaten mehr als 5000 natürliche Personen betrifft[6].

Dieser neue – von einigen bereits als „zu starr" kritisierte[7] – Ansatz ist jedenfalls insofern bemerkenswert, als sich das EU-Parlament in Kenntnis anderweitiger Tendenzen im EU-Rat[8] immerhin für die explizite Regelung einer *Bestellungspflicht* auf europäischer Ebene ausgesprochen hat. Der Rat hatte demgegenüber zuletzt lediglich eine Art Öffnungsklausel vorgesehen, wonach die Mitgliedstaaten in ihren nationalen Datenschutzvorschriften eine Bestellungspflicht vorsehen können. Im Rahmen der bevorstehenden Verhandlungen dürften die ursprünglichen Zielsetzungen der EU-Kommission zur Harmonisierung und Entbürokratisierung bei gleichzeitiger Verantwortlichkeitsverlagerung in die Unternehmen in Erinnerung gerufen werden. In diesem Zusammenhang hat die Kommission eine europaweite Bestellungspflicht auch als Ausgleich für die Abschaffung der Meldepflicht vorgesehen.

2. Risikoträchtige Kernaktivitäten

In Ergänzung zu dem zahlenmäßigen Schwellenwert sollte bereits nach dem Berichtsentwurf eine Bestellungspflicht – unabhängig von der Unternehmensgröße[9] – auch dann bestehen,

* Der Autor ist Rechtsanwalt in Köln und Repräsentant der Gesellschaft für Datenschutz und Datensicherheit (GDD) in internationalen Angelegenheiten. Er hat die von der EU-Kommission durchgeführten Konsultationen und das bisherige parlamentarische Verfahren zum Erlass der EU-Datenschutz-Grundverordnung aktiv begleitet. Als Vertreter der GDD hat er an den bisherigen Stellungnahmen des europäischen Datenschutz-Dachverbandes CEDPO (www.cedpo.eu) federführend mitgewirkt. Der Beitrag spiegelt seine persönliche Einschätzung der aktuellen Debatte wieder.

1 Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres.

2 51 zu 1 Stimmen bei 3 Enthaltungen.

2a 621 zu 10 Stimmen bei 22 Enthaltungen.

3 Vgl. Gola/Schultz, RDV 2013, 1 (7).

4 Siehe hierzu bereits Klug, RDV 2013, 14; ders., RDV 2013, 75; ders., RDV 2013, 143.

5 Nachfolgend als Berichtsentwurf bezeichnet.

6 Demgegenüber hatte der Berichtsentwurf noch eine Bestellungspflicht bereits bei 500 Betroffenen vorgesehen.

7 Vgl. etwa GDD unter http://www.gdd.de/aktuelles/nachrichten (Meldung vom 23.10.2013).

8 Vgl. Council Doc. 10227/13 vom 31.05.2013 (Ziff. 24).

9 Vgl. Erwägungsgrund 75 des Kompromisstextes.

wenn die *Kernaktivitäten* des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters aus der Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 Abs. 1 der Verordnung bestehen. Diese Vorschrift hat das EU-Parlament in Art. 35 Abs. 1 (d) des Kompromisstextes dahingehend erweitert, dass eine Bestellungspflicht auch dann bestehen soll, wenn die Kernaktivitäten die Verarbeitung von *Standortdaten*, Daten von *Kindern oder Beschäftigten* in groß angelegten Dateisystemen betreffen. Insbesondere hinsichtlich des insoweit maßgeblichen Verarbeitungsumfangs bedarf es jedenfalls noch der Konkretisierung, um die gewünschte Rechtssicherheit zu gewährleisten. In diesem Zusammenhang ist auf eine parlamentarische Ergänzung in Erwägungsgrund 75 hinzuweisen, die darauf schließen lässt, dass archivierte Daten, die bestimmten Verwendungsrestriktionen unterliegen, offenbar unberücksichtigt bleiben sollen[10].

3. Bestellungsoptionen

a) Interne und externe Datenschutzbeauftragte

Anzumerken ist, dass auch der Kompromisstext des EU-Parlaments den Unternehmen einige Flexibilität bei der Bestellung von Datenschutzbeauftragten zubilligt. Die Bestellung von internen Datenschutzbeauftragten soll ebenso möglich sein wie die Beauftragung externer Dienstleister. Der entsprechende Vorschlag der EU-Kommission zu Art. 35 Abs. 8 ist insofern unangetastet geblieben[11].

b) Voll- und Teilzeit-Datenschutzbeauftragte

Die internen Datenschutzbeauftragten können ihren Aufgaben nach der Vorstellung von EU-Kommission und EU-Parlament in Voll- oder Teilzeit nachgehen, was durch Einfügungen des Parlaments in den Erwägungsgrund 75 und 75a nochmals verdeutlicht wird. Soll ein Beschäftigter die Funktion als Datenschutzbeauftragter nur in Teilzeit wahrnehmen, gilt es allerdings nach Art. 35 Abs. 6 Interessenskonflikte zu vermeiden.

c) Hauptverantwortliche Datenschutzbeauftragte in Unternehmensgruppen

Begrüßenswert ist die vom EU-Parlament vorgesehene Klarstellung der Möglichkeit der Bestellung von hauptverantwortlichen Datenschutzbeauftragten in Unternehmensgruppen. Insofern ist anzumerken, dass der Kompromisstext in Ergänzung des Kommissionsentwurfs ausdrücklich eine *einfache Erreichbarkeit* des hauptverantwortlichen Datenschutzbeauftragten fordert, ohne allerdings weitere Konkretisierungen (beispielsweise hinsichtlich der Zurverfügungstellung von Hilfspersonal oder der Überwindung von Sprachbarrieren) vorzunehmen. Grundvoraussetzung für die Bestellung von hauptverantwortlichen Datenschutzbeauftragten muss freilich auch deren Qualifikation nach Art. 35 Abs. 5 sein. Wesentliches Kriterium für die Qualifikation des Datenschutzbeauftragten ist im Fall ihrer Anwendbarkeit auch eine profunde Kenntnis der EU-DS-GVO. Die vorgenannten Gesichtspunkte lassen unter Umständen insbesondere die Bestellung von in entlegenen Drittländern ansässigen Haupt-Datenschutzbeauftragten als nicht unproblematisch erscheinen, zumal auch in solchen Fällen die Anforderungen der Art. 35 bis 37 zumindest eine Ausstrahlungswirkung entfalten dürften.

d) Bestellungsdauer

Des Weiteren wurde vom EU-Parlament erkannt, dass die noch im Berichtsentwurf vorgesehene Mindestbestelldauer für interne Datenschutzbeauftragte von 2 Jahren mit Blick auf die Gewährleistung einer effektiven betrieblichen Datenschutzpraxis und die Unabhängigkeit der Datenschutzbeauftragten zu kurz bemessen wäre. Vorgesehen ist nunmehr eine Mindestbestelldauer von 4 Jahren für interne und 2 Jahren für externe[12] Datenschutzbeauftragte (Art. 35 Abs. 7).

II. Rechtsstellung

1. Unabhängigkeit

a) Unmittelbares Vortragsrecht des Datenschutzbeauftragten

Begrüßenswert ist, dass das EU-Parlament die Notwendigkeit einer unabhängigen Aufgabenwahrnehmung durch die Datenschutzbeauftragten sowohl durch Ergänzungen in Erwägungsgrund 75 als auch im Text von Art. 36 anerkennt und betont.

Durch Einfügung von Satz 2 in Art. 36 Abs. 2 trägt das EU-Parlament der Forderung nach einer direkten Berichtslinie zur obersten Geschäftsleitung Rechnung, was für die Unabhängigkeit des Datenschutzbeauftragten und seine Akzeptanz im Unternehmen essentiell wichtig ist. Es wird jedoch darauf zu achten sein, dass die unmittelbare Anbindung an die oberste Geschäftsleitung nicht durch eine Fehlinterpretation des ebenfalls neu eingefügten Folgesatzes (Art. 36 Abs. 2 Satz 3) konterkariert werden kann; dieser hat folgenden Wortlaut:

„The controller or processor shall for this purpose designate an executive management member who shall be responsible for the compliance with the provisions of this Regulation."

Vorgesehen ist demnach die Benennung eines Mitglieds der obersten Geschäftsleitung (Vorstands- oder Geschäftsführungsmitglied). Es sollte jedoch nochmals klargestellt werden, dass eine Delegation dieser Verantwortlichkeit auf Ebenen unterhalb der obersten Geschäftsleitung – z.B. auf den Compliance-Beauftragten – ausgeschlossen ist. Hierfür spricht nicht nur der Wortlaut von Art. 36 Abs. 2 Satz 3 des Parlamentsvorschlags[13]; aus gutem Grund stellt das EU-Parlament auch durch eine Ergänzung in Erwägungsgrund 75 die datenschutzrechtliche Letztverantwortlichkeit der Unternehmensleitung klar.

10 Gemeint sein könnten hier z.B. gesperrte Daten, die lediglich aufgrund von Aufbewahrungsvorschriften oder nach § 31 BDSG vorgehalten werden.

11 Zur Flexibilität vgl. auch die Rede der Vizepräsidentin der EU-Kommission, Viviane Reding, vom 08.03.2013, abrufbar unter http://europa.eu/rapid/press-release_SPEECH-13-209_en.htm.

12 Ähnlich zum externen Datenschutzbeauftragten 14. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich zuständigen Aufsichtsbehörde an den Landtag des Landes Brandenburg (LT-Drucksache 4/6537), Ziff. 3.1.4.

13 … „for this purpose" … „an executive management member" … .

b) Unterstützungspflicht der Daten verarbeitenden Stellen

Gegenüber dem Kommissionsentwurf stellt der Kompromisstext des EU-Parlaments nochmals klar, dass dem Datenschutzbeauftragten *alle zur* ordnungsgemäßen Aufgabenerfüllung notwendigen Mittel zur Verfügung zu stellen sind. Eine weitere Einfügung des EU-Parlaments in Art. 36 Abs. 3, die mit der Einfügung eines neuen Erwägungsgrundes 75a korrespondiert, verdeutlicht, dass Unternehmen und Behörden gehalten sein sollen, ihren Datenschutzbeauftragten die zur Pflege der Fachkunde erforderlichen Fortbildungsmaßnahmen zu ermöglichen, was angesichts der Dynamik im Bereich des Datenschutzes als sinnvoll erscheint.

c) Verschwiegenheitspflicht des Datenschutzbeauftragten

Zu befürworten ist ferner die vom EU-Parlament in Art. 36 Abs. 4 vorgesehene Einführung einer grundsätzlichen Verschwiegenheitspflicht von Datenschutzbeauftragten bezüglich der Identität von Betroffenen bzw. in Bezug auf Umstände, die den Betroffenen identifizierbar machen. Die Unabhängigkeit des Datenschutzbeauftragten wird hierdurch gefördert, da er das Recht und zugleich die Pflicht hat, in bestimmten Fällen – auch gegenüber der Leitung der verantwortlichen Stelle – Stillschweigen zu bewahren.

d) Kündigungsschutz

Nach bereits in dem Berichtsentwurf geäußerter Auffassung hat die Erfahrung gezeigt, dass eine unabhängige Aufgabenwahrnehmung durch den Datenschutzbeauftragten einen Kündigungsschutz erfordert. Insofern wird in dem Kompromisstext des EU-Parlaments im Rahmen einer Ergänzung von Erwägungsgrund 75 ein besonderer Kündigungsschutz für Datenschutzbeauftragte befürwortet. Die Formulierung der vom EU-Parlament ergänzten Passage legt dabei einen Kündigungsschutz unabhängig von der gewählten Bestellungsoption[14] nahe[15].

III. Qualifikation des Datenschutzbeauftragten

Durch die Einfügung eines neuen Erwägungsgrundes 75a beschreibt das EU-Parlament dezidiert Mindestanforderungen an die Qualifikation von Datenschutzbeauftragten. Hierzu gehören demnach:

Umfangreiche Kenntnisse des Datenschutzrechts und seiner Anwendung, einschließlich der technischen und organisatorischen Maßnahmen und Verfahren; die Beherrschung der technischen Anforderungen zur Realisierung von Privacy by Design, Privacy by Default und zur Gewährleistung der Datensicherheit; branchenspezifische Kenntnisse unter Berücksichtigung der Unternehmensgröße und der Sensibilität der zu verarbeitenden Daten; die Fähigkeit zur Durchführung von Kontrollen, Konsultationen, Dokumentationen und Protokolldateianalysen und die Fähigkeit zur Zusammenarbeit mit der Arbeitnehmervertretung[16].

Das EU-Parlament schlägt somit freilich einen relativ hohen europaweiten Mindeststandard[17] vor. Zu erwägen wäre eine klarere Differenzierung zwischen den Grundkenntnissen, die jeder Datenschutzbeauftragte haben sollte, und solchen, die im Rahmen von Fortbildungsmaßnahmen – unternehmensspezifisch – ergänzend erworben werden können. Aus guten Gründen sind aber neben den essentiell wichtigen juristischen Kenntnissen auch Fähigkeiten im technisch-organisatorischen Bereich bzw. im Datenschutz-Management reflektiert. Die ausdrückliche Erwähnung von by Design und Privacy by Default trägt dabei der gewachsenen Bedeutung des Systemdatenschutzes im Rahmen ubiquitärer Datenverarbeitung Rechnung.

IV. Aufgaben des Datenschutzbeauftragten

Das EU-Parlament ist bestrebt, das Aufgabenfeld des Datenschutzbeauftragten durch Ergänzungen in Art. 37 sowie den Erwägungsgründen 75 und 75 a (neu) zu ergänzen bzw. zu präzisieren. Die Ergänzungen in § 37 Abs. 1 a betonen die wichtige Aufgabenstellung der Schaffung eines Datenschutzbewusstseins innerhalb der Daten verarbeitenden Stelle und die besondere Relevanz technischer und organisatorischer Maßnahmen und Vorgehensweisen. Mit dem letztgenannten Aspekt korrespondiert die Einfügung einer Passage in Erwägungsgrund 75, wonach der Datenschutzbeauftragte insbesondere vor der Planung, Beschaffung, Entwicklung und Einrichtung von Datenverarbeitungssystemen zu konsultieren ist, um die Wahrung der Grundsätze „Privacy by Design, Privacy by Default" sicherzustellen.

Durch die Einfügung von Buchstabe i in Art. 37 Abs. 1 soll der Datenschutzbeauftragte gehalten sein, die Verordnungskonformität im Rahmen der Vorabkonsultationsmechanismen nach Art. 34 zu verifizieren. In diesem Zusammenhang bleibt die konkret vorgesehene Rolle des Datenschutzbeauftragten im Rahmen der vom Parlament nochmals modifizierten Datenschutzfolgenabschätzung allerdings weiterhin nebulös[18].

Schließlich schlägt das EU-Parlament in einem neuen Buchstaben j von Art. 37 Abs. 1 vor, dem Datenschutzbeauftragten auch die Aufgabe der Information der Mitarbeitervertretung über die Verarbeitung von Beschäftigtendaten zu übertragen. Eine derartige Aufgabenzuweisung an den Datenschutzbeauftragten wäre im Fall fehlender Zustimmung der Geschäftsleitung mit Blick auf das Betriebsverfassungsrecht und den dort verankerten Grundsatz der Unabhängigkeit der Betriebsparteien nicht unbedenklich. Nachzugehen wäre ggf. der Frage, ob und inwieweit die vom BAG[19] festgestellte Regelungslücke

14 Siehe oben I. 3. a) und b).

15 Zur deutschen Rechtsprechung in Bezug auf den Kündigungsschutz von (Teilzeit-) Datenschutzbeauftragten vgl. Gola/Schomerus, BDSG (11. Aufl.), § 4f Rdnr. 40 ff. sowie Gola/Jaspers, RDV 1998, 47.

16 Zur notwendigen Fortbildung siehe oben 2. b).

17 Ähnlich Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 24./25. November 2010, wiedergegeben in: BfDI-Info 4 (Anhang 10), abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO4.pdf.

18 Zu insoweit notwendigen Klarstellungen der konkreten Rolle des Datenschutzbeauftragten vgl. bereits Klug, RDV 2013, 14 (16) sowie die Vorschläge des Parlaments zu Art. 32 a (neu) ff.; zur Konsultation der Aufsichtsbehörde durch den Datenschutzbeauftragten vgl. Klug, RDV 2001, 12 (17).

19 BAG, RDV 1998, 64.

zum Verhältnis zwischen Datenschutzbeauftragtem und Betriebsrat durch eine derartige Regelung gefüllt werden könnte.

V. Fazit und Ausblick

Das EU-Parlament hat – nicht nur – zur zukünftigen Rolle des Datenschutzbeauftragten Ergänzungen und Änderungen des Kommissionsvorschlags in die Diskussion eingebracht und ein klares Mandat zur Aufnahme von Verhandlungen mit dem Rat und der Kommission gegeben. Bevor es allerdings zu offiziellen Verhandlungen im Rahmen des sogenannten Trilogs kommen kann, bedarf es noch einer abgestimmten Positionierung im Rat.

Während ein kurzfristiger Kompromiss mit der EU-Kommission möglich erscheint, entscheidet sich die Konsensfähigkeit der Vorschläge des Parlaments letztlich an der Positionierung des Rates der EU. Dieser hat indes anlässlich seiner Sitzung am 06.12.2013 erkennen lassen, dass noch wesentliche Fragen klärungsbedürftig sind, bevor politische Entscheidungen getroffen werden können. Im Hinblick auf den Fortgang des Gesetzgebungsverfahrens hat die Griechische Ratspräsidentschaft bereits zahlreiche Arbeitssitzungen ab Januar 2014 anberaumt. Ob und inwieweit der Rat hierbei bereit ist, seine bisherige Position zum Datenschutzbeauftragten an den Kompromisstext des EU-Parlaments anzupassen, bleibt abzuwarten.

Anmerkungen zu den Verhaltensregeln der Deutschen Versicherungswirtschaft

Rechtsanwalt Dr. Georg Wronka, Bonn*

1. Verhaltensregeln nach § 38a BDSG

Die Verhaltensregeln (im folgenden verkürzt als „CoC" – Code of Conduct – bezeichnet) des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. („GDV") sind das erste – und bisher einzige – Regelwerk, das von den Aufsichtsbehörden nach den Vorgaben von § 38a BDSG geprüft und anerkannt wurde.

Die Feststellung der Übereinstimmung des Inhalts des CoC des GDV mit den gesetzlichen Bestimmungen, die Ende 2012 durch den Berliner Datenschutzbeauftragten erfolgte, schafft zum einen Rechtssicherheit für die Versicherungswirtschaft im Hinblick auf typische Datenverarbeitungsprozesse[1], zum anderen erhöhen solche Verhaltensregeln zugunsten der Betroffenen (= der Versicherungsnehmer „VN") die Transparenz über die Art und Verwendung ihrer Daten durch die Versicherungsgesellschaften.

Verhaltensregeln als selbstdisziplinäres Regulierungsinstrument besitzen keine Gesetzeskraft; sie ersetzen deshalb auch nicht die Normen des BDSG, sondern sind nach allg. Meinung nur als Konkretisierung der gesetzlichen Bestimmungen im Hinblick auf gruppen- oder branchenspezifische Datenverarbeitungspraktiken zu verstehen[2]. Da ihnen der Charakter als Rechtsvorschrift fehlt, kommt auch die Subsidiaritätsanordnung des § 1 Abs. 3 BDSG nicht zum Tragen.

2. Verbindlichkeit von CoC

Die Verhaltensregeln der Versicherungswirtschaft stellen eine gemeinsame Selbstverpflichtung der vom GDV vertretenen Organisationen dar. Die Unternehmen verpflichten sich auf freiwilliger Basis zu ihrer Einhaltung. Freiwillige Selbstverpflichtungen sind grundsätzlich nicht bindend in dem Sinn, dass sie Rechtsansprüche der Betroffenen begründen[3]. Soweit es in der Einleitung der CoC der Versicherungswirtschaft heißt, dass sich die beitretenden Mitgliedsunternehmen „zu deren Einhaltung verpflichten", bedeutet dies nur, dass sich die Unternehmen verbandsintern dem Regime der Regeln unterwerfen. Verstoßen sie gegen die vereinbarten Regeln, bleibt dies zwar nicht folgenlos[4], hat aber auf die Rechtsstellung, insbesondere die Befugnisse, der VN keinen Einfluss.

Bindungswirkung entfalten die CoC-Regeln indes in einer anderen Richtung. Die Aufsichtsbehörden haben sich bundesweit darauf verständigt, den CoC des GDV anzuerkennen und sich damit auf eine einheitliche Beurteilungspraxis festgelegt[5]. Den Versicherungsunternehmen werden damit Diskussionen mit einzelnen Aufsichtsbehörden erspart, die ggf. eine von an-

* Der Autor ist Rechtsanwalt in Bonn mit dem Arbeitsschwerpunkt Datenschutzrecht.

1 Vgl. Kinast, in: Taeger/Gabel, Kommentar zum BDSG (2010), § 38a Rn. 3; „Orientierungshilfe der Datenschutzaufsichtsbehörden für den Umgang mit Verhaltensregeln nach § 38a BDSG", Beschluss des Düsseldorfer Kreises in der Sitzung vom 26./27. Februar 2013.

2 Vgl. Bizer, DuD 2001, S. 126.

3 Vgl. Dammann/Simitis, EG-Datenschutzrichtlinie, Kommentar (1997), Art. 27 Rn. 1.

4 Vgl. nachfolgend unter 5.

5 Vgl. Hoeren, RDV 2011, 1.

deren Länderkontrollinstanzen abweichende Auffassung vertreten könnten. Dies müsste im Übrigen wohl auch im Hinblick auf die BaFin gelten. Bei der Feststellung der Vereinbarkeit der CoC-Regeln mit dem BDSG durch die Aufsichtsbehörden handelt es sich um einen feststellenden Verwaltungsakt[6]. Sein Inhalt ist nicht nur für die Verfahrensbeteiligten, sondern nach den allgemeinen verwaltungsverfahrensrechtlichen Grundsätzen auch für andere Behörden bindend[7]. Für Gerichte besteht naturgemäß eine solche Bindungswirkung nicht.

3. Die Bedeutung des CoC der Versicherungswirtschaft im datenschutzrechtlichen Regelungskonzept

Der CoC muss vor dem Hintergrund des die Verarbeitung personenbezogener Daten bestimmenden Prinzips des „Verbots mit Erlaubnisvorbehalt" bewertet werden, wie es in § 4 Abs. 1 BDSG zum Ausdruck gebracht wird. Der Bestimmung zufolge sind grundsätzlich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten untersagt, sofern sie nicht durch einen der drei alternativen Legitimationstatbestände – Einwilligung, spezielle Rechtsvorschriften außerhalb des BDSG oder im BDSG verankerte Zulässigkeitsbestimmungen – gerechtfertigt werden. Spezialgesetzliche Regelungen sind im Rahmen von § 4 Abs. 1 BDSG – anders als dies in Bezug auf § 1 Abs. 3 BDSG der Fall sein kann[8] – für die Datenverarbeitung von Versicherungsgesellschaften, wenn überhaupt, allenfalls peripher relevant. Zentrale Bedeutung für die DV-Prozesse haben deshalb die Einwilligung und die allgemeinen BDSG-Normen, namentlich die §§ 3 und 28.

Grundsätzlich stehen die Gestattungstatbestände Einwilligung und BDSG-Erlaubnisregelungen gleichwertig nebeneinander. Theoretisch ließen sich also alle DV-Prozesse in einer Versicherungsgesellschaft mit Hilfe einer Einwilligung der Betroffenen (=VN) rechtfertigen. Gleichwohl bestehen gegen eine solche Vorgehensweise praktische und dogmatische Bedenken.

Die Anforderungen an eine formal und inhaltlich korrekte („informierte") Einwilligung sind hoch. Die reichhaltige Rechtsprechung zeigt die Schwachstellen praktizierter Klauseln sehr deutlich auf. Gerade weil formalisierte Einwilligungsklauseln auch AGB-rechtlichen (Transparenz-)Anforderungen genügen müssen, liegt in ihrem Einsatz ein nicht unbeträchtliches Risiko für die Versicherungsunternehmen. Als Allheilmittel kann die Einwilligung nicht angesehen werden.

Überdies wird herrschend mit guten Gründen die Ansicht vertreten, der zufolge eine Einwilligung als Gestattungstatbestand nur dann in Betracht kommen dürfe, wenn die BDSG-Bestimmungen keine sichere Rechtsgrundlage für den jeweiligen Datenumgang bieten[9]. Aus diesem Grund sollte von ihnen immer erst auf der Basis des BDSG geprüft werden, wozu sie befugt sind, so dass sie – abgesehen von zwingenden Gesetzesbestimmungen (vgl. §§ 3 Abs. 9, 28 Abs. 7, 8 BDSG) – sozusagen nur hilfsweise auf die Einwilligung zurückgreifen sollten.

Angesichts dieser Konstellation der Zulässigkeitsbedingungen erhält der CoC der Versicherungswirtschaft seine besondere Bedeutung. Er ist als „amtlich anerkannte Interpretationshilfe"[10] der einschlägigen BDSG-Bestimmungen und –institute zu verstehen, an denen sich ein Versicherungsunternehmen orientieren kann. Er macht das Gesetz für das Unternehmen verständlicher, leichter anwend- und besser durchführbar[11] – bei einem relativ hohen Maß an Rechtssicherheit, wenn es sich an ihm ausrichtet. Wohlgemerkt: Absolut „gerichtsfest" ist der CoC nicht. Entscheidend bleibt die Vereinbarkeit der DV-Maßnahmen mit dem Gesetz, für die zwar ihre Kompatibilität mit dem CoC eine gewisse Garantie bietet. Aber in der „Orientierungshilfe" der Datenschutzaufsichtsbehörden vom 26./27.02.2013 heißt es klarstellend ausdrücklich[12]: „Kommt es trotz positiver Überprüfung einer Aufsichtsbehörde (Anerkennung) zu einem Widerspruch zwischen gesetzlicher Regelung und Verhaltensregel, geht das Gesetz vor".

4. Konfliktlösung durch CoC und neue Einwilligungsklauseln

Die Vorbehalte gegen einen universellen Einsatz von Einwilligungsklauseln zur Absegnung umfassender Verarbeitungsprozesse stützen sich maßgeblich auf Konfliktsituationen, die bei einem Widerruf der Einwilligung durch den Betroffenen entstehen können. Eine derartige Kassierung der Zustimmung könnte dazu führen, dass notwendige Verarbeitungen durch sie nicht mehr gerechtfertigt würden, obwohl sie an sich bei Anwendung der gesetzlichen Erlaubnisnormen – insbesondere § 28 BDSG – gestattet wären. Zudem wird bezweifelt, ob überhaupt die Freiwilligkeit der Einwilligung anzunehmen ist, wenn der Betroffene darauf hingewiesen wird, dass die Verarbeitung auch ohne seine Zustimmung durch eine gesetzliche Bestimmung legitimiert werden kann[13].

Die Versicherungswirtschaft hat diese Situation durchaus gesehen. Die Gesellschaften haben bislang in ihren „Merkblättern zur Datenverarbeitung", die die Einwilligungsklauseln flankierten, darauf hingewiesen, dass sie mit der Einwilligung der VN unabhängig von der Gesetzeslage „eine sichere Rechtsgrundlage" für die Datenverarbeitung schaffen wollten, sich aber den Rückzug auf die gesetzlichen Zulässigkeitsbestimmungen ausdrücklich vorbehalten. So heißt es dort u.a.: „Trotz Widerruf oder ganz bzw. teilweise gestrichener Einwilligungs-

6 Kinast, in: Taeger/Gabel, § 38a Rn. 29; Petri in Simitis (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 7. Aufl. (2011), § 38a Rn. 22.

7 Vgl. Kopp/Ramsauer, Kommentar zum Verwaltungsverfahrensgesetz, 14. Aufl (2013), § 43 Rn. 16, 18.

8 Zum Verhältnis von § 4 Abs. 1 zum § 4 Abs. 3 vgl. Gola/Schomerus, BDSG, Kommentar, 11. Aufl. (2012), § 4 Rn. 7.

9 Vgl. Gola/Schomerus, § 4 Rn. 16; Taeger in Taeger/Gabel, § 4 Rn. 45: „Nur dann, wenn danach keine Erlaubnis aufgrund eines Gesetzes besteht, kann die Einwilligung als weitere Möglichkeit zur Legitimation einer Erhebung, Verarbeitung oder Nutzung eingeholt werden". Im gleichen Sinn auch Sokol in Simitis (Hrsg.), § 4 Rn. 6.

10 Kinast, in: Taeger/Gabel, § 38a Rn. 3; Weichert in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, Kompaktkommentar, 4. Aufl. (2014), § 38a Rn. 6: „amtlich bestätigte Interpretationshilfen".

11 Vgl. Hullen, in: Plath (Hrsg.) BDSG Kommentar (2013), § 38a Rn. 18.

12 Abschnitt A am Ende.

13 Weichert in Däubler/Klebe/Wedde/Weichert, § 4 Rn. 4.

erklärung kann eine Datenverarbeitung und -nutzung in dem begrenzten gesetzlich zulässigen Rahmen … erfolgen."

Diese von den Aufsichtsbehörden geduldete Vorgehensweise ist in der Vergangenheit wiederholt mit dem Argument kritisiert worden, dass der betroffene VN irregeführt werde, wenn von den Versicherern Verarbeitungsprozesse durchgeführt würden, die seiner Einwilligungserklärung zuwider liefen bzw. von ihr nicht expressis verbis abgedeckt wurden. Ob die damit reklamierte Missachtung des Rechts auf informationelle Selbstbestimmung des VN dogmatischer Kritik standhält, mag dahinstehen. Nicht von der Hand zu weisen ist jedenfalls eine Gefährdung des vom VN in „seine" Versicherungsgesellschaft gesetzten Vertrauens, wenn sie sich entgegen den zunächst geweckten Erwartungen und Vorstellungen des VN verhält.

Das nunmehrige Zulässigkeitsregime, also die Kombination von CoC und neuen Einwilligungsklauseln, verhindert ein derartiges potentielles Auseinanderdriften von Erklärungsinhalt der Einwilligung und gesetzlicher Verarbeitungsbefugnis. Der CoC regelt nämlich Sachverhalte, die bislang weitgehend über umfassende – und bisweilen wenig übersichtliche – Einwilligungserklärungsformeln legitimiert werden sollten. Lediglich die Verarbeitungen, die Gesundheitsdaten und sonstige unter § 203 StGB fallende Daten zum Gegenstand haben, bedürfen jetzt einer datenschutzrechtlichen Einwilligung (vgl. auch die entsprechende Passage in der Einleitung des CoC). Es besteht daher ein großes Interesse der Versicherungsunternehmen, ihre DV-Abläufe so zu gestalten und ggf. neu auszurichten, dass sie den im CoC behandelten Sachverhalten entsprechen. Die Kongruenz von CoC-Regelungstatbeständen und tatsächlich praktizierten Verfahren enthebt sie, kurz gesagt, der Notwendigkeit, ausufernde Einwilligungstexte ihren VN vorzulegen. Nicht nur durch den CoC allein, sondern gerade auch durch die Verschlankung solcher Klauseln auf § 203 StGB- bzw. § 3 Abs. 9 BDSG-spezifische Daten(verarbeitungen) wird den VN ein Höchstmaß an Transparenz und gleichzeitig beiden Seiten die Gewähr rechtskonformen Verhaltens geboten.

5. Exklusivwirkung des CoC der Versicherungswirtschaft

Die durch die aufsichtsbehördliche Genehmigung zum Ausdruck gebrachte Erklärung der Vereinbarkeit mit dem BDSG bedeutet, dass die CoC-Regeln jedenfalls nicht hinter dem Schutzstandard des BDSG zurückbleiben und auch nicht mit den BDSG-Vorschriften kollidieren. Die in der Literatur ausgetragenen Streitfrage, ob und inwieweit sie über die gesetzlichen Minimalanforderungen hinaus eine Erhöhung des Schutzniveaus, einen sog. „Mehrwert" bewirken müssen, um die Voraussetzungen des § 38a BDSG zu erfüllen[14], bedarf hier keiner Diskussion. Unstrittig verbietet ein CoC jedenfalls nicht Datenverarbeitungen, die ein Unternehmen unter stringenteren Voraussetzungen, d.h. unter Anhebung des behördlich gebilligten Datenschutzstandards durchführen will. Der Beitritt zu dem CoC der Versicherungswirtschaft hindert ein Unternehmen also nicht, im Weg der Selbstbeschränkung den ihm durch den CoC eingeräumten Freiraum weiter einzugrenzen[15].

Zudem sind die CoC-Regeln teilweise allgemein gehalten. In der Einleitung zum CoC wird ausdrücklich darauf hingewiesen, dass die Unternehmen dadurch in die Lage versetzt werden sollen, sie in „unternehmensspezifischen Regelungen (zu) konkretisieren". Überdies soll der CoC auch nicht bestehende „spezielle Vereinbarungen oder Absprachen zu besonders datenschutzrechtlichen Verfahrensweisen" aushebeln, die ihm beigetretene Unternehmen mit den zuständigen Aufsichtsbehörden bereits getroffen haben. Kurzum: Der CoC schöpft nicht alle Möglichkeiten aus, die das Gesetz einem Versicherungsunternehmen bietet. Er bedeutet kein starres Korsett für die Durchführung der Datenverarbeitung durch die Versicherungsunternehmen und bindet sie nicht sklavisch an den Wortlaut, sondern lässt durchaus Raum für individuelle flexible Lösungen – vorausgesetzt, sie sind mit den gesetzlichen Rahmenvorgaben kompatibel.

Schließlich besteht eine Exklusivität des CoC auch nicht mit der Maßgabe, dass seine Anwendbarkeit und Wirkung auf die Mitgliedsunternehmen des GDV beschränkt wären. Die Regeln sind keineswegs für die GDV-Mitglieder reserviert. Auch Versicherungsgesellschaften außerhalb des GDV-Verbunds können sie ihrer Datenverarbeitung zugrunde legen und dürfen damit rechnen, dass bei Konformität keine Beanstandungen durch die Aufsichtsbehörden erfolgen.

6. Sanktionen bei Verstößen gegen den CoC?

Verletzungen von Verhaltensregeln als solchen sind nach dem BDSG sanktionslos; sie sind in den Katalog des § 43 BDSG nicht aufgenommen worden und werden auch von § 44 BDSG nicht angesprochen. Erst wenn sie zugleich einen Verstoß gegen gesetzliche Datenschutzbestimmungen darstellen, die nach den §§ 43, 44 BDSG bußgeld- bzw. strafbewehrt sind, treten die dort vorgesehen Rechtsfolgen ein[16].

Allerdings ist zu beachten, dass ein Zuwiderhandeln von Verbandsmitgliedern gegen den CoC, der aufgrund der dem GDV satzungsgemäß zustehenden Kompetenz verabschiedet wurde, eine Verletzung von mitgliedschaftlichen Verpflichtungen bedeuten kann. Gem. § 4 Abs. 2 der Satzung des GDV haben die Versicherungsunternehmen, die Mitglieder des GDV sind, „die im Rahmen der Satzung getroffenen Verbandsentscheidungen mitzutragen". Wenn sie demzufolge verpflichtet sind, diese Entscheidung auch in der Praxis zu befolgen, kann ein abweichendes Verhalten u.U. als Satzungsverstoß bewertet und ggf. unter den näheren Voraussetzungen von § 5 der GDV-Satzung geahndet werden. Das gilt vorliegend umso mehr, als die GDV-Mitglieder nicht automatisch zur Befolgung des CoC

14 Zur Diskussion dieses „Mehrwerts" vgl. nur Abel, RDV 2003, 11 (14); Karstedt-Merierrieks, DuD 2001, 287 (288); Weichert in Däubler/Klebe/Wedde/Weichert, § 38a Rn. 6; Hullen in Plath, § 38a Rn. 17; vgl. auch „Orientierungshilfe der Datenschutzaufsichtsbehörden" vom 26./27.02.2013 unter Abschnitt B 5.

15 Vgl. auch die Einleitung des CoC: „Darüber hinaus ist es den Unternehmen unbenommen, Einzelregelungen mit datenschutzrechtlichem Mehrwert…zu treffen."

16 Kinast, in: Taeger/Gabel, § 38a Rn. 33.

verpflichtet werden, sondern ihm erst Kraft ausdrücklichen Erklärungsakts (Beitritt) für ihr Geschäftsverhalten verbindlich übernehmen.

Schließlich sind auch wettbewerbsrechtliche Konsequenzen zu bedenken. Veröffentlichte Verhaltensregeln werden als Werbeinstrumente angesehen[17]. Zwar ist die Missachtung solcher Regeln nicht nach Maßgabe von §§ 3, 4 Nr. 11 UWG als unlauter zu bewerten, da ihnen die Rechtsnormqualität fehlt[18], doch können die Nichteinhaltung bzw. ein Verstoß das Kriterium der Irreführung gem. § 5 UWG erfüllen. Der CoC des GDV erfüllt die Voraussetzungen von § 2 Abs. 1 Nr. 5 UWG. Stellt eine Versicherungsgesellschaft heraus, dass sie dem CoC beigetreten ist, kann dies für sie ein effizientes Werbeargument sein. Der Hinweis auf den Beitritt vermag den Eindruck von besonderer Seriosität und Zuverlässigkeit zu erwecken. Daran knüpfen die Irreführungstatbestände des § 5 Abs. 1 Satz 2 Nr. 6 UWG und die Nr. 1 des Anhangs zu § 3 Abs. 3 UWG an[19]. Ein Versicherungsunternehmen, das sich regelwidrig verhält, ist also vor Abmahnungen/Klagen von nach § 8 UWG anspruchsberechtigten Stellen nicht gefeit.

17 Vgl. Kahlert, DuD 2003, 412f.

18 Vgl. Schröder, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct, nach US-amerikanischem und deutschem Recht, 2007, S. 284f.

19 Vgl. Köhler, in: Hefermehl/Köhler/Bornkamm, UWG-Kommentar, 27. Aufl., § 2 Rn. 117.

Rechtsprechung

Entlassung wegen HIV-Infektion ist diskriminierend (Ls)

(**Bundesarbeitsgericht**, Urteil vom 19. Dezember 2013 – 6 AZR 190/12 –)

Kündigt der Arbeitgeber das Arbeitsverhältnis eines an einer symptomlosen HIV-Infektion erkrankten Arbeitnehmers in der gesetzlichen Wartezeit des § 1 KSchG, so ist die auf Grund dieser Behinderung erfolgten Kündigung im Regelfall diskriminierend und damit unwirksam. Dies gilt zumindest dann, wenn der Arbeitgeber durch angemessene Vorkehrungen den Einsatz des Arbeitnehmers trotz seiner Behinderung ermöglichen kann.

(Nicht amtliche Leitsätze)

Beweisverwertungsverbot bei heimlicher Videoüberwachung am Arbeitsplatz

(**Bundesarbeitsgericht**, Urteil vom 21. November 2013 – 2 AZR 797/11 –)

Ein prozessuales Verwertungsverbot heimlich erfolgter Videoaufzeichnungen ergibt sich aus der Verletzung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, wenn die Aufzeichnung nicht durch überwiegende Beweisinteressen gerechtfertigt ist. Inwieweit dies auch unmittelbar aus § 6b BDSG oder § 32 BDSG folgt, kann dahinstehen.

(Nicht amtlicher Leitsatz)

Aus den Gründen:

Bei der Prüfung, ob die ordentliche Kündigung vom 11. September 2009 wegen erwiesener Pflichtwidrigkeiten der Klägerin sozial gerechtfertigt ist, darf das Landesarbeitsgericht seine Überzeugung nicht auf den Inhalt der in Augenschein genommenen Videoaufzeichnungen stützen. Deren Verwertung ist prozessual unzulässig. Ob dies unmittelbar aus § 6b BDSG oder doch § 32 BDSG folgt, kann im Ergebnis offen bleiben. Ein Verwertungsverbot ergibt sich in jedem Fall aus einer Verletzung des allgemeinen Persönlichkeitsrechts der Klägerin aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, die nicht durch überwiegende Beweisinteressen der Beklagten gerechtfertigt ist.

Allerdings kennt die Zivilprozessordnung selbst für rechtswidrig erlangte Informationen oder Beweismittel kein – ausdrückliches – prozessuales Verwendungs- bzw. Beweisverwertungsverbot. Aus § 286 ZPO i.V.m. Art. 103 Abs. 1 GG folgt vielmehr die grundsätzliche Verpflichtung der Gerichte, den von den Parteien vorgetragenen Sachverhalt und die von ihnen angebotenen Beweise zu berücksichtigen (BVerfG 9. Oktober 2002 – 1 BvR 1611/96 ua. – Rn. 60, BVerfGE 106, 28; BAG 16. Dezember 2010 – 2 AZR 485/08 – Rn. 30 mwN). Dementsprechend bedarf es für die Annahme eines Beweisverwertungsverbots, das zugleich die Erhebung der angebotenen Beweise hindert, einer besonderen Legitimation und gesetzlichen Grundlage (vgl. BAG 13. Dezember 2007 – 2 AZR 537/06 – Rn. 37; Musielak/Foerste ZPO 10. Aufl. § 284 Rn. 23; MüKoZPO/Prütting 4. Aufl. § 284 Rn. 64).

Im gerichtlichen Verfahren tritt der Richter den Verfahrensbeteiligten in Ausübung staatlicher Hoheitsgewalt gegenüber. Er

ist daher nach Art. 1 Abs. 3 GG bei der Urteilsfindung an die insoweit maßgeblichen Grundrechte gebunden und zu einer rechtsstaatlichen Verfahrensgestaltung verpflichtet (BVerfG 13. Februar 2007 – 1 BvR 421/05 – Rn. 93 mwN, BVerfGE 117, 202). Dabei können sich auch aus materiellen Grundrechten wie Art. 2 Abs. 1 GG Anforderungen an das gerichtliche Verfahren ergeben, wenn es um die Offenbarung und Verwertung von persönlichen Daten geht, die grundrechtlich vor der Kenntnis durch Dritte geschützt sind. Das Gericht hat deshalb zu prüfen, ob die Verwertung von heimlich beschafften persönlichen Daten und Erkenntnissen, die sich aus diesen Daten ergeben, mit dem allgemeinen Persönlichkeitsrecht des Betroffenen vereinbar ist (BVerfG 13. Februar 2007 – 1 BvR 421/05 – a.a.O.; BGH 15. Mai 2013 – XII ZB 107/08 – Rn. 21). Dieses Recht schützt nicht allein die Privat- und Intimsphäre, sondern schützt in seiner speziellen Ausprägung als Recht am eigenen Bild auch die Befugnis eines Menschen, selbst darüber zu entscheiden, ob Filmaufnahmen von ihm gemacht und möglicherweise gegen ihn verwendet werden dürfen (BAG 26. August 2008 – 1 ABR 16/07 – Rn. 15, BAGE 127, 276). Auch wenn keine spezielle Ausprägung des allgemeinen Persönlichkeitsrechts betroffen ist, greift die Verwertung von personenbezogenen Daten in das Grundrecht auf informationelle Selbstbestimmung ein, das die Befugnis garantiert, selbst über die Preisgabe und Verwendung persönlicher Daten zu befinden (BVerfG 11. März 2008 – 1 BvR 2074/05 ua. – BVerfGE 120, 378). Der Achtung dieses Rechts dient zudem Art. 8 Abs. 1 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) (BGH 15. Mai 2013 – XII ZB 107/08 – Rn. 14).

Die Bestimmungen des BDSG über die Anforderungen an eine zulässige Datenverarbeitung konkretisieren und aktualisieren den Schutz des Rechts auf informationelle Selbstbestimmung und am eigenen Bild. Sie regeln, in welchem Umfang im Anwendungsbereich des Gesetzes Eingriffe in diese Rechtspositionen zulässig sind (für das DSG NRW vgl. BAG 15. November 2012 – 6 AZR 339/11 – Rn. 16). Dies stellt § 1 BDSG ausdrücklich klar. Liegt keine Einwilligung des Betroffenen vor, ist die Datenverarbeitung nach dem Gesamtkonzept des BDSG nur zulässig, wenn eine 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. Dieser Grundsatz des § 4 Abs. 1 BDSG prägt das deutsche Datenschutzrecht (Gola/Schomerus BDSG 11. Aufl. § 4 Rn. 3; ErfK/Franzen 13. Aufl. § 4 BDSG Rn. 1; Simitis/Sokol BDSG 7. Aufl. § 4 Rn. 1).

In diesem Sinne regelt § 6b BDSG die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen. Die Bestimmung gilt ua. für Videoaufzeichnungen in öffentlich zugänglichen Verkaufsräumen (BT-Drucks. 14/4329, S. 38). Unerheblich ist, ob das Ziel der Beobachtung die Allgemeinheit ist oder die dort beschäftigten Arbeitnehmer sind (vgl. BAG 21. Juni 2012 – 2 AZR 153/11 – Rn. 36). Nach § 6b Abs. 1 Nr. 3 BDSG ist die Überwachung nur zulässig, wenn und soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Gemäß dem zum 1. September 2009 in Kraft getretenen § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach dessen Begründung für seine Durchführung oder Beendigung erforderlich ist. Nach Abs. 1 Satz 2 der Regelung dürfen zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zu deren Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten am Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Im Streitfall bestehen keine Anhaltspunkte dafür, dass die Kassen des Getränkemarkts vom übrigen Verkaufsraum abgegrenzt waren und die verdeckte Videoüberwachung deshalb keinen „öffentlichen Raum" iSd. § 6b BDSG betraf (zur Problematik Simitis/Scholz BDSG 7. Aufl. § 6b Rn. 51; Bayreuther NZA 2005, 1038). Im Ergebnis kommt es darauf nicht an. Ebenso kann offen bleiben, ob § 32 BDSG auf Überwachungen Anwendung findet, die vor seinem Inkrafttreten bereits beendet waren, und wie der Anwendungsbereich dieser Vorschrift zu dem des § 6b BDSG abzugrenzen ist (dazu ErfK/Franzen 13. Aufl. § 6b BDSG Rn. 2; Simitis/Scholz a.a.O.; Bayreuther DB 2012, 2222). Schließlich kann dahinstehen, ob Videoaufzeichnungen, die nicht von den Erlaubnistatbeständen des BDSG gedeckt sind, ohne weiteres einem prozessualen Beweisverwertungsverbot unterliegen oder ob es für ein solches Verbot einer weitergehenden Abwägung der betroffenen Grundrechte bedarf, in die freilich die im Bundesdatenschutzgesetz getroffene Interessenabwägung einzubeziehen wäre (dazu Bayreuther DB 2012, 2222, 2225; Grimm/Schiefer RdA 2009, 329, 349; Lunk NZA 2009, 457; Thüsing Anm. zu BAG 21. Juni 2012 – 2 AZR 153/11 – EzA BGB 2002 § 611 Persönlichkeitsrecht Nr. 13). Die Verwertung des verdeckt gewonnenen Videomaterials allein für den Beweis der Richtigkeit der Behauptung der Beklagten, die Klägerin habe sich bei der – als solcher unstreitigen – Entnahme von „Klüngelgeld" „versichernd umgeschaut", ist unter keinem rechtlichen Gesichtspunkt zulässig.

Greift die prozessuale Verwertung eines Beweismittels in das allgemeine Persönlichkeitsrecht einer Prozesspartei ein, überwiegt das Interesse an der Verwertung der Videoaufnahmen und der Funktionstüchtigkeit der Rechtspflege das Interesse am Schutz dieses Grundrechts nur dann, wenn weitere, über das schlichte Beweisinteresse hinausgehende Aspekte hinzutreten. Das Interesse, sich ein Beweismittel zu sichern, reicht für sich allein nicht aus (BVerfG 13. Februar 2007 – 1 BvR 421/05 – BVerfGE 117, 202). Vielmehr muss sich gerade diese Art der Informationsbeschaffung und Beweiserhebung als gerechtfertigt erweisen (BVerfG 9. Oktober 2002 – 1 BvR 1611/96, 1 BvR 805/98 – zu C II 4 a der Gründe, BVerfGE 106, 28; BAG 21. Juni 2012 – 2 AZR 153/11 – Rn. 29; 13. Dezember 2007 – 2 AZR 537/06 – Rn. 36 mwN).

Dementsprechend sind Eingriffe in das Recht des Arbeitnehmers am eigenen Bild durch heimliche Videoüberwachung und die Verwertung entsprechender Aufzeichnungen dann 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 das praktisch einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist (grundlegend BAG 27. März 2003 – 2 AZR 51/02 – zu B I 3 b cc der Gründe, BAGE 105, 356; 21. Juni 2012 – 2 AZR 153/11 – Rn. 30 – beide Male vor Inkrafttreten des § 32 BDSG). Der Verdacht muss sich in Bezug auf eine konkrete strafbare Handlung oder andere schwere Verfehlung zu Lasten des Arbeitgebers gegen einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern richten. Er darf sich einerseits nicht auf die allgemeine Mutmaßung beschränken, es könn-

ten Straftaten begangen werden. Er muss sich andererseits nicht notwendig nur gegen einen einzelnen, bestimmten Arbeitnehmer richten. Auch im Hinblick auf die Möglichkeit einer weiteren Einschränkung des Kreises der Verdächtigen müssen weniger einschneidende Mittel als eine verdeckte Videoüberwachung zuvor ausgeschöpft worden sein (BAG 21. Juni 2012 – 2 AZR 153/11 – a.a.O.; 27. März 2003 – 2 AZR 51/02 – zu B I 3 b dd (1) der Gründe, a.a.O.).

Das in § 6b Abs. 2 BDSG normierte Kennzeichnungsgebot steht einer Verwertung von Daten, die aus einer verdeckten Videoüberwachung gewonnen wurden, nicht zwingend entgegen (BAG 21. Juni 2012 – 2 AZR 153/11 – Rn. 41; Bauer/Schansker NJW 2012, 3537; Thüsing Anm. zu BAG 21. Juni 2012 – 2 AZR 153/11 – EzA BGB 2002 § 611 Persönlichkeitsrecht Nr. 13; wohl auch Bayreuther DB 2012, 2222 ff.). Das gegenteilige Normverständnis, das zu einem absoluten, nur durch bereichsspezifische Spezialregelungen (etwa durch § 100c, § 100h StPO) eingeschränkten Verbot verdeckter Videoaufzeichnungen in öffentlich zugänglichen Räumen führte, begegnete mit Blick auf die durch Art. 12 Abs. 1, Art. 14 Abs. 1 GG geschützten Integritätsinteressen des Arbeitgebers verfassungsrechtlichen Bedenken.

Die Regelung des § 32 BDSG baut auf den von der Rechtsprechung entwickelten allgemeinen Grundsätzen auf. Nach der Gesetzesbegründung sollte sie diese nicht ändern, sondern lediglich zusammenfassen (vgl. BT-Drucks. 16/13657, S. 21). Dementsprechend setzt § 32 Abs. 1 Satz 2 BDSG voraus, dass die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Aufdeckung einer Straftat erforderlich ist, und verlangt insoweit eine am Verhältnismäßigkeitsprinzip orientierte, die Interessen des Arbeitgebers und des Beschäftigten abwägende Einzelfallentscheidung. Diese muss zumindest den schon bisher geltenden Voraussetzungen für die Zulässigkeit einer heimlichen Videoüberwachung entsprechen (Thüsing Anm. zu BAG 21. Juni 2012 – 2 AZR 153/11 – EzA BGB 2002 § 611 Persönlichkeitsrecht Nr. 13; Wybitul BB 2010, 2235).

Es kann dahinstehen, ob § 32 Abs. 1 Satz 2 BDSG weitergehend verlangt, dass sich der Verdacht auf ein strafbares Verhalten richtet und deshalb auch der Verdacht auf schwere Pflichtverletzungen, ohne dass zugleich ihre Strafbarkeit feststünde, die Beobachtung nicht rechtfertigen könnte. Ebenso kann offenbleiben, ob die Regelung zusätzliche Anforderungen an die personelle Konkretisierung des Verdachts sowie dessen Dokumentation stellt (zweifelnd Bauer/Schansker NJW 2012, 3537, 3539; Thüsing Anm. zu BAG 21. Juni 2012 – 2 AZR 153/11 – EzA BGB 2002 § 611 Persönlichkeitsrecht Nr. 13). Hier fehlt es schon an der Erfüllung der bisher geltenden Anforderungen an die Zulässigkeit einer verdeckten Videoüberwachung und der Verwertung des daraus gewonnenen Materials. Damit liegt auch ein gesetzlicher Erlaubnistatbestand nicht vor.

Die im Berufungsurteil getroffenen Feststellungen rechtfertigen nicht die Annahme, für die verdeckte Beobachtung des Kassenbereichs habe ein hinreichender Anlass bestanden. Zwar ist – mangels zulässiger Verfahrensrügen der Revision – davon auszugehen, dass im ersten Halbjahr 2009 im Getränkemarkt Leergutdifferenzen iHv. insgesamt 7.081,63 Euro zu verzeichnen waren. Es ist weder dargetan noch festgestellt, durch welche konkreten Maßnahmen die Beklagte ausgeschlossen haben will, dass Leergut nicht etwa aus dem Lager entwendet worden ist. Ihr Vorbringen, sie habe „keine Fehlbestände an Leergut im Lager und im Kassenbereich festgestellt" bleibt im Allgemeinen haften. Es lässt nicht erkennen, dass sie stichprobenartige Kontrollen ausreichend oft durchgeführt hätte. Überdies macht ihr Vortrag nicht deutlich, ob vergleichbare Fehlbestände schon früher aufgetreten, ob diese ggf. als „auflaufender Posten" in die Berechnungen des Jahres 2009 eingeflossen sind und wie Fehlbuchungen als mögliche Ursache ausgeschlossen wurden. Selbst wenn die Beklagte die Ursache der Leergutdifferenzen berechtigterweise im Kassenbereich hätte vermuten dürfen, fehlt es an Vortrag und Feststellungen dazu, weshalb die Videoüberwachung das praktisch einzig verbliebene Mittel gewesen sein soll, die Unregelmäßigkeiten aufzuklären oder doch den Verdacht in personeller Hinsicht weiter einzugrenzen. So ist nicht erkennbar, weshalb nicht stichprobenartige Überprüfungen der Menge des an der – einzigen – Leergutkasse abgegebenen Pfandguts und der jeweiligen Kassenabschlüsse zusammen mit Kontrollen der Mitarbeiter beim Verlassen des Arbeitsplatzes geeignete Maßnahmen hätten sein können.

Die Würdigung des Landesarbeitsgerichts berücksichtigt im Übrigen nicht ausreichend, dass der fragliche Kündigungssachverhalt der Beklagten nur „zufällig" bekannt geworden ist. Auf seine Entdeckung war die heimliche Videoüberwachung nicht gerichtet.

Zwar mögen solche „Zufallsfunde" – unbeschadet der Regelung in § 6b Abs. 3 BDSG – nicht in jedem Fall deshalb unverwertbar sein, weil sie außerhalb des Beobachtungszwecks liegen (vgl. Grimm/Schiefer RdA 2009, 329, 340; aA wohl Bergwitz NZA 2012, 353, 358). Auch bezogen auf „Zufallserkenntnisse" muss aber das Beweisinteresse des Arbeitgebers höher zu gewichten sein als das Interesse des Arbeitnehmers an der Achtung seines allgemeinen Persönlichkeitsrechts. Das ist nur anzunehmen, wenn das mittels Videodokumentation zu beweisende Verhalten eine wenn nicht strafbare, so doch schwerwiegende Pflichtverletzung zum Gegenstand hat und die verdeckte Videoüberwachung nicht selbst dann noch unverhältnismäßig ist. Erreicht das in Rede stehende Verhalten diesen Erheblichkeitsgrad nicht, muss die Verwertung des Videomaterials unterbleiben.

So liegt es hier. Zwischen den Parteien ist die Existenz der „Klüngelgeld-Kasse" ebenso unstreitig wie der Umstand, dass die Klägerin daraus gelegentlich kleinere Geldstücke entnommen hat. Die Beweisaufnahme durch Augenschein sollte allein dem Nachweis dienen, dass sich die Klägerin bei der Geldentnahme „versichernd umgesehen" hat und deshalb vermutlich Zueignungsabsicht besaß. Das rechtfertigt keine Verwertung der heimlichen Videoaufzeichnungen. Zum einen hat die Beklagte nicht dargelegt, dass die Verwertung erforderlich war, um die Einlassung der Klägerin zum Fehlen ihrer Zueignungsabsicht zu widerlegen. Zum anderen ist die heimliche Videoüberwachung zum Nachweis der Absicht, sich einige Münzen im Wert von Centbeträgen zuzueignen, schlechthin unverhältnismäßig.

Verpflichtung zur Nutzung einer elektronischen Signaturkarte und der dazu erforderlichen Datenweitergabe an den Zertifizierungsdiensteanbieter

(**Bundesarbeitsgericht**, Urteil vom 25. September 2013 – 10 AZR 270/12 –)

1. Ein Arbeitgeber kann von seinem Arbeitnehmer die Beantragung und Nutzung einer elektronischen Signaturkarte verlangen, wenn dies für die Erbringung der vertraglich geschuldeten Arbeitsleistung erforderlich und dem Arbeitnehmer zumutbar ist.

2. Da die Bestimmungen des Signaturgesetzes die Beantragung einer qualifizierten Signaturkarte durch den Arbeitgeber nicht zulassen, kann der Arbeitnehmer angewiesen werden, seine Personalausweisdaten an den Zertifizierungsanbieter zu Identifizierungszwecken zu übermitteln.

(Leitsatz zu 2 nicht amtlich)

Sachverhalt:

Am 10. Dezember 2003 beschloss die Bundesregierung, die Vergabeverfahren aller Bundesbehörden sukzessive auf ein elektronisches Vergabesystem umzustellen. Am 8./13. März 2006 schloss das Bundesministerium für Verkehr, Bau und Stadtentwicklung (im Folgenden: BMVBS) mit dem bei ihm gebildeten Hauptpersonalrat eine „Dienstvereinbarung zur Nutzung qualifizierter digitaler Signaturen" (DV Digitale Signaturen).

Mit Erlass vom 11. Dezember 2009 verfügte das BMVBS, dass ab dem 1. Januar 2010 alle Vergabebekanntmachungen gemäß der Verdingungsordnung für Leistungen (VOL) und der Verdingungsordnung für freiberufliche Leistungen (VOF) über die elektronische Vergabeplattform des Bundes zu erstellen und entsprechend zu veröffentlichen seien.

Voraussetzung für die Veröffentlichung von Vergabeunterlagen auf der elektronischen Vergabeplattform des Bundes ist ein qualifiziertes Zertifikat mit qualifizierter elektronischer Signatur (im Folgenden: elektronische Signaturkarte) nach dem Signaturgesetz (SigG), das nur natürlichen Personen erteilt wird (§ 2 Nr. 7 SigG). Die Ausstellung einer elektronischen Signaturkarte setzt voraus, dass der Antragsteller von dem Zertifizierungsdiensteanbieter anhand des Personalausweises oder gleichwertiger Dokumente identifiziert worden ist (§ 5 Abs. 1 SigG, § 3 Abs. 1 SigV).

Mit Schreiben vom 15. März 2010 forderte die Amtsleitung des WSA die Klägerin auf, bei der T GmbH, einem Tochterunternehmen der D AG, eine elektronische Signaturkarte zu beantragen. Mit Schreiben vom 18. März 2010 teilte die Klägerin mit, sie sei nicht bereit, einen entsprechenden Antrag zu stellen, weil sie Bedenken habe, ihre persönlichen Daten einer privaten Firma zur Verfügung zu stellen. Das WSA wandte sich daraufhin über das BMVBS an die Bundesnetzagentur. Diese teilte mit E-Mail vom 4. Mai 2010 mit, dass aus ihrer Sicht kein Anlass bestehe, an der Datensicherheit und der Integrität der Systeme des von der Beklagten verwendeten Zertifizierungsdiensteanbieters zu zweifeln. Anschließend forderte die Amtsleitung des WSA die Klägerin mit Schreiben vom 22. Juni 2010 erneut auf, eine elektronische Signaturkarte zu beantragen. Nachdem sich die Klägerin zunächst wiederum weigerte, beantragte sie am 7. September 2010 „unter Vorbehalt und unter Protest" eine elektronische Signaturkarte, die sie kurz darauf erhielt.

Die Klägerin hat die Auffassung vertreten, sie sei nicht verpflichtet, eine elektronische Signaturkarte zu beantragen und zu nutzen. Eine Nutzung der elektronischen Signaturkarte durch sie sei nicht erforderlich. Die Diplom-Ingenieure, welche die Ausschreibungsunterlagen erstellten, könnten diese selbst auf der elektronischen Vergabeplattform des Bundes veröffentlichen. Außerdem gebe es andere Beschäftigte im WSA, die bereits über eine Signaturkarte verfügten und daher in der Lage seien, die Veröffentlichungen vorzunehmen. Entgegen den Vorgaben der DV Digitale Signaturen sei die Klägerin im Umgang mit der elektronischen Signaturkarte nicht geschult worden. Darüber hinaus verletze die Weisung der Beklagten das Recht der Klägerin auf informationelle Selbstbestimmung, weil sie ihre persönlichen Daten gegen ihren Willen einer privaten Firma mitteilen müsse. Sie habe Angst, dass mit ihren Daten Missbrauch getrieben werde.

Aus den Gründen:

Die Klage ist unbegründet. Die Weisung der Beklagten ist wirksam.

1. Nach § 106 Satz 1 GewO kann der Arbeitgeber Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrags oder gesetzliche Vorschriften festgelegt sind.

2. Die Veröffentlichung von Ausschreibungsunterlagen unter Einsatz einer elektronischen Signaturkarte gehört zum vertraglich vereinbarten Aufgabenbereich der Klägerin.

a) Die Klägerin wird gemäß § 1 des Arbeitsvertrags vom 13. Februar 1980 als Angestellte beschäftigt; aufgrund des 2. Nachtrags zum Arbeitsvertrag vom 29. Mai 1981 wurde sie in die Vergütungsgruppe VII BAT höhergruppiert und später in die EG 5 TVöD übergeleitet. Das Direktionsrecht des Arbeitgebers im öffentlichen Dienst erstreckt sich bei einer Vertragsgestaltung, die den vertraglichen Aufgabenbereich allein durch eine allgemeine Tätigkeitsbezeichnung und die Nennung der Vergütungsgruppe beschreibt, auf solche Tätigkeiten des allgemein umschriebenen Aufgabenbereichs, welche die Merkmale der Vergütungsgruppe erfüllen, in die der Arbeitnehmer eingestuft ist. Dem Arbeitnehmer können andere, dem allgemein umschriebenen Aufgabenbereich zuzuordnende Tätigkeiten nur zugewiesen werden, soweit sie den Merkmalen dieser Vergütungsgruppe entsprechen (st. Rspr., zuletzt z.B. BAG 17. August 2011 – 10 AZR 322/10 – Rn. 15).

b) Die Veröffentlichung von Vergabeunterlagen gehört zum Aufgabenbereich der Klägerin und entspricht den Merkmalen der Vergütungsgruppe VII BAT (nunmehr EG 5 TVöD). Nach der Dienstpostenbeschreibung vom 12. Juni 1996, die zwischen den Parteien ebenso wenig im Streit steht wie die Eingruppierung selbst, gehört zu den Aufgaben der Klägerin die Durchführung des inneren Dienstes der Dienststelle einschließlich der Zusammenstellung von Ausschreibungsunterlagen. Zu den administrativen Aufgaben im Zusammenhang mit Ausschreibungsunterlagen gehört nach der Verkehrsanschauung (vgl. ErfK/Preis 13. Aufl. § 106 GewO Rn. 5) auch deren Veröffentlichung. Dementsprechend hat die Klägerin bereits in der Vergangenheit regelmäßig Vergabeunterlagen – unter anderem im Intranet – veröffentlicht. Der geforderte Einsatz einer elektronischen Signaturkarte verändert den Aufgabenbereich der Klägerin nicht; lediglich die Art und Weise der Veröffentlichung und die dazu genutzten Arbeitsmittel werden technischen Entwicklungen angepasst.

3. Die Weisung der Beklagten ist unter Wahrung der Mitbestimmungsrechte nach dem BPersVG erfolgt (vgl. zur Theorie der Wirksamkeitsvoraussetzung im Anwendungsbereich des BPersVG zuletzt: BAG 22. Mai 2012 – 1 AZR 94/11 – Rn. 29). Der Hauptpersonalrat des BMVBS (§ 82 Abs. 1, § 53 Abs. 1 BPersVG) hat seine Rechte nach dem BPersVG im Zusammenhang mit der Einführung qualifizierter digitaler Signaturen (vgl. § 75 Abs. 3 Nr. 17 BPersVG) durch den Abschluss der DV Digitale Signaturen ausgeübt.

Die Weisung der Beklagten verstößt auch nicht gegen Vorschriften dieser Dienstvereinbarung. Insbesondere wurden entgegen der Rechtsauffassung der Klägerin die Vorgaben für die Schulung der Beschäftigten eingehalten. Dabei kann dahinstehen, ob deren Verletzung überhaupt zu einer Unwirksamkeit der Weisung führen oder nur einen nachträglichen Schulungsanspruch auslösen würde. Mit dem Schreiben der Amtsleitung des WSA vom 15. März 2010 wurde der Klägerin eine Kopie der Dienstvereinbarung übersandt. In dem Schreiben wird zudem auf eine „geplante Schulung in der IT-Anwendung" Bezug genommen. Eine weitere Schulung fand im März 2011 statt. Dass die Klägerin an dieser krankheitsbedingt

nicht teilnehmen konnte, stellt die Erfüllung der Pflichten aus der Dienstvereinbarung durch die Beklagte nicht infrage. Es gibt keine Anhaltspunkte dafür, dass die Beklagte die Schulung der Klägerin vorenthalten wollte oder sie nicht nachschulen würde, soweit die Klägerin hieran mitwirkt und teilnimmt.

4. Die Weisung zur Beantragung und Nutzung der elektronischen Signaturkarte verstößt nicht gegen Bestimmungen des BDSG.

a) Die Beklagte selbst erhebt, verarbeitet oder nutzt im Zusammenhang mit der Beantragung des qualifizierten Zertifikats mit qualifizierter elektronischer Signatur und der Erstellung der Signaturkarte keine Daten iSd. Bestimmungen des BDSG.

aa) Zwar ist das WSA als Bundesbehörde (vgl. Art. 87 Abs. 1 Satz 1, Art. 89 Abs. 2 GG) eine öffentliche Stelle iSd. § 1 Abs. 2 Nr. 1, § 2 Abs. 1 Satz 1 BDSG. Bei den Daten, welche die Klägerin im Rahmen der Beantragung der elektronischen Signaturkarte mitzuteilen hat, handelt es sich auch um personenbezogene Daten iSd. § 3 Abs. 1 BDSG. In Bezug auf diese Daten ist das WSA jedoch nicht verantwortliche Stelle iSd. BDSG.

1) Normadressat der im BDSG niedergelegten Rechte und Pflichten ist die jeweils verantwortliche Stelle (ErfK/Franzen § 1 BDSG Rn. 12; Simitis/Dammann BDSG 7. Aufl. § 3 Rn. 224 f.; Gola/Schomerus BDSG 11. Aufl. § 3 Rn. 48). Das ist gemäß § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(2) Personenbezogene Daten, die für die Erstellung und Nutzung einer elektronischen Signaturkarte erforderlich sind, werden von dem betreffenden Zertifizierungsdiensteanbieter unter Berücksichtigung der Vorgaben des SigG erhoben, verarbeitet und genutzt (§ 5 ff. SigG). Hinsichtlich des Umgangs mit diesen Daten unterliegt der Zertifizierungsdiensteanbieter daher – neben den speziellen Datenschutzbestimmungen des SigG – den Regelungen des BDSG (vgl. Roßnagel/Roßnagel Handbuch Datenschutzrecht Abschnitt 7.7 Rn. 29). Er ist insoweit die verantwortliche Stelle iSd. § 3 Abs. 7 BDSG.

(3) Das WSA ist demgegenüber weder in die Beschaffung noch in die Verarbeitung der Daten eingeschaltet. Vielmehr wurde die Klägerin aufgefordert, die elektronische Signaturkarte direkt beim Zertifizierungsdiensteanbieter zu beantragen (vgl. Schreiben vom 15. März 2010; DV Digitale Signaturen „Antragstellung durch den Beschäftigten"). Diese Vorgehensweise entspricht dem Modell des BDSG, wonach personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind (§ 4 Abs. 2 Satz 1 BDSG), und den Vorgaben des Signaturgesetzes (§ 14 Abs. 1 SigG). Das WSA nutzt auch nicht die zur Ausstellung der elektronischen Signaturkarte durch die T GmbH erhobenen Daten. Ein Nutzen von Daten iSv. § 3 Abs. 5 BDSG liegt vor, wenn die Daten mit einer bestimmten Zweckbestimmung ausgewertet, zusammengestellt, abgerufen oder ansonsten zielgerichtet zur Kenntnis genommen werden sollen (Gola/Schomerus BDSG § 3 Rn. 42; Gola/Wronka Handbuch zum Arbeitnehmerdatenschutz 5. Aufl. Rn. 911). Bei einem Einsatz der elektronischen Signaturkarte durch die Klägerin werden deren personenbezogene Daten durch das WSA nicht zielgerichtet zur Kenntnis genommen. Das WSA hat keinen Zugriff auf diese Daten.

bb) Zwischen dem WSA und dem Zertifizierungsdiensteanbieter besteht kein Auftragsverhältnis iSd. § 3 Abs. 7, § 11 BDSG. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag ist dadurch gekennzeichnet, dass sich eine verantwortliche Stelle eines Dienstleistungsunternehmens bedient, das lediglich weisungsgebunden mit den Daten umgeht (Gola/Schomerus BDSG § 11 Rn. 3; Simitis/Petri BDSG § 11 Rn. 20). Die verantwortliche Stelle bestimmt weiterhin allein über die Erhebung, Verarbeitung und Nutzung der Daten und behält die uneingeschränkte Verfügungsgewalt (Gola/Wronka Handbuch zum Arbeitnehmerdatenschutz Rn. 983; Wedde in Däubler/Klebe/Wedde/Weichert BDSG 3. Aufl. § 11 Rn. 5). Der Bereich der Auftragsdatenvergabe wird verlassen, sobald dem Dienstleistungsunternehmen eine eigenständige rechtliche Zuständigkeit für die Aufgabe, deren Erfüllung die Datenverarbeitung oder -nutzung dient, zugewiesen wird (Gola/Schomerus BDSG § 11 Rn. 9). Nach den Vorgaben des SigG ist der Zertifizierungsdiensteanbieter allein für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten des Antragstellers verantwortlich. Er entscheidet selbst über den Umgang mit den von ihm erhobenen Daten und hat dabei die zwingenden gesetzlichen Vorgaben insbesondere des SigG zu beachten. Das WSA hat keinen Zugriff auf und damit keine Verfügungsgewalt über die Daten. Ihm stehen auch keinerlei Kontroll- oder Weisungsrechte im Hinblick auf den Umgang mit den Daten zu.

b) Ein Verstoß gegen Bestimmungen des BDSG im Zusammenhang mit der Datenerhebung durch die T GmbH als Zertifizierungsdiensteanbieter ist nicht erkennbar.

aa) Das Unternehmen ist verantwortliche Stelle iSd. BDSG, es erhebt, verarbeitet und nutzt im Zusammenhang mit der Ausstellung der elektronischen Signaturkarte als nicht-öffentliche Stelle Daten der Klägerin (§ 1 Abs. 2 Nr. 3, § 2 Abs. 4 Satz 1, § 3 Abs. 7 BDSG).

bb) Die Erhebung der Daten erfolgt unmittelbar bei der Klägerin auf Grundlage der DV Digitale Signaturen (§ 4 Abs. 1, Abs. 2 Satz 1 BDSG); ihre Einwilligung (§ 4a BDSG) ist deshalb nicht erforderlich.

(1) Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene einwilligt. Rechtsvorschriften in diesem Sinne sind auch Tarifverträge (BAG 25. Juni 2002 – 9 AZR 405/00 – zu A II 4 d der Gründe, BAGE 101, 357) und Betriebs- oder Dienstvereinbarungen (BAG 27. Mai 1986 – 1 ABR 48/84 – zu B II 3 b aa der Gründe, BAGE 52, 88; 20. Dezember 1995 – 7 ABR 8/95 – zu B III 2 der Gründe, BAGE 82, 36 [jeweils zu Betriebsvereinbarungen]; ErfK/Franzen § 4 BDSG Rn. 2).

(2) Eine solche Erlaubnis enthalten die Bestimmungen der DV Digitale Signaturen. Danach wird jeder IT-Arbeitsplatz im Bereich der elektronischen Vergabe mit einem Kartenlesegerät und Chipkarten nach den Regelungen des SigG ausgestattet. Durch den jeweiligen Beschäftigten persönlich erfolgt eine entsprechende Antragstellung beim Zertifizierungsdiensteanbieter, die seine zuverlässige Identifizierung anhand der Personalausweisdaten erfordert. Unter diese Dienstvereinbarung fällt auch die Klägerin; sie gilt unmittelbar und zwingend (§§ 73, 75 Abs. 3 Nr. 17 BPersVG; Weber in Richardi/Dörner/Weber Personalvertretungsrecht 4. Aufl. § 73 BPersVG Rn. 21). Dem steht nicht entgegen, dass die Dienstvereinbarung eine Hergabe der Daten an Dritte verlangt. Durch § 2 Nr. 7 SigG ist vorgegeben, dass eine elektronische Signaturkarte nur von einer natürlichen Person beantragt werden kann und ihre Ausstellung durch Zertifizierungsdiensteanbieter erfolgt (§ 4 f. SigG).

Bedenken gegen die Wirksamkeit der DV Digitale Signaturen hat die Klägerin nicht geltend gemacht, sie sind auch nicht ersichtlich. Insbesondere begrenzt die Dienstvereinbarung den Kreis der Zertifizierungsdiensteanbieter auf solche, die gemäß § 15 SigG akkreditiert sind und damit einer weitergehenden aufsichtsbehördlichen Kontrolle unterliegen. Auch beinhaltet die DV Digitale Signaturen weitere Bestimmungen zum Schutz der Beschäftigten, wie beispielsweise eine Haftungsausschlussregelung. Die Dienstvereinbarung beschränkt insgesamt den Eingriff in das Recht der Beschäftigten auf informationelle Selbstbestimmung auf das zur Erfüllung

der Arbeitsaufgaben zwingend notwendige Maß; ein übermäßiger Eingriff wird durch sie nicht erlaubt (vgl. im Einzelnen zu 5 b dd).

c) Die Klägerin hat nicht behauptet, das WSA erhebe, verarbeite oder nutze Daten der Klägerin im Zusammenhang mit dem Einsatz der elektronischen Signaturkarte, Feststellungen hat das Landesarbeitsgericht hierzu nicht getroffen. Allerdings liegt nahe, dass die bei der elektronischen Vergabe notwendigen Außenverbindungen zum Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitung in streng zweckgebundenen Protokolldateien registriert werden (§ 14 Abs. 4 BDSG; vgl. zum Inhalt der Zweckbindung z.B. Simitis/Dammann BDSG § 14 Rn. 114). Dabei ergeben sich durch den Einsatz der elektronischen Signaturkarte keine Besonderheiten. Vielmehr erhöht diese die Sicherheit, dass der Kommunikationsinhalt unverändert übermittelt wird und Dritte von dessen Kenntnisnahme ausgeschlossen werden (Roßnagel/Roßnagel Handbuch Datenschutzrecht Abschnitt 7.7 Rn. 16). Zur Leistungs- und Verhaltenskontrolle dürfen eventuell anfallende Daten nach den Bestimmungen der DV Digitale Signaturen nicht genutzt werden.

5. Die Weisung der Beklagten entspricht billigem Ermessen.

a) Eine Leistungsbestimmung entspricht billigem Ermessen, wenn die wesentlichen Umstände des Falls abgewogen und die beiderseitigen Interessen angemessen berücksichtigt worden sind (st. Rspr., zuletzt zB BAG 29. August 2012 – 10 AZR 385/11 – Rn. 45; 12. Oktober 2011 – 10 AZR 746/10 – Rn. 26, BAGE 139, 283). Das bei der Ausübung des Leistungsbestimmungsrechts zu wahrende billige Ermessen wird inhaltlich durch die Grundrechte des Arbeitnehmers mitbestimmt. Kollidieren diese mit dem Recht des Arbeitgebers, dem Arbeitnehmer eine von der vertraglichen Vereinbarung gedeckte Tätigkeit zuzuweisen, sind die gegensätzlichen Rechtspositionen grundrechtskonform auszugleichen (vgl. BAG 24. Februar 2011 – 2 AZR 636/09 – Rn. 23 mwN, BAGE 137, 164; 13. August 2010 – 1 AZR 173/09 – Rn. 10, BAGE 135, 203). Dabei sind die betroffenen Interessen des Arbeitnehmers und des Arbeitgebers im Sinne einer praktischen Konkordanz so abzuwägen, dass die geschützten Rechtspositionen für alle Beteiligten möglichst weitgehend wirksam werden (BAG 23. August 2012 – 8 AZR 804/11 – Rn. 36; 24. Februar 2011 – 2 AZR 636/09 – a.a.O.). Ob die Entscheidung der Billigkeit entspricht, unterliegt der vollen gerichtlichen Kontrolle (BAG 26. September 2012 – 10 AZR 311/11 – Rn. 28; 12. Oktober 2011 – 10 AZR 746/10 – Rn. 46 mwN, a.a.O.).

b) Diese Sachentscheidung ist wegen der zu berücksichtigenden Umstände des Einzelfalls vorrangig den Tatsachengerichten vorbehalten (BAG 12. Oktober 2011 – 10 AZR 746/10 – Rn. 46, a.a.O.; 10. Mai 2005 – 9 AZR 294/04 – zu B II 3 b und B IV 1 der Gründe; vgl. zur Kontroverse über den Umfang der revisionsrechtlichen Überprüfung: GMP/Müller-Glöge 8. Aufl. § 73 Rn. 10). Unabhängig hiervon hält die Entscheidung des Landesarbeitsgerichts auch einer uneingeschränkten Überprüfung stand.

aa) Die Beklagte hat ein berechtigtes Interesse daran, die Vergabe öffentlicher Aufträge mithilfe eines elektronischen Vergabesystems durchzuführen. Wie sich dem Beschluss der Bundesregierung vom 10. Dezember 2003 entnehmen lässt, dient die Einführung des elektronischen Vergabesystems der Steigerung von Effizienz und Kompetenz bei der Beschaffung von Gütern und Dienstleistungen durch die öffentliche Hand. Durch die elektronische Vergabe öffentlicher Aufträge sollen erhebliche Einsparungen sowohl bei den Kosten der Vergabe als auch bei den Preisen für die beschafften Leistungen erzielt werden. Die Einführung des elektronischen Vergabesystems dient damit legitimen Zwecken.

bb) Die Amtsleitung des WSA hat keine Möglichkeit, die Veröffentlichung von Vergabeunterlagen anders zu gestalten. Das WSA ist eine dem BMVBS nachgeordnete Behörde. Der Erlass des BMVBS vom 11. Dezember 2009, nach dem ab dem 1. Januar 2010 alle Vergabebekanntmachungen über die elektronische Vergabeplattform des Bundes zu veröffentlichen sind, ist daher für das WSA bindend (vgl. Ehlers in Erichsen/Ehlers Allgemeines Verwaltungsrecht 13. Aufl. § 2 Rn. 62 ff.). Eine Veröffentlichung der Vergabeunterlagen auf anderem Wege scheidet aus. Das betrifft alle Bediensteten der nachgeordneten Behörden gleichermaßen.

cc) Der Einwand der Klägerin, eine Veröffentlichung der Vergabeunterlagen durch sie selbst sei nicht erforderlich, weil die Unterlagen auch durch Diplom-Ingenieure oder Beschäftigte, die bereits über ein Signaturkarte verfügen, veröffentlicht werden könnten, steht der Weisung der Beklagten nicht entgegen.

(1) Dem Gericht obliegt nicht die Prüfung, ob die Weisung der Beklagten die beste, effizienteste oder wirtschaftlich vernünftigste Lösung darstellt. Im Rahmen der Ausübung des Direktionsrechts steht dem Arbeitgeber ein nach billigem Ermessen auszufüllender Entscheidungsspielraum zu. Innerhalb dieses Spielraums können ihm mehrere Entscheidungsmöglichkeiten zur Verfügung stehen. Dem Gericht obliegt (lediglich) die Prüfung, ob der Arbeitgeber als Gläubiger die Grenzen seines Bestimmungsrechts beachtet hat (vgl. BAG 26. September 2012 – 10 AZR 311/11 – Rn. 28; 13. Juni 2012 – 10 AZR 296/11 – Rn. 28; BGH 18. Oktober 2007 – III ZR 277/06 – Rn. 20, BGHZ 174, 48).

(2) Das ist hier der Fall. Die Diplom-Ingenieure sind für die Erstellung und den Inhalt der Vergabeunterlagen verantwortlich. Angesichts ihrer besonderen Ausbildung und Qualifikation ist es nachvollziehbar und nicht zu beanstanden, wenn sich die Beklagte dazu entschließt, sie nicht mit rein administrativen Tätigkeiten wie der Veröffentlichung der Vergabeunterlagen zu betrauen, sondern diese Aufgabe von anderen Beschäftigten erledigen zu lassen. Dass andere Beschäftigte des WSA bereits über eine elektronische Signaturkarte verfügen, lässt das Bedürfnis für die Beantragung und Nutzung einer elektronische Signaturkarte durch die Klägerin ebenfalls nicht entfallen. Abwesenheitszeiten einzelner Mitarbeiter (zB aufgrund von Krankheit oder Urlaub) können es erforderlich machen, dass mehrere Mitarbeiter über eine elektronische Signaturkarte verfügen. Nur so kann sichergestellt werden, dass die Vergabeunterlagen unabhängig von den jeweils in der Dienststelle anwesenden Beschäftigten zeitnah veröffentlicht werden können. Es lag nahe, auch die Klägerin für diese Tätigkeit heranzuziehen, weil die Veröffentlichung von Vergabeunterlagen bereits vor dem 1. Januar 2010 zu ihrem Aufgabengebiet gehörte.

dd) Der mit der Weisung verbundene Eingriff in das Recht der Klägerin auf informationelle Selbstbestimmung ist dieser zumutbar.

(1) Das in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verankerte Recht auf informationelle Selbstbestimmung gewährleistet dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen und darüber zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (BVerfG 15. Dezember 1983 – 1 BvR 209/83, 1 BVR 269/83 ua – zu C II 1 a der Gründe, BVerfGE 65, 1; 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 – Rn. 180, BVerfGE 120, 274). Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entschei-

den (BVerfG 4. April 2006 – 1 BvR 518/02 – Rn. 69, BVerfGE 115, 320). Dabei kommt es nicht darauf an, ob es sich um Daten der Privat- oder gar der Intimsphäre handelt. Ein „belangloses" Datum gibt es aus Sicht der Verfassung nicht (vgl. BVerfG 15. Dezember 1983 – 1 BvR 209/83, 1 BvR 269/83 ua. – zu C II 2 der Gründe, a.a.O.). Das Recht auf informationelle Selbstbestimmung findet eine Entsprechung im Unionsrecht. Gemäß Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) In das Recht der Klägerin auf informationelle Selbstbestimmung wird durch die streitgegenständliche Weisung eingegriffen, weil die Klägerin nicht mehr frei entscheiden kann, wann sie wem welche Daten zur Verfügung stellt. Durch die Weisung wird sie verpflichtet, einem von der Beklagten ausgewählten Zertifizierungsdiensteanbieter die aus dem Personalausweis ersichtlichen Daten zur Verfügung zu stellen.

(3) Dieser Eingriff ist der Klägerin zumutbar (ebenso für die an einen Beamten gerichtete Anordnung, eine elektronische Signaturkarte zu beantragen und zu nutzen: Bayer. VGH 2. November 2011 – 6 CE 11.1342 –).

(a) Die Veröffentlichung der Vergabeunterlagen durch die Klägerin ist ohne Eingriff in ihr Recht auf informationelle Selbstbestimmung nicht möglich. Nach den für den Senat bindenden Feststellungen des Landesarbeitsgerichts (§ 559 Abs. 2 ZPO) ist für die Veröffentlichung von Vergabeunterlagen auf der elektronischen Vergabeplattform des Bundes der Einsatz einer elektronischen Signaturkarte unverzichtbar. Dieser Einsatz setzt wiederum zwingend voraus, dass die Klägerin selbst die Karte unter Mitteilung ihrer personenbezogenen Daten beim Zertifizierungsdiensteanbieter beantragt hat. Gemäß § 2 Nr. 7 SigG kann eine elektronische Signaturkarte nur von einer natürlichen Person beantragt werden (vgl. Spindler/Schuster/Gramlich Recht der elektronischen Medien 2. Aufl. § 2 SigG Rn. 16). Die Beantragung einer elektronischen Signaturkarte für die gesamte Dienststelle oder auch nur für mehrere Beschäftigte ist nicht möglich. Auch die Nutzung einer für einen anderen Beschäftigten ausgestellten elektronischen Signaturkarte durch die Klägerin kommt nicht in Betracht, weil die mit der Signaturkarte verbundenen Rechte nur von den jeweiligen Antragstellern ausgeübt werden dürfen; dies legt die DV Digitale Signaturen („Rechte und Pflichten") ausdrücklich fest. Im Übrigen würde eine solche Handhabung dem Zweck der elektronischen Signaturkarte als sicherem Identifizierungsmittel des jeweiligen Absenders zuwiderlaufen.

(b) Die Weisung stellt keinen besonders schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar. Die aus dem Personalausweis ersichtlichen Daten betreffen den äußeren Bereich der Privatsphäre. Insbesondere Name, Alter und Adresse gehören zu den „Stammdaten" des Arbeitnehmers, deren Erhebung für die Durchführung eines Arbeitsverhältnisses regelmäßig erforderlich ist (BAG 23. August 2012 – 8 AZR 804/11 – Rn. 38 mwN). Diese Daten werden auch im allgemeinen Geschäftsverkehr häufig eingesetzt. Bei den Angaben im Personalausweis handelt es sich nicht um besonders sensible Daten iSv. § 3 Abs. 9 BDSG, für die nach § 4a Abs. 3, § 28 Abs. 6 bis Abs. 9 BDSG erhöhte Anforderungen an die Erhebung und Speicherung zu stellen sind (vgl. zum Umgang mit solchen Daten im Rahmen der Personalaktenführung: BAG 12. September 2006 – 9 AZR 271/06 – BAGE 119, 238). Dass die Angaben – insbesondere das Passfoto und die ausgewiesene Staatsangehörigkeit – mittelbar Rückschlüsse auf die ethnische Herkunft zulassen, reicht für eine Anwendung der genannten Vorschriften nicht aus, weil eine entsprechende Auswertungsabsicht nicht besteht; die Datenerhebung dient allein der Identifizierung (vgl. Gola/Schomerus BDSG § 3 Rn. 56a; zur Abgrenzung von Staatsangehörigkeit und ethnischer Herkunft: BAG 21. Juni 2012 – 8 AZR 364/11 – Rn. 31).

Darüber hinaus werden die Daten nicht der allgemeinen Öffentlichkeit oder einer unbestimmten Anzahl von Personen bekanntgegeben, sondern nur einem einzigen Zertifizierungsdiensteanbieter übermittelt. Dieser darf die Daten zudem nur insoweit erheben und nutzen, als dies für Zwecke einer elektronischen Signaturkarte erforderlich ist (§ 14 Abs. 1 Satz 1 SigG). Zu anderen Zwecken dürfen die Daten nur verwendet werden, wenn das SigG es erlaubt oder der Betroffene eingewilligt hat (§ 14 Abs. 1 Satz 3 SigG).

(c) Der Schutz der personenbezogenen Daten der Klägerin wird durch Vorschriften des Signaturgesetzes und der Signaturverordnung sichergestellt. Einen Zertifizierungsdienst darf danach nur anbieten, wer die für den Betrieb erforderliche Zuverlässigkeit und Fachkunde nachweist (§ 4 Abs. 2 Satz 1 SigG) und der zuständigen Behörde ein Sicherheitskonzept vorgelegt hat, in dem die Maßnahmen zur Erfüllung der Sicherheitsanforderungen nach dem SigG und der SigV im Einzelnen aufgezeigt werden (§ 4 Abs. 2 Satz 4 SigG, § 2 SigV). Der Zertifizierungsdiensteanbieter hat für die Ausübung der Zertifizierungstätigkeit zuverlässiges Personal und zuverlässige Produkte für elektronische Signaturen einzusetzen (§ 5 Abs. 5 SigG, § 5 Abs. 3 SigV). Die Daten eines Antragstellers dürfen nur unmittelbar bei diesem selbst und grundsätzlich nur für Zwecke einer elektronischen Signaturkarte erhoben werden (§ 14 Abs. 1 Satz 1 SigG). Der Zertifizierungsdiensteanbieter hat das Sicherheitskonzept einschließlich etwaiger Änderungen, die Unterlagen zur Fachkunde der im Betrieb tätigen Personen und die vertraglichen Vereinbarungen mit den Antragstellern zu dokumentieren (§ 10 Abs. 1 SigG, § 8 SigV). Dem Antragsteller ist auf Verlangen jederzeit Einblick in die ihn betreffenden Daten zu gewähren (§ 10 Abs. 2 SigG).

Über diese zwingenden gesetzlichen Vorgaben hinaus bestimmt die DV Digitale Signaturen, dass als Zertifizierungsdiensteanbieter nur solche in Betracht kommen, die sich gemäß § 15 ff. SigG bei der zuständigen Behörde freiwillig akkreditiert haben. Die freiwillige Akkreditierung beinhaltet eine regelmäßige Überprüfung des Sicherheitskonzepts des Zertifizierungsdiensteanbieters durch öffentlich anerkannte fachkundige Dritte (§ 15 Abs. 2, § 18 SigG) und gewährleistet damit ein Sicherheitskonzept von besonders hoher Qualität (vgl. Spindler/Schuster/Gramlich Recht der elektronischen Medien § 15 SigG Rn. 6; Roßnagel/Roßnagel Handbuch Datenschutzrecht Abschnitt 7.7 Rn. 26). Der von der Beklagten ausgewählte Zertifizierungsdiensteanbieter entspricht diesen Vorgaben.

(d) Angesichts der Sicherheitsvorkehrungen bestehen keine Anhaltspunkte für die Befürchtung der Klägerin, mit ihren Daten könnte Missbrauch getrieben werden. Konkrete Tatsachen, die auf die Möglichkeit eines Missbrauchs hindeuten, hat die Klägerin nicht vorgetragen. Die Beklagte hat die Bedenken der Klägerin dennoch aufgegriffen und sich bei der gemäß § 3 SigG zuständigen Bundesnetzagentur nach der Reputation der T GmbH erkundigt. Auch nach Auskunft der Bundesnetzagentur besteht kein Anlass, an der Datensicherheit und der Integrität der Systeme zu zweifeln.

ee) Die Weisung der Beklagten stellt zwar einen Eingriff in die durch Art. 2 Abs. 1 GG geschützte Vertragsfreiheit (vgl. BVerfG 16. Juli 2012 – 1 BvR 2983/10 – Rn. 21 mwN) der Klägerin dar, weil sie verpflichtet wird, gegen ihren Willen ein Vertragsverhältnis mit dem Zertifizierungsdiensteanbieter einzugehen. Dieser Eingriff ist der Klägerin aber ebenfalls zumutbar. Zur Begründung kann auf die obigen Ausführungen verwiesen werden. Ergänzend ist zu berücksichtigen, dass der vom Arbeitgeber geforderte Vertragsschluss einen unmittelbaren Bezug zur geschuldeten Arbeitsleistung aufweist und der Klägerin durch ihn keine Zahlungspflichten auferlegt

werden. Sämtliche Kosten für die Leistungen des Zertifizierungsdiensteanbieters trägt nach der DV Digitale Signaturen die Beklagte.

ff) Soweit die Weisung die Verpflichtung der Klägerin beinhaltet, die elektronische Signaturkarte bei der Veröffentlichung der Vergabeunterlagen zu nutzen, begegnet sie ebenfalls keinen Bedenken. Besondere, speziell mit der dienstlichen Nutzung der elektronischen Signaturkarte für sie verbundene Gefahren benennt die Klägerin nicht. Die Klägerin hat nach den Bestimmungen der DV Digitale Signaturen einen Schulungsanspruch gegenüber der Beklagten; die Dienstvereinbarung legt bestimmte Verhaltensweisen zur sicheren Nutzung durch die Beschäftigten fest. Den Interessen der Klägerin wird zudem durch eine Haftungsfreistellung Rechnung getragen: Nach der DV Digitale Signaturen stellt das BMVBS die Beschäftigten von etwaigen Haftungsansprüchen des Zertifizierungsdiensteanbieters oder anderer Dritter frei, die im Zusammenhang mit einer fehlerhaften Nutzung der Signaturkarte zu dienstlichen Zwecken erhoben werden können. Die DV Digitale Signaturen („Anwendung") stellt schließlich klar, dass aufgrund des Einsatzes der elektronischen Signaturkarte beim Arbeitgeber gewonnene Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden dürfen. Eine Nutzung der elektronischen Signaturkarte über den dienstlichen Einsatz hinaus, insbesondere zu privaten Zwecken, wird von der Klägerin nicht verlangt.

Verwertung von Beweismitteln aus heimlicher Schrankkontrolle

(**Bundesarbeitsgericht**, Urteil vom 20. Juni 2013 – 2 AZR 546/12 –)

1. **Der prozessualen Verwertung von Beweismitteln, die der Arbeitgeber aus einer in Abwesenheit und ohne Einwilligung des Arbeitnehmers durchgeführten Kontrolle von dessen Schrank erlangt hat, kann schon die Heimlichkeit der Durchsuchung entgegenstehen.**

2. **Hat der Arbeitgeber dem Betriebsrat bestimmte Kündigungsgründe nicht mitgeteilt, ist sein entsprechender Sachvortrag im Kündigungsschutzprozess gleichwohl verwertbar, wenn der Arbeitnehmer die ordnungsgemäße Anhörung des Betriebsrats erklärtermaßen nicht rügt.**

Sachverhalt:

Die Parteien streiten über die Wirksamkeit einer außerordentlichen und einer vorsorglichen ordentlichen Kündigung.

Die Beklagte betreibt sog. Cash & Carry-Märkte. Der 1971 geborene Kläger war in einem ihrer Großhandelsmärkte seit August 1994 als Verkaufsmitarbeiter in der Getränkeabteilung tätig. In dem Markt beschäftigt die Beklagte regelmäßig mehr als zehn Arbeitnehmer.

Am 4. März 2011 war der Kläger in der Spätschicht von 15:00 bis 22:00 Uhr eingesetzt. Wegen eines laut gewordenen Diebstahlverdachts öffnete der zuständige Geschäftsleiter im Beisein eines Betriebsratsmitglieds während der Arbeitszeit den verschlossenen Spind des Klägers und durchsuchte ihn. Nach Behauptung der Beklagten wurde dabei vom Kläger entwendete Damenunterwäsche entdeckt. Der Geschäftsleiter äußerte daraufhin seine Absicht, gegen Ende der Schicht unter Hinzuziehung zweier Betriebsratsmitglieder eine Taschen-/Personenkontrolle durchzuführen. Dem Kläger gelang es, den Markt schon vorher unkontrolliert zu verlassen. Die Umstände, unter denen dies geschah, sind streitig.

Die Beklagte erstattete nach Schichtende Strafanzeige gegen den Kläger wegen Diebstahls von vier Teilen Damenunterwäsche. Eine unmittelbar darauf beim Kläger – mit dessen Einverständnis – polizeilich durchgeführte Wohnungsdurchsuchung verlief ergebnislos. Gegen 22:30 Uhr durchsuchte der Geschäftsleiter den Spind des Klägers in Gegenwart eines Betriebsratsmitglieds ein weiteres Mal. Die Beklagte hat behauptet, dabei seien die Wäschestücke nicht mehr aufgefunden worden.

In der Zeit vom 5. bis zum 13. März 2011 war der Kläger arbeitsunfähig erkrankt. Am 7. März 2011 teilte ihm die Beklagte schriftlich mit, er stehe im Verdacht, zum Verkauf bestimmte Damenunterwäsche aus dem Markt entwendet zu haben. Sie lud ihn zu einem Gespräch am 11. März 2011, alternativ gab sie ihm Gelegenheit zur schriftlichen Stellungnahme bis zum 14. März 2011. Der Kläger ließ den Gesprächstermin verstreichen und gab binnen der Frist auch keine schriftliche Erklärung ab. Auf Befragen durch den Geschäftsleiter äußerte er, er werde zu dem Vorwurf keine Angaben machen.

Nach Anhörung des Betriebsrats und mit dessen Zustimmung kündigte die Beklagte das Arbeitsverhältnis der Parteien mit Schreiben vom 17. März 2011 fristlos, mit einem weiteren Schreiben vom selben Tage kündigte sie „hilfsweise" ordentlich zum 31. Oktober 2011.

Die Vorinstanzen haben der Klage stattgegeben. Mit der Revision verfolgt die Beklagte ihr Begehren weiter, die Klage abzuweisen.

Aus den Gründen:

Die Revision der Beklagten ist begründet. Sie führt zur Aufhebung des Berufungsurteils (§ 562 Abs. 1 ZPO) und zur Zurückverweisung der Sache an das Landesarbeitsgericht (§ 563 Abs. 1 Satz 1 ZPO). Mit der von ihm gegebenen Begründung durfte das Landesarbeitsgericht der Klage nicht stattgeben (I.). Ob das Arbeitsverhältnis der Parteien durch die außerordentliche fristlose Kündigung vom 17. März 2011 aufgelöst worden ist, steht noch nicht fest (II.).

I. Die Feststellungen des Landesarbeitsgerichts tragen nicht das Ergebnis, ein wichtiger Grund iSd. § 626 Abs. 1 BGB liege nicht vor. Zwar ist die fristlose Kündigung nicht wegen einer erwiesenen Pflichtverletzung gerechtfertigt. Nicht frei von Rechtsfehlern ist jedoch die Auffassung des Landesarbeitsgerichts, die Kündigung sei auch als Verdachtskündigung unwirksam. Der Beklagten ist es, anders als das Landesarbeitsgericht angenommen hat, nicht aus betriebsverfassungsrechtlichen Gründen verwehrt, sich auf den Verdacht einer schwerwiegenden Pflichtverletzung als Kündigungsgrund zu berufen.

1. Nach § 626 Abs. 1 BGB kann ein Arbeitsverhältnis von jedem Vertragsteil aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, aufgrund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses selbst bis zum Ablauf der Kündigungsfrist nicht zugemutet werden kann. Dabei sind vom Arbeitnehmer zu Lasten des Arbeitgebers begangene Vermögensdelikte regelmäßig geeignet, eine außerordentliche Kündigung aus wichtigem Grund zu rechtfertigen, und zwar auch dann, wenn die rechtswidrige Handlung Sachen von nur geringem Wert betrifft oder zu einem nur geringfügigen, möglicherweise zu gar keinem Schaden geführt hat (BAG 21. Juni 2012 – 2 AZR 153/11 – Rn. 17; 10. Juni 2010 – 2 AZR 541/09 – Rn. 26, BAGE 134, 349; jeweils mwN).

2. Auch der Verdacht einer schwerwiegenden Pflichtverletzung kann einen wichtigen Grund iSv. § 626 Abs. 1 BGB bilden. Ein solcher Verdacht stellt gegenüber dem Vorwurf, der Arbeitnehmer habe die Tat begangen, einen eigenständigen Kündigungsgrund dar. Eine auf ihn gestützte Kündigung kann gerechtfertigt sein, wenn sich der Verdacht auf objektive Tatsachen gründet, die Verdachtsmomente geeignet sind, das für die Fortsetzung des Arbeitsverhältnisses erforderliche Vertrauen zu zerstören, und der

Arbeitgeber alle zumutbaren Anstrengungen zur Aufklärung des Sachverhalts unternommen, insbesondere dem Arbeitnehmer Gelegenheit zur Stellungnahme gegeben hat (st. Rspr., BAG 25. Oktober 2012 – 2 AZR 700/11 – Rn. 13; 24. Mai 2012 – 2 AZR 206/11 – Rn. 16). Der Verdacht muss auf konkrete – vom Kündigenden darzulegende und ggf. zu beweisende – Tatsachen gestützt sein. Der Verdacht muss ferner dringend sein. Es muss eine große Wahrscheinlichkeit dafür bestehen, dass er in der Sache zutrifft (BAG 25. Oktober 2012 – 2 AZR 700/11 – Rn. 14; 25. November 2010 – 2 AZR 801/09 – Rn. 17). Die Umstände, die ihn begründen, dürfen nach allgemeiner Lebenserfahrung nicht ebenso gut durch ein Geschehen zu erklären sein, das eine außerordentliche Kündigung nicht zu rechtfertigen vermöchte. Bloße, auf mehr oder weniger haltbare Vermutungen gestützte Verdächtigungen reichen dementsprechend zur Rechtfertigung eines dringenden Tatverdachts nicht aus (BAG 24. Mai 2012 – 2 AZR 206/11 – Rn. 17; 29. November 2007 – 2 AZR 724/06 – Rn. 30).

3. Die kündigungsrechtliche Beurteilung des in Rede stehenden Verhaltens hängt – auch soweit es Grundlage eines Verdachts ist – nicht von der strafrechtlichen Bewertung des mitgeteilten Kündigungssachverhalts ab. Entscheidend ist der mit dem Verhalten oder dem Verdacht einhergehende Vertrauensverlust (BAG 25. Oktober 2012 – 2 AZR 700/11 – Rn. 15; 24. Mai 2012 – 2 AZR 206/11 – Rn. 18; 25. November 2010 – 2 AZR 801/09 – Rn. 17).

4. Die Würdigung, ob dem Arbeitnehmer ein Vermögensdelikt zum Nachteil seines Arbeitgebers oder eine ähnlich schwerwiegende Pflichtverletzung anzulasten ist oder ob zumindest ein dahingehender, dringender Verdacht besteht, liegt im Wesentlichen auf tatsächlichem Gebiet und ist Gegenstand der tatrichterlichen Würdigung iSd. § 286 ZPO. Diese ist revisionsrechtlich nur daraufhin überprüfbar, ob das Berufungsgericht den Inhalt der Verhandlung berücksichtigt und alle erhobenen Beweise gewürdigt hat, ob eine Beweiswürdigung in sich widerspruchsfrei, ohne Verletzung von Denkgesetzen sowie allgemeinen Erfahrungssätzen erfolgt und ob sie rechtlich möglich ist (vgl. BAG 18. Oktober 2012 – 6 AZR 289/11 – Rn. 43; 24. Mai 2012 – 2 AZR 206/11 – Rn. 29).

5. Danach ist die fristlose Kündigung vom 17. März 2011 nicht deshalb gerechtfertigt, weil dem Kläger eine strafbare Handlung oder eine ähnlich schwerwiegende Pflichtverletzung zum Nachteil der Beklagten vorzuwerfen wäre.

a) Das Landesarbeitsgericht hat angenommen, ein solcher Tatvorwurf könne dem Kläger deshalb nicht gemacht werden, weil die Beklagte nicht nachgewiesen habe, dass er sich Waren aus ihrem Bestand tatsächlich angeeignet habe. Davon sei zwar auszugehen, falls am 4. März 2011 im Spind des Klägers Damenunterwäsche und zuvor im Mülleimer der Getränkeabteilung die dazugehörigen Preisetiketten gefunden worden sein sollten. Für ihr – vom Kläger bestrittenes – Vorbringen habe die Beklagte aber keinen geeigneten Beweis angeboten. Ihre Kenntnis vom Inhalt des Spinds beruhe auf einem unverhältnismäßigen und damit rechtswidrigen Eingriff in das allgemeine Persönlichkeitsrecht des Klägers. Das schließe die gerichtliche Beweiserhebung über das Ergebnis der Spindkontrolle aus.

b) Dagegen wendet sich die Beklagte ohne Erfolg. Die Würdigung des Landesarbeitsgerichts hält sich, was die für einen Tatnachweis vorgetragenen Indiztatsachen betrifft, im tatrichterlichen Beurteilungsspielraum. Sie verstößt nicht gegen Denkgesetze oder Erfahrungssätze. Das Landesarbeitsgericht hat § 286 ZPO auch nicht dadurch verletzt, dass es eine Beweiserhebung zum Ergebnis der Durchsuchung des Spinds unterlassen hat. Die darauf bezogene Rüge der Beklagten ist – ihre Zulässigkeit unterstellt – unbegründet (zu den Anforderungen an die Zulässigkeit einer Aufklärungsrüge vgl. BAG 23. April 2009 – 6 AZR 189/08 – Rn. 16, BAGE 130, 347). Die Verwertung von Beweismitteln, die die Beklagte aufgrund der in Abwesenheit des Klägers und insoweit für ihn heimlich erfolgten Durchsuchung gewonnen hat, ist im Streitfall ausgeschlossen. Dies folgt – sofern sich ein entsprechendes Verbot nicht bereits unmittelbar aus § 32 BDSG ergibt – daraus, dass mit der prozessualen Verwertung der Beweismittel durch Beweiserhebung ein – erneuter bzw. fortgesetzter – Eingriff in das allgemeine Persönlichkeitsrecht des Klägers einherginge, ohne dass ein solcher Eingriff durch überwiegende Interessen der Beklagten gerechtfertigt wäre. Das Verwertungsverbot impliziert ein Erhebungsverbot und schließt es aus, Personen, die die Schrankkontrolle selbst durchgeführt haben oder zu ihr hinzugezogen wurden, als Zeugen zu vernehmen (zum Beweiserhebungsverbot vgl. BAG 23. April 2009 – 6 AZR 189/08 – Rn. 26, a.a.O.; 10. Dezember 1998 – 8 AZR 366/97 – zu II 1 der Gründe).

aa) Die Zivilprozessordnung kennt für rechtswidrig erlangte Informationen oder Beweismittel kein – ausdrückliches – prozessuales Verwendungs- bzw. Verwertungsverbot. Aus § 286 ZPO i.V.m. Art. 103 Abs. 1 GG folgt im Gegenteil die grundsätzliche Verpflichtung der Gerichte, den von den Parteien vorgetragenen Sachverhalt und die von ihnen angebotenen Beweise zu berücksichtigen (BVerfG 9. Oktober 2002 – 1 BvR 1611/96 ua. – Rn. 60, BVerfGE 106, 28; BAG 13. Dezember 2007 – 2 AZR 537/06 – Rn. 37; 27. März 2003 – 2 AZR 51/02 – zu B I 3 b cc der Gründe, BAGE 105, 356). Dementsprechend bedarf es für die Annahme eines Beweisverwertungsverbots, das zugleich die Erhebung der angebotenen Beweise hindern soll, einer besonderen Legitimation in Gestalt einer gesetzlichen Grundlage (vgl. BAG 13. Dezember 2007 – 2 AZR 537/06 – a.a.O.; Musielak/Foerste ZPO 10. Aufl. § 284 Rn. 23; MünchKommZPO/Prütting 4. Aufl. § 284 Rn. 64).

bb) Im gerichtlichen Verfahren tritt der Richter den Verfahrensbeteiligten in Ausübung staatlicher Hoheitsgewalt gegenüber. Er ist daher nach Art. 1 Abs. 3 GG bei der Urteilsfindung an die insoweit maßgeblichen Grundrechte gebunden und zu einer rechtsstaatlichen Verfahrensgestaltung verpflichtet (BVerfG 13. Februar 2007 – 1 BvR 421/05 – Rn. 93 mwN, BVerfGE 117, 202). Dabei können sich auch aus materiellen Grundrechten wie Art. 2 Abs. 1 GG Anforderungen an das gerichtliche Verfahren ergeben, wenn es um die Offenbarung und Verwertung von persönlichen Daten geht, die grundrechtlich vor der Kenntnis durch Dritte geschützt sind (BVerfG 13. Februar 2007 – 1 BvR 421/05 – Rn. 94 mwN, a.a.O.). Das Gericht hat deshalb zu prüfen, ob die Verwertung von heimlich beschafften persönlichen Daten und Erkenntnissen, die sich aus diesen Daten ergeben, mit dem allgemeinen Persönlichkeitsrecht des Betroffenen vereinbar ist (BVerfG 13. Februar 2007 – 1 BvR 421/05 – a.a.O.; BGH 15. Mai 2013 – XII ZB 107/08 – Rn. 21). Dieses Recht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen des Einzelnen Rechnung (BVerfG 11. März 2008 – 1 BvR 2074/05 ua. – BVerfGE 120, 378; BAG 21. Juni 2012 – 2 AZR 153/11 – Rn. 28). Es gewährleistet die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Diesem Schutz dient auch Art. 8 Abs. 1 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) (BGH 15. Mai 2013 – XII ZB 107/08 – Rn. 14).

cc) Die gesetzlichen Anforderungen an eine zulässige Datenverarbeitung im BDSG konkretisieren und aktualisieren den Schutz des Rechts auf informationelle Selbstbestimmung und regeln, in

welchem Umfang im Anwendungsbereich des Gesetzes Eingriffe in dieses Recht zulässig sind (vgl. für das Datenschutzgesetz NRW BAG 15. November 2012 – 6 AZR 339/11 – Rn. 16). Dies stellt § 1 BDSG ausdrücklich klar. Liegt keine Einwilligung des Betroffenen vor, ist die Datenverarbeitung nach dem Gesamtkonzept des BDSG nur zulässig, wenn eine verfassungsgemäße Rechtsvorschrift diese erlaubt. Fehlt es an der danach erforderlichen Ermächtigungsgrundlage oder liegen deren Voraussetzungen nicht vor, ist die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten verboten. Dieser das deutsche Datenschutzrecht prägende Grundsatz ist in § 4 Abs. 1 BDSG kodifiziert (Gola/Schomerus BDSG 11. Aufl. § 4 Rn. 3; ErfK/Franzen 13. Aufl. § 4 BDSG Rn. 1; Simitis/Sokol BDSG 7. Aufl. § 4 Rn. 1).

dd) Gemäß der – zum 1. September 2009 in Kraft getretenen und damit im Streitfall anwendbaren – Bestimmung des § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach dessen Begründung für seine Durchführung oder Beendigung erforderlich ist. Nach Abs. 1 Satz 2 der Regelung dürfen zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten am Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

ee) Es spricht viel dafür, dass es sich bei der in Rede stehenden Schrankkontrolle tatbestandlich um eine Datenerhebung iSv. § 32 Abs. 1 BDSG handelt (so Brink in jurisPR-ArbR 20/2013). Nach der Begriffsbestimmung in § 3 Abs. 1 Satz 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Um die Gewinnung und Verwertung solcher Daten geht es hier. Die Durchsuchung des dem Kläger zugeordneten Spinds hatte zum Ziel, Erkenntnisse über dessen Inhalt zu gewinnen, um festzustellen, ob der Kläger im Besitz nicht bezahlter Waren aus dem Bestand der Beklagten war. § 32 BDSG setzt nicht voraus, dass die Datenerhebung zum Zwecke ihrer Nutzung und Verarbeitung in automatisierten Dateien erfolgt. Durch § 32 Abs. 2 BDSG wird die grundsätzliche Beschränkung der Anwendung des dritten Abschnitts des BDSG auf dateigebundene bzw. automatisierte Verarbeitungen (§ 1 Abs. 2 Nr. 2, § 27 Abs. 1 BDSG) ausdrücklich aufgehoben. Die Vorschrift erfasst damit sowohl nach ihrem Wortlaut als auch nach ihrem Regelungsgehalt die Datenerhebung durch rein tatsächliche Handlungen (Gola/Schomerus BDSG 11. Aufl. § 32 Rn. 7; ErfK/Franzen 13. Aufl. § 32 BDSG Rn. 2; Simitis/Seifert BDSG 7. Aufl. § 32 Rn. 14, 100).

ff) Im Streitfall kann offen bleiben, ob § 32 BDSG einschlägig ist. Für die Prüfung der Verhältnismäßigkeit der Durchsuchung des Spinds ergeben sich aus § 32 Abs. 1 Satz 2 BDSG gegenüber einer unmittelbar an Art. 2 Abs. 1 GG orientierten Überprüfung der Rechtmäßigkeit des Eingriffs in das Persönlichkeitsrecht des Klägers keine anderen Vorgaben. Entsprechendes gilt mit Blick auf die Frage, ob der durch § 32 BDSG oder unmittelbar durch Art. 2 Abs. 1 GG gewährleistete Schutz des Persönlichkeitsrechts die prozessuale Verwertung der durch die Spindkontrolle gewonnenen Erkenntnisse und Beweismittel ausschließt. Auf die im Schrifttum umstrittene Frage, ob § 32 BDSG der Durchführung rein präventiver Kontrollen entgegensteht (zum Meinungsstand ErfK/Franzen 13. Aufl. § 32 BDSG Rn. 7; Gola/Schomerus BDSG 11. Aufl. § 43 Rn. 7), kommt es nicht an. Um eine solche Maßnahme handelt es sich hier nicht.

(1) Nach der Gesetzesbegründung sollte die Regelung des § 32 BDSG die bislang von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen. § 32 Abs. 1 Satz 2 BDSG orientiert sich im Wortlaut an § 100 Abs. 3 Satz 1 TKG und inhaltlich an den Anforderungen, die das Bundesarbeitsgericht ua. in seinem Urteil vom 27. März 2003 (– 2 AZR 51/02 – BAGE 105, 356) zur verdeckten Überwachung von Beschäftigten aufgestellt hat (vgl. BT-Drucks. 16/13657, S. 21). Dementsprechend setzt § 32 Abs. 1 Satz 2 BDSG voraus, dass die Erhebung, Verarbeitung und Nutzung der Daten zur „Aufdeckung [einer Straftat] erforderlich ist". Das verlangt eine am Verhältnismäßigkeitsprinzip orientierte, die Interessen des Arbeitgebers und des Beschäftigten berücksichtigende Abwägung im Einzelfall, so wie sie ua. bei der heimlichen Videoüberwachung eines Arbeitnehmers vorzunehmen ist (statt vieler: Thüsing Anm. zu BAG 21. Juni 2012 – 2 AZR 153/11 – EzA BGB 2002 § 611 Persönlichkeitsrecht Nr. 13; Wybitul BB 2010, 2235; zur Videoüberwachung BAG 21. Juni 2012 – 2 AZR 153/11 – Rn. 30; 27. März 2003 – 2 AZR 51/02 – zu B I 3 b dd (1) der Gründe, a.a.O.). Auch körperliche und sonstige Untersuchungen wie die Kontrolle des persönlichen Schranks des Arbeitnehmers, mitgeführter Taschen oder von Kleidungsstücken stellen grundsätzlich einen Eingriff in das Persönlichkeitsrecht des Arbeitnehmers dar. Da das Persönlichkeitsrecht im Arbeitsverhältnis – jedenfalls außerhalb des unantastbaren Kernbereichs privater Lebensführung – nicht schrankenlos gewährleistet ist, können solche Eingriffe aufgrund überwiegender schutzwürdiger Interessen des Arbeitgebers gerechtfertigt sein. Das ist im Rahmen einer Güterabwägung festzustellen (BAG 13. Dezember 2007 – 2 AZR 537/06 – Rn. 35, 36). Mitentscheidend ist die Intensität des Eingriffs (ErfK/Schmidt 13. Aufl. Art. 2 GG Rn. 100). In diesem Zusammenhang gibt auch das Unionsrecht nichts anderes vor (vgl. BAG 21. Juni 2012 – 2 AZR 153/11 – Rn. 43).

(2) Der persönliche Schrank eines Arbeitnehmers und dessen Inhalt sind Teil der Privatsphäre. Sie sind gleichwohl nicht unter allen Umständen einer Kontrolle durch den Arbeitgeber entzogen. Betroffen ist nicht der absolut geschützte Kernbereich privater Lebensgestaltung, sondern der nur relativ geschützte Bereich des allgemeinen Persönlichkeitsrechts (zur Abgrenzung vgl. BVerfG 14. September 1989 – 2 BvR 1062/87 – BVerfGE 80, 367; vgl. auch BAG 29. Juni 2004 – 1 ABR 21/03 – zu B I 2 c der Gründe, BAGE 111, 173). Stellt der Arbeitgeber dem Arbeitnehmer – ggf. zur Erfüllung seiner Verpflichtungen aus § 6 Abs. 2 ArbStättV i.V.m. Nr. 4.1 Abs. 3 des Anhangs – einen abschließbaren Schrank zur Verfügung, berührt diese Überlassung auch seine eigenen Belange. Zum einen besteht die Möglichkeit, dass ein Arbeitnehmer den Spind nicht bestimmungsgemäß nutzt, möglicherweise darin Gegenstände aufbewahrt, von denen Gefahren ausgehen, die der Arbeitgeber abzuwenden verpflichtet ist. Zum anderen kann es das Vorhandensein von Orten, auf die der Arbeitgeber keinen Zugriff hat, böswilligen Arbeitnehmern erleichtern, Handlungen zum Nachteil des Arbeitgebers oder anderer Mitarbeiter zu begehen. Dass dies u.U. Kontrollen des Arbeitgebers erforderlich machen kann, muss einem Arbeitnehmer bewusst sein.

(3) Arbeitnehmer müssen gleichwohl darauf vertrauen können, dass ihnen zugeordnete Schränke nicht ohne ihre Einwilligung geöffnet, dort eingebrachte persönliche Sachen nicht ohne ihr

Einverständnis durchsucht werden. Geschieht dies dennoch, liegt regelmäßig ein schwerwiegender Eingriff in ihre Privatsphäre vor. Er kann nur bei Vorliegen zwingender Gründe gerechtfertigt sein. Bestehen konkrete Anhaltspunkte für eine Straftat und zählt der Arbeitnehmer zu dem anhand objektiver Kriterien eingegrenzten Kreis der Verdächtigen, kann sich zwar aus dem Arbeitsvertrag i.V.m. § 242 BGB eine Verpflichtung ergeben, Aufklärungsmaßnahmen zu dulden (ErfK/Schmidt 13. Aufl. Art. 2 GG Rn. 100). Erforderlich iSd. § 32 Abs. 1 Satz 2 BDSG bzw. verhältnismäßig im Sinne einer Beschränkung des allgemeinen Persönlichkeitsrechts kann eine Schrankkontrolle aber nur sein, wenn sie geeignet, erforderlich und angemessen ist. Dem Arbeitgeber dürfen keine ebenso effektiven, den Arbeitnehmer weniger belastenden Möglichkeiten zur Aufklärung des Sachverhalts zur Verfügung stehen. Außerdem muss die Art und Weise der Kontrolle als solche den Verhältnismäßigkeitsgrundsatz wahren.

(4) Sowohl die Gerichte für Arbeitssachen als auch die ordentlichen Gerichte sind befugt, Erkenntnisse zu verwerten, die sich eine Prozesspartei durch Eingriffe in das allgemeine Persönlichkeitsrecht verschafft hat, wenn eine Abwägung der beteiligten Belange ergibt, dass das Interesse an einer Verwertung der Beweise trotz der damit einhergehenden Rechtsverletzung das Interesse am Schutz der Daten überwiegt. Das allgemeine Interesse an einer funktionstüchtigen Rechtspflege und das Interesse, sich ein Beweismittel für zivilrechtliche Ansprüche zu sichern, reichen dabei für sich betrachtet nicht aus, dem Verwertungsinteresse den Vorzug zu geben (BAG 21. Juni 2012 – 2 AZR 153/11 – Rn. 29). Dafür bedarf es zusätzlicher Umstände. Sie können etwa darin liegen, dass sich der Beweisführer mangels anderer Erkenntnisquellen in einer Notwehrsituation oder einer notwehrähnlichen Lage befindet (BAG 13. Dezember 2007 – 2 AZR 537/06 – Rn. 36; BGH 15. Mai 2013 – XII ZB 107/08 – Rn. 22; jeweils mwN). Die besonderen Umstände müssen gerade die in Frage stehende Informationsbeschaffung und Beweiserhebung als gerechtfertigt ausweisen (BVerfG 9. Oktober 2002 – 1 BvR 1611/96, 1 BvR 805/98 – zu C II 4 a der Gründe, BVerfGE 106, 28; BAG 21. Juni 2012 – 2 AZR 153/11 – a.a.O.).

gg) Nach diesen Grundsätzen ist die vom Landesarbeitsgericht vorgenommene Interessenabwägung fehlerfrei. Zugunsten der Beklagten kann unterstellt werden, dass zum Zeitpunkt der Schrankkontrolle ein durch objektive – im Anwendungsbereich des § 32 Abs. 1 Satz 2 BDSG zu dokumentierende – Tatsachen begründeter Verdacht gegen den Kläger bestand, sich Unterwäsche aus dem Bestand der Beklagten rechtswidrig zugeeignet oder zu einer solchen Tat zumindest unmittelbar angesetzt zu haben. Der Eingriff erweist sich auch dann als unverhältnismäßig. Die Beklagte hätte den Kläger zur Kontrolle seines Schranks hinzuziehen müssen. Ein Grund, der unter Berücksichtigung der Intensität des Eingriffs eine „heimliche“ Durchsuchung hätte rechtfertigen können, liegt nicht vor.

(1) Eine in Anwesenheit des Arbeitnehmers durchgeführte Schrankkontrolle ist gegenüber einer heimlichen Durchsuchung das mildere Mittel. Die Kontrolle in seinem Beisein gibt dem Arbeitnehmer nicht nur die Möglichkeit, auf die Art und Weise ihrer Durchführung Einfluss zu nehmen. Er kann sie u.U. – etwa durch freiwillige Herausgabe gesuchter Gegenstände – sogar ganz abwenden. Die verdeckte Ermittlung führt ferner dazu, dass dem Betroffenen vorbeugender Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erschwert wird. Die Heimlichkeit einer in Grundrechte eingreifenden Maßnahme erhöht typischerweise das Gewicht der Freiheitsbeeinträchtigung (BAG 26. August 2008 – 1 ABR 16/07 – Rn. 21 mwN, BAGE 127, 276).

(2) Die Beklagte hat keine Umstände vorgetragen, aus denen sich ergäbe, dass eine Kontrolle im Beisein des Klägers gegenüber der heimlichen weniger effektiv gewesen wäre. Zwar mögen „ertappte“ Arbeitnehmer im Falle offener Kontrollen einwenden können, sie hätten die bei ihnen aufgefundene, unbezahlte Ware vor Verlassen des Betriebs noch bezahlen wollen. Eine solche Einlassung ist aber auch bei heimlich durchgeführter Kontrolle nicht auszuschließen. Im Streitfall kommt – ausgehend vom eigenen Vorbringen der Beklagten – hinzu, dass die Etiketten der im Besitz des Klägers vermuteten Unterwäsche im Abfall der Getränkeabteilung gefunden worden waren. Dies hätte – als wahr unterstellt – eine (mögliche) Behauptung des Klägers, er habe die in seinem Spind gefundene Ware noch bezahlen wollen, ohne weiteres als Schutzbehauptung entlarvt. Das gilt erst recht, wenn im Betrieb die Anweisung bestanden haben sollte, keinerlei für den Verkauf bestimmte Ware im Spind aufzubewahren. Dagegen kann die Beklagte nicht erfolgreich einwenden, in ihren Märkten würden gelegentlich auch nicht ausgezeichnete Waren zum Verkauf angeboten. Darauf musste es dem Landesarbeitsgericht in Anbetracht des von der Beklagten unterbreiteten Geschehensablaufs nicht ankommen. Aus diesem Grund ist auch die von der Beklagten im vorliegenden Zusammenhang erhobene Rüge, das Landesarbeitsgericht habe gegen seine Hinweispflicht verstoßen, nicht berechtigt.

(3) Es kann dahinstehen, ob schon diese Begründung des Landesarbeitsgerichts seine Entscheidung trägt. Die Schrankkontrolle erweist sich jedenfalls mit Blick auf die beabsichtigte anschließende Taschen-/Personenkontrolle als unverhältnismäßig. Mit seiner entsprechenden Würdigung hat das Landesarbeitsgericht nicht, wie die Beklagte offenbar meint, eine allgemeine, gegenüber einer Vielzahl von Arbeitnehmern angeordnete Taschenkontrolle oder eine Videoüberwachung als „milderes Mittel“ angesehen. Es hat einen überschießenden Eingriff in das Persönlichkeitsrecht des Klägers vielmehr darin erblickt, dass die heimliche Schrankkontrolle lediglich der Vorbereitung einer geplanten Taschenkontrolle diente und deshalb nicht zwingend erforderlich war. Die Würdigung ist rechtsfehlerfrei. Die Beklagte hat selbst vorgetragen, sie habe abwarten wollen, ob der Kläger die Ware bis Dienstschluss noch bezahle. Dies kann nur so verstanden werden, dass auch sie selbst – aus der maßgebenden Sicht ex ante – in der Ausgangskontrolle das effektivere Mittel erblickt hatte, den Kläger zu überführen. Die Schrankdurchsuchung sollte lediglich dazu dienen, die Grundlage für eine passgenaue Taschenkontrolle zu schaffen. Das reicht nicht aus, um den mit der verdeckten Durchsuchung verbundenen intensiven Eingriff in das Persönlichkeitsrecht zu rechtfertigen. Dies gilt ungeachtet dessen, dass Arbeitnehmer in großen Einkaufsmärkten während der Geschäftszeiten in aller Regel – so auch hier – mehrere Möglichkeiten haben, den Arbeitsplatz zu verlassen. Die Beklagte hat nicht dargelegt, weshalb sie den sich daraus ergebenden Schwierigkeiten nicht durch eine intensivere Beobachtung des Klägers hätte begegnen können. Eine plausible Begründung dafür, dass sie nicht den Kündigungssachverhalt ebensogut durch eine (Personen-)Kontrolle des Klägers beim Verlassen des Marktes und ggf. eine anschließende – offene – Schrankkontrolle hätte aufklären können, hat sie nicht gegeben.

(4) Zu Unrecht meint die Beklagte, ihr müsse hinsichtlich mehrerer zur Verfügung stehender Aufklärungsmöglichkeiten ein Bewertungsspielraum zugebilligt werden; nicht jeder „Fehlgriff“ dürfe zur Unverhältnismäßigkeit der gewählten Maßnahme führen. Es ist stattdessen nicht Sache des Arbeitgebers, die Grenzen zu bestimmen, innerhalb derer Arbeitnehmer Schutz vor Eingriffen in ihr Persönlichkeitsrecht beanspruchen können. Wie Sachverhalte zu beurteilen sind, bei denen der Arbeitgeber unter mehreren gleich effektiven Aufklärungsmaßnahmen diejenige ergreift, die

den Arbeitnehmer – geringfügig – stärker belastet, bedarf keiner Entscheidung; so liegt der Streitfall nicht.

(5) Die – bestrittene – Behauptung der Beklagten, ihre Vorgehensweise sei mit zwei Mitgliedern des Betriebsrats abgestimmt gewesen, von denen eines an der Kontrolle teilgenommen habe, rechtfertigt kein anderes Ergebnis. Aus persönlichkeitsrechtlicher und datenschutzrechtlicher Sicht ist der Eingriff deshalb nicht weniger intensiv. Vielmehr ist davon auszugehen, dass die Privatsphäre des Arbeitnehmers umso stärker verletzt wird, je mehr Personen ohne sein Einverständnis an dem Eingriff beteiligt sind (vgl. Brink jurisPR-ArbR 20/2013).

(6) Eine Beweiserhebung über das Ergebnis der Schrankdurchsuchung war deshalb ausgeschlossen. Dies gilt auch dann, wenn sich der Kläger am 4. März 2011 – wie von der Beklagten behauptet – einer Ausgangskontrolle bewusst entzogen haben sollte. Dies ändert nichts an der Unverhältnismäßigkeit der von der Beklagten ergriffenen Aufklärungsmaßnahmen.

hh) Auf die Frage, ob Personalaufenthaltsräume einschließlich dort vorhandener Schränke als „Wohnung" iSv. Art. 13 GG zu qualifizieren sind (bejahend für nicht allgemein zugängliche Personalaufenthaltsräume Papier in Maunz/Dürig <2013> Art. 13 GG Rn. 11) und ob die Erkenntnisse aus einer heimlichen Schrankdurchsuchung durch den Arbeitgeber auch mit Blick auf Art. 13 Abs. 2 GG, § 105 Abs. 1 Satz 1 StPO einem Verwertungsverbot unterliegen, kommt es nicht an. Ebenso wenig braucht der Frage nachgegangen zu werden, ob die Beklagte ihre Erkenntnisse aus der Schrankkontrolle mitbestimmungswidrig erlangt hat (zur Problematik vgl. BAG 13. Dezember 2007 – 2 AZR 537/06 – Rn. 26).

6. Auch wenn die Beklagte den Beweis fällig geblieben ist, dass der Kläger tatsächlich Unterwäsche entwendet hat, folgt daraus nicht notwendig, dass ein wichtiger Grund zur Kündigung i.S.d. § 626 Abs. 1 BGB nicht vorliegt. Die Beklagte hat die Kündigung auch auf den Verdacht der rechtswidrigen Entwendung gestützt. Dies war ihr prozessual – anders als das Landesarbeitsgericht angenommen hat – nicht deshalb verwehrt, weil sie den Betriebsrat zu diesem Kündigungsgrund nicht ordnungsgemäß angehört hätte. Zum einen ist auf der Grundlage der bisherigen Feststellungen des Landesarbeitsgerichts davon auszugehen, dass der Betriebsrat erkennen konnte, er solle auch zu einer Verdachtskündigung angehört werden. Zum anderen setzt die gerichtliche Würdigung, der Arbeitgeber sei mangels Anhörung des Betriebsrats gehindert, sich auf bestimmte Kündigungsgründe zu berufen, voraus, dass die Parteien über die ordnungsgemäße Beteiligung des Betriebsrats überhaupt streiten. Daran fehlt es hier.

a) Nach § 102 Abs. 1 BetrVG ist der Betriebsrat vor jeder Kündigung zu hören. Eine ohne Anhörung ausgesprochene Kündigung ist unwirksam. Dabei steht die nicht ordnungsgemäße Anhörung der unterbliebenen gleich (BAG 22. April 2010 – 2 AZR 991/08 – Rn. 13 mwN). Im Falle der auf einen bloßen Verdacht gestützten Kündigung zählt zur ordnungsgemäßen Unterrichtung des Betriebsrats über die Kündigungsgründe die Mitteilung, das Arbeitsverhältnis solle gerade (auch) deshalb gekündigt werden, weil der Arbeitnehmer eines bestimmten rechtswidrigen Verhaltens dringend verdächtig sei. Eine solche Mitteilung gibt dem Betriebsrat weit stärkeren Anlass für ein umfassendes Tätigwerden im Anhörungsverfahren als eine Unterrichtung wegen einer als erwiesen dargestellten Handlung (vgl. BAG 27. Januar 2011 – 2 AZR 825/09 – Rn. 28, BAGE 137, 54; 3. April 1986 – 2 AZR 324/85 – zu II 1 c cc der Gründe).

b) Hat der Arbeitgeber dem Betriebsrat mitgeteilt, er beabsichtige, das Arbeitsverhältnis wegen einer nach dem geschilderten Sachverhalt für erwiesen erachteten Handlung zu kündigen, und stützt er die Kündigung im Prozess bei unverändert gebliebenem Sachverhalt auch darauf, der Arbeitnehmer sei dieser Handlung zumindest verdächtig, so ist er mit dem Kündigungsgrund des Verdachts wegen fehlender Anhörung des Betriebsrats ausgeschlossen (BAG 3. April 1986 – 2 AZR 324/85 – zu II 1 c der Gründe; vgl. auch BAG 23. Februar 2010 – 2 AZR 804/08 – Rn. 24; 11. Dezember 2003 – 2 AZR 536/02 – Rn. 27).

c) Nach den im angefochtenen Urteil getroffenen Feststellungen wurde der Betriebsrat über die Absicht der Beklagten, eine Kündigung auch wegen des Verdachts eines pflichtwidrigen Verhaltens des Klägers auszusprechen, ausreichend unterrichtet. Die gegenteilige Würdigung des Landesarbeitsgerichts lässt wesentliche Umstände, die für die Auslegung der Anhörung von Bedeutung sind, außer Acht.

aa) Die Beklagte hat sich im Anhörungsschreiben vom 15. März 2011 für die Darstellung der Kündigungsgründe auf ein Protokoll vom 7. März 2011 bezogen. Darin heißt es einleitend, der Kläger habe seit längerer Zeit „unter Verdacht des Diebstahls" gestanden. Es folgt eine Darstellung tatsächlicher Ereignisse, die sich am 4. März 2011 zugetragen haben sollen, ohne dass die Geschehnisse einer Beurteilung dahingehend unterzogen würden, ob sie den Verdacht aus Sicht der Beklagten endgültig bestätigt oder nur erhärtet haben. Unter diesen Umständen bedarf es für die Annahme, die Beklagte habe ihren Kündigungsentschluss ausschließlich mit einer nachgewiesenen Tat und nicht (auch) mit dem bloßen Verdacht der in Rede stehenden Pflichtwidrigkeit des Klägers begründen wollen, besonderer Anhaltspunkte.

bb) Solche Anhaltspunkte sind nicht ersichtlich, insbesondere dann nicht, wenn der Betriebsrat im Anhörungszeitpunkt auch vom Inhalt eines Gesprächsprotokolls vom 14. März 2011 Kenntnis hatte, wie vom Landesarbeitsgericht zugunsten der Beklagten unterstellt. Sowohl der in dem Protokoll angegebene Betreff „Verdacht des Diebstahls" als auch der darin enthaltene Hinweis auf die Anhörung des Klägers zu einem gegen ihn gerichteten entsprechenden Verdacht legen vielmehr den Schluss nahe, dass die Beklagte trotz des Ergebnisses ihrer Ermittlungen weiterhin nur von einem – wenngleich verfestigten – Diebstahlsverdacht ausging.

d) Im Ergebnis kommt es hierauf nicht an. Über die Anhörung des Betriebsrats streiten die Parteien nicht mehr.

aa) Hat sich der Arbeitnehmer rechtzeitig iSv. §§ 4, 6 KSchG auf eine Unwirksamkeit der Kündigung nach § 102 Abs. 1 Satz 3 BetrVG berufen, ist es Sache des Arbeitgebers, im Prozess die ordnungsgemäße Anhörung des Betriebsrats darzulegen und ggf. zu beweisen. Das betreffende Vorbringen des Arbeitgebers hat das mit der Sache befasste Gericht grundsätzlich selbst dann auf seine Schlüssigkeit hin zu überprüfen, wenn der Arbeitnehmer ihm im weiteren Verlauf des Prozesses nicht nochmals entgegengetreten ist (BAG 24. Mai 2012 – 2 AZR 206/11 – Rn. 49).

bb) Das gilt jedoch nicht, wenn der Arbeitnehmer deutlich zum Ausdruck gebracht hat, dass er an der betriebsverfassungsrechtlichen Rüge als solcher nicht mehr festhalte. Dann ist die Wirksamkeit der Kündigung unter dem Aspekt des § 102 Abs. 1 BetrVG nicht zu überprüfen (BAG 24. Mai 2012 – 2 AZR 206/11 – Rn. 50). Zwar führt die Rüge des Arbeitnehmers, die Kündigung sei auch aus einem anderen Grund als dem der Sozialwidrigkeit unwirksam, nicht zu einem Wechsel des Streitgegenstands, sondern nur zu einer Erweiterung des Sachvortrags im Kündigungsschutzprozess (BAG 18. Januar 2012 – 6 AZR 407/10 – Rn. 26 mwN, BAGE 140, 261). Die Regelung des § 6 KSchG ist aber Beleg dafür, dass der Arbeitnehmer über die Einführung der Unwirksamkeitsgründe frei

entscheiden und den Prozessstoff insoweit von vorneherein begrenzen oder in den zeitlichen Grenzen des § 6 Satz 1 KSchG erweitern kann. Das gilt über § 13 Abs. 1 Satz 2 KSchG für die außerordentliche Kündigung entsprechend.

cc) Unterliegt es in diesem rechtlichen Rahmen der Disposition des Arbeitnehmers, den Umfang der gerichtlichen Überprüfung einer Kündigung zu bestimmen, ist regelmäßig davon auszugehen, dass sich der Prozessstoff entsprechend reduziert, falls der Arbeitnehmer im Verlauf des Rechtsstreits zweifelsfrei zu erkennen gibt, sich auf bestimmte, rechtlich eigenständige Unwirksamkeitsgründe nicht (mehr) berufen zu wollen (vgl. BAG 24. Mai 2012 – 2 AZR 206/11 – Rn. 50). An eine solche Beschränkung des Sachvortrags, die grundsätzlich bis zum Schluss der mündlichen Verhandlung in zweiter Instanz möglich ist, sind die Gerichte selbst dann gebunden, wenn sich aus dem eigenen Vorbringen des Arbeitgebers Zweifel hinsichtlich der Wirksamkeit der Kündigung unter dem betreffenden Gesichtspunkt ergeben.

dd) Danach ist die ordnungsgemäße Anhörung des Betriebsrats hier nicht mehr Streitstoff. Der Kläger hat auf Seite 21 seines – erstinstanzlichen – Schriftsatzes vom 8. August 2011 ausgeführt: „Die Rüge, dass der Betriebsrat nicht ordnungsgemäß angehört wurde, bleibt nicht aufrechterhalten". Die sich daraus ergebende Beschränkung des Prozessstoffs hat nicht nur mit Blick auf den Unwirksamkeitsgrund des § 102 Abs. 1 Satz 3 BetrVG als solchen Bedeutung. Sie verbietet es zugleich, bei der materiell-rechtlichen Überprüfung der Wirksamkeit der Kündigung den von der Beklagten geltend gemachten Verdacht außer Acht zu lassen, selbst wenn er dem Betriebsrat nicht explizit als Kündigungsgrund unterbreitet worden sein sollte.

(1) Das sich aus einer unvollständigen Unterrichtung des Betriebsrats ergebende Verbot der Berücksichtigung nicht mitgeteilter Kündigungsgründe dient der Absicherung der Beteiligungsrechte aus § 102 BetrVG. Der Betriebsrat soll Gelegenheit haben, im Vorfeld der Kündigung auf die Willensbildung des Arbeitgebers Einfluss zu nehmen und sein Widerspruchsrecht auszuüben (vgl. BAG 13. Dezember 2012 – 6 AZR 608/11 – Rn. 75; 22. September 1994 – 2 AZR 31/94 – zu II 2 der Gründe, BAGE 78, 39). Dem widerspräche es, wenn sich der Arbeitgeber im Kündigungsschutzprozess auf Kündigungsgründe berufen könnte, zu denen Stellung zu nehmen der Betriebsrat keine Gelegenheit hatte.

(2) Auf ein – betriebsverfassungsrechtlich begründetes – Verbot der Verwertung von Sachvortrag kommt es nur an, wenn sich die Frage nach einer ordnungsgemäßen Anhörung des Betriebsrats überhaupt stellt. Erklärt der Arbeitnehmer ausdrücklich, er erhebe insoweit keine Rüge, gibt er zu erkennen, dass die ordnungsgemäße Beteiligung der Arbeitnehmervertretung für den Kündigungsrechtsstreit keine Rolle spielen soll. Der Arbeitgeber hat dann keine Veranlassung (mehr), entsprechenden Vortrag zu leisten oder doch zu vertiefen und/oder entsprechende Beweise zu sichern (vgl. BAG 23. Februar 2010 – 2 AZR 804/08 – Rn. 24).

(3) Ob der Arbeitnehmer den Prozessstoff auch in der Weise einschränken kann, dass er zwar den Unwirksamkeitsgrund des § 102 Abs. 1 Satz 3 BetrVG nicht geltend machen wolle, wohl aber mögliche Folgen, die sich aus einer objektiv unvollständigen Anhörung für die Beachtlichkeit von Kündigungsgründen im Prozess ergeben, bedarf keiner Entscheidung. Für eine solche Differenzierung gibt die Erklärung des Klägers nichts her.

II. Der Rechtsfehler führt zur Aufhebung des Berufungsurteils und zur Zurückverweisung der Sache an das Landesarbeitsgericht. Dessen Entscheidung stellt sich nicht aus anderen Gründen als richtig dar (§ 561 ZPO). Der Rechtsstreit ist nicht zur Endentscheidung reif (§ 563 Abs. 3 ZPO).

1. Dem Feststellungsbegehren des Klägers kann nicht deshalb stattgegeben werden, weil das Vorbringen der Beklagten, aus dem sie einen schwerwiegenden, die außerordentliche Kündigung tragenden Verdacht gegen ihn herleiten will, dafür gänzlich untauglich wäre.

2. Ein anderer Grund, der der Wirksamkeit der fristlosen Kündigung entgegenstünde, ist auf der Grundlage der bisherigen Feststellungen des Landesarbeitsgerichts ebenso wenig erkennbar. Es fehlt für eine Wirksamkeit der Verdachtskündigung nicht an der erforderlichen vorhergehenden Anhörung des Klägers. Die Beklagte hatte ihm mit Schreiben vom 5. März 2011 unter Bezug auf eine von ihr erstattete Strafanzeige mitgeteilt, er stehe im Verdacht, am 4. März 2011 Unterwäsche „entnommen" und diese nach Feierabend „ohne Bezahlung mitgenommen" zu haben. Sie hatte ihn für den 11. März 2011 zu einem Gespräch darüber geladen. Hilfsweise hatte sie ihm für eine schriftliche Äußerung eine Frist bis zum 14. März 2011 gesetzt. Sie hatte ihn in einem Gespräch am 14. März 2011 nochmals mit den Vorwürfen konfrontiert und ihm erneut Gelegenheit zur Äußerung gegeben. Der Kläger lehnte eine konkrete Stellungnahme zu den Vorwürfen ab. Danach ist die Beklagte – auch angesichts der zeitweiligen Erkrankung des Klägers – ihrer Verpflichtung zur Anhörung hinreichend nachgekommen. Die Zweiwochenfrist des § 626 Abs. 2 BGB ist gewahrt.

3. Über die materielle Berechtigung der Verdachtskündigung kann der Senat nicht abschließend entscheiden. Das Landesarbeitsgericht hat insoweit – aus seiner Sicht folgerichtig – keine zureichenden Feststellungen getroffen. Dies wird es – unter der Fragestellung, ob die von der Beklagten vorgebrachten Tatsachen auch ohne das Ergebnis der Schrankkontrolle den dringenden Verdacht begründen, der Kläger habe ein Vermögensdelikt zu ihrem Nachteil begangen – nachzuholen haben. Sollte es auf die vorsorglich erklärte ordentliche Kündigung ankommen, wird das Landesarbeitsgericht davon ausgehen müssen, dass auch diese nicht wegen erwiesener Tat gerechtfertigt ist. Insoweit gelten die Ausführungen zur fristlosen Kündigung gleichermaßen.

Keine AGG-Entschädigungsansprüche gegenüber Personalvermittler (Ls)

(**Bundesarbeitsgericht**, Urteil vom 23. Januar 2013 – 8 AZR 118/13 –)

Ansprüche auf Entschädigung bei Verstößen gegen das Allgemeine Gleichbehandlungsgesetz (AGG) nach § 15 Abs. 2 müssen gegen den Arbeitgeber gerichtet werden. Wird bei der Ausschreibung von Stellen ein Personalvermittler eingeschaltet, haftet dieser für solche Ansprüche nicht.

(Nicht amtlicher Leitsatz)

Unzulässige Androhung einer Datenübermittlung an die Schufa

(**Oberlandesgericht Celle**, Urteil vom 19. Dezember 2013 – 13 U 64/13 –)

1. Die Inaussichtstellung einer Datenübermittlung an die Schufa Holding AG kann unzulässig sein, wenn sie keinen

gesetzlich vorgesehenen Zweck erfüllt, insbesondere weil der vermeintliche Schuldner die Forderung bereits bestritten hat.

2. Der Hinweis auf die Möglichkeit einer solchen Datenübermittlung begründet trotz eines Zusatzes, dass eine Übermittlung nur bei einredefreien und unbestrittenen Forderungen erfolgen wird, insbesondere dann eine Erstbegehungsgefahr, wenn der vermeintliche Schuldner die Forderung zuvor schriftlich bestritten und das Inkassounternehmen aufgefordert hat, weitere Drohungen mit einer Datenübermittlung zu unterlassen.

Aus den Gründen:

2. Dem Kläger steht ein Anspruch aus einer entsprechenden Anwendung der §§ 12, 823 Abs. 1, 1004 BGB i. V. m. Art. 1, 2 GG gegenüber der Beklagten zu, es zu unterlassen, seine Daten an die Schufa Holding AG weiterzuleiten.

a) Eine solche Weiterleitung würde den Kläger bei der derzeitigen Sachlage widerrechtlich in seinem allgemeinen Persönlichkeitsrecht verletzen.

Eine durch das Bundesdatenschutzgesetz nicht gedeckte Übermittlung personenbezogener Daten stellt eine Verletzung des allgemeinen Persönlichkeitsrechts dar, das als „sonstiges Recht" i. S. d. § 823 Abs. 1 BGB auch negatorischen Schutz nach den allgemeinen Vorschriften genießt (BGH, Urteil vom 7. Juli 1983 – III ZR 159/82, juris Tz. 14).

Die Weitergabe der Daten von der Beklagten an die Schufa Holding AG wäre nach § 28 a BDSG nur in den dort in Abs. 1 genannten Fällen zulässig. Die hierfür bestehenden alternativen Voraussetzungen lagen und liegen jedoch nicht vor. Insbesondere war und ist eine Datenübermittlung nicht nach § 28 a Abs. 1 Satz 1 Nr. 4 BDSG zulässig, da der Kläger die Forderung bestritten hat. Erstmalig hat er die Forderung mit Schreiben vom 9. Mai 2012 gegenüber der Zedentin bestritten. Zwar hat die Beklagte dies zunächst in Abrede gestellt, ihr Bestreiten jedoch nach Vorlage des Rückscheins im Termin zur mündlichen Verhandlung vor dem Landgericht am 18. Februar 2013 nicht mehr substantiiert, weshalb das Landgericht diesen Vortrag des Klägers im Tatbestand des angefochtenen Urteils zu Recht als unstreitig dargestellt hat. Ein weiteres Mal hat der Kläger die Forderung durch Anwaltsschreiben vom 6. Juli 2012 gegenüber der Beklagten selbst bestritten.

b) Aufgrund der dennoch von der Beklagten vorgenommenen Hinweise auf die Möglichkeit einer Datenübermittlung an die Schufa Holding AG bestand die ernstlich drohende und unmittelbare Gefahr, dass die Beklagte die Datenübermittlung vornahm und damit das allgemeine Persönlichkeitsrecht des Klägers verletzte.

3. Dem Kläger steht weiter aus § 823 Abs. 2 BGB i. V. m. §§ 240, 22, 23 StGB ein Anspruch gegen die Beklagte zu, es zu unterlassen, mit der Meldung seiner Daten an die Schufa Holding AG zu drohen. Der Hinweis auf die Möglichkeit der Datenübermittlung in der zweiten Mahnung vom 13. August 2012 stellte eine rechtswidrige Drohung mit einem empfindlichen Übel dar, die den Kläger zu einer Handlung – nämlich der Begleichung der angemahnten Forderung – nötigen sollte. Unerheblich ist im vorliegenden Zusammenhang, welcher der für die Beklagte handelnden Personen dies strafrechtlich zuzurechnen wäre.

a) Der Hinweis stellte dem Kläger ausdrücklich ein empfindliches Übel, nämlich die Datenmitteilung an die Schufa Holding AG und die damit verbundene Möglichkeit der Verschlechterung seiner Bonität vor Augen. Es steht zur Überzeugung des Senats fest, dass diese Mitteilung den Zweck hatte, den Kläger zur Zahlung der geltend gemachten Forderung zu bewegen. Die Androhung des Übels zu diesem angestrebten Zweck ist als verwerflich anzusehen (§ 240 Abs. 2 StGB).

Die Unterrichtung über die Möglichkeit der Datenübermittlung erfüllt im konkreten Fall keinen gesetzlichen vorgesehenen Zweck. Sie ist zwar in § 28 a Abs. 1 Satz 1 Nr. 4 c BDSG vorgesehen. In diesem Zusammenhang war sie jedoch vorliegend ohne Bedeutung, da nach dieser Alternative die Datenübermittlung nur bei unbestrittenen Forderungen zulässig ist, die von der Beklagten hier geltend gemachte Forderung von dem Kläger bereits zweifach bestritten worden war. Zwar war eine Datenübermittlung darüber hinaus insbesondere nach § 28 a Abs. 1 Satz 1 Nr. 1 BDSG bei einer gerichtlichen Feststellung der Forderung möglich. Allein die zum Zeitpunkt der zweiten Mahnung noch nicht konkret absehbare Möglichkeit einer Mitteilung nach einer gerichtlichen Feststellung der Forderung rechtfertigte den Hinweis im Mahnschreiben jedoch nicht, zumal dieser diese einschränkende Voraussetzung nicht ausdrücklich benannte sondern vielmehr – wie vorstehend dargelegt – suggerierte, dass eine Mitteilungsmöglichkeit bereits aktuell bestehe.

Für eine Verwerflichkeit im Sinne des § 240 Abs. 2 StGB spricht demgegenüber, dass die in Aussichtstellung der Möglichkeit einer solchen Datenübermittlung regelmäßig bereits als konkret drohendes erhebliches Übel aufgefasst werden wird. Ohne dass es hier darauf entscheidend ankäme, ist anzumerken, dass der Schlusssatz des Hinweises, in dem die Mitteilungsmöglichkeit auf bestrittene und einredefreie Forderungen beschränkt wird, regelmäßig entweder gar nicht oder angesichts der in dem vorangehenden Satz enthaltenen Verdeutlichung der Nachteile einer solchen Mitteilung häufig nicht mit der gebotenen Deutlichkeit zur Kenntnis genommen werden wird (in diesem Sinne auch OLG Düsseldorf, a. a. O.).

Kommt – wie vorliegend – hinzu, dass der Hinweis auf diese Übermittlungsmöglichkeit vorgenommen wird, obwohl die Forderung längst bestritten ist und die Beklagte sogar bereits zur Unterlassung und zur Abgabe einer Unterlassungserklärung aufgefordert worden war, musste dies die Sorge steigern, dass eine solche Mitteilung erfolgte, wenn die Forderung nicht kurzfristig beglichen würde. Die Beklagte hat damit die grundsätzlich vorgesehene Möglichkeit eines Hinweises auf die Datenmitteilung als außerprozessuales Druckmittel zur Forderungsdurchsetzung (einen derartigen Missbrauch befürchtend: BR-Drs. 548/1/08, S. 9) missbraucht.

c) Der Senat ist weiter davon überzeugt, dass die bei der Erteilung dieses Hinweises handelnden Mitarbeiter der Beklagten jedenfalls bedingt vorsätzlich handelten. Angesichts des Umstandes, dass der Kläger auch unmittelbar zuvor die Forderung bestritten und die Beklagte zur Abgabe einer Unterlassungserklärung aufgefordert hatte, spricht viel dafür, dass es den Mitarbeitern der Beklagten bekannt war, dass die Forderungen für eine Datenmitteilung nicht vorlagen und der Hinweis daher nur den Zweck haben konnte, den Kläger zur Zahlung zu nötigen. Selbst wenn die Beklagte jedoch – wie von ihrem Prozessbevollmächtigten in der mündlichen Verhandlung vor dem Senat vermutet – den fraglichen Hinweis ohne nähere Prüfung der Umstände des Einzelfalls in die zweite Mahnungen aufgenommen haben sollte, so hätten die maßgeblichen Entscheidungsträger der Beklagten es in Kauf genommen und zur Erreichung des Nötigungszwecks gebilligt, dass dieser Hinweis auch in denjenigen Fällen erfolgt, in denen die Forderung bestritten ist und der Hinweis daher keinen gesetzlich vorgesehenen Zweck verfolgt.

d) Die durch den Erstverstoß begründete Wiederholungsgefahr hat die Beklagte nicht ausgeräumt.

4. Dem Kläger steht demgegenüber kein Anspruch auf Ersatz der vorprozessualen Anwaltskosten zu. Die gebührenausgleichende Tätigkeit seines Anwalts – insbesondere die Fertigung dessen Schreibens vom 6. Juli 2012 – erfolgte zu einem Zeitpunkt, in dem noch kein Unterlassungsanspruch bestand.

Unzumutbare Belästigung durch trotz Widerspruch „An die Bewohner des Hauses" gerichtete Werbepost

(**Oberlandesgericht München**, Urteil vom 5. Dezember 2013 – 29 U 2881/13 –)

Die wiederholte Übersendung teiladressierter Werbeschreiben (Schreiben ohne Empfängernamen im Adressfeld) an Verbraucher, die dem Unternehmen mitgeteilt haben, dass sie von diesem keine Werbung erhalten möchten, sind auch dann unzulässig, wenn der Empfänger keinen entsprechenden Hinweis am Briefkasten angebracht hat.

Aus den Gründen:

Der vom Kläger geltend gemachte Unterlassungsanspruch ergibt sich hinsichtlich der ohne Empfängernamen teiladressierten Postwurfsendungen aus § 8 Abs. 1, Abs. 3 Nr. 3, § 7 Abs. 2 Nr. 1 UWG.

2. Mit Übersendung der teiladressierten Postwurfsendungen hat die Beklagte dem Verbraucher S. im Sinne des § 7 Abs. 2 Nr. 1 UWG Werbung unter Verwendung eines für den Fernabsatz geeigneten kommerziellen Kommunikationsmittels hartnäckig übersandt, obwohl er dies erkennbar nicht wünschte.

a) Bei den teiladressierten Postwurfsendungen handelt es sich um ein für den Fernabsatz geeignetes Mittel der kommerziellen Kommunikation. Erfasst sind alle Kommunikationsmittel, die zwischen einem Verbraucher und einem Unternehmer ohne gleichzeitige körperliche Anwesenheit der Vertragsparteien eingesetzt werden können (Köhler/Bornkamm, a.a.O., § 7 Rn. 101). Dies ist bei teiladressierten Postwurfsendungen der Fall.

b) Die Beklagte hat dem Verbraucher S. die Sendungen zukommen lassen, obwohl er dies erkennbar nicht wünschte. Der Verbraucher S. hat in seiner E-mail vom 26.05.2012 unmissverständlich klargemacht, dass er keinerlei Verträge mit der Beklagten mehr abschließen werde, selbst wenn die Beklagte ihm die Leistungen schenken würde, und dass er deshalb mit Werbung der Beklagten zukünftig verschont werden möchte. Diese E-mail erfolgte als Reaktion auf das Schreiben der Beklagten vom 23.05.2012, das als vollständig adressierter Brief übersandt worden war. Daraus lässt sich aber nicht schließen, dass sich der Widerspruch des Verbrauchers S. nur gegen Werbung durch vollständig adressierte Briefe richtete. Eine solche Einschränkung auf dieses eine Kommunikationsmittel lässt sich der E-mail in keiner Weise entnehmen. Der Verbraucher S. hat vielmehr unmissverständlich deutlich gemacht, dass er keinerlei Werbung mehr von der Beklagten erhalten möchte.

Im vorliegenden Fall kommt noch erschwerend dazu, dass die Beklagte dem Verbraucher S. exakt das gleiche Angebot, das sie ihm zunächst mittels vollständig adressierten Briefs übermittelt hat, sodann nach seiner E-mail vom 26.05.2012 noch zweimal mittels teiladressierter Postwurfsendung geschickt hat. Das Vorbringen der Beklagten, es sei für sie nicht erkennbar gewesen, dass Herr S. an der Übersendung des Angebots kein Interesse hatte, ist angesichts dessen, dass Herr S. ihr bereits mitgeteilt hatte, dass er das Angebot nicht einmal geschenkt annähme und sich die Übersendung weiterer Werbung verbete, nicht nachvollziehbar.

Entgegen der Auffassung der Beklagten ist § 7 Abs. 2 Nr. 1 UWG unter Berücksichtigung der Grundrechte der Beklagten aus Art. 5 GG und Art. 12 GG auch nicht verfassungskonform dahingehend auszulegen, dass das Ansprechen nur dann „erkennbar" unerwünscht ist, wenn der Empfänger seinen Briefkasten mit einem entsprechenden Aufkleber wie „Werbung nein danke" versehen hat und nicht etwa auch dann, wenn der Empfänger – wie hier – dem Unternehmer eine entsprechende Mitteilung hat zukommen lassen. § 7 Abs. 2 Nr. 1 UWG dient der Umsetzung der Nr. 26 Satz 1 Anhang I der UGP-Richtlinie. Bezüglich der im Anhang I der UGP-Richtlinie genannten Geschäftspraktiken ist der Richtliniengeber unter Berücksichtigung der in Rede stehenden Grundrechte (vgl. Erwägungsgrund 25 der Richtlinie 2005/29/EG) zu dem Ergebnis gelangt, dass diese unter allen Umständen als unlauter gelten. In Nr. 26 Satz 1 Anhang 1 der UGP-Richtlinie ist das Wort „erkennbar" sogar gar nicht enthalten, in der Richtlinie ist nur von „unerwünschtem Ansprechen" die Rede. Das Merkmal „erkennbar" ist daher nicht erweiternd dahingehend auszulegen, dass die Erkennbarkeit auf eine bestimmte Art und Weise zu Tage treten muss, sondern bedarf einer richtlinienkonformen einschränkenden Auslegung (vgl. Köhler/Bornkamm, a.a.O. § 7 Rn. 102b). Aufgrund der deutlichen E-mail vom 26.05.2012 war für die Beklagte somit „erkennbar", dass der Verbraucher S. von der Beklagten keine Werbung mehr erhalten wollte, auch wenn dieser seinen Briefkasten nicht entsprechend gekennzeichnet hatte.

c) Die Beklagte hat den Verbraucher S. mit Werbung enthaltenden teiladressierten Postwurfsendungen auch hartnäckig angesprochen, nämlich nach Eingang der E-mail von Herrn S. noch insgesamt fünfmal. Für die Hartnäckigkeit kommt es allein auf die Wiederholung, nicht aber auf eine besonders intensive Einwirkung an (Köhler/Bornkamm, a.a.O. § 7 Rn. 102a).

Kein Anspruch auf Medienöffentlichkeit von Gemeinderatssitzungen (Ls)

(**Hessischer Verwaltungsgerichtshof**, Urteil vom 31. Oktober 2013 – 8 C 127/13.N –)

1. **Gemeindevertreter und von ihnen gebildete Fraktionen haben in Hessen kein wehrfähiges Recht auf Herstellung der sog. Medienöffentlichkeit von Sitzungen der Gemeindevertretung.**

2. **§ 52 Abs. 1 HGO gewährleistet lediglich die sog. Saalöffentlichkeit. Die Herstellung der sog. Medienöffentlichkeit ist ausschließlich aufgrund einer entsprechenden allgemeinen Regelung in der Hauptsatzung der Gemeinde zulässig (§ 52 Abs. 3 HGO).**

3. **Eine solche Regelung in der Hauptsatzung einer Gemeinde kann nicht im Wege prinzipaler Normenkontrolle (§ 47 VwGO), sondern allenfalls durch eine sog. Normerlassklage durchgesetzt werden. Für eine solche Klage ist in erster Instanz nicht das Oberverwaltungsgericht (der Verwaltungsgerichtshof), sondern das jeweilige Verwaltungsgericht zuständig.**

BR-Zuständigkeit bei Regelung der angestrebten unternehmensweiten Vorlagepflicht von Arbeitsunfähigkeitsbescheinigungen (Ls)

(**Landesarbeitsgericht Köln**, Beschluss vom 21. August 2013 – 11 Ta 87/13 –)

1. **Macht der Arbeitgeber von seinem Regelungsspielraum des § 5 Abs. 1 EFZG, Arbeitsunfähigkeitsbescheinigungen seiner Arbeitnehmer auch dann zu verlangen, wenn die Arbeitsunfähigkeit nicht länger als drei Tage dauert, Gebrauch, so betrifft dies die betriebliche Ordnung. Der Betriebsrat hat dann ein zwingendes Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG.**
2. **In mitbestimmten Angelegenheiten, für deren Regelung der Betriebsrat zuständig ist, kann eine zwischen ihm und dem Arbeitgeber geschlossene Betriebsvereinbarung nicht durch eine zwischen Gesamtbetriebsrat und Arbeitgeber geschlossene Betriebsvereinbarung abgelöst werden.**
3. **Der Arbeitgeber kann die Zuständigkeit des Gesamtbetriebsrats gemäß § 50 Abs. 1 BetrVG nicht dadurch begründen, dass er eine unternehmensweite Regelung zur Regelung der Anzeige- und Nachweispflichten im Krankheitsfall verlangt.**

Zur Zulässigkeit der Anordnung eines Drogentests durch die Agentur für Arbeit (Ls)

(**Landgericht Heidelberg**, Urteil vom 22. August 2013 – 3 O 403/11 –)

1. **Die Untersuchung einer Leistungsbezieherin der Grundsicherung für Arbeitssuchende auf eine Suchtmittelabhängigkeit ist für die Entscheidung über die Leistung nur dann erforderlich gemäß § 62 SGB I, wenn es aus dem Verhalten der Antragstellerin oder sonst zugänglichen Informationen Hinweise hierauf gibt.**
2. **Erfolgt eine solche Untersuchung (hier: Drogenscreening einer Urinprobe sowie Untersuchung einer Blutprobe auf Blutalkohol) ohne genügende konkrete Hinweise auf eine Suchtmittelabhängigkeit, stellt dies einen rechtswidrigen Eingriff in das allgemeine Persönlichkeitsrecht gemäß Art. 1 Abs.1, Art. 2 Abs. 1 GG dar.**
3. **Ein Anspruch auf Geldentschädigung kommt jedoch nur in Betracht, wenn der Eingriff derart schwerwiegend ist, dass dieser nur durch eine Geldentschädigung ausgeglichen werden kann.**
4. **Das ist noch nicht der Fall, wenn sich die nachteiligen Auswirkungen des Eingriffs in engen Grenzen halten, weil – da der Verdacht einer Suchtmittelabhängigkeit nicht an die Öffentlichkeit gelangt ist – kein Anlass für die Annahme besteht, dass die Bundesagentur für Arbeit gegenüber Leistungsbeziehern der Grundsicherung für Arbeitssuchende generell in gleicher oder ähnlicher Weise vorgeht und Anlass und Beweggründe der handelnden Personen im vorliegenden Fall nicht so schwer wiegen, dass zum Ausgleich eine Geldentschädigung geboten erscheint.**

Diskriminierung bei Ablehnung einer Bewerberin mit 7-jährigem Kind (Ls)

(**Landesarbeitsgericht Hamm**, Urteil vom 6. Juni 2013 – 11 Sa 335/13 –)

1. **Wenn der Arbeitgeber auf dem zurückgesandten Lebenslauf einer Bewerberin neben der Textzeile „Verheiratet, ein Kind" handschriftlich vermerkt „7 Jahre alt" und die sich dann ergebende Wortfolge „ein Kind, 7 Jahre alt!" durchgängig unterstreicht, lässt das darin liegende Abstellen auf das Problem der Vereinbarkeit von Kinderbetreuung und Berufstätigkeit auf eine mittelbare Diskriminierung wegen des weiblichen Geschlechts schließen (§3 Abs. 2, § 1 AGG).**
2. **Die durch den Vermerk des Arbeitgebers gemäß § 22 AGG begründete Vermutung einer mittelbaren Diskriminierung wird nicht dadurch widerlegt, dass der Arbeitgeber eine besser qualifizierte junge Frau ohne Kind eingestellt hat.**

(Nicht amtliche Leitsätze)

Berichte, Informationen, Sonstiges

BMJV: „Mailen, Surfen, Chatten – wie ist die Privatsphäre zu retten?“

Konferenz von BMJV und BITKOM am „Safer Internet Day“ diskutiert Fragen zur Sicherheit der digitalen Kommunikation.

Fast 80 Prozent aller Deutschen nutzen zumindest gelegentlich das Internet. Das Internet hat unser Alltagsleben revolutioniert, uns eine schier unübersehbare Vielfalt von neuen Einkaufsmöglichkeiten geliefert, Informationsquellen aufgetan und neue Kommunikationsmöglichkeiten geschaffen. Neben den Vorteilen sind aber mehr und mehr auch die besonderen Gefahren der digitalen Kommunikation offenbar geworden: Unternehmen können Millionen Daten über Kunden sammeln und auswerten, Kriminelle können – wie jüngst bekannt wurde – Online-Zugangsdaten und Passwörter stehlen. Je mehr Daten, desto größer die Möglichkeiten der Auswertung, desto größer aber auch die Gefahr des Missbrauchs und des Kontrollverlustes. Auch angesichts der zahlreichen Enthüllungen über die Aktivitäten verschiedener Geheimdienste seit Sommer letzten Jahres werden Fragen zum Schutz der Privatsphäre nicht nur in Deutschland, sondern auch europa- und weltweit intensiv diskutiert.

„Im digitalen Zeitalter sind für Verbraucher viele Möglichkeiten der Kommunikation, des Preisvergleichs, der schnellen Information entstanden, aber auch Datenschutz und Privatheit in nie gekannter Weise gefährdet. Deshalb sind wir alle, Staat, Wirtschaft, Gesellschaft und der Einzelne, gefordert“, sagte Verbraucherschutzminister Maas. Es stellen sich zahlreiche Fragen. Wie können Unternehmen ihrer Verantwortung für die Daten ihrer Kunden gerecht werden? Was kann jeder Einzelne tun, um seine Daten besser zu schützen? Wann muss der Staat aktiv werden, um Bürger und Verbraucher wirksam zu schützen?

Nach den Ergebnissen einer repräsentativen Umfrage im Auftrag des Hightech-Verbands BITKOM ist das Vertrauen der Internetnutzer in die Sicherheit ihrer Daten infolge der Abhöraktionen der Geheimdienste massiv eingebrochen. Danach halten 80 Prozent der Internetnutzer in Deutschland ihre persönlichen Daten im Internet für unsicher. Bei einer gleich lautenden Umfrage im Jahr 2011 waren es erst 55 Prozent. „Das Misstrauen der Nutzer trifft vor allem diejenigen, die persönliche Daten von Bürgern oder Kunden verarbeiten: Staat und Wirtschaft“, sagte BITKOM-Präsident Prof. Dieter Kempf. Laut Umfrage misstrauen 68 Prozent der Internetnutzer staatlichen Stellen beim Umgang mit ihren persönlichen Daten im Web. Im Jahr 2011 waren es erst 40 Prozent. Nur wenig besser sind die Ergebnisse für die Wirtschaft: 64 Prozent der befragten Internetnutzer misstrauen der „Wirtschaft allgemein“, wenn es um den Umgang mit ihren Daten im Netz geht. Im Jahr 2011 waren es 46 Prozent. „Das Vertrauen der Internetnutzer in Datenschutz und Datensicherheit wurde durch die NSA-Affäre schwer erschüttert“, sagte Kempf. „Wirtschaft und Politik sind jetzt gefordert, für mehr technische und rechtliche Sicherheit im Internet zu sorgen.“ Die politische Aufarbeitung der Abhöraffäre müsse mit Nachdruck vorangebracht werden. Gleichzeitig müssten die Internetnutzer dabei unterstützt werden, die Sicherheit ihrer Geräte und Anwendungen über die bestehenden Standards hinaus zu erhöhen.

Negative Erfahrungen der Nutzer mit Verletzungen der Privatsphäre, Datenklau oder Betrug sind im Internet weit verbreitet. Laut der BITKOM-Umfrage haben 38 Prozent der Internetnutzer in Deutschland allein im vergangenen Jahr entsprechende Erfahrungen gemacht. Das entspricht rund 21 Millionen Betroffenen. 24 Prozent der befragten Internetnutzer sagen, dass ihre Computer mit Schadproprogrammen infiziert wurden. 14 Prozent geben an, dass ihre Zugangsdaten zu Internetdiensten wie Online-Shops, sozialen Netzwerken oder Online-Banken ausgespäht wurden. 10 Prozent haben durch Schadprogramme oder infolge eines Datendiebstahls einen finanziellen Schaden erlitten. 9 Prozent sind in den vergangenen zwölf Monaten bei Transaktionen wie Einkäufen oder Auktionen im Internet betrogen worden.

„Ein höheres Sicherheitsniveau erreichen wir auf dreierlei Weise: bessere Produkte und Dienste, mehr Rechtssicherheit und ein steigendes Sicherheitsbewusstsein der Internetnutzer“, sagte BITKOM-Präsident Kempf. So unterstütze der BITKOM die Schaffung eines einheitlichen Datenschutzrechts in der Europäischen Union und fordert u.a. intensive Verhandlungen über internationale No-Spy-Abkommen. Gleichzeitig sollten Initiativen gestärkt werden, die Internetnutzer in Sicherheitsfragen informieren und beraten. Kempf: „Jeder Nutzer kann etwas tun. Damit schützt er sich nicht nur vor schnüffelnden Geheimdiensten, sondern auch vor kriminellen Hackern.“

Bundesverbraucherschutzminister Maas nannte zwei konkrete Projekte, die die Bundesregierung in den nächsten Monaten konkret angehen will. „Wir müssen auf EU-Ebene mit der schon viel zu lange diskutierten Datenschutz-Grundverordnung weiter kommen, damit endlich alle Unternehmen, die ihre Angebote an europäische Verbraucher richten, dem europäischen Recht unterliegen. Da darf es keine Schlupflöcher geben.“ Auf nationaler Ebene kündigte Maas die Ergänzung des Unterlassungsklagengesetzes an. In Zukunft sollen Verbraucherschutzorganisationen gegen alle Formen der rechtswidrigen Verwendung von Verbraucherdaten durch Unternehmen mit Abmahnung und Unterlassungsklage vorgehen können. Bisher waren solche Klagen nur dann möglich, wenn durch die allgemeinen Geschäftsbedingungen gegen Datenschutzvorschriften verstoßen wurde. „Bis Ende April wird das Bundesministerium der Justiz und für

Verbraucherschutz dazu einen Referentenentwurf vorlegen. Damit werden wir eine Lücke schließen, die die Verbraucherorganisationen schon seit längerem beklagt haben. Der Verbraucherdatenschutz wird erheblich verbessert. Wir schützen damit auch seriöse Unternehmen, die es mit dem Datenschutz erst nehmen, vor unlauterer Konkurrenz", erklärte Verbraucherschutzminister Maas.

(Pressemitteilung vom 11.02.2014)

EU-Datenschutz-Konföderation CEDPO im Aufwind

Mit dem Beitritt von drei weiteren nationalen Mitgliedsverbänden untermauert der auf Initiative der GDD gegründete Dachverband CEDPO (Confederation of European Data Protection Organisations) seine Schlüsselrolle im Europäischen Datenschutz. Inzwischen vereint die Dachorganisation über seine nationalen Mitgliedsverbände tausende Datenschutzbeauftragte und andere Datenschutzpraktiker aus der Europäischen Union.

Gemeinsam mit den neuen Mitgliedsverbänden aus Irland (ADPO), Österreich (ARGE DATEN) und Polen (SABI) fördert CEDPO eine Stärkung der Rolle von betrieblichen und behördlichen Datenschutzbeauftragten und tritt generell für einen ausgewogenen, praktikablen und effektiven Datenschutz ein. Ebenso wie die Gründungsmitglieder von CEDPO aus Deutschland (GDD), Frankreich (AFCDP), den Niederlanden (NGFG) und Spanien (APEP) verfügen auch die neuen Mitgliedsverbände über einen reichen Erfahrungsschatz bei der praktischen Umsetzung von europäischen Datenschutzbestimmungen.

Die drei neuen Mitgliedsverbände haben die Möglichkeit zum CEDPO-Beitritt ausdrücklich begrüßt. „Als führende Datenschutzorganisation in Österreich bilden wir Datenschutzbeauftragte bereits seit über zwanzig Jahren aus. Wir freuen uns über die Möglichkeit, unser Fachwissen und unsere Erfahrungen im Sinne einer effektiven Datenschutzpraxis weit über unsere Landesgrenze hinaus teilen zu können, erklärt Dr. Hans G. Zeger, Vorsitzender der österreichischen ARGE DATEN. ähnlich sieht es Fintan Swanton, Vorsitzender des irischen Verbandes für Datenschutzbeauftragte ADPO: „Wir begrüßen es, Ideen zur Harmonisierung des Datenschutzrechts und zu Best Practices austauschen zu können. Hierbei können wir unter anderem unsere Erfahrungen aus Workshops und Konferenzen zu aktuellen Praxisthemen wie beispielsweise BYOD und Cookies einbringen." Nicht zuletzt mit Blick auf ein aktuelles Gesetzgebungsverfahren in Polen plädiert Maciej Byczkowski, Vorsitzender des polnischen Verbandes SABI, für eine Stärkung der Rolle von Datenschutzbeauftragten. „In diesem Sinne führen wir bereits Gespräche mit unserer nationalen Datenschutzbehörde GIODO sowie mit Regierungs- und Parlamentsvertretern. Gerne schließen wir uns unseren europäischen Kollegen an, um die Dinge nun auch in größerem Rahmen mit voranzubringen" informiert Byczkowski.

Zur Auskunft über Scorewertberechnung

Nach einer Entscheidung des BGH (Urteil vom 28.1.2014 – VI ZR 156/13 –) zählen konkrete Angaben zu den Vergleichsgruppen nicht zu den Elementen des Scoringverfahrens, über die nach § 34 Abs. 4 S. 1 Nr. 4 BDSG Auskunft zu geben ist. Gleiches gelte für die Gewichtung der in den Scorewert eingeflossenen Merkmale. Das Auskunftsrecht erstrecke sich nur darauf, welche personenbezogenen, insbesondere kreditrelevanten Daten gespeichert und in die Berechnung der Wahrscheinlichkeitswerte eingeflossen sind.

Dem Auskunftsanspruch des § 34 Abs. 4 BDSG liegt die gesetzgeberische Intention zugrunde, trotz der Schaffung einer größeren Transparenz bei Scoringverfahren Geschäftsgeheimnisse der Auskunfteien, namentlich die sog. Scoreformel, zu schützen. Die Auskunftsverpflichtung soll dazu dienen, dass der Betroffene den in die Bewertung eingeflossenen Lebenssachverhalt erkennen und darauf reagieren kann. Hierzu bedarf es keiner Angaben zu Vergleichsgruppen und zur Gewichtung einzelner Elemente.

Das gesetzgeberische Ziel eines transparenten Verfahrens wird dadurch erreicht, dass dür den Betroffenen ersichtlich ist, welche konkreten Umstände als Berechnungsgrundlage in die Ermittlung des Wahrscheinlichkeitswerts eingeflossen sind.

Zudem sind die Verbraucher darüber zu informieren, welche Wahrscheinlichkeitswerte in den letzten zwölf Monaten an Dritte übermittelt wurden, wie der aktuell berechnete Scorewert lautet und welche Daten zur Berechnung genutzt wurden.

Der LDI NRW nimmt hierzu u.a. wie folgt Stellung: „Die für die Verbraucher notwendige Transparenz zu ihren Bonitätswerten bleibt auf halber Strecke stehen. Ich fordere die neue Bundesregierung auf, die gesetzliche Regelung im Bundesdatenschutzgesetz zur Auskunft über das Scoringverfahren datenschutzfreundlicher zu gestalten. Dazu gehört Klarheit über die verwendeten Verfahren. Es dürfen zudem nur Daten verwendet werden, die für die Zahlungsfähigkeit von Bedeutung sind. Da die Arbeiten zur Evaluierung der Bundesdatenschutz-Novelle aus dem Jahr 2009 derzeit laufen, bietet sich hierzu auch eine gute Chance."

Literaturhinweise

Buchbesprechungen

Wolfgang Däubler/Thomas Klebe/Peter Wedde/Thilo Weichert, **Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG, 4., vollständig neu bearbeitete Auflage,** Bund-Verlag, Frankfurt, 2014, 902 S., 89,90 €

Völlig zu Recht hat sich der Gemeinschaftskommentar – der sich bis zur 2. Auflage als „Basiskommentar" bezeichnete und seit der Vorauflage als „Kompaktkommentar" im Untertitel ausweist – einen festen Platz unter den immer zahlreicheren BDSG-Erläuterungswerken erworben. Die Kompetenz der Autoren ist unbestritten und das Gewicht ihrer Argumente beachtlich.

Drei der vier Verfasser sind ausgewiesene Experten des Arbeitsrechts – nicht erstaunlich also, dass zur Veranschaulichung diesem Rechtsbereich viele Anwendungsfälle entnommen sind, die gerade auch einem Einsteiger in die Datenschutzmaterie das Gesetz näher bringen. Dass die betreffenden Beispiele und Passagen eine unverkennbare Positionierung der Kommentatoren zeigen, muss man durchaus als Bereicherung bei der Meinungsbildung ansehen: Die Arbeitgeberseite gehört jedenfalls nicht zu dem von ihnen bevorzugt behandelten Adressatenkreis bei der Interpretation einzelner Normen. Insoweit sollte sich der Leser nicht einer kritischen Auseinandersetzung mit manchen Exegesen entziehen.

Gegenüber der Vorauflage hat der Umfang der 4. Auflage um knapp 10 Prozent zugelegt. Dies kommt nicht nur der Aktualisierung der Erläuterungen durch die Verarbeitung neuerer Literatur und Rechtsprechung zugute, sondern auch der Vertiefung einzelner Ausführungen. So werden z.B. bei § 32 BDSG – hier wurde die Kommentierung um ein Viertel umfangreicher – die sozialen Netzwerke behandelt oder bei § 38a BDSG die mit der Bestimmung verbundenen Handlungsmöglichkeiten und mit ihr verfolgten gesetzgeberischen Absichten stärker verdeutlicht und der erste „Umsetzungsfall" – die Verhaltensregeln der Versicherungswirtschaft – beschrieben.

Das Werk ist in inhaltlicher Tiefe, Konzeption und Stil rund und kaum verbesserungsfähig. Die Erläuterungen sind schnörkellos, klar und für jeden verständlich – die Lektüre bereitet Vergnügen. Vielleicht nur ein Hinweis: Bei manchen Ausführungen wurde die Lesbarkeit durch die Einfügung von Zwischenüberschriften erhöht, z.B. bei § 4a BDSG. Dagegen fällt – zugegeben, bei überkritischer Betrachtung – auf, dass an anderen Stellen die Hervorhebung von Satzteilen oder Wortverbindungen durch Fettdruck etwas uneinheitlich und willkürlich erscheint. Der Verzicht auf derartige drucktechnische Betonungen etwa bei § 28 BDSG wirkt sich jedenfalls keineswegs nachteilig aus.

Kurzum: Das Werk ist eine hervorragend gelungene Gemeinschaftsarbeit von absoluten Sachkennern. Seine Anschaffung ist ein „Muss" für jeden, der sich mit dem BDSG zu befassen hat.

(Rechtsanwalt Dr. Georg Wronka, Bonn)

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.

Nina Dierks
Social Media im Unternehmen – zur Zweckmäßigkeit des Verbots der (privaten) Nutzung unter besonderer Berücksichtigung von § 88 TKG, K&R 2014, S. 1 ff.
Die Autorin hält ein Verbot schon deshalb für nicht geboten, da sie die Anwendung des § 88 TKG im Arbeitsverhältnis ablehnt. Gleichwohl hält sie angemessene Regelungen für angezeigt.

Peter Gola/Christoph Klug
Die Entwicklung des Datenschutzrechts im zweiten Halbjahr 2013, NJW 2014, S. 667 ff.
Der Übersichtsbeitrag beschränkt sich angesichts der Breite und Vielfalt der Datenschutzthemen auf Grundsatzfragen des BDSG und die klassischen Bereiche der Telekommunikation, des Beschäftigten- und des Kundendatenschutzes.

Sebastian J. Golla
Abgenickt von Algorithmik – Aktuelles zum Verbot automatisierter Entscheidungen, PinG 2014, S. 61 ff.
Der Autor geht der Bedeutung des § 6a BDSG im Hinblick auf Big Data, d.h. den Einsatz von Algorythmen zur Analyse großer Datenmengen und die damit verbundenen Gefährdungen des Persönlichkeitsrechts nach. Er kommt zu dem Ergebnis, dass § 6a BDSG noch nicht die klare rechtliche Einordnung solcher Entscheidungs- und Bewertungsergebnisse leistet. Vor allem die Voraussetzung, dass ein Datum zur Bewertung von Persönlichkeitsmerkmalen dienen müsse, sei aus sich heraus nicht verständlich.

Stephanie Herzog
Der digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, S. 3745 ff.
Auf wen die Verfügungsbefugnis über die von ihm gespeicherten Daten beim Tode des Betroffenen übergeht, ist bei privaten wie dienstlichen Daten weitgehend ungeklärt. Die Autorin entwickelt Lösungen an Hand des Erbrechts und zeigt Gestaltungsmöglichkeiten auch für Unternehmen auf.

Rudi Kramer
Datenschutzrechtliche Besonderheiten bei der Beauftragung eines Steuerberaters durch Unternehmen, PinG 2014, S.77 ff.
Der Beitrag stellt klar, das ein Steuerberater im Rahmen einer Funktionsübertragung tätig wird und dies auf Grund des Steuerberatungsgesetzes auch dann, wenn der Steuerberater die Lohn- und Gehaltsabrechnung übernimmt – eine Tätigkeit, die bei einem gewerblichen Anbieter als Auftragsdatenverarbeitung einzuordnen ist. Zudem weist er auf die sich aus den Verschwiegenheitsvorgaben aus §§ 57 Abs. 1, 64 Abs. 2 StBerG, 203 Abs. 1 Nr. 3 StGB ergebenden Probleme hin.

Anne Lauber-Rönsberg
Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet – Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen, MMR 2014, S. 10 ff.
Der Beitrag zeigt das Spannungsfeld zwischen der durch Art. 5 Abs. 1 GG geschützten Anonymität der Nutzung und der zum Schutz des allgemeinen Persönlichkeitsrechts gebotenen Verantwortung des Portalbetreibers.

Keven Marschall
Strafrechtliche Haftungsrisiken des betrieblichen Datenschutzbeauftragten? ZD 2014, S. 66 ff.
Gegenstand der Rechtsprechung war der Aspekt der strafrechtlichen Haftung des DSB bislang nicht. Ob es dazu tatsächlich einmal kommen wird, ist zweifelsohne mehr als offen. Allein die Literatur hat sich mit der Täterschaft durch positives Tun bzw. durch Unterlassen befasst. Dem letztgenannten Aspekt widmet sich der Beitrag von *Marschall* vorwiegend, wobei dem DSB für den Beweisfall die Anlage hilfreicher Dokumentation empfohlen wird.

Bruno Schierbaum
Datenschutzrecht für Beschäftigte, CuA 3/2014, S. 27 ff.
In einem ersten Teil der mehrteiligen Abhandlung widmet sich der Autor der „Transparenz der Datenverarbeitung" im Arbeitsverhältnis und gibt einen ausführlichen Überblick über die sich aus verschiedenen Rechtsgrundlagen ergebenden Informations- und Auskunftspflichten des Arbeitgebers.

Fabian Schuster
Der Arbeitgeber und das „Telekommunikationsgesetz", CR 2014, S. 21 ff.
Der Autor schließt sich der Auffassung an, dass der Arbeitgeber auch bei der Gestattung der privaten Nutzung der betrieblichen Kommunikationstechnik nicht zum Telediensteanbieter wird.

Wenn der Schweinekönig kommt

Kinder lieben Smartphonespiele. Solange sie klein sind, spielen sie mit einem digitalen Tamagotchi, der aussieht wie ein Hundehaufen und mit einer Ortungsfunktion versehen ist. Man kann ihn füttern, kleiden und hätscheln. Vergisst man das, verlangt er laut nach Aufmerksamkeit. Etwas ältere Kinder spielen mit wütenden Vögeln und bösen Schweinchen. Da zieht man für einen Schweinekönig los. Wenn man eine lang Zeit nicht spielt, schickt er eine Nachricht auf das Handy. Er teilt mit, dass man vermisst wird und dass man geholt wird, wenn man nicht bald wieder spielt.

Diese Spiele sind widerlich. Dabei weiß man gar nicht, worüber man sich am meisten aufregen soll.

Darüber, dass Kinder aus dem Netz mit psychologischen Tricks hinter dem Rücken der Eltern zum Spielen animiert werden, obwohl diese für die Dauer der Mediennutzung verantwortlich sind?

Darüber, dass es Ziel der Spieleanbieter ist, das Spielverhalten kleiner Kinder zu erfassen und auszuwerten. Informationen über Zuverlässigkeit, Hartnäckigkeit, Intelligenz, Geschick und Mut werden gesammelt, denn diese Eigenschaften können vermarktet werden.

Darüber, dass die NSA auch Daten von Spielen abzapft? Was will sie von Kindern?

Darüber, dass man seine Kinder nicht guten Gewissens von diesen Spielen fernhalten kann und will, um sie nicht auszugrenzen?

Darüber, dass der Hundehaufen mit einer Funktion versehen ist, die das Handy ortet und seinen Besitzer finden kann?

Wie kann man seine Kinder schützen? Das ist schwierig. Die Ortung kann man zwar ausschalten. Aber nur der Spieleentwickler wird einem sagen können, ob man wenigstens gefahrlos im Flugmodus spielen kann oder ob die Daten bei der nächsten Verbindung mit dem Netz gesammelt verschickt werden.

Würde ein Schweinekönig sich in der körperlichen Welt an Kindern vergreifen, dann würde man ihm die Leviten lesen. Beim virtuellen Schweinekönig geht das nicht. Dabei hat er viel Macht über Kinder und Zugriff auf ihre digital gezeigte Persönlichkeit. Er spielt nicht nur. Er verführt, frisst, speichert und verarbeitet auch. Sein Lebenszweck ist es, diese Informationen zu vermarkten. Gerade wenn wir unsere Kinder nicht vom Schweinekönig fernhalten können, sollten wir ihnen erklären, mit wem sie es zu tun haben und was er wirklich von ihnen will.