

Zeitschrift für
Datenschutz-,
Informations- und
Kommunikationsrecht

RDV

1/2018

Recht der Datenverarbeitung

Herausgegeben von

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

Aufsätze

PILTZ, Datenübertragbarkeit im Beschäftigungsverhältnis –
Arbeitgeberwechsel: Und die Daten kommen mit?

GOLLAND, Reformation 2.0 – Umsetzung der Anforderungen der
Datenschutz-Grundverordnung durch die evangelische und die
katholische Kirche

THÜSING, Automatisierte Einzelentscheidung in der PKV – zur
Europarechtskonformität des neuen § 37 Abs. 1 Nr. 2 BDSG

Kurzbeiträge

WRONKA, Betriebliche Hausverbote und Datenschutz

GOLA, Aus den aktuellen Berichten der Aufsichtsbehörden (33):
Die Digitalisierung des Bewerbermanagements – Videointerviews
bei der Bewerbung

Rechtsprechung

Aus dem Inhalt

BGH, Zur Einwilligungserklärung in die Nutzung von Cookies (Ls)

BGH, Zum Auskunftsanspruch nach § 101 Abs. 2. S. 1 Nr. 3 UrhG
gegen den Internet-Provider (Ls)

KG BERLIN, Influencer Marketing (Ls)

OLG CELLE, Bußgeld wegen Dashcam-Aufzeichnungen zwecks
Anzeige von Verkehrsordnungswidrikeiten

KG BERLIN, Für Facebook gilt deutsches Datenschutzrecht –
Datenweitergabe bedarf wirksamer Einwilligung (Ls)

OLG NÜRNBERG, Voraussetzungen zur Verwertbarkeit von Dashcam-
Aufzeichnungen im Zivilprozess

34. Jahrgang
Februar 2018
Seiten 1–62



Gesellschaft für Datenschutz
und Datensicherheit e.V.



www.rdv-online.de

DSGVO für die Unternehmenspraxis.

Wächter
Datenschutz im Unternehmen
5. Auflage. 2017. XX, 483 Seiten.
Kartonierte € 69,-
ISBN 978-3-406-71525-9

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



Mit der DSGVO

wird ein neues Kapitel Datenschutzgeschichte geschrieben. Der Band erläutert die Änderungen durch die Datenschutz-Grundverordnung und die Anpassung des BDSG gezielt für die **Unternehmenspraxis**. Schwerpunkte bilden besonders:

- neue Anforderungen an die Rechtmäßigkeit der Datenverarbeitung
- neue Dokumentations-, Transparenz- und Organisationsanforderungen
- Datenverarbeitung im Auftrag und Datenverarbeitung im Konzern
- Aktualisierung der Fragestellungen zum Arbeitnehmerdatenschutz
- Analyse, Steuerung und Vernetzung von Mensch und Maschine in Arbeiten 4.0 und Industrie 4.0
- Haftung und Datenschutzversicherung

Der Autor

Dr. Michael **Wächter** ist Unternehmensjurist. In seiner beruflichen Tätigkeit im Vertrags- und Personalwesen in der IT-Branche ist er seit vielen Jahren mit neuen Entwicklungen der Unternehmens- und Arbeitsorganisation und den damit im Zusammenhang stehenden Rechtsfragen befasst.

Die Benutzer

sind Personal- und EDV-Abteilungen, Datenschutzbeauftragte, Betriebsräte, Rechtsanwälte, Justiziarer und Richter.

Inhaltsverzeichnis

Editorial

Veranstaltungen

Aufsätze

Dr. Carlo PILTZ

Datenübertragbarkeit im Beschäftigungsverhältnis –
Arbeitgeberwechsel: Und die Daten kommen mit?

Alexander GOLLAND

Reformation 2.0 – Umsetzung der Anforderungen der
Datenschutz-Grundverordnung durch die evangelische
und die katholische Kirche

Prof. Dr. Gregor THÜSING

Automatisierte Einzelentscheidung in der PKV
– zur Europarechtskonformität des neuen § 37
Abs. 1 Nr. 2 BDSG

Kurzbeiträge

Dr. Georg WRONKA

Betriebliche Hausverbote und Datenschutz

Prof. Peter GOLA

Aus den aktuellen Berichten der Aufsichtsbehörden
(33): Die Digitalisierung des Bewerbermanagements
– Videointerviews bei der Bewerbung

Rechtsprechung

Zur Einwilligungserklärung in die Nutzung von
Cookies (Ls)
(BGH, Beschluss vom 05.10.2017)

Zum Auskunftsanspruch nach § 101 Abs. 2. S. 1
Nr. 3 UrhG gegen den Internet-Provider (Ls)
(BGH, Urteil vom 21.09.2017)

Influencer Marketing (Ls)
(KG Berlin, Beschluss vom 11.10.2017)

Bußgeld wegen Dashcam-Aufzeichnungen zwecks
Anzeige von Verkehrsordnungswidrikeiten
(OLG Celle, Beschluss vom 04.10.2017)

Für Facebook gilt deutsches Datenschutzrecht –
Datenweitergabe bedarf wirksamer Einwilligung (Ls)
(KG Berlin, Urteil vom 22.09.2017)

Voraussetzungen zur Verwertbarkeit von Dashcam-
Aufzeichnungen im Zivilprozess
(OLG Nürnberg, Beschluss vom 10.08.2017)

Information des Betriebsrats über Schwangerschaften
(LAG München, Beschluss vom 27.09.2017)

1	Ton- und Bildaufnahmen durch den Leistungsberechtigten im Jobcenter (Ls) (LSG München, Beschluss vom 17.10.2017)	47
2	Der Einsatz von Wildkameras unterliegt den BDSG-Regeln (OVG Saarlouis, Urteil vom 14.09.2017)	47
	Zum Recht auf Vergessenwerden (Ls) (LG Frankfurt/M., Urteil vom 26.10.2017)	52
3	Unterlassung einer negativen Bewertung auf einer Internetplattform (Ls) (LG Augsburg, Urteil vom 17.08.2017)	52
	Zum Umfang des datenschutzrechtlichen Auskunftsrechts (AG Dortmund, Urteil von 29.08.2017)	52
8	Kündigung wegen verdeckter Videoaufnahmen von Sportlerinnen (Ls) (ArbG Berlin, Urteil vom 01.11.2017)	54
14	Berichte, Informationen, Sonstiges	
	Kommentar zu Stephan Pötters, Peter Gola: Wer ist datenschutzrechtlich „Verantwortlicher“ im Unter- nehmen? Betriebsrat und andere selbstständige Einheiten als Adressaten des Datenschutzrechts, RDV 6/2017 (CAUMANN)	55
	Fitness-App-Anbieter geben kaum Auskunft über Datennutzung	56
21	Bundesnetzagentur geht gegen Kinderuhren mit Abhörfunktion vor	57
24	Transparenz bei Videoüberwachung nach der DS-GVO	57
28	Literaturhinweise	
	Buchbesprechungen	
	Carlo Piltz, BDSG. Vorschriften für nichtöffentliche Stellen (GOLA)	59
	Sebastian Bauer, Soziale Netzwerke und straf- prozessuale Ermittlungen, (GOLA)	59
	Schantz/Wolff, Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundes- datenschutzgesetz in der Praxis (SCHRIFTLÉITUNG)	59
	Ehmann/Selmayr, Datenschutz-Grundverordnung (SCHWARTMANN)	59
	Neuerscheinungen	
35	Aufsätze	61
42	Nachgefasst	62

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

Prof. Dr. Rolf SCHWARTMANN, Leiter der Kölner Forschungsstelle für Medienrecht,
Technische Hochschule Köln

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

in Kooperation mit der

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

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

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

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

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

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

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

Prof. Dr. Karl LINNENKOHLE, Universität Kassel

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

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

Prof. Dr. Michael RONELLENFITSCH, Hessischer Datenschutzbeauftragter

Prof. Dr. Friedhelm ROST, Vorsitzender Richter am Bundesarbeits-
gericht a.D.

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

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

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

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 1/2018; DATAKONTEXT, Frechen

Manuskripte:

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

Urheber- und Verlagsrechte:

Sie sind einschließlich der Veröffentlichung als PDF im Online-Archiv vorbehalten. Sie erstrecken sich auch auf die veröffentlichten Gerichtsentscheidungen und deren Leitsätze; diese sind geschützt, soweit sie vom Einsender oder von der Schriftleitung erstellt oder bearbeitet sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen: Diese bedürfen zur Auswertung einer Genehmigung des Verlages.

Der Verlag gestattet in der Regel die Herstellung von Fotokopien zu innerbetrieblichen Zwecken, wenn dafür eine Gebühr an die VG Wort, Abteilung Wissenschaft, Goethestraße 49, 80336 München, entrichtet wird, von der die Zahlungsweise zu erfragen ist.

Schriftleitung

Prof. Peter Gola (federführend)

RA Dr. Georg Wronka

RA Andreas Jaspers

RDV-Schriftleitung@gdd.de

Redaktionsanschrift

Birgit Koppitsch

Heinrich-Böll-Ring 10, 53119 Bonn

Telefon: (02 28) 96 96 75-00

Telefax: (02 28) 96 96 75-25

RDV-Redaktion@gdd.de

Erscheinungsweise

6 x jährlich

Bezugspreis

Jahresabonnement

€ 139,-

Einzelheft

€ 25,-

MwSt. im Preis enthalten

jeweils zzgl. Versandkosten

Bestellungen

DATAKONTEXT GmbH, Frechen

Jürgen Weiß

Augustinusstraße 9d

D-50226 Frechen-Königsdorf

Telefon: (0 22 34) 9 89 49-71

Telefax: (0 22 34) 9 89 49-32

E-Mail: weiss@datakontext.com

www.datakontext.com

Geschäftsführer: Dr. Karl Ulrich

Leitung: Hans-Günter Böse

HRB 337678

Abbestellungen

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

Verlag

DATAKONTEXT GmbH, Frechen

Augustinusstraße 9d

D-50226 Frechen-Königsdorf

Telefon: (0 22 34) 9 89 49-30

Telefax: (0 22 34) 9 89 49-32

www.datakontext.com

Geschäftsführung: Dr. Karl Ulrich;

Hans-Günter Böse

HRB 337678

Satz

alka mediengestaltung gmbh

Willmuthstraße 30, 53332 Bornheim-Sechtem

Druck

AZ Druck und Datentechnik GmbH

Heisinger Straße 16, 87437 Kempten

Anzeigenverwaltung

DATAKONTEXT GmbH, Frechen

Thomas Reinhard-Rief

Hultschiner Straße 8

D-81677 München

Telefon: (089) 21 83-89 35

Telefax: (089) 21 83-96 02 33

E-Mail: reinhard@datakontext.com

www.datakontext.com

Geschäftsführer: Dr. Karl Ulrich

Leitung: Hans-Günter Böse

HRB 337678

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
34. Jahrgang 2018 Heft 1
Seiten 1–62

RDV

Recht der Datenverarbeitung

34. Jahrgang · Dezember 2017 · Seiten 1–62

Editorial

Praxisnaher Datenschutz?

Unternehmen und Behörden befinden sich in der Zielphase der Umsetzung der DS-GVO. Verbände und Fachorganisationen wie die GDD entwickeln Arbeitshilfen, Praxisleitfäden und Muster, um die Vorgaben der DS-GVO und des BDSG pragmatisch, aber rechtskonform umzusetzen.

Neben diesen Praxishilfen veröffentlicht auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) sogenannte Kurzpapiere zur DS-GVO. Diese Kurzpapiere sollen „als erste Orientierung dienen, wie die Datenschutz-Grundverordnung im praktischen Vollzug angewendet werden sollte“. Bei genauere Betrachtung werfen einige dieser Kurzpapiere aber erhebliche Fragen zur Praxis-tauglichkeit auf, insbesondere diejenigen, die sich mit den Informationspflichten befassen.

Problematisch für die Praxis der Informationserteilung nach Art. 13 DS-GVO sind insbesondere die Kurzpapiere Nr. 10 und 15. So fordert Kurzpapier Nr. 10 unter Verweis auf Art. 12 DS-GVO, dass die leicht zugängliche Form auch bedeute, dass die Informationen in der konkreten Situation verfügbar sein müssten. Sollen die Daten also von einer anwesenden Person erhoben werden, dürfe die Person in der Regel nicht auf Informationen im Internet verwiesen werden“. Bei den Pflichtinformationen zur Videoüberwachung seien, so Kurzpapier Nr. 15, alle Angaben des Art. 13 DS-GVO ebenfalls „am

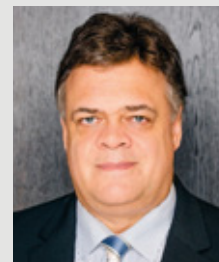
Ort der Videoüberwachung an einer für die betroffene Person zugänglichen Stelle bereit bzw. zur Verfügung zu stellen, beispielsweise als vollständiges Informationsblatt (Aushang)“. Gar nicht angesprochen wird die Regelung in § 4 Abs. 3 BDSG 2018, wonach nur der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen sind.

Beide Kurzpapiere, die ja für sich in Anspruch nehmen, als Orientierung für den praktischen Vollzug zu dienen, ignorieren die für die Praxis wichtige Frage des Medienbruchs bei den Informationspflichten. Dabei plädierten die in Art. 29-Datenschutzgruppe zusammengeschlossenen Aufsichtsbehörden der EU bereits im Working Paper 100 dafür, dass „Informationen für die Betroffenen auf mehreren Ebenen verteilt werden, solange die Gesamtheit dieser Ebenen den rechtlichen Anforderungen entspricht.“ Die Art. 29-Datenschutzgruppe hält im aktuellen WP 260 an der gestuften Information fest. Auch der EuGH hat mit Urteil v. 30.03.2017 hinsichtlich der RL 2005/29 entschieden, dass räumliche oder zeitliche Beschränkungen eines Kommunikationsmediums es rechtfertigen können, die notwendigen Informationen auf anderem Wege zur Verfügung zu stellen. Die Ignorierung des § 4 BDSG mit seiner speziellen Transparenzanforderung bei der Videoüberwachung lässt zu-

sätzlich großen Zweifel an der Praxis-tauglichkeit dieser Kurzpapiere aufkommen.

Die DSK als Verantwortliche für diese Interpretation der DS-GVO und des neuen BDSG müssen sich fragen lassen, ob sie mit ihrer strengen und dogmatischen Auslegung des neuen Datenschutzrechts als Ansprechpartner ernst genommen werden wollen. Sie müssen sich zudem selber fragen, ob sie damit der Sache des Datenschutzes dienen. Von Wirtschaft und Verwaltung zu verlangen, die Bürger mit den umfangreichen, sich in der Regel wiederholenden Vorgaben immer und überall und mit weitgehend dem gleichen Inhalt zu belehren, wird Abwehrreaktionen hervorrufen. Datenschutz wird als belästigende Bürokratie wahrgenommen werden. Das ist kontraproduktiv.

Andreas Jaspers



RA Andreas Jaspers

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

Termin	Thema	Ort	Kontakt
28.06.2018	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V. und DATAKONTEXT
05.07.2018	Löschen nach DS-GVO	Köln	GDD e.V. und DATAKONTEXT
06.-08.08.2018	GDD-Sommer-Workshop	Timmendorfer Strand	GDD e.V. und DATAKONTEXT
03.09.2018	Auftragsverarbeitung nach DS-GVO	Düsseldorf	GDD e.V. und DATAKONTEXT
04.09.2018	ISO 27001 und Datenschutz	Köln	GDD e.V. und DATAKONTEXT
05.09.2018	Basiswissen IT-Sicherheit	Köln	GDD e.V. und DATAKONTEXT
06.09.2018	Die ePrivacy-Verordnung im Zusammenspiel mit der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
10.-14.09.2018	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Bonn	GDD e.V. und DATAKONTEXT
11.09.2018	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Köln	GDD e.V. und DATAKONTEXT
18.09.2018	Beschäftigtendatenverarbeitung: Zulässigkeit und Organisation	Köln	GDD e.V. und DATAKONTEXT
20.09.2018	Big Data-Analysen nach DS-GVO und BDSG neu	Köln	GDD e.V. und DATAKONTEXT
24.-25.09.2018	Update-Workshop zur DS-GVO	Köln	GDD e.V. und DATAKONTEXT
25.09.2018	Datenschutz-Bußgeldrisiken schnell und effizient identifizieren	Köln	GDD e.V. und DATAKONTEXT
26.09.2018	Verzeichnis von Verarbeitungstätigkeiten, Datenschutz-Folgeabschätzung	Frankfurt/M.	GDD e.V. und DATAKONTEXT
27.09.2018	Tätigkeitsbericht des betrieblichen Datenschutzbeauftragten	Frankfurt/M.	GDD e.V. und DATAKONTEXT
27.09.2018	Der Dialog mit der Datenschutz-Aufsichtsbehörde	Köln	GDD e.V. und DATAKONTEXT
09.10.2018	Datenlöschung und andere SAP-Funktionen für den Datenschutz	Berlin	GDD e.V. und DATAKONTEXT
08.-10.10.2018	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Berlin	GDD e.V. und DATAKONTEXT
11.10.2018	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
16.10.2018	Videoüberwachung nach neuem BDSG und DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
17.10.2018	Strafverfolgung, Whistleblowing, Internal Investigations – Datenschutz und Strafrecht	Köln	GDD e.V. und DATAKONTEXT
24.10.2018	Datenschutzkonforme Unternehmenskommunikation	München	GDD e.V. und DATAKONTEXT
06.-07.11.2018	Datenschutz-Management – Teil 3	Berlin	GDD e.V. und DATAKONTEXT
06.-07.11.2018	Neues Datenschutzrecht kompakt	Köln	GDD e.V. und DATAKONTEXT
08.11.2018	Grenzüberschreitender Datenverkehr unter neuen Spielregeln	Köln	GDD e.V. und DATAKONTEXT

Aufsätze

Dr. Carlo Piltz

Datenübertragbarkeit im Beschäftigungsverhältnis – Arbeitgeberwechsel: Und die Daten kommen mit?

Das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO stellt, im Vergleich zu den übrigen Rechten des Betroffenen in Kapitel III der DS-GVO (z. B. Auskunft oder Löschung), eine Neuerung im europäischen Datenschutzrecht dar.¹ Nicht nur, weil ein solches Recht auf „Mitnahme“ der Daten von einem Verantwortlichen zu einem anderen Verantwortlichen bisher nicht existierte. Die Neuerung dieses Rechts besteht vor allem auch darin, dass mit Art. 20 DS-GVO eine Art „wettbewerbsrechtlicher Fremdkörper“ im Datenschutzrecht Platz findet.² Ziel der Regelung ist es, den Betroffenen die Kontrolle über „ihre“ personenbezogenen Daten zurückzugeben.³

Der ursprünglich intendierte Anwendungsbereich dieses Rechts liegt im Online-Bereich. In den Ratsdokumenten zur DS-GVO werden als Anwendungsbeispiele sogar speziell soziale Netzwerke im Internet genannt.⁴ Einige Delegationen im Rat wollten das Recht allein auf Angebote sozialer Medien im Internet begrenzen.⁵ Der finale Wortlaut der Vorschrift beschränkt den Anwendungsbereich jedoch nicht etwa auf Plattformanbieter im Internet oder von Apps. Mangels einer solchen Begrenzung stellt sich daher die Frage, ob und wenn ja, inwieweit Art. 20 DS-GVO auch im Verhältnis zwischen Arbeitgebern und Arbeitnehmern anwendbar ist.

I. Anwendbarkeit im Beschäftigungsverhältnis

1. Keine Beschränkungen durch den nationalen Gesetzgeber

Als Teil der Rechte des Betroffenen des Kapitels III der DS-GVO hätte der nationale Gesetzgeber in Deutschland die Möglichkeit gehabt, Art. 20 DS-GVO im Rahmen der Anforderungen des Art. 23 Abs. 1 DS-GVO zu beschränken. Der Bundesrat empfahl dem deutschen Gesetzgeber die Prüfung von Einschränkungen analog zum Auskunftsrecht.⁶ Der Empfehlung wurde jedoch nicht gefolgt. Dem Grunde nach gilt Art. 20 DS-GVO mithin ohne besondere Einschränkungen auch in Deutschland.

2. Vorrang besonderer Regelungen zum Beschäftigtendatenschutz?

Hinsichtlich der Antwort auf die Frage, ob Art. 20 DS-GVO überhaupt im Beschäftigtenverhältnis Anwendung findet, muss zudem geprüft werden, ob nationale Vorschriften zum Umgang mit Beschäftigtendaten auf der Grundlage der Spezifizierungsmöglichkeit des Art. 88 Abs. 1 DS-GVO⁷ vorrangig vor den Regelungen der DS-GVO anzuwenden sind und damit etwa auch eine Beschränkung oder gar ein Ausschluss des Rechts auf Datenübertragbarkeit im Beschäftigungsverhältnis durch solche nationalen Vorschriften vorrangig gilt. Auf die bereits in der Literatur geführte Diskussion, ob na-

tionale Vorschriften, die auf der Grundlage des Art. 88 Abs. 1 DS-GVO geschaffen werden, den „allgemeinen“ Vorschriften der DS-GVO im Sinne von *lex specialis*-Regelungen vorgehen, kann hier verwiesen werden, ohne jedoch den Diskussionsstand näher zu beleuchten.⁸ Denn der deutsche Gesetzgeber sieht in § 26 BDSG nF keine Regelungen zum Recht auf Datenübertragbarkeit vor, die gegenüber Art. 20 DS-GVO als speziellere Vorgaben zu berücksichtigen wären. Im Ergebnis lässt sich mithin feststellen, dass Art. 20 DS-GVO weder allgemein noch speziell im hier interessierenden Kontext der Datenverarbeitung im Beschäftigungsverhältnis beschränkt oder gar ausgeschlossen wird.

1 Kamann/Braun, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 2 m.w.N.; Piltz, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 1.

2 Von Lewinski, in: BeckOK Datenschutzrecht, Wolff/Brink 22. Edition Stand: 01.11.2017, Art. 20; AA Sydow, in: Sydow, Europäische Datenschutzgrundverordnung, 2017, Art. 20 Rn. 23.

3 Ratsdokument 5879/14, 31.1.2014, S. 2

4 Ratsdokument 5879/14, 31.1.2014, S. 2; Ratsdokument 8172/14, 25.3.2014, S. 4 dort Fn. 4 und 5.

5 Piltz, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 6 m.w.N.

6 BR Drs. 110/17 (Beschluss), S. 3.

7 „Spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten“, Art. 88 Abs. 1 DS-GVO.

8 Zu § 26 BDSG 2018: Piltz, BDSG, 1. Aufl. 2018, § 26 Rn. 17 ff.; für einen Vorrang im Sinne der *lex specialis*: Riesenhuber, in: BeckOK Datenschutzrecht, Wolff/Brink, 22. Edition, Stand: 01.11.2017, Art. 88 Rn. 16; Selk, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 88 Rn. 52.

3. Ausschluss aufgrund des intendierten Zwecks der Vorschrift?

Zuletzt lässt sich überlegen, ob Art. 20 DS-GVO bereits an sich so auszulegen und anzuwenden ist, dass allein solche Verantwortlichen von den Pflichten umfasst sind, die Dienste im Online-Bereich anbieten. Hierfür lassen sich sicherlich die gesetzgeberische Intention der Vorschrift und in den Ratsverhandlungen ausdrücklich erwähnte Beispielfälle anführen.⁹ Gegen eine solche Auslegung und Anwendung des Art. 20 DS-GVO spricht jedoch der eindeutige Wortlaut der Vorschrift, der, wie bereits erwähnt, gerade keine Differenzierung oder Einschränkung im Anwendungsbereich vornimmt.¹⁰ Verpflichtet ist der Verantwortliche iSd Art. 4 Nr. 7 DS-GVO. Gegen eine Herausnahme von Arbeitgebern als Verantwortlichen bereits auf Ebene des Anwendungsbereichs spricht zudem, dass der europäische Gesetzgeber Art. 20 DS-GVO durchaus inhaltlichen Beschränkungen unterworfen hat, die sich auf seinen Anwendungsbereich auswirken. So gilt das Recht auf Datenübertragbarkeit nach Art. 20 Abs. 3 S. 2 DS-GVO nämlich nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 6 Abs. 1 lit. e) DS-GVO). Dies zeigt, dass der Gesetzgeber durchaus eine Beschränkung des Anwendungsbereichs intendierte und diese auch für spezielle Datenverarbeitungssituationen umsetzte; nur eben nicht bezogen auf bestimmte Wirtschaftszweige oder Rollen von Verantwortlichen.

Zum Teil wird auch argumentiert, dass Recht auf Datenübertragbarkeit zwar im Beschäftigungsverhältnis grundsätzlich für anwendbar zu erklären, die Ausübung durch den Arbeitgeber jedoch allein auf die Situation des Arbeitgeberwechsels und sogar noch weitergehend nur auf Fälle der vorherigen Einwilligung des Arbeitnehmers zu beschränken.¹¹ Auch diese Interpretation lässt sich jedoch mit dem Wortlaut der Vorschrift kaum vereinbaren.

4. Zwischenergebnis

Art. 20 DS-GVO ist daher dem Grunde nach auch im Beschäftigungsverhältnis anwendbar.¹² Eine andere, nachfolgend behandelte Frage ist, ob wirklich auch stets alle Tatbestandsvoraussetzungen für einen Anspruch des betroffenen Arbeitnehmers gegen seinen Arbeitgeber erfüllt sind und ob der Umfang des Rechts eventuell durch die Rechte des Arbeitgebers oder anderer Dritter beschränkt ist.

II. Voraussetzungen des Art. 20 DS-GVO

1. Einwilligung oder Vertrag

Nach ErWG 68 S. 4 DS-GVO gilt das Recht auf Datenübertragbarkeit nicht, wenn die Verarbeitung auf einer anderen Rechtsgrundlage als der Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a) DS-GVO) oder eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person (Art. 6 Abs. 1 lit. b) DS-GVO) erfolgt. Dies ergibt sich auch direkt aus Art. 20 Abs. 1 lit. a) DS-GVO, der

das Vorliegen einer dieser beiden Erlaubnistatbestände als zwingende Voraussetzung des Rechts auf Datenübertragbarkeit qualifiziert.¹³

Fraglich ist jedoch, ob eine Datenverarbeitung im Rahmen des Beschäftigungsverhältnisses auf einer Einwilligung gemäß Art. 6 Abs. 1 lit. a) DS-GVO oder Art. 9 Abs. 2 lit. a) DS-GVO oder auf einem Vertrag gemäß Art. 6 Abs. 1 lit. b) DS-GVO beruht. Oder stellen eventuell der § 26 Abs. 1 und Abs. 2 BDSG nF einen eigenen gesetzlichen Erlaubnistatbestand neben Art. 6 Abs. 1 und Art. 9 Abs. 2 DS-GVO dar? Denn würde man davon ausgehen, dass personenbezogene Daten im Beschäftigtenverhältnis, etwa zur Durchführung des Arbeitsvertrages, allein auf der Grundlage des § 26 Abs. 1 S. 1 BDSG nF verarbeitet werden, läge keine Verarbeitung gemäß Art. 6 Abs. 1 lit. b) DS-GVO vor. Hierbei geht es nicht um die, oben erwähnte, Diskussion, ob nationale Regelungen in Ausformung des Art. 88 Abs. 1 DS-GVO als *lex specialis* zu den übrigen Vorgaben der DS-GVO anzusehen sind. Vielmehr ist hier von Relevanz, ob auf nationaler Ebene eigen- und selbstständige Erlaubnistatbestände geschaffen werden können.

a. Für eigene Erlaubnistatbestände im nationalen Recht

Nach Art. 88 Abs. 1 DS-GVO können die Mitgliedstaaten durch Rechtsvorschriften „spezifischere Vorschriften“ zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigendaten im Beschäftigungskontext vorsehen. Fraglich ist, ob der europäische Gesetzgeber von den „spezifischere Vorschriften“ auch „eigenständige“ Vorschriften zur Rechtmäßigkeit umfasst sieht. Nach ErWG 10 S. 6 DS-GVO schließt die DS-GVO nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist. Rein dem Wortlaut nach bezieht sich der ErWG 10 S. 6 DS-GVO auf die „genauere Bestimmung der Voraussetzungen“ der Rechtmäßigkeit. Die Voraussetzungen der „Rechtmäßigkeit der Verarbeitung“ ergeben sich aus Art. 6 DS-GVO, also den Erlaubnistatbeständen, der auch entsprechend betitelt ist. Daher könnte man davon ausgehen, dass der Gesetzgeber von den spezifischeren Vorschriften auch eigenständige nationale

9 Ratsdokument 5879/14, 31.1.2014, S. 2; Ratsdokument 8172/14, 25.3.2014, S. 4 dort Fn. 4 und 5.

10 Im Ergebnis ebenso: Kamann/Braun, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 5.

11 So wohl Wybitul/Rauer, ZD 2012, 160, 162. V. Lewsinski, in: BeckOK Datenschutzrecht, Wolff/Brink, 22. Edition Stand: 01.11.2017, Art. 20 Rn. 26 sieht Art. 20 DS-GVO in diesem Fall nur dann anwendbar, wenn ein Personalinformationssystem auf der Einwilligung beruht und ausschließlich vom Betroffenen bereitgestellte Daten enthalten würde.

12 Ebenso: Gola, in: Gola, Datenschutz-Grundverordnung, 2017, Einl. Rn. 28; Unabhängiges Datenschutzzentrum Saarland, 26. Tätigkeitsbericht 2015/2016, S. 18; Art. 29-Datenschutzgruppe, Working Paper 242 rev 01, S. 10; Stiftung Datenschutz, Praktische Umsetzung des Rechts auf Datenübertragbarkeit, 2017, S. 43; Wybitul/Rauer, ZD 2012, 160, 162; a.A. wohl v. Lewsinski, in: BeckOK Datenschutzrecht, Wolff/Brink 22. Edition Stand: 01.11.2017, Art. 20 Rn. 26.

13 Piltz, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 15.

Rechtsgrundlagen umfasst sieht, wenn er hinsichtlich der spezifischen Vorschriften gerade auf die genaueren Bestimmungen der Rechtmäßigkeit verweist.

b. Gegen eigene Erlaubnistatbestände im nationalen Recht

Ebenso wie der Wortlaut der DS-GVO jedoch für die Befugnis des nationalen Gesetzgebers spricht, eigenständige Erlaubnistatbestände im nationalen Recht zu schaffen, lässt sich der Wortlaut auch gegen eine solche Interpretation anführen. Denn ErwG 10 S. 6 DS-GVO bezieht sich nur auf die „genauere Bestimmung der Voraussetzungen“ der Rechtmäßigkeit. Jedoch wird nicht von „neuen“ oder „anderen“ Bestimmungen gesprochen, die der nationale Gesetzgeber schaffen dürfte. Weiter ist zu beachten, dass ErwG 10 S. 5 DS-GVO davon spricht, dass die DS-GVO den Mitgliedstaaten „einen Spielraum für die Spezifizierung ihrer Vorschriften“ bietet. Dies impliziert aber zugleich, dass es einen mit (hier: regulatorischen) Grenzen versehen Raum geben muss. Auch bei der Spezifizierung müssen Mitgliedstaaten also im Rahmen der Vorgaben der DS-GVO bleiben und können keine daneben und außerhalb des Spielraums geltenden Vorschriften schaffen.¹⁴ Die Schaffung eigener, unabhängiger nationaler Erlaubnistatbestände würde diesen Spielraum verlassen.

Gerade mit Blick auf Datenverarbeitungen im Beschäftigungsverhältnis lässt sich zudem anführen, dass der europäische Gesetzgeber ausweislich der Begründungen in ErwG 48 DS-GVO davon auszugehen scheint, dass auch die Verarbeitung von Arbeitnehmerdaten immer noch auf einem Erlaubnistatbestand nach Art. 6 Abs. 1 DS-GVO beruhen muss. Denn nach ErwG 48 DS-GVO können Verantwortliche ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Beschäftigten, zu übermitteln. ErwG 48 DS-GVO nimmt hier Bezug auf Art. 6 Abs. 1 lit. f) DS-GVO und erwähnt etwa nicht noch zusätzlich zu schaffende nationale Rechtsgrundlagen für eine Übermittlung von Beschäftigten-daten. Der europäische Gesetzgeber ging also davon aus, dass auch bei einer Verarbeitung von Mitarbeiterdaten für Zwecke des Beschäftigungsverhältnisses die Vorgaben der Art. 6 Abs. 1 DS-GVO zu beachten sind.¹⁵

Als weiteres Argument gegen die Möglichkeit, im nationalen Recht eigenständige, von den Art. 6 Abs. 1 DS-GVO unabhängige Erlaubnistatbestände zu schaffen, lässt sich zudem die Gesetzgebungshistorie der DS-GVO anführen. Die Europäische Kommission stellte während der Diskussionen im Rat der Europäischen Union zum Beschäftigtendatenschutz im Hinblick auf die in Art. 88 Abs. 1 DS-GVO gleichstufig neben den Rechtsvorschriften erwähnten Kollektivvereinbarungen (zu denen auch Betriebsvereinbarungen gehören) klar, dass Datenverarbeitungen im Beschäftigungskontext durch nationale Betriebsvereinbarungen auf der Grundlage des Erlaubnistatbestandes nach Art. 6 Abs. 1 lit. c) DS-GVO (Erfüllung gesetzlicher Verpflichtungen) gestattet sind.¹⁶ Wenn Betriebsvereinbarungen an sich aber keine eigenständigen nationalen Erlaubnistatbestände darstellen, sondern

stets iVm Art. 6 Abs. 1 lit. c) DS-GVO anzuwenden sind, dann muss rein systematisch dasselbe für die gleichstufig neben den Kollektivvereinbarungen erwähnten Rechtsvorschriften in Art. 88 Abs. 1 DS-GVO gelten.¹⁷ Eine Unterscheidung hinsichtlich des eröffneten Gestaltungsspielraums für die Mitgliedstaaten macht der europäische Gesetzgeber nicht. Die besseren Gründe sprechen daher dafür, eine Möglichkeit der Mitgliedstaaten, nationale Erlaubnistatbestände neben Art. 6 Abs. 1 DS-GVO zu schaffen, abzulehnen.¹⁸

c. Zwischenergebnis

Für die Anwendung des Art. 20 DS-GVO bedeutet dies, dass auch wenn Beschäftigtendaten zur Durchführung oder Beendigung eines Beschäftigungsverhältnisses auf der Basis des § 26 Abs. 1 BDSG nF verarbeitet werden, diese Verarbeitung gleichzeitig stets immer noch auf Grundlage des Art. 6 Abs. 1 lit. b) DS-GVO (zur Durchführung des Arbeitsvertrages) oder auch auf der Grundlage des Art. 6 Abs. 1 lit. a) DS-GVO (Einwilligung) erfolgt. Damit ist auch die erste zwingende Voraussetzung nach Art. 20 Abs. 1 DS-GVO erfüllt, dass die Verarbeitung auf der Rechtsgrundlage der Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a) oder eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person (Art. 6 Abs. 1 lit. b) erfolgen muss.

2. Betriebsvereinbarungen, öffentlicher Bereich und Interessenabwägung

Das Recht auf Datenübertragbarkeit gilt aber nicht, wenn die Verarbeitung auf einer anderen Rechtsgrundlage als der Einwilligung der betroffenen oder eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person erfolgt (ErwG 68 S. 4 DS-GVO). Insbesondere die Verarbeitung von Beschäftigtendaten auf der Grundlage der Interessenabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO ist daher nicht vom Anwendungsbereich des Art. 20 DS-GVO erfasst. Ebenso wenig sind solche Daten zu berücksichtigen, die der Verantwortliche zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, verarbeitet (Art. 6 Abs. 1 lit. c) DS-GVO). Wie bereits erwähnt, betrifft dies Datenverarbeitungen auf der Grundlage von Betriebsvereinbarungen. Betriebsvereinbarungen stellen nationale Regelungen iSd Art. 6 Abs. 1 lit. c) DS-GVO dar, die den Arbeitsgeber verpflichten, da sie ihn normativ binden.¹⁹ Verarbeiten Arbeitgeber als Verantwortliche die Daten von Beschäftigten auf

14 Zu § 26 BDSG 2018: Piltz, BDSG, 1. Aufl. 2018, § 26 Rn. 25.

15 Zu § 26 BDSG 2018: Piltz, BDSG, 1. Aufl. 2018, § 26 Rn. 25; wohl auch: Sörup/Marquardt, ArbRAktuell 2016, 103, 104.

16 Ratsdokument 15108/14, 05.11.2014, S. 2.

17 Zu § 26 BDSG 2018: Piltz, BDSG, 1. Aufl. 2018, § 26 Rn. 26.

18 So auch: Hanloser, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 2017, Teil IV, Kapitel 1, Beschäftigtendatenschutz, Rn. 11 ff.

19 Hanloser, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 2017, Teil IV, Kapitel 1, Beschäftigtendatenschutz, Rn. 14; Gola, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 6 Rn. 120; Wybitul/Sörup/Pötters, ZD 2015, 559, 560; Wurzberger, ZD 2017, 258, 259; zu § 26 BDSG 2018: Piltz, BDSG, 1. Aufl. 2018, § 26 Rn. 26.

der Grundlage einer gesetzlichen Verpflichtung, sind diese Daten nach Art. 20 Abs. 3 S. 2 DS-GVO nicht vom Recht auf Datenübertragbarkeit umfasst. Dies betrifft beispielsweise gesetzliche Pflichten zur Meldung von Arbeitnehmerdaten an Krankenversicherungen (§ 28a SGB IV).²⁰

Zuletzt gilt Art. 20 DS-GVO damit auch dann nicht, wenn die Verarbeitung durchgeführt wird, weil sie für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, erforderlich ist (Art. 6 Abs. 1 lit. e) DS-GVO). Dies dürfte vor allem für öffentliche Stellen zutreffen. Art. 20 Abs. 3 S. 2 DS-GVO stellt dies noch einmal ausdrücklich klar. Sollten jedoch öffentliche Stellen privatrechtliche Anstellungsverträge mit Mitarbeitern abschließen und auf dieser Grundlage Daten verarbeitet werden, ist der Anwendungsbereich nach Art. 20 Abs. 1 lit. a) DS-GVO grundsätzlich eröffnet.

3. Bereitgestellte Daten

Das Recht auf Datenübertragbarkeit erstreckt sich nach Art. 20 Abs. 1 DS-GVO nur auf solche personenbezogenen Daten, die der Betroffene einem Verantwortlichen bereitgestellt hat. Im Beschäftigungsverhältnis werden mithin nur solche Daten erfasst, die der Arbeitnehmer dem Arbeitgeber auf der Grundlage einer Einwilligung oder eines Vertrages bereitgestellt hat.

Was konkret mit den „bereitgestellten“ Daten gemeint ist, wird in der Literatur bereits strittig diskutiert. Die Art. 29 Datenschutzgruppe geht in ihren Leitlinien zum Recht auf Datenübertragbarkeit davon aus, dass damit sowohl personenbezogene Daten gemeint sind, die wissentlich und aktiv von der betroffenen Person bereitgestellt werden, aber auch solche Daten, die aus der Beobachtung der Tätigkeiten eines Nutzers resultieren (sog. „beobachtete Daten“).²¹ Hierzu zählt die Art. 29 Datenschutzgruppe etwa Daten, die in Tätigkeitsprotokollen oder in Webseiten- bzw. Suchverläufen verarbeitet werden. Diese, sehr weitgehende, Ansicht der Art. 29 Datenschutzgruppe ist abzulehnen.²²

Bereits nach dem Wortlaut beinhaltet der Begriff „Bereitstellen“ als auch der in ErwG 68 S. 3 DS-GVO verwendete Begriff „zur Verfügung gestellt hat“ ein aktives und wissentliches Verhalten der betroffenen Person.²³ Zudem ergibt sich aus einer systematischen Betrachtung zu den übrigen Betroffenenrechten, insbesondere jenem auf Auskunft (Art. 15 DS-GVO), dass der Gesetzgeber den Umfang des Anspruchs auf Datenübertragbarkeit durch die Formulierung der „bereitgestellten“ Daten beschränken wollte.²⁴ Im Anwendungsbereich des Art. 20 DS-GVO geht es gerade nicht um alle bei einem Verantwortlichen vorhandenen personenbezogenen Daten. Ansonsten würden die Grenzen zwischen dem Recht auf Auskunft und jenem auf Datenübertragbarkeit verschwinden.

Geht man davon aus, dass die „bereitgestellten“ Daten solche Datenarten erfassen, die vom Betroffenen aktiv zur Verfügung gestellt wurden, so stellt sich mit Blick auf das Beschäftigungsverhältnis die Frage, welche Datenarten umfasst sein könnten. Beispielfhaft ist etwa an Zeugnisse, vor-

malige Bewertungen oder andere arbeitsrelevante Unterlagen zu denken, die der Arbeitnehmer seinem Arbeitgeber zur Verfügung stellt. Ebenso kommen Daten aus Anmelde-masken oder Online-Formularen (z. B. im Intranet) in Betracht.²⁵ Umfasst sind auch direkt an den Arbeitgeber (bzw. für ihn handelnde Vorgesetzte des Arbeitgebers) übermittelte oder ihm offengelegte Daten (z. B. in E-Mails). Nicht erfasst wären hingegen solche Daten, die der Arbeitgeber selbst generiert und aus vorhandenen Daten über den Arbeitnehmer ableitet, auch wenn er diese dem Arbeitnehmer danach zur Verfügung stellt. Denn Art. 20 Abs. 1 DS-GVO bezieht sich ausdrücklich auf durch den Betroffenen bereitgestellte Daten und erfasst nicht die entgegengesetzte Richtung der Bereitstellung durch den Verantwortlichen.

4. Beschränkung durch Abs. 4

Nach Art. 20 Abs. 4 DS-GVO darf das Recht gemäß Abs. 2 die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Zunächst ist herauszustellen, dass es sich bei dem Verweis auf Abs. 2 in der deutschen Fassung wohl um ein redaktionelles Versehen handelt.²⁶ Dafür sprechen zum einen die anderen Sprachfassungen, die auf Abs. 1 verweisen.²⁷ Zudem ergibt sich dieses Versehen aus den Verhandlungsdokumenten des Rates. Dort wurde der ursprüngliche Abs. 1 gestrichen und der damalige Art. 20 Abs. 2 DS-GVO wurde zum jetzigen Abs. 1. Die Anpassung des Verweises in Abs. 4 von Abs. 2 auf Abs. 1 wurde vergessen.²⁸ Der Vorbehalt der Nichtbeeinträchtigung der Rechte anderer Personen gilt nicht nur für die Direktübermittlung nach Art. 20 Abs. 2 DS-GVO, sondern für alle Ansprüche auf Datenportabilität.²⁹

a. Arbeitgeber als „andere Person“

Eine Einschränkung des Rechts auf Datenübertragbarkeit im Beschäftigungsverhältnis käme in Betracht, wenn von der Ausnahmeregelung nach Art. 20 Abs. 4 DS-GVO das Verhältnis zwischen Arbeitgeber und Arbeitnehmer erfasst wäre. Dafür müsste es sich bei dem Arbeitgeber, als Verantwortlichen, um die in Art. 20 Abs. 4 DS-GVO benannte „andere Person“ handeln, deren Rechte und Freiheiten bei der Ausübung des Betroffenenrechts nicht beeinträchtigt werden

20 Weitere Beispiele: bitkom, Stellungnahme, Zum Recht auf Datenübertragbarkeit nach Art. 20 Datenschutz-Grundverordnung, 14.03.2017, Anlage 2.

21 Art. 29-Datenschutzgruppe, Working Paper 242 rev 01, S. 11.

22 Ebenso: Brüggemann, in: Tagungsband DSRI-Herbstakademie 2017, 1, 4.

23 Kamann/Braun, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 13; Brüggemann, in: Tagungsband DSRI-Herbstakademie 2017, 1, 4; Piltz, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 14; ders., K&R 2016, 634; a.A. Jülicher/Röttgen/v. Schönfeld, ZD 2016, 358, 359.

24 Brüggemann, in: Tagungsband DSRI-Herbstakademie 2017, 1, 4.

25 V. Lewinski, in: BeckOK Datenschutzrecht, Wolff/Brink 22. Edition Stand: 01.11.2017, Art. 20 Rn. 41.

26 Piltz, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 35.

27 Insbesondere auch die englische Sprachfassung.

28 Piltz, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 35.

29 V. Lewinski, in: BeckOK Datenschutzrecht, Wolff/Brink 22. Edition Stand: 01.11.2017, Art. 20 Rn. 92.

dürfen. Dem Wortlaut nach bezieht sich Art. 20 Abs. 4 DS-GVO nicht nur auf Rechte und Freiheiten in Bezug auf den Schutz personenbezogener Daten, sondern ist umfassend zu verstehen.³⁰ ErwG 68 S. 8 DS-GVO bezieht sich zwar allein auf die Konstellation, dass von dem Recht auf Datenübertragbarkeit die Rechte und Freiheiten einer anderen betroffenen Person berührt werden.³¹ Art. 20 Abs. 4 DS-GVO selbst bezieht sich aber nicht nur auf die, in Art. 4 Nr. 1 DS-GVO legal definierte, betroffene Person oder etwa nur andere natürliche Personen. Auch der Verantwortliche wird in Art. 4 Nr. 7 DS-GVO legal definiert, jedoch in Art. 20 Abs. 4 DS-GVO nicht erwähnt.³² Die Erwähnung der betroffenen Personen in ErwG 68 S. 8 DS-GVO dürfte daher als ein, aus Sicht des Gesetzgeber eventuell gerade auch der relevante, Fall anzusehen sein, wann die Beschränkung eingreifen soll. Mit Blick auf den Wortlaut in Art. 20 Abs. 4 DS-GVO betrifft die Ausnahmeregelung aber eben nicht nur betroffene Personen.³³ Hierfür spricht zudem, dass die DS-GVO an vielen anderen Stellen den Terminus der „Rechte und Freiheiten“ nutzt und ausdrücklich entweder mit natürlichen Personen (Art. 24 Abs. 1, Art. 25 Abs. 1 DS-GVO) oder betroffenen Personen (Art. 30 Abs. 5 DS-GVO) in Verbindung setzt, jedoch gerade nicht in Art. 20 Abs. 4 DS-GVO. Auch der Arbeitgeber als Verantwortlicher kann sich daher auf die Ausnahmeregelung nach Art. 20 Abs. 4 DS-GVO berufen.

b. Rechte und Freiheiten des Arbeitgebers

Die Begrifflichkeit „Rechte und Freiheiten“ umfasst jedes vom europäischen Primärrecht geschützte Individualinteresse.³⁴ Es geht auch, jedoch nicht nur, um die Rechte in Bezug auf den Schutz personenbezogener Daten.³⁵ So verweist Art. 20 Abs. 4 DS-GVO gerade nicht etwa nur auf Rechte aus der DS-GVO. Zudem ergibt sich aus ErwG 4 S. 2 DS-GVO, dass die Verordnung (und damit auch das in Art. 20 DS-GVO statuierte Recht auf Datenübertragbarkeit) mit allen Grundrechten im Einklang steht und alle Freiheiten und Grundsätze achtet, die mit der Charta der Grundrechte der Europäischen Union (GRCh) anerkannt wurden und in den Europäischen Verträgen verankert sind.³⁶ Das Recht auf Schutz personenbezogener Daten muss mithin mit anderen Grundrechten und Freiheiten in Einklang gebracht werden. Hierzu zählt auch die unternehmerische Freiheit.

Die Ausnahme nach Art. 20 Abs. 4 DSGVO erfasst mithin auch die Rechte und Freiheiten von Arbeitgebern. In der Praxis dürfte sich die Beschränkung des Rechts auf Datenübertragbarkeit vor allem mit Blick auf Herausgabe (Abs. 1) oder Direktübermittlung (Abs. 2) von solchen Informationen als kritisch erweisen, die aus Sicht des (alten) Arbeitgebers Geschäfts- und Betriebsgeheimnisse darstellen. Eine Definition der Geschäftsgeheimnisse findet sich in der DS-GVO nicht. Auf europäischer Ebene kann auf die Begriffsbestimmung in der Richtlinie EU 2016/943 zurückgegriffen werden.³⁷ Nach Art. 2 Nr. 1 lit. a) bis c) Richtlinie EU 2016/943 sind Geschäftsgeheimnisse solche Informationen, die Kreisen, welche üblicherweise mit dieser Art von Informationen umgehen, nicht allgemein bekannt oder ohne

weiteres zugänglich sind, gerade aufgrund der Tatsache, dass sie geheim sind, einen kommerziellen Wert haben und durch entsprechende Geheimhaltungsmaßnahmen des rechtmäßigen Inhabers der Information geschützt werden.³⁸ Eine ausdrückliche Verankerung finden Geschäftsgeheimnisse in der GRCh zwar nicht. Jedoch werden als Anknüpfungspunkte das Eigentumsrecht gemäß Art. 17 Abs. 1 GRCh und die unternehmerische Freiheit gemäß Art. 16 GRCh herangezogen.³⁹ Nach der Rechtsprechung des EuGH stellt der Schutz von Geschäftsgeheimnissen in jedem Fall einen allgemeinen Grundsatz des Unionsrechts dar.⁴⁰ Der Bereich, für den dieser Grundsatz gilt, beschränkt sich nicht auf Geschäftsgeheimnisse im eigentlichen Sinne, d.h. vertrauliche Geschäftsinformationen, sondern umfasst auch sonstige vertrauliche Informationen.⁴¹ Geschäftsgeheimnisse eines Arbeitgebers werden daher von den in Art. 20 Abs. 4 DS-GVO erwähnten „Rechten und Freiheiten“ erfasst.

Hierfür spricht auch ErwG 63 S. 5 DS-GVO zu dem Recht auf Auskunft (Art. 15 DS-GVO). Danach sollte dieses Recht die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen. ErwG 63 S. 5 DS-GVO referenziert auf Art. 15 Abs. 4 DS-GVO, der übereinstimmend mit Art. 20 Abs. 4 DS-GVO vorgibt, dass „die Rechte und Freiheiten anderer Personen“ nicht beeinträchtigt werden dürfen. Aus der klarstellenden Erläuterung in ErwG 63 S. 5 DS-GVO lässt sich der Schluss ziehen, dass von der Formulierung „die Rechte und Freiheiten anderer Personen“ gerade auch Geschäftsgeheimnisse umfasst sind. Gründe dafür, den Begriff hier, im Rahmen des Rechts auf Auskunft, anders auszulegen als im Anwendungsbereich des Rechts auf Datenübertragbarkeit, sind nicht ersichtlich, und in der DS-GVO finden sich auch keine Anhaltspunkte hierfür.

30 Piltz, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 36; v. Lewinski, in: BeckOK Datenschutzrecht, Wolff/Brink 22. Edition Stand: 01.11.2017, Art. 20 Rn. 102.

31 „sollte das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach dieser Verordnung unberührt lassen“.

32 V. Lewinski, in: BeckOK Datenschutzrecht, Wolff/Brink 22. Edition Stand: 01.11.2017, Art. 20 Rn. 102.

33 Piltz, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 36; wohl auch: Kamann/Braun, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 31, „alle Rechte und Freiheiten Dritter“.

34 V. Lewinski, in: BeckOK Datenschutzrecht, Wolff/Brink 22. Edition Stand: 01.11.2017, Art. 20 Rn. 93.

35 Herbst, in: Kühling/Buchner, Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 18.

36 V. Lewinski, in: BeckOK Datenschutzrecht, Wolff/Brink 22. Edition Stand: 01.11.2017, Art. 20 Rn. 103.

37 Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. L 157 vom 15.06.2016, S. 1–18.

38 V. Lewinski, in: BeckOK Datenschutzrecht, Wolff/Brink 22. Edition Stand: 01.11.2017, Art. 20 Rn. 99.

39 Schoch, Informationsfreiheitsgesetz, 2. Aufl. 2016, § 6 Rn. 14 m.w.N.

40 EuGH, Urt. v. 29.03.2012 – C-1/11 (Interseroh/SAM), Rz. 43 m.w.N.

41 Generalanwalt Szpunar, Schlussantrag vom 21.07.2016 – C-162/15 P, Rz. 41.

III. Schluss

Das Recht auf Datenübertragbarkeit dürfte in der Praxis noch für einige Überraschungen sorgen. Wie gezeigt, ist der Anwendungsbereich dieses Rechts, wenn auch durch den Gesetzgeber ursprünglich vielleicht nicht intendiert, in seiner finalen Fassung sehr umfassend ausgestaltet und betrifft auch das Beschäftigungsverhältnis. Für Arbeitgeber besteht jedoch die Möglichkeit, entgegenstehende Rechte geltend zu machen, sollten entweder die an den Arbeitgeber als betroffene Person herauszugebenen oder aber dem neuen Arbeitgeber direkt zu übermittelnden Daten solche Informationen enthalten, die als Geschäftsgeheimnisse zu qualifizieren sind.



Dr. Carlo Piltz

ist Rechtsanwalt bei reuschlaw Legal Consultants. Seit Beginn seiner anwaltlichen Tätigkeit fokussierte er sich auf das Datenschutzrecht. Im März 2017 war er Sachverständiger zur Anhörung des neuen Bundesdatenschutzgesetzes im Innenausschuss des Bundestages. Der zertifizierte Datenschutzbeauftragte (TÜV®) und Certified Information Privacy Professional/

Europe (CIPP/E) berät mittlere und große Unternehmen aus Industrie und Handel schwerpunktmäßig im nationalen und internationalen Datenschutzrecht und im IT-Recht. Er ist Autor und Herausgeber des Kommentars „BDSG – Praxiskommentar für die Wirtschaft“ zum neuen Bundesdatenschutzgesetz.

Alexander Golland

Reformation 2.0 – Umsetzung der Anforderungen der Datenschutz-Grundverordnung durch die evangelische und die katholische Kirche

Die Datenschutz-Grundverordnung (DS-GVO) enthält zahlreiche Öffnungsklauseln. Eine bislang kaum beachtete Öffnungsklausel ist Art. 91 DS-GVO, welcher Religionsgemeinschaften zugesteht, eigene Regelungen zum Schutz personenbezogener Daten beizubehalten, und eine eigene (unabhängige) Datenschutzaufsicht erlaubt. Damit wurde 500 Jahre nach Luthers Thesenanschlag an der Wittenberger Schlosskirche

eine weitere Reformation angestoßen: Das Datenschutzrecht der Evangelischen Kirche in Deutschland und das der Römisch-katholischen Kirche in Deutschland wurden den Anforderungen der DS-GVO angepasst. Der folgende Beitrag skizziert die neuen Regelungen im Bereich des kirchlichen Datenschutzes und beleuchtet einige zentrale Probleme, die sich bei der Anwendung dieser Vorschriften ergeben werden.

I. Überblick

Am 15. November 2017 hat die Evangelische Kirche auf ihrer Synode das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)¹ beschlossen. Wenige Tage später, am 20. November 2017, zog die Katholische Kirche nach und beschloss auf der Vollversammlung des Verbandes der Diözesen Deutschlands das Gesetz über den Kirchlichen Datenschutz (KDG).² Mit diesen Regelwerken unternehmen die beiden großen deutschen Kirchen einen Versuch, die ihnen durch die DS-GVO eröffneten Spielräume zum Schutz personenbezogener Daten zu regulieren.

1. Das Kirchengesetz über den Datenschutz der Evangelischen Kirche

Wird das DSG-EKD oberflächlich betrachtet, fallen auf den ersten Blick erhebliche Parallelen zur DS-GVO auf. Das DSG-EKD übernimmt weitgehend die Systematik der DS-GVO. So

finden sich in Kapitel 1 die „Allgemeinen Bestimmungen“ (§§ 1–4 DSG-EKD), wobei § 3 DSG-EKD mit der Sonderregelung zu Seelsorgegeheimnis und Amtsverschwiegenheit auffällt. Die Grundsätze der Datenverarbeitung sind in dem mit „Verarbeitung personenbezogener Daten“ überschriebenen Kapitel 2 (§§ 5–15 DSG-EKD) geregelt. Hier finden sich einige Regelungen, die in der Systematik des Europäischen Datenschutzrechts wie ein Fremdkörper erscheinen. Ein Beispiel, das Anlass zur Prüfung der Wirksamkeit einer Abweichung von der DS-GVO gibt, ist die Regelung der Verantwortlichkeit für Fälle der Offenlegung an kirchliche Stellen (§ 8 Abs. 2 DSG-EKD). In dieser für die Pflichten der Gesetzesadressaten zentralen Passage wird bestimmt, dass – an-

¹ Abrufbar unter https://www.ekd.de/ekd_de/ds_doc/s17_03_Beschluss_Datenschutzgesetz.pdf.

² Abrufbar unter <https://www.datenschutz-kirche.de/sites/default/files/KDG%20i.d.%20Fassung%20des%20Beschlusses%20der%20VV%20vom%2020.11.2017.pdf>.

ders als es Art. 4 Nr. 7 DS-GVO vorsieht – nicht der Offenlegende für die Offenlegung verantwortlich sein soll,³ sondern der um die Offenlegung Ersuchende. Zwar kann es, da die Europäische Union über keine Regelungskompetenz für das Staatskirchenrecht verfügt, strenggenommen keine „Europarechtskonformität“ i.e.S. geben. Gleichwohl können Unionsrechtsakte, die auf nicht religionsbezogenen Kompetenznormen beruhen, auf die Tätigkeit der Religionsgesellschaften einwirken, wie es bei der DS-GVO der Fall ist.⁴ Auf die Grundsätze der Verarbeitung folgen die Betroffenenrechte in Kapitel 3 (§§ 16–25 DSGVO-EKD). Pflichten von Verantwortlichen und Auftragsverarbeitern finden sich in den Kapitel 4 (§§ 26–35 DSGVO-EKD). Die Anforderungen hinsichtlich der Datenschutzbeauftragten finden sich in dem separaten Kapitel 5 (§§ 36–38 DSGVO-EKD). Kapitel 6 (§§ 39–45 DSGVO-EKD) befasst sich mit der Datenschutzaufsicht; Kapitel 7 (§§ 46–48 DSGVO-EKD) regelt Rechtsbehelfe und Schadensersatz. Besondere Verarbeitungssituationen sind in Kapitel 8 (§§ 49–53 DSGVO-EKD) geregelt. Das letzte Kapitel (§§ 54–56 DSGVO-EKD) enthält die Schlussbestimmungen.

2. Das Gesetz über den kirchlichen Datenschutz

Das wenige Tage später von der katholischen Kirche in Deutschland beschlossene KDG folgt derselben Systematik. Dies trifft uneingeschränkt auf die Kapitel 1 bis 3 (§§ 1–25 KDG) zu, welche bei der Offenlegung an kirchliche Stellen mit § 9 Abs. 3 KDG einen ähnlichen Sonderweg einschlagen. Das mit „Verantwortlicher und Auftragsverarbeiter“ betitelte 4. Kapitel (§§ 26–38 KDG) orientiert sich stark an der DSGVO und enthält auch die – beim evangelischen Pendant separierten – Regeln über die Bestellung und die Aufgaben des Datenschutzbeauftragten. Im 5. Kapitel (§§ 39–41 KDG) finden sich dann die Normen, die die Übermittlung personenbezogener Daten an und in Drittländer regeln. Auf diese Vorschriften folgt das die Datenschutzaufsicht regelnde Kapitel 6 (§§ 42–47 KDG) sowie Kapitel 7 (§§ 48–51 KDG), welches Rechtsbehelfe und Schadensersatz regelt. Besondere Verarbeitungssituationen sind, genauso wie beim DSGVO-EKD, im 8. Kapitel (§§ 52–55 KDG) geregelt. Ebenso weist das KDG ein letztes Kapitel mit Schlussbestimmungen auf (§§ 56–58 KDG).

3. Kirchendatenschutzgerichtsbarkeit

Während das weltliche Datenschutzrecht einen zweigeteilten Weg einschlägt und in einigen Konstellationen die Verwaltungsgerichtsbarkeit, in anderen Konstellationen die ordentliche Gerichtsbarkeit zuständig ist, geht das Kirchendatenschutzrecht andere Wege. § 47 Abs. 1 DSGVO-EKD zentralisiert den Rechtsschutz bei den Verwaltungsgerichten der evangelischen Kirche. Einen Schritt weiter geht die das KDG flankierende Kirchliche Datenschutzgerichtsordnung (KDSGO), welche im Entwurf vorliegt.⁵ Der KDSGO-Entwurf sieht die Bildung eines kirchlichen Datenschutzgerichts mit einer kleinen Datenschutzkammer und einer großen Datenschutzkammer als Berufungsinstanz vor, welches für alle Rechtsstreitigkeiten im Bereich des KDG zuständig ist. Damit nimmt die ka-

tholische Kirche womöglich eine Entwicklung vorweg, die es im weltlichen Datenschutzrecht und seiner Zersplitterung in Verwaltungs- und ordentliche Gerichtsbarkeit (bislang) nicht gibt. Dies ist zu begrüßen, erscheint doch die Bildung spezieller Zuständigkeiten für datenschutzrechtliche Streitigkeiten im digitalen Zeitalter des 21. Jahrhunderts nur zeitgemäß.

II. Öffnungsklausel für kirchlichen Datenschutz

Einschlägige Öffnungsklausel für die Anwendung von kirchendatenschutzrechtlichen Vorschriften ist Art. 91 DSGVO. Art. 91 Abs. 1 DSGVO erlaubt die weitere Anwendung umfassender Datenschutzregeln durch die Kirchen, religiösen Vereinigungen und religiösen Gemeinschaften, soweit diese mit der DSGVO „in Einklang stehen“. Art. 91 Abs. 2 DSGVO gestattet diesen ferner eine eigene Datenschutzaufsicht. Angesprochen von diesen europarechtlichen Begrifflichkeiten sind die korporativ-institutionellen Organisationen mit religiösem bzw. weltanschaulichem Proprium.⁶ Dies schließt u.a. die beiden großen christlichen Kirchen in Deutschland ein. Die beiden Gesetze treten nach § 56 DSGVO-EKD bzw. § 58 Abs. 1 KDG am 24. Mai 2018, einen Tag vor Anwendbarkeit der DSGVO, in Kraft. Bei ihnen handelt es sich, ebenso wie bei ihren Vorgängerregelungen,⁷ um umfassende Regelungen zum Datenschutz.

Die kirchlichen Datenschutzgesetze sind aber nur insoweit anwendbar, als sie mit der DSGVO „in Einklang stehen“ (vgl. Art. 91 Abs. 1 DSGVO). Nach zum Teil vertretener Ansicht besteht damit dieselbe Bindung an die Vorgaben der DSGVO wie für die Mitgliedstaaten, sodass die kirchlichen Datenschutzvorschriften grundsätzlich von der DSGVO weder „nach oben“ abweichen noch diese konkretisieren dürfen; vielmehr seien die Spielräume maßgeblich, die auch die DSGVO den Mitgliedstaaten lässt.⁸ Die wohl herrschende Meinung gesteht den Religionsgemeinschaften zwar eine nicht auf die mitgliedstaatlichen Spielräume begrenzte Möglich-

3 Die Verantwortung trifft nach der DSGVO stets denjenigen, der die Zwecke und Mittel des jeweiligen Verarbeitungsvorganges festlegt, d.h. im Falle des Offenlegens den Offenlegenden.

4 Siehe Herbst, in: Kühling/Buchner, Datenschutz-Grundverordnung, 2017, Art. 91 Rn. 1. Aus Gründen der besseren Lesbarkeit werden im Folgenden die Begriffe „Europarechtskonformität“ und „europarechtskonforme Auslegung“ unter dem Gesichtspunkt der Vereinbarkeit mit den Anforderungen und Wertungen der DSGVO in den Grenzen der auf die Religionsgesellschaften ausstrahlenden Wirkung selbiger verwendet (siehe hierzu unten 2.).

5 Abrufbar unter <https://www.datenschutz-kirche.de/sites/default/files/KDSGO-Entwurf%20i.d.Fassung%20des%20Beschlusses%20der%20VV%20vom%2020.11.2017.pdf>.

6 Streinz, in: Streinz, Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 2. Aufl. 2012, Art. 17 AEUV Rn. 6; Waldhoff, in: Calliess/Ruffert, EUV/AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 5. Aufl. 2016, Art. 17 AEUV Rn. 18; ausführlich zum Begriff der Kirchen und Religionsgemeinschaften Classen, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 62. EL, Art. 17 Rn. 21 ff.

7 Herbst, in: Kühling/Buchner (Fn. 4), Art. 91 Rn. 11; Jacob, in: Auerhammer, DSGVO/BDSG, 5. Aufl. 2017, Art. 91 Rn. 12.

8 Ehmann/Kranig, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 91 Rn. 19; Herbst, in: Kühling/Buchner (Fn. 4), Art. 91 Rn. 15.

keit der Konkretisierung zu, allerdings nur insoweit diese bei objektiver Auslegung den Wertungen der DS-GVO entspricht.⁹ Unstreitig ist damit, dass eine Vereinbarkeit der kirchenrechtlichen Spezifika mit Art. 91 DS-GVO jedenfalls nur dann in Betracht kommt, wenn keine Abweichung von den Wertungen der DS-GVO vorliegt.

Eine abschließende Bewertung ist hier eindeutig verfrüht. Allerdings zeigen sich in beiden Gesetzen einzelne Passagen, die in erheblichem Widerspruch zu Wertungen der DS-GVO stehen. Ein simples Beispiel ist § 4 Nr. 2 lit. a DSGVO-EKD bzw. § 4 Nr. 2 KDG. In den zitierten Paragraphen übernehmen beide Gesetze die Definition der besonderen Arten personenbezogener Daten aus Art. 9 Abs. 1 DS-GVO. Zugleich ergänzen beide Gesetze diese Definition aber darum, dass Daten über die Kirchenzugehörigkeit kein besonderes personenbezogenes Datum i.S.d. jeweiligen Norm darstellen sollen. Die Kirchenzugehörigkeit ist jedoch allgemein als Datum über die religiöse Überzeugung und damit als besonderes personenbezogenes Datum anerkannt.¹⁰ Die Vorschriften der § 4 Nr. 2 lit. a Halbsatz 2 DSGVO-EKD und § 4 Nr. 2 Satz 2 KDG sind folglich nicht mit der DS-GVO vereinbar¹¹ und daher nicht anzuwenden.

Schutzlücken entstehen dadurch nicht: Bei nicht bis zur Geltung der DS-GVO mit dieser in Einklang gebrachten Regelungen ist die DS-GVO subsidiär anwendbar.¹² Dasselbe muss auch dann gelten, wenn eine Norm nicht von der Öffnungsklausel gedeckt und damit unanwendbar ist, da ansonsten dieselbe Gefährdungslage für die informationelle Selbstbestimmung des Betroffenen einträte. Daraus folgt, dass in Bereichen überschießender Regelungen durch DSGVO-EKD oder KDG die Anforderungen der Öffnungsklausel des Art. 91 Abs. 1 DS-GVO nicht erfüllt sind und in diesen Fällen die DS-GVO – ggf. auch mitgliedstaatliche Umsetzungen, soweit den Mitgliedsstaaten Regelungsspielräume eingeräumt werden – Anwendung findet.

III. Ausgesuchte Problemfelder im Einzelnen

Einige problematische Aspekte der neuen Kirchendatenschutzgesetze wurden bereits angedeutet. Im Folgenden werden zentrale Problemfelder aufgezeigt, die sich in der Praxis beider Kirchen und vor allem in der Zusammenarbeit mit diesen als Fallstricke herausstellen könnten.

1. Anwendbarkeit der kirchlichen Datenschutzgesetze auf nicht-kirchliche Auftragsverarbeiter?

Der Anwendungsbereich der Kirchendatenschutzgesetze ergibt sich aus § 2 DSGVO-EKD bzw. §§ 2, 3 KDG. Dabei enthält § 2 Abs. 1 DSGVO-EKD eine Legaldefinition der „kirchlichen Stelle“, welche alle maßgeblichen Stellen der evangelischen Kirche in Deutschland umfasst. Demgegenüber enthält § 3 Abs. 1 KDG eine gegliederte Aufzählung der Stellen der katholischen Kirche. Weit beachtlicher ist jedoch die Regelung für Auftragsverarbeiter: So regelt § 2 Abs. 3 DSGVO-EKD, dass das Gesetz auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer kirchlichen Stelle oder in deren Auftrag anwendbar ist. § 3 Abs. 2 KDG bestimmt,

dass das KDG auf die Verarbeitung personenbezogener Daten anwendbar ist, soweit diese im Rahmen der Tätigkeiten eines Verantwortlichen oder eines Auftragsverarbeiters erfolgt, wenn diese im Rahmen oder im Auftrag einer kirchlichen Stelle erfolgt. Die nähere Ausgestaltung der Rechtsfigur der Auftragsverarbeitung findet sich dann in § 30 DSGVO-EKD bzw. § 29 KDG.

Dem Wortlaut nach wäre das jeweilige Kirchendatenschutzgesetz unmittelbar auf einen nicht-kirchlichen Auftragsverarbeiter anwendbar, wenn dieser im Auftrag einer kirchlichen Stelle personenbezogene Daten verarbeitet. Erfasst wären davon etwa eine Vielzahl privatrechtlich organisierter Dienstleister, etwa Cloud-Computing-Anbieter, derer sich die kirchliche Stelle bedient, oder Versanddienstleister, die z.B. den Versand des Gemeindebriefs an einen festgelegten Stamm von Gemeindegliedern übernehmen. Sofern also nicht-kirchliche Stellen im Auftrag einer kirchlichen Stelle tätig werden wollten, müssten sie sämtliche Anforderungen des DSGVO-EKD und/oder KDG einhalten. Eine andere Auslegung wäre nur denkbar, wenn die jeweilige Regelung als kumulative – d.h. neben dem jeweiligen Absatz 1 erforderliche – Bedingung für die Anwendbarkeit des Kirchendatenschutzrechts interpretiert wird. Hierfür gibt es jedoch keine Anhaltspunkte in Wortlaut oder Systematik der jeweiligen Norm. Darüber hinaus wäre die Regelung obsolet, wenn sie lediglich die bereits in § 2 Abs. 1 DSGVO-EKD bzw. § 3 Abs. 1 KDG benannten kirchlichen Stellen erfassen wollte. Einzig aus § 30 Abs. 5 Satz 1 DSGVO-EKD ergibt sich implizit, dass es Konstellationen geben kann, in denen auf einen Auftragsverarbeiter, der für eine kirchliche Stelle tätig wird, das DSGVO-EKD keine Anwendung findet. Dieser Widerspruch zur naheliegenden Interpretation des § 2 Abs. 3 DSGVO-EKD lässt sich nicht auflösen. Noch unverständlicher wird die Rechtslage durch § 30 Abs. 5 Satz 3 DSGVO-EKD, der eine Pflicht des Auftragsverarbeiters vorsieht, sich der kirchlichen Datenschutzaufsicht zu unterwerfen – wie der Auftragsverarbeiter unmittelbarer Adressat dieser Pflicht werden soll, ohne Adressat des Gesetzes zu sein, erschließt sich jedoch nicht.

Damit tun sich allerdings grundlegende Zweifel an der Europarechtskonformität der Erstreckung des Anwendungsbereichs auf nicht-kirchliche Auftragsverarbeiter auf. Sinn und Zweck der Öffnungsklausel Art. 91 Abs. 1 DS-GVO ist der Ausgleich des Rechts des Einzelnen auf Schutz personenbezogener Daten und des durch die korporative Religionsfreiheit gewährleisteten religionsgemeinschaftlichen Selbstverwaltungsrechts.¹³ Nicht-kirchliche Stellen können schon

9 Grages, in: Plath, BDSG/DS-GVO, 2. Aufl., 2016, Art. 91 Rn. 1; Hense, in: Sydow, Europäische Datenschutzgrundverordnung, 2017, Art. 91 Rn. 21; Jacob, in: Auernhammer (Fn. 7), Art. 91 Rn. 13; Pauly, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 91 Rn. 25.

10 Frenzel, in: Paal/Pauly (Fn. 9), Art. 9 Rn. 13; Schiff, in: Ehmann/Selmayr (Fn. 8), Art. 9 Rn. 19; Schulz, in: Gola, Datenschutz-Grundverordnung, 2017, Art. 9 Rn. 12.

11 Vgl. auch Hense, in: Sydow (Fn. 9), Art. 91 Rn. 21, der bei Definitionen eine Kongruenz von kirchlichem Datenschutz und DS-GVO fordert.

12 Herbst, in: Kühling/Buchner (Fn. 4), Art. 91 Rn. 15.

13 Hense, in: Sydow (Fn. 9), Art. 91 Rn. 1.

naturgemäß von diesem religionsgemeinschaftlichen Selbstverwaltungsrecht nicht erfasst sein, sodass als unmittelbare Adressaten des Gesetzes nur kirchliche Stellen in Betracht kommen.

Hiervon unbenommen bleibt allerdings die Möglichkeit, kirchlichen Stellen als unmittelbare Adressaten des jeweiligen Kirchendatenschutzgesetzes die Pflicht aufzuerlegen, bestimmte Anforderungen an nicht-kirchliche Stellen vertraglich „durchzureichen“, wie es § 30 Abs. 3 DS-GVO und § 29 Abs. 3, 4 KDG vorsehen. Eine solche Einschränkung der Kontraktionsfreiheit ist zumindest unter datenschutzrechtlichen Gesichtspunkten nicht zu beanstanden und entspricht weitgehend der Regelung in Art. 28 Abs. 3 DS-GVO. Auch unter dem Gesichtspunkt des Betroffenen schutzes ist eine Ausweitung des Anwendungsbereichs des Kirchendatenschutzrechts nicht erforderlich. Bei Auftragsverarbeitern, die ihre Dienstleistungen den beiden großen deutschen Kirchen anbieten, findet die DS-GVO ohnehin gem. Art. 3 Abs. 2 lit. a DS-GVO Anwendung. Aufgrund des Umstands, dass DS-GVO und KDG mit der DS-GVO „in Einklang“ stehen müssen, liegt in den Fällen, in denen der Auftragsverarbeiter durch die DS-GVO verpflichtet ist, ein gleichwertiges Datenschutzniveau bei diesem vor. Ferner wären die Festlegungen in der Auftragsverarbeitungsvereinbarung, mit denen der Verantwortliche zentrale Grundsätze von DS-GVO und KDG an den Auftragsverarbeiter weiterreicht und deren Einhaltung vertraglich sicherstellt, letztlich obsolet, wäre letzterer ohnehin unmittelbarer Adressat sämtlicher Anforderungen. Vielmehr scheint es ausreichend, wenn der Auftragsverarbeiter, der ohnehin die DS-GVO-Anforderungen einhalten muss, im Vertragswege Adressat etwaiger kirchendatenschutzrechtlicher Pflichten wird.

Nach hier vertretener Ansicht ist daher eine Korrektur im Wege europarechtskonformer Auslegung der § 2 Abs. 3 DS-GVO und § 3 Abs. 2 KDG geboten. Diese sind restriktiv auszulegen und erfassen nur kirchliche Auftragsverarbeiter. Auf nicht-kirchliche Auftragsverarbeiter, die für die beiden großen Kirchen in Deutschland tätig werden, gilt damit – je nachdem, ob diese in der EU eine datenschutzrelevante Niederlassung haben – allein die DS-GVO nach Art. 3 Abs. 1 oder 2 DS-GVO sowie die Anforderungen, die dem Auftragsverarbeiter im Wege der gem. § 30 DS-GVO bzw. § 29 KDG abzuschließenden Auftragsverarbeitungsvereinbarung auferlegt werden.

2. Drittlandtransfers

Das evangelische Datenschutzrecht thematisiert die Frage der Datentransfers in EU-Drittstaaten in § 10 DS-GVO und bildet in diesem nahezu vollständig die Vorschriften der Artt. 45, 49 DS-GVO ab. Einzig auffällig ist, dass ein wesentliches Instrument für Drittstaatentransfers, die von einer Aufsichtsbehörde genehmigten „verbindlichen internen Datenschutzvorschriften“ (vgl. Art. 47 DS-GVO), häufig als Binding Corporate Rules („BCR“) bezeichnet, fehlen. Die Verwendung solcher BCR mag sich für die evangelische Kirche nicht unbedingt aufdrängen, ist dem Grunde nach aber

denkbar, etwa wenn sie oder eine ihrer Gliedkirchen eine dauerhafte Einrichtung in einem Drittstaat ohne äquivalentes Datenschutzniveau unterhält und dort personenbezogene Daten verarbeitet. Hier wurde die Chance vertan, ein zentrales Instrument, welches die Kompetenzen der evangelischen Datenschutzaufsicht rechtmäßig erweitert hätte, in das DS-GVO zu überführen.

Dagegen bedarf das katholische Datenschutzrecht in Hinblick auf EU-Drittstaaten einer genaueren Würdigung. So finden sich in §§ 39-41 KDG umfassende Vorschriften über die Übermittlung von Daten in diese Staaten. Die Angemessenheitsbeschlüsse finden sich in § 40 Abs. 1 KDG wieder. Im Gegensatz zu § 10 DS-GVO erwähnt § 40 Abs. 2 lit. a KDG die „in einem rechtsverbindlichen Instrument“ vorgesehenen „geeigneten Garantien“. Zwar werden diese nicht genauer bezeichnet; in Anlehnung an Art. 46 DS-GVO werden hiervon jedoch alle der in Art. 46 Abs. 2 DS-GVO (genehmigungsfreie Garantien) und Art. 46 Abs. 3 DS-GVO (genehmigungspflichtige Garantien), einschließlich der BCR, erfasst sein. Kritisch ist hingegen § 40 Abs. 2 lit. b KDG zu betrachten: Diese Norm enthält eine Regelung für den Fall, dass kein rechtsverbindliches Instrument zur Gewährleistung eines adäquaten Schutzniveaus besteht. In diesem Fall ist eine Übermittlung – ohne dass es einer Genehmigung durch die Datenschutzaufsicht bedarf – auch zulässig, wenn der Verantwortliche davon ausgehen kann, es würden beim Empfänger geeignete Garantien bestehen. Die Vorschrift unterläuft damit die Bewertungskompetenz, die der Europäischen Kommission bei Angemessenheitsentscheidungen sowie Standarddatenschutzklauseln¹⁴ und den Datenschutzaufsichtsbehörden hinsichtlich der genehmigungspflichtigen Garantien zusteht. Im Gegenzug erhält der Verantwortliche einen Beurteilungsspielraum, mit der Folge, dass er im Ergebnis selbst Angemessenheitsentscheidungen treffen kann. Damit droht im Falle einer Fehleinschätzung eine nicht unerhebliche Gefährdung des Betroffenen schutzes. Insbesondere setzt eine solche Vorschrift, die einer datenschutzrechtlichen Selbstkontrolle gleichkommt, ökonomische Anreize, das Bestehen geeigneter Garantien bloß zu behaupten.¹⁵ Entsprechend ist es ein Verstoß gegen die Wertungen der DS-GVO, einen Datentransfer allein auf Grundlage einer Einschätzung des Verantwortlichen vorzunehmen.

Etwas versteckt ist in einer Regelung zur Auftragsverarbeitung, § 29 Abs. 11 Satz 2 KDG, außerdem eine Regelung enthalten, die die Auftragsverarbeitung mit Drittstaaten-Auftragsverarbeitern im Fall des Bestehens eines Angemessenheitsbeschlusses regelt und offenbar davon ausgeht, dass die einzelnen Datenschutzaufsichtsbehörden, einschließlich der katholischen Datenschutzaufsicht, selbst Angemessenheitsbeschlüsse i.S.d. Art. 45 DS-GVO erlassen

¹⁴ Bislang wurden die Standarddatenschutzklauseln als Standardvertragsklauseln („standard contractual clauses“) bezeichnet; diese sind abrufbar unter https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

¹⁵ Vgl. Golland, DSB 2014, 213.

können. Eine eindeutige Befugnis fehlt jedoch; die Norm des § 44 Abs. 3 lit. l KDG, welcher die Aufsicht ermächtigt, „jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten [zu] erfüllen“ – eine offenbar dem Art. 57 Abs. 1 lit. v DS-GVO entlehnte Formulierung – ist zu unbestimmt. Auch geht § 40 Abs. 1 KDG davon aus, dass die Kompetenz für Angemessenheitsentscheidungen bei der Kommission liegt. Zugleich wird mit erwähntem § 29 Abs. 11 Satz 2 KDG die Zulässigkeit des Datentransfers in Drittländer allein auf die Basis von Angemessenheitsbeschlüssen gestellt; gleichwertige Garantien wie Standarddatenschutzklauseln oder BCR werden nicht genannt. Damit entsteht nicht nur ein Widerspruch zu den Wertungen der DS-GVO, sondern auch ein interner Widerspruch zu §§ 40 Abs. 2, 41 KDG. Daher spricht viel für eine extensive Auslegung des § 29 Abs. 11 Satz 2 KDG über den Wortlaut hinaus: Auch wenn andere geeignete Garantien i.S.d. § 40 Abs. 1 oder Abs. 2 lit. a KDG vorhanden sind, ist der Drittlandtransfer von Daten, einschließlich des Einsatzes von Auftragsverarbeitern im Drittland, stets zulässig.

3. Bußgelder

Sowohl DSGVO-EKD wie auch KDG begrenzen die Höhe der Bußgelder auf 500.000 Euro (§ 45 Abs. 5 DSGVO-EKD bzw. § 51 Abs. 5 KDG). Bereits die Begrenzung der Höhe erscheint fragwürdig: Ob bei einem kirchlichen Verantwortlichen, der jährlich mehrere hundert Millionen Euro umsetzt, eine absolute Deckelung auf 500.000 Euro geeignet ist, dass die Geldbuße stets „wirksam, verhältnismäßig und abschreckend“ (vgl. Art. 83 Abs. 1 DS-GVO) ist, muss bezweifelt werden. Die Kirchendatenschutzgesetze schlagen damit einen anderen Weg ein als die vor allem am Umsatz orientierte DS-GVO.

Fraglich ist jedoch, welche Adressaten überhaupt von der potentiellen Sanktion erfasst werden. § 45 Abs. 1 DSGVO-EKD nennt als mögliche Bußgeldadressaten verantwortliche Stellen und kirchliche Auftragsverarbeiter, wobei erstere nur dann erfasst sein sollen, wenn sie „als Unternehmen i.S.d. § 4 Nr. 19 am Wettbewerb teilnehmen“, wobei sich die Definition des „Unternehmens“ an dem funktional geprägten Unternehmensbegriff des Europarechts¹⁶ orientiert. Einige Adressaten des DSGVO-EKD wären damit ausgeklammert, sodass sich die Frage stellt, ob Pflichten ohne bußgeldbewährte Sanktion überhaupt einen ausreichenden Anreizcharakter entfalten. Daneben stellt sich die Frage, warum eine unternehmerische Teilnahme am Wettbewerb zur Voraussetzung für die Verhängung von Bußgeldern erhoben wird, da die Risiken für die informationelle Selbstbestimmung der Betroffenen nicht von einem etwaigen unternehmerischen Tätigwerden abhängen.

Ein ähnliches Problem stellt sich im katholischen Datenschutzrecht: Nach § 51 Abs. 6 KDG können kirchliche Stellen, soweit sie im weltlichen Rechtskreis öffentlich-rechtlich verfasst sind, nicht Adressaten eines Bußgelds sein. In der Praxis wären damit kirchliche Verantwortliche und kirchliche Auftragsverarbeiter nicht erfasst, sodass hinsicht-

lich dieser ein erhebliches Sanktionsdefizit auftritt. Letztlich blieben dann nur noch die nicht-kirchlichen Auftragsverarbeiter als mögliche Bußgeldadressaten. Diese sind aber bei der hier vertretenen europarechtskonformen Auslegung des § 3 Abs. 2 KDG¹⁷ nicht vom Gesetz erfasst. De facto gäbe es damit unter dem KDG keine Bußgelder.

4. Besondere Verarbeitungssituationen

In dem jeweils vorletzten Kapitel der kirchlichen Datenschutzgesetze werden die „besonderen Verarbeitungssituationen“ geregelt. So wird beispielsweise das im neuen BDSG vermisste Medienprivileg durch § 51 DSGVO-EKD und § 55 KDG geregelt.

Auch die Videoüberwachung, die der deutsche Gesetzgeber aus § 6b BDSG a.F. in die neue Norm § 4 BDSG überführte und die vor allem, soweit sie nicht-öffentliche Verarbeiter adressiert, als unionsrechtswidrig zu betrachten ist,¹⁸ findet sich in den Kirchendatenschutzgesetzen. Dabei entsprechen § 52 DSGVO-EKD und § 52 KDG weitgehend § 6b BDSG a.F. bzw. § 4 BDSG. Während dem deutschen Gesetzgeber im Rahmen der Zulässigkeitstatbestände durch die Öffnungsklausel in Art. 6 Abs. 2 DS-GVO jedoch enge Grenzen gesetzt sind, ist die Öffnungsklausel des Art. 91 Abs. 1 DS-GVO weiter¹⁹ und die Regelung der Videoüberwachung in den kirchlichen Datenschutzgesetzen damit wirksam. Denn bei allen (berechtigten) Zweifeln an der Regelungskompetenz des deutschen Gesetzgebers für die Videoüberwachung wird die typisierte Abwägung in § 4 BDSG regelmäßig zu den gleichen Ergebnissen kommen wie die offene Abwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO.²⁰ Selbiges gilt aufgrund der Nähe des Wortlauts auch für § 52 DSGVO-EKD und § 52 KDG. Damit entsprechen die kirchendatenschutzrechtlichen Vorschriften zur Videoüberwachung wertungsmäßig der DS-GVO.

Problematisch ist hingegen § 53 DSGVO-EKD, welcher die Aufzeichnung und Übertragung von Gottesdiensten erlaubt, wenn die Teilnehmer „durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden“. Trotz der Regelungsnähe zur Videoüberwachung bedarf es keiner (typisierten) Interessenabwägung, vielmehr reicht nach § 53 DSGVO-EKD die bloße Information des Betroffenen aus. Zur Information der Betroffenen ist der Verantwortliche allerdings ohnehin aus § 17 DSGVO-EKD verpflichtet, sodass die Aufzeichnung und Übertragung eines

16 Vgl. die ständige Rechtsprechung des EuGH, wonach ein Unternehmen „jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung“ ist; grundlegend EuGH, Slg. 1991, I-1979, Rn. 21.

17 Siehe dazu oben 3.1.

18 Siehe auch Ziebarth, ZD 2017, 467 (469); für eine unionsrechtskonforme Auslegung des neuen § 4 BDSG hingegen Wolff, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 636 ff.

19 Anderes gilt nur, sofern angenommen wird, dass den Religionsgemeinschaften nur die den Mitgliedstaaten entsprechende Regelungskompetenz im Bereich des kirchlichen Datenschutzes zustehe, siehe die Nachweise in Fn. 8.

20 Vgl. Lachenmann, ZD 2017, 407 (410), wonach ein „über Art. 6 Abs. 1 Satz 1 lit. f DS-GVO hinausgehender Normgehalt [...] nicht zu erkennen“ sei.

Gottesdienstes letztlich an keine weiteren Zulässigkeitsvoraussetzungen geknüpft wäre. Überdies macht die Norm keinen Unterschied zwischen einer nur für Gottesdienstbesucher oder deren Angehörige durchgeführten Aufzeichnung für den Gebrauch im kleinen Kreis, und einem weltweit öffentlich zugänglichen Livestream, der womöglich intime Momente der einzelnen Gläubigen zeigt. Dies ist mit der Wertung des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO und dem (regelmäßig) intensiven Eingriff in das Persönlichkeitsrecht der Gottesdienstbesucher unvereinbar. Ein solch eklatanter Widerspruch kann nicht „in Einklang“ mit der DS-GVO stehen; die Norm ist folglich unanwendbar.

5. Rechtsweg zum EuGH?

Bislang ist völlig offen, ob die kirchlichen Verwaltungs- bzw. Datenschutzgerichte im Rahmen eines Vorabentscheidungsverfahrens vor dem EuGH vorlageberechtigt und -verpflichtet i.S.d. Art. 267 Abs. 2, 3 AEUV sind. Dieses Problem stellt sich dann, wenn der Adressat einer kirchendatenschutzaufsichtsbehördlichen Verfügung die streitentscheidende Norm unter dem Gesichtspunkt der Europarechtskonformität rügt (etwa, weil der in Rede stehende Verstoß gegen DSGVO-EKD bzw. KDG keinen Verstoß gegen die DS-GVO darstellt). Das für die kirchendatenschutzrechtliche Streitigkeit zuständige Gericht hätte dann zu prüfen und ggf. dem EuGH vorzulegen, inwieweit die Norm, gegen die verstoßen wurde, von der Öffnungsklausel des Art. 91 Abs. 1 DS-GVO gedeckt ist. Die Frage stellt sich auch in umgekehrten Konstellationen dann, wenn der Verarbeiter lediglich die Vorschrift des Kirchendatenschutzrechts beachtet, diese aber wertungsmäßig hinter ihrem strengeren Pendant der DS-GVO zurückbleibt.

IV. Fazit

Die hohe Regelungsdichte, zu der Art. 91 DS-GVO zwingt („umfassende Regeln“), aber zugleich eine Wesensgleichheit zur DS-GVO forciert („in Einklang gebracht“), führt naturgemäß zu einem hohen Konfliktpotential. Angesichts dieser Regelungen bestehen an der Europarechtskonformität einiger Vorschriften in DSGVO-EKD und KDG erhebliche Zweifel. Sofern die jeweilige Datenschutzaufsicht das jeweilige kirchliche Datenschutzgesetz seiner Konzeption getreu anwendet, sind Konflikte mit kirchlichen und nicht-kirchlichen Stellen vorprogrammiert. Insbesondere beim Outsourcing von IT-Pro-

zessen, welche typischerweise im Wege der Auftragsverarbeitung durch große Cloud-Computing-Anbieter aus den USA erbracht werden, besteht angesichts unzureichender Vorschriften in Bezug auf die Auftragsverarbeitung und in Bezug auf Drittlandtransfers ein gewisses Konfliktpotential. Ein zweifelhafter Ausgleich wird dadurch geschaffen, dass die Bußgeldnormen in zahlreichen Fällen wohl nicht zur effektiven Sanktion geeignet sind.

Einige Normen lassen die Möglichkeit einer Auslegung anhand der Parallelvorschriften in der DS-GVO zu, wodurch unbillige Ergebnisse vermieden werden können. Andere wiederum sind derart formuliert, beispielhaft seien die Regelungen über besondere Arten personenbezogener Daten oder die Zulässigkeit der Übertragung von Gottesdiensten genannt, dass sie einer solchen Auslegung nicht oder nicht widerspruchsfrei zugänglich sind. In diesen Fällen sind die jeweiligen Normen von DSGVO-EKD und KDG nicht anzuwenden, sondern die entsprechenden, subsidiär geltenden Vorschriften der DS-GVO. Hier ist vor allem die sinnvolle Auslegung und Anwendung der jeweiligen Vorschriften durch die kirchlichen Datenschutzaufsichtsbehörden erforderlich.

Die Ausräumung unauflöslicher Konflikte wird schließlich Aufgabe der Gerichte sein. In diesem Bereich ist die Bildung von Spezialzuständigkeiten erfreulich. Ungeklärt ist die Vorlageberechtigung der Kirchengerichte bei wertungsmäßigen Differenzen von DS-GVO und Kirchendatenschutzrecht. Es ist bereits jetzt absehbar, dass mit dieser Reformation 2.0 auf sämtliche Beteiligten – Verantwortliche, Auftragsverarbeiter, kirchliche Datenschutzaufsicht und Gerichte – erhebliche Arbeit zukommen wird.



Alexander Golland

Der Autor ist Rechtsreferendar am Landgericht Bochum, Datenschutzbeauftragter und promoviert zu einer datenschutzrechtlichen Fragestellung. Er beschäftigt sich schwerpunktmäßig mit Fragen des europäischen Datenschutzrechts im Zusammenhang mit Big Data, Cloud Computing, Connected Car und Social Media, sowie mit der Umsetzung der Anforderungen der Datenschutz-Grundverordnung in Unternehmen.

Professor Dr. Gregor Thüsing

Automatisierte Einzelentscheidung in der PKV – Zur Europarechtskonformität des neuen § 37 Abs. 1 Nr. 2 BDSG –*

Private Krankenversicherer verarbeiten personenbezogene Gesundheitsdaten per automatisierter Einzelentscheidung. Bisher hat diese Praxis niemand ernsthaft in Frage gestellt – jedenfalls nicht aus datenschutztechnischen Gründen. Die europäischen und nationalen Vorgaben des Datenschutzrechts verschieben sich allerdings zum 25. Mai 2018.

Der Beitrag setzte sich mit den im Bereich der automatisierten Einzelentscheidung relevanten europäischen Verordnungsvorgaben auseinander und zeigt auf, dass die durch die nationalen Gesetzgeber geschaffene Neuregelung in § 37 Abs. 1 Nr. 2 BDSG n.F. entgegen anderslautender Aussagen des Bayerischen Datenschutzbeauftragten europarechtlich unbedenklich ist.

I. Much ado about nothing?

Mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) vom 30. Juni 2017 wurde § 37 Abs. 1 Nr. 2 BDSG n.F. eingeführt:

„Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und [...]

2. die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und der Verantwortliche für den Fall, dass dem Antrag nicht vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung zählt; der Verantwortliche informiert die betroffene Person über diese Rechte spätestens im Zeitpunkt der Mitteilung, aus der sich ergibt, dass dem Antrag der betroffenen Person nicht vollumfänglich stattgegeben wird.“

Danach also ist ab dem 25. Mai dieses Jahres eine automatisierte Einzelentscheidung auch von Gesundheitsdaten weiterhin zulässig in dem Maße, wie es bereits aktuell praktiziert wird.¹ Dennoch wird diese Regelung von nicht unmaßgeblicher Stelle als europarechtswidrig kritisiert. So führt der Bayerische Datenschutzbeauftragte Thomas Petri mit Blick auf die Bundesregierung an, diese sei nicht gewillt, „das EU-Recht ganz ernst zu nehmen“. Explizit bezogen auf automatisierte Einzelentscheidungen durch private Krankenkassen – gemeint ist § 37 Abs. 1 Nr. 2 BDSG n.F. – hegt er sogar Zweifel, „ob das mit EU-Recht im Einklang steht“.² Aber stimmt das?

Sicherlich nicht, und das soll begründet werden: Zunächst ist die bisherige Rechtslage nach Maßgabe des § 6a Abs. 2 BDSG und der Datenschutzrichtlinie 95/46/EG (nachfolgend DSRL) in den Blick zu nehmen und anschließend mit der ab 25. Mai 2018 geltenden Rechtslage unter dem Regime des § 37 Abs. 1 Nr. 2 BDSG n.F. sowie Art. 9 Abs. 2 lit. g), 22 Abs. 4 Verordnung (EU) 2016/679 (im Folgenden DS-GVO) zu vergleichen. Dabei ist zu prüfen, ob sich hieraus für die oben aufgeworfene Rechtsfrage unter Beachtung unionsrechtlicher Vorgaben Änderungen ergeben. Darauf aufbauend kann detailliert auf die Europarechtskonformität des § 37 Abs. 1 Nr. 2 BDSG n.F. eingegangen werden. Im Zuge dessen werden die Voraussetzungen der Art. 9 Abs. 2 lit. g), 22 Abs. 4 DS-GVO betrachtet. In diesem Kontext wird vor allem der Frage nachzugehen sein, ob ein erhebliches öffentliches Interesse für automatisierte Entscheidungen im Bereich der privaten Krankenversicherungen besteht und angemessene sowie spezifische Maßnahmen zur Sicherung der Rechte des von der Datenverarbeitung Betroffenen getroffen wurden. Dabei muss auch die Verhältnismäßigkeit der Zwecksetzung untersucht werden, bevor zuletzt die Wahrung des – schwer fassbaren – Wesensgehalts des Datenschutzgrundrechts überprüft wird. Eine Summa fasst die gefundenen Ergebnisse zusammen.

II. Was bisher galt – und warum sich nur wenig geändert hat

Eine Europarechtswidrigkeit des aktuellen Rechts hat bislang noch niemand behauptet – aber ändert sich nun so viel?

* Der Praxis danke ich für die Anregung des Beitrages – Herrn *Sebastian Rombey* für die vielfältige und eingehende Diskussionsbereitschaft.

1 S. z.B. Art. 13 des Code of Conduct der deutschen Versicherungswirtschaft, abrufbar unter https://www.europa.de/fileadmin/pdf-extern/allgemein/europa_codeofconduct.pdf, Abruf v. 04.01.2018.

2 Vgl. etwa Passauer Neue Presse v. 31.01.2017, abrufbar unter http://www.pnp.de/nachrichten/bayern/2383787_Bayerischer_Datenschutz_rueffelt_Bundesregierung.html, Abruf v. 04.01.2018.

1. Die Verarbeitung von Gesundheitsdaten, § 6a Abs. 2 BDSG und die Vorgaben der Datenschutzrichtlinie

Dass Gesundheitsdaten überhaupt verarbeitet werden dürfen durch die Krankenversicherer – unabhängig von der Frage automatisierter Einzelentscheidung – ist unbestritten und europarechtlich unbedenklich – wenn auch die Datenerhebung bei Dritten besonderen Grenzen unterliegt, s. § 213 VVG. Allerdings gilt für Gesundheitsdaten ein besonderer Schutz nach Art. 8 DSRL. Nach dessen Abs. 1 untersagen die Mitgliedstaaten grundsätzlich die Verarbeitung personenbezogener Daten aus besonderen Kategorien, wozu Gesundheitsdaten gehören, wenn eine Einwilligung nicht vorliegt. Davon wiederum ordnet Art. 8 Abs. 2 DSRL Ausnahmen an, denen die Mitgliedstaaten nach Art. 8 Abs. 4 DSRL bei ihrer Umsetzung der Richtlinie vorbehaltlich angemessener Garantien aus Gründen eines „wichtigen öffentlichen Interesses“ weitere hinzufügen können.

Dazu aber kommt die besondere Frage der automatisierten Einzelentscheidung. § 6 Abs. 1 S. 1 BDSG normiert bis zum 25. Mai ein generelles Verbot, Entscheidungen über Persönlichkeitsmerkmale, die zu rechtlichen oder nachteiligen Folgen für den Betroffenen führen können, ausschließlich einer automatisierten Datenverarbeitung zu überlassen. In § 6 Abs. 1 S. 2 BDSG konkretisiert das Gesetz die Wendung der ausschließlich auf automatisierte Verarbeitung gestützten Entscheidung dahingehend, dass eine solche insbesondere dann vorliegt, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat – so wie im Falle automatisierter Einzelentscheidungen durch private Krankenkassen bzgl. besonders sensibler personenbezogener Gesundheitsdaten.

Die Bestimmung verfolgt den Zweck, Risiken zu begegnen, die entstehen können, wenn anonyme Datenverarbeitungssysteme unabhängig vom Ansehen der Person automatisiert und für die Betroffenen meist nur schwer nachvollziehbar Entscheidungen fällen, die Persönlichkeitsmerkmale betreffen.³ Oder, um es mit anderen Worten zu sagen: Es soll verhindert werden, dass der Betroffene zum bloßen Objekt der automatisierten Erstellung von Persönlichkeitsprofilen wird.⁴ Damit setzt § 6a BDSG zugleich Art. 15 Abs. 1 DSRL nahezu wortlautgetreu um,⁵ der ebenfalls anordnet, dass ausschließlich auf automatisierter Datenverarbeitung beruhende Entscheidungen hinsichtlich der Bewertung einzelner Aspekte der betroffenen Person grundsätzlich unzulässig sind.

Dieses grundsätzliche Verbot automatisierter Einzelentscheidungsprozesse unterliegt jedoch – ebenfalls unionsrechtlich determinierten – Einschränkungen. Art. 15 Abs. 2 DSRL verpflichtet die Mitgliedstaaten nämlich dazu, Ausnahmen für Fälle vorzusehen, in denen entweder die automatisierte Einzelentscheidung im Rahmen eines Vertragschlusses respektive der Vertragserfüllung erfolgt und dem Begehren des Betroffenen damit abgeholfen wird (lit. a)) oder die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen sichergestellt und dies durch Gesetz zugelassen ist (lit. b)). Diese Ausnahmetatbe-

stände finden ihre nationale Umsetzung in § 6a Abs. 2 BDSG – unabhängig davon, ob es sich um Gesundheitsdaten handelt oder nicht.

Dabei ist insbesondere § 6a Abs. 2 Nr. 2 BDSG für die hier diskutierte Frage von Relevanz. Auslegungsbedürftig sind dabei vor allem die „berechtigten Interessen“, deren Beachtung gewährleistet werden muss, damit die automatisierte Einzelentscheidung datenschutzrechtlich zulässig ist, sowie die zur Erreichung dieses Ziels geeigneten Maßnahmen. Die berechtigten Interessen des von der Datenverarbeitung Betroffenen liegen vor dem Hintergrund des oben genannten Regelungszwecks der Norm darin, dass an irgendeiner Stelle des Entscheidungsprozesses eine natürliche Person in die Entscheidungsfindung mit eingebunden werden muss, sodass individuelle Besonderheiten, die möglicherweise in der Person des Betroffenen liegen, Berücksichtigung finden können.⁶ Zentral ist allerdings die Fragestellung, welche geeigneten Maßnahmen hierzu ergriffen werden müssen.

Vor der Novellierung des BDSG im Jahre 2009 enthielt § 6a Abs. 2 Nr. 2 S. 2, 3 BDSG a.F. noch eine Konkretisierung der geeigneten Maßnahmen. Eine Maßnahme galt dann als geeignet im Sinne der Norm, wenn der Betroffene die Möglichkeit hatte, seinen Standpunkt geltend zu machen, sodass die verantwortliche Stelle dazu verpflichtet war, die automatisiert getroffene Entscheidung zu überprüfen. Zwar ist diese Ergänzung mit der erwähnten Novellierung im Jahre 2009 weggefallen – Grund war aber nach allgemeiner Meinung allein ein gesetzgeberisches Redaktionsversehen.⁷ Auswirkungen auf die Auslegung der Norm sind mithin nicht erkennbar.⁸ Die Wendung kann also weiterhin zur Bestimmung der geeigneten Maßnahmen herangezogen werden. Gestützt wird dies in systematischer Hinsicht durch einen Vergleich mit Art. 15 Abs. 2 lit. a) DSRL, der die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen, als spiegelstrichartiges Beispiel für eine geeignete Maßnahme anführt. Damit soll letztlich eine am Ende der Datenverarbeitung stehende personale Verantwortung für den Entscheidungsprozess sichergestellt werden.⁹ Deshalb ist es denklogisch, dass eine derartige Überprüfung der automatisiert getroffenen Einzelentscheidung nicht in der bloßen Wiederholung derselben liegen kann, sondern bei der Überprüfung vielmehr ein Mitarbeiter in den Prozess mit einbezogen werden muss.¹⁰ In der Literatur wird jedoch z.T. er-

3 Simitis/Scholz, BDSG, 8. Aufl. 2014, § 6a Rn. 3.

4 Simitis/Scholz, BDSG, 8. Aufl. 2014, § 6a Rn. 3; beispielhaft zu nennen ist hier das sog. Scoring, vgl. dazu Roßnagel, NZA 2009, 2719.

5 Streitig ist in diesem Kontext allerdings, ob Art. 15 DSRL lediglich die Zulässigkeit automatisierter Entscheidungen einschränkt (so etwa Ehmann/Helfrich, EG-Datenschutzrichtlinie, 1. Aufl. 1999, Art. 15 Rn. 3 ff.) oder gar ein dahingehendes generelles Verbot enthält (in diese Richtung Brühmann/Zerdick, CR 1996, 443).

6 Simitis/Scholz, BDSG, 8. Aufl. 2014, § 6a Rn. 32.

7 Auernhammer/Herbst, DS-GVO und BDSG, 5. Aufl. 2017, § 6a Rn. 17; so auch BeckOK-DatenschutzR/von Lewinski, BDSG, 21. Edition 2017, § 6a Rn. 43.

8 Eingehend Taeger/Gabel/Mackenthun, BDSG, 2. Aufl. 2013, § 6a Rn. 22.

9 Dammann/Simitis, EG-Datenschutzrichtlinie, 1. Aufl. 1997, Art. 15 Rn. 10.

10 Instruktiv Duhr/Naujok/Peter/Seiffert, DuD 2002, 26.

gänzend darauf hingewiesen, dass es für den Betroffenen überdies möglich sein müsse, die Bewertungsmaßstäbe, die im Rahmen des automatisierten Systems an die Entscheidungsfindung angelegt werden, erfahren zu können.¹¹

Nach diesen Maßstäben ist ein automatisierter Datenverarbeitungsprozess, innerhalb dessen private Krankenkassen automatisierte Einzelentscheidungen verwenden können, *de lege lata* unter den genannten Voraussetzungen des § 6a Abs. 2 Nr. 2 BDSG möglich – das hat bislang niemand bestritten. Wiederum ist auf die bisherige Praxis der Versicherungsunternehmen¹² zu verweisen:

„Art. 13 Automatisierte Einzelentscheidungen

(1) Entscheidungen, die für die Betroffenen eine negative rechtliche oder wirtschaftliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, werden grundsätzlich nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Dies wird organisatorisch sicher gestellt. Die Informationstechnik wird grundsätzlich nur als Hilfsmittel für eine Entscheidung herangezogen, ohne dabei deren einzige Grundlage zu bilden. Dies gilt nicht, wenn einem Begehren der Betroffenen in vollem Umfang stattgegeben wird.

(2) Sofern automatisierte Entscheidungen zu Lasten der Betroffenen getroffen werden, wird dies den Betroffenen von der verantwortlichen Stelle unter Hinweis auf das Auskunftsrecht mitgeteilt. Auf Verlangen werden den Betroffenen auch der logische Aufbau der automatisierten Verarbeitung sowie die wesentlichen Gründe dieser Entscheidung mitgeteilt und erläutert, um ihnen die Geltendmachung ihres Standpunktes zu ermöglichen. Die Information über den logischen Aufbau umfasst die verwendeten Datenarten sowie ihre Bedeutung für die automatisierte Entscheidung. Die Entscheidung wird auf dieser Grundlage in einem nicht ausschließlich automatisierten Verfahren erneut geprüft.

(3) Der Einsatz automatisierter Entscheidungshilfen wird dokumentiert.“

2. § 37 Abs. 1 Nr. 2 BDSG n.F. und die Vorgaben der DS-GVO

Noch nicht beantwortet ist damit die Frage, ob sich durch das ab 25. Mai 2018 anwendbare BDSG n.F. und die DS-GVO die bestehenden Demarkationslinien unter Beachtung europarechtlicher Implikationen verschoben haben, so wie es der Bayerische Datenschutzbeauftragte angedeutet hat. Art. 9 Abs. 1 DS-GVO verbietet dem Grunde nach die Verarbeitung personenbezogener Daten, die in besondere Kategorien fallen und damit auch die enumerativ aufgezählten Gesundheitsdaten im Sinne der Legaldefinition des Art. 4 Nr. 15 DS-GVO. Davon macht die zwischen den Ausnahmetatbeständen des Art. 9 Abs. 2 DS-GVO versteckte Generalklausel des Art. 9 Abs. 2 lit. g) DS-GVO wiederum eine Ausnahme für Fälle, in denen ein „erhebliches öffentliches Interesse“ vorliegt. Dabei handelt es sich um eine Öffnungsklausel, die mit Art. 8 Abs. 4 DSRL korrespondiert.¹³ Zentral ist in diesem Zusammenhang, dass allein „erhebliche öffentliche Interessen“ ausreichen können. In systema-

tischer Hinsicht wird anhand von Art. 9 Abs. 2 lit. e) DS-GVO, der jegliche öffentliche Aufgaben umfasst, deutlich, dass die Erheblichkeit erst gegeben sein kann, wenn das Allgemeinwohl in besonderem Maße tangiert wird.¹⁴

Dies steht im Zusammenhang mit Art. 22 DS-GVO. Nach Art. 22 Abs. 1 DS-GVO hat der Betroffene zwar das Recht, nicht einer Entscheidung ausgesetzt zu werden, die ausschließlich auf einer automatisierten Datenverarbeitung beruht. Grund dessen ist die bereits hervorgehobene Sensibilität der Gesundheitsdaten und deren Aussagekraft im Hinblick auf die Persönlichkeit des Betroffenen. Dieses Verbot automatisierter Einzelentscheidungen gilt aber gemäß Art. 22 Abs. 4 DS-GVO dann nicht, wenn der genannte Art. 9 Abs. 2 lit. g) DS-GVO eingreift. Art. 22 Abs. 4 DS-GVO kommt hinsichtlich Art. 9 Abs. 2 lit. g) DS-GVO insoweit eine verschärfende Funktion dahingehend zu, dass zusätzlich angemessene Maßnahmen getroffen werden müssen, die sicherstellen, dass die berechtigten Interessen des Betroffenen gewahrt werden.¹⁵ Möglich sind allerdings auch rein klarstellende Bestimmungen, soweit diese erforderlich sind, um Friktionen mit dem nationalen Recht vermeiden zu können.¹⁶ Was unter angemessenen Maßnahmen zu verstehen ist, wird für Art. 9 Abs. 2 lit. h) DS-GVO in Art. 9 Abs. 3 DS-GVO konkretisiert. Danach ist eine Maßnahme angemessen, wenn entweder die Daten durch Fachpersonal verarbeitet werden, das dem Berufsgeheimnis unterliegt, oder eine Person die Daten verarbeitet, die jedenfalls einer Geheimhaltungspflicht unterworfen ist. Dies wird man auch auf Art. 9 Abs. 2 lit. g) DS-GVO übertragen können – es wäre sinnwidrig, im einen Buchstaben einen anderen Maßstab zu verlangen als im anderen. Beider Male geht es um dasselbe Schutzgut. Gleichwohl wird man konstatieren können, dass sich die Anforderungen an die Angemessenheit der Maßnahmen im Einzelfall nach dem Grad der Sensibilität der in Rede stehenden Daten richten müsse.¹⁷

Diesen unionsrechtlichen Vorgaben kommt § 37 Abs. 1 Nr. 2 BDSG n.F. nach. Ausweislich der Gesetzesbegründung¹⁸ sollen gerade im Bereich der privaten Krankenversicherungswirtschaft automatisierte Einzelentscheidungen weiterhin zulässig sein, soweit angemessene Maßnahmen zur Wahrung der berechtigten Interessen des Betroffenen ergriffen werden – das Schutzniveau der Art. 9 Abs. 2 lit. g), 22 Abs. 4 DS-GVO wird dadurch nicht ausgehebelt.

11 ErfK/Fanzen, BDSG, 18. Aufl. 2018, § 6a Rn. 2.

12 Eingefangen in Art. 13 des Code of Conduct der deutschen Versicherungswirtschaft, abrufbar unter https://www.europa.de/fileadmin/pdf-extern/allgemein/europa_codeofconduct.pdf, Abruf v. 04.01.2018.

13 Sydow/Kampert, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9 Rn. 35.

14 So explizit Sydow/Kampert, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9 Rn. 36.

15 Auernhammer/Herbst, DS-GVO und BDSG, 5. Aufl. 2017, Art. 22 Rn. 19 f.; s. auch Sydow/Helfrich, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 22 Rn. 76.

16 Paal/Pauly/Martini, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 22 Rn. 43.

17 So auch Auernhammer/Herbst, DS-GVO und BDSG, 5. Aufl. 2017, Art. 22 Rn. 21.

18 Siehe BT-Drucks. 18/11325, S. 106.

3. Folgerungen: Keine Änderung der europäischen Vorgaben der Sache nach

Was folgt daraus? Maßgeblich unterscheiden sich Art. 8 Abs. 4 DSRL und Art. 9 Abs. 2 lit. g) DS-GVO mithin dadurch, dass das vormals „wichtige“ nun ein „erhebliches“ öffentliches Interesse sein muss.¹⁹ Weiterhin werden aus angemessenen Garantien im Sinne des Art. 15 Abs. 2 lit. b) DSRL, die die Mitgliedstaaten hinsichtlich der Betroffenenrechte zu treffen haben, angemessene Maßnahmen gemäß Art. 22 Abs. 4 DS-GVO. Diese – rein graduellen – Modifikationen des Wortlautes deuten aber *prima facie* nicht auf eine Verengung der materiellen Rechtslage hin – im Gegenteil: Viel mehr indizieren sie eine leichte Absenkung der europarechtlichen Vorgaben. Dies zeigt bereits das semantische Verständnis der genannten Begriffe. Das Wort „wichtig“ beschreibt nach allgemeinem Sprachgebrauch eine Gegebenheit, die für jemanden von wesentlicher Bedeutung ist, sodass davon viel abhängt.²⁰ Die Bezeichnung der öffentlichen Interessen als „erheblich“ dagegen meint allein, dass diese ins Gewicht fallen und damit beträchtlich sind.²¹ Während zuvor also das öffentliche Interesse von besonderer Bedeutung sein und viel davon abhängen musste, fällt es nach künftiger Rechtslage unter mehreren Faktoren nur noch ins Gewicht. Ähnlich verhält es sich mit den angemessenen „Garantien“, die die Mitgliedstaaten vorsehen können, und die bald nur noch angemessene „Maßnahmen“ sind. Wer etwas garantiert, übernimmt eine Gewähr für sein Tun, wer eine Maßnahme trifft, handelt dagegen nur, um etwas zu bewirken, ohne jedoch für den Erfolg eintreten zu wollen oder zu müssen.²²

Die unionsrechtlichen Maßstäbe haben sich damit auf den ersten Blick minimal gelockert. Dies zeigt sich nicht zuletzt auch daran, dass der Ausnahmekatalog des Art. 9 Abs. 2 DS-GVO im Vergleich zu Art. 8 Abs. 2 DSRL deutlich erweitert wurde.²³ Entgegen der Auffassung des Bayerischen Datenschutzbeauftragten scheint die Bundesregierung mit § 37 Abs. 1 Nr. 2 BDSG n.F. die Vorgaben des EU-Rechts also sehr wohl ernst zu nehmen. Dennoch soll im Folgenden eine etwas eingehendere Betrachtung der datenschutzrechtlichen Hürden sowie der Europarechtskonformität des § 37 Abs. 1 Nr. 2 BDSG n.F. erfolgen.

III. Unveränderte Europarechtskonformität

Schon die obige Gegenüberstellung spricht für eine unveränderte Europarechtskonformität der bisherigen Verfahren und auch des künftigen Rechts: Wer dessen Europarechtswidrigkeit behauptet, der müsste auch die Europarechtswidrigkeit des *status quo* behaupten. Das aber überzeugt nicht. Zur Betrachtung der Europarechtskonformität des § 37 Abs. 1 Nr. 2 BDSG n.F. sind nun die Vorgaben der Art. 22 Abs. 4, 9 Abs. 2 lit. g) DS-GVO näher in den Blick zu nehmen:

1. Erhebliches öffentliches Interesse gemäß Art. 9 Abs. 2 lit. g) DS-GVO

Nach Art. 9 Abs. 2 lit. g) DS-GVO muss – wie dargestellt – die Datenverarbeitung aus Gründen eines erheblichen öf-

fentlichen Interesses erforderlich sein. Aus Erwägungsgrund 46 – beispielhaft genannt sind dort die „Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen“ – und auch Art. 6 Abs. 1 lit. e) DS-GVO, der jegliche öffentliche Aufgabe genügen lässt, ergibt sich, dass das von der Generalklausel geforderte erhebliche öffentliche Interesse ein qualifiziertes sein muss, das gewichtig genug ist, eine mitgliedstaatliche Ausnahmenorm zu legitimieren, wobei dem nationalen Gesetzgeber diesbezüglich ein weiter Gestaltungsspielraum zugestanden wird.²⁴ Demnach kann das erhebliche öffentliche Interesse fraglos in der Abwehr von Gefahren für absolut geschützte Rechtsgüter wie etwa Leib und Leben liegen. Dies ergibt sich bereits aus Art. 9 Abs. 2 lit. c) DS-GVO. In Ansehung der ebenfalls von Art. 9 Abs. 2 lit. g) DS-GVO geforderten spezifischen Maßnahmen genügt es jedoch auch, wenn die Unversehrtheit der Rechtsordnung sichergestellt wird.²⁵

a) Warum die vollautomatisierte Verarbeitung der Effizienz dient

Dabei hört es aber nicht auf. Verarbeiten private Krankenversicherungen Gesundheitsdaten per automatisierter Einzelentscheidung, dient dies der Effizienz. Und eine effiziente private Krankenversicherung liegt erheblich im öffentlichen Interesse – nicht nur im Interesse des Versicherten. Denn: Würde jede Entscheidung im Bereich der Krankenversicherung durch einen Mitarbeiter gefällt, entstünden deutlich höhere Personalkosten. An diesen höheren Kosten würden auch die Versicherten durch höhere Beiträge zur privaten Krankenversicherung partizipieren. Das automatisierte Verfahren dagegen ist kostengünstiger, da weniger personalintensiv. Die so zu Stande kommenden niedrigeren Beiträge zur privaten Krankenversicherung kommen also der Gesamtheit der Privatversicherten zugute. Ähnlich verhält es sich auch mit der Bearbeitungsdauer. Diese ist durch die Automatisierung ebenfalls erheblich kürzer, jedenfalls soweit es um Anträge der Versicherten geht. Dies erkennt auch Erwägungsgrund 52 an, wenn er davon spricht, dass die „Gewährleistung der öffentlichen Gesundheit und

19 Paal/Pauly/Frenzel, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 9 Rn. 38.

20 Vgl. Duden, Stichwort „wichtig“, abrufbar unter <https://www.duden.de/rechtschreibung/wichtig>, Abruf v. 04.01.2018.

21 Vgl. Duden, Stichwort „erheblich“, abrufbar unter <https://www.duden.de/rechtschreibung/erheblich>, Abruf v. 04.01.2018.

22 Anders und damit von gleichbleibenden europäischen Vorgaben ausgehend Sydow/Kampert, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9 Rn. 39 mit der Begründung, dass „Garantien“ und „Maßnahmen“ in der DS-GVO zugleich verwendet würde, wie überdies ein Vergleich der verschiedenen Sprachfassungen von Art. 9 Abs. 2 lit. b) und Art. 9 Abs. 2 lit. g) DS-GVO zeige, sodass sich beide Begrifflichkeiten inhaltlich entsprechen.

23 Eine ausführliche Genese findet sich bei Paal/Pauly/Frenzel, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 9 Rn. 3 ff.

24 Auernhammer/Greve, DS-GVO und BDSG, 5. Aufl. 2017, Art. 9 Rn. 19; vgl. auch Sydow/Kampert, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9 Rn. 36.

25 So Paal/Pauly/Frenzel, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 9 Rn. 39.

der Verwaltung von Leistungen der Gesundheitsversorgung, insbesondere wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen sichergestellt werden soll“ als Ausnahme vom Verbot der Verarbeitung sensibler Daten in Betracht kommt.

Aber nicht nur diese Praktikabilitätsabwägungen begründen das erhebliche öffentliche Interesse. Auch ist zu berücksichtigen, dass das Verarbeitungsprogramm letztlich nichts anders macht als ein Mitarbeiter, der die Entscheidung fällt. Schließlich müssen sich doch sowohl Programm als auch Mensch bei der Entscheidung an Vorgaben der privaten Krankenversicherung halten. Um es plastisch zu machen: So existieren etwa hinsichtlich der Frage, ob ein künstliches Hüftgelenk gewährt wird, von den Krankenversicherern vorgegebene Prüfkriterien. Ob Prüfung und darauf basierende Entscheidung nun durch einen Mitarbeiter oder ein automatisiertes Programm erfolgt, kann also keinen Unterschied machen. Der Prüfungsumfang ist derselbe.

b) Das öffentliche Interesse in der Rechtsprechung des EuGH

Und dieses Mehr an Effizienz ist ein öffentliches Interesse. Das öffentliche Interesse wird, da letztlich eine Vielzahl von Fallkonstellationen denkbar ist, in denen die Verarbeitung von Gesundheitsdaten im öffentlichen Interesse liegen kann, eher weit verstanden,²⁶ sodass auch die Effizienz der Krankenversicherung darunter fallen kann. Dies zeigt sich ebenfalls anhand einer Durchsicht der einschlägigen EuGH-Rechtsprechung. Danach kann nahezu alles ein öffentliches Interesse sein: Vom öffentlichen Interesse an der Kulturpolitik,²⁷ über das öffentliche Interesse an der Bekanntgabe von Umweltinformationen²⁸ bis hin zu dem – und für uns näherliegend – Schutz der Volksgesundheit,²⁹ um nur drei Beispiele willkürlich herauszugreifen. Maßgeblich ist allein, dass es sich um eine mit den bereits bekannten Fallgruppen des öffentlichen Interesses vergleichbare Konstellation handelt. So wird man es auch im Rahmen des Art. 9 Abs. 2 lit. g) DS-GVO halten können. Jedenfalls dann, wenn das erhebliche öffentliche Interessen den sonstigen Verarbeitungsausnahmen des Art. 9 Abs. 2 DS-GVO gleicht, wird man es anerkennen müssen.³⁰ Es ist offensichtlich, dass neben diesen eher weit verstandenen und breit definierten öffentlichen Interessen auch die Effizienz der Krankenversicherung ein erhebliches öffentliches Interesse begründen kann.

2. Angemessene Sicherungen (Art. 22 Abs. 4, Art. 9 Abs. 2 lit. g DS-GVO)

Dies allein reicht freilich nicht. Zusätzlich ergibt sich aus der Zusammenschau von Art. 9 Abs. 2 lit. g) und Art. 22 Abs. 4 DS-GVO, dass angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und der berechtigten Interessen der betroffenen Person vorgesehen werden müssen. Spezifisch sind die Maßnahmen allemal, da sie auf Gesundheitsdaten bezogen sind. Jedoch müssen sie auch angemessen sein. Damit verlangt die Öffnungsklausel dem

nationalen Recht viel ab. § 37 Abs. 1 Nr. 2 BDSG n.F. ist dem jedoch nachgekommen. So verpflichtet der deutsche Gesetzgeber den jeweiligen privaten Krankenversicherer, selbst angemessene Maßnahmen zu treffen. Durch das Adverb „mindestens“ wird deutlich gemacht, dass zu diesen das „Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen“, das „Recht auf Darlegung des eigenen Standpunktes“ und das „Recht auf Anfechtung der Entscheidung“ zählen. Über diese Rechte muss die verantwortliche Krankenversicherung den Betroffenen denkbare Informationen, spätestens ab dem Zeitpunkt der Mitteilung der ablehnenden Entscheidung. Die aufgezählten Rechte kommen den Vorstellungen des europäischen Verordnungsgebers gleich, wie er sie in Erwägungsgrund 71 festgehalten hat, und stellen die Wahrung der berechtigten Interessen des Betroffenen sicher. Denn dieser kann für den Fall, dass dessen Antrag nicht stattgegeben wird, eine Überprüfung der automatisiert getroffenen Entscheidung erreichen, sodass – ganz im Sinne der Ratio der Art. 9 Abs. 2 lit. g), 22 Abs. 4 DS-GVO – Besonderheiten der Person Berücksichtigung finden können. Der Schutz verlagert sich damit im Verfahren also nur weiter nach hinten – das Schutzniveau jedoch sinkt nicht ab.

Im Gegenteil: Es steigt leicht an. Denn diese ausdifferenzierten Vorgaben des § 37 Abs. 1 Nr. 2 BDSG n.F. gehen tendenziell weiter als das noch aktuell zum Zuge kommende dreischrittige Vorgehen gemäß § 6a Abs. 2 Nr. 2 BDSG. Danach steht am Anfang die Information des Betroffenen über die automatisierte Einzelentscheidung, anschließend erfolgen Mitteilung und Erläuterung der Gründe für die Entscheidung, soweit der Betroffene dies wünscht, und zuletzt muss die Möglichkeit für den Betroffenen bestehen, den eigenen Standpunkt deutlich zu machen, um eine Überprüfung und ggf. auch eine Revision der Entscheidung zu erreichen.³¹ Bisher konnte der Betroffene also lediglich durch Darlegung des eigenen Standpunktes versuchen, eine Überprüfung der automatisiert getroffenen Entscheidung durch einen Mitarbeiter zu erreichen – nach künftiger Rechtslage unter dem Regime der DS-GVO und dem BDSG n.F. kann er eine solche durch Geltendmachung seines Recht auf Eingreifen einer Person seitens des Verantwortlichen leichter herbeiführen. Da die Vorgaben des § 37 Abs. 1 Nr. 2 BDSG n.F. mithin weiter gehen als die Erfordernisse des § 6a Abs. 2 Nr. 2 BDSG, und das trotz leicht gelockerter europarechtlicher Vorgaben, spricht viel dafür, dass der Gesetzgeber angemessene Maßnahmen zur Wahrung der berechtigten Interessen des Betroffenen getroffen hat. Die Voraussetzungen der Öffnungsklausel wurden also in dieser Hinsicht erfüllt.

26 Sydow/Kampert, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9 Rn. 35.

27 EuGH v. 25.07.1991 – C-353/89, EuZW 1992, 56 Rn. 30 (Mediawet).

28 So erst jüngst EuGH v. 13.07.2017 – C-60/15 P, NVwZ 2017, 1276 Rn. 60 (Saint-Gobain Glass Deutschland GmbH).

29 EuGH v. 17.07.1997 – C-183/95, EuZW 1997, 730 Rn. 61 (Affish BV).

30 Dafür Sydow/Kampert, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9 Rn. 35.

31 Paal/Pauly/Frenzel, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 22, Rn. 42; vgl. dazu auch Gola/Schomerus, BDSG, 12. Aufl. 2015, § 6a Rn. 14 ff.

3. Eben deshalb: Verhältnismäßige Zweckverfolgung (Art. 9 Abs. 2 lit. g DS-GVO)

Der Rest ist dann schnell erzählt. Was ohnehin selbstverständlich ist, ordnet der europäische Ordnungsgeber explizit an: Die nationale Norm muss verhältnismäßig sein, oder wie es der Wortlaut sagt „in angemessenem Verhältnis zu dem verfolgten Ziel“ stehen. Nach der Rechtsprechung des EuGH in Bezug auf Maßnahmen der Mitgliedstaaten verlangt der Grundsatz der Verhältnismäßigkeit, dass die „ergriffenen Maßnahmen nicht die Grenzen dessen überschreiten, was zur Erreichung der (...) verfolgten Ziele geeignet und erforderlich ist. Dabei ist, wenn mehrere geeignete Maßnahmen zur Auswahl stehen, die am wenigsten belastende zu wählen; ferner müssen die verursachten Nachteile in angemessenem Verhältnis zu den angestrebten Zielen stehen“.³² Danach orientiert sich die Verhältnismäßigkeit an den Maßstäben der Geeignetheit, Erforderlichkeit und Angemessenheit, wobei der EuGH dazu tendiert, die Angemessenheit im Rahmen der Erforderlichkeit zu thematisieren.³³ Die Verarbeitung personenbezogener Gesundheitsdaten per automatisierter Einzelentscheidung, wie in § 37 Abs. 1 Nr. 2 BDSG n.F. vorgesehen, ist zunächst geeignet, das angestrebte Ziel, die private Krankenversicherung effizienter zu machen, zu fördern. Wie bereits zuvor dargelegt, sinken Kosten und Bearbeitungsdauer für Anträge der Versicherten – und das bei gleichbleibendem Prüfumfang anhand der von den Krankenversicherungsträgern ohnehin vorgegebenen Kriterien. Dies ist unter allen denkbaren zur Verfügung stehenden Mitteln auch das am wenigsten belastende. Denn die Rechte der von der Datenverarbeitung Betroffenen werden durch die automatisierte Einzelentscheidung nicht beschnitten. Vielmehr verlagert sich der Schutz im Verfahren ein Stück weit nach hinten, wird dafür aber auch angehoben, indem unter Geltung des § 37 Abs. 1 Nr. 2 BDSG n.F. im Anschluss an eine ablehnende oder bloß nicht vollumfänglich dem Antrag des Versicherten stattgebende Entscheidung der Krankenkasse auf den Leistungsantrag des Versicherten hin eine Überprüfung des Verfahrens durch einen Mitarbeiter stattzufinden hat. Diese erst auf eine nachträgliche Überprüfung durch eine natürliche Person zielende Verfahrensweise steht auch in einem ausgewogenen Verhältnis zur Erreichung einer effizienten (privaten) Krankenversicherung, da durch die Mindestrechte des § 37 Abs. 1 Nr. 2 BDSG n.F. eine am Ende des Bearbeitungsprozesses stehende personale Verantwortung sichergestellt ist, sodass individuelle Besonderheiten, die unter Umständen in der Natur des Versicherten liegen, in jedem Fall Berücksichtigung finden können. Die Verhältnismäßigkeit der Zweckverfolgung nach Art. 9 Abs. 2 lit. g) DS-GVO ist also zu bejahen.

4. Eben deshalb: Wahrung des Wesensgehalts des Rechts auf Datenschutz (Art. 9 Abs. 2 lit. g DS-GVO)

Wurden all diese Voraussetzungen beachtet, fordert die Norm weiterhin, dass der Wesensgehalt des Rechts auf Datenschutz gewahrt bleiben muss. Damit hat der europäische

Verordnungsgeber ein *Hapax legomenon* des Datenschutzrechts geschaffen. Denn der Begriff des Wesensgehalts taucht in der DS-GVO nur an einer einzigen Stelle erneut auf (nämlich in Art. 23 Abs. 1 DS-GVO), dort aber bezogen auf alle Grundrechte und Grundfreiheiten.³⁴ Damit handelt es sich um eine singulär vorkommende und dem Datenschutzrecht fremde Begrifflichkeit, die schwer bestimmbar ist. Denn: Was genau der Wesensgehalt des Datenschutzrechts ist, bleibt offen. Selbst der EuGH hat bislang keine Konkretisierung des Wesensgehalts des Datenschutzrechts vorgenommen.³⁵ Auch nach deutschem Recht – dort sei etwa an Art. 19 Abs. 2 GG erinnert – handelt es sich um eine schwierige Begrifflichkeit.³⁶ Insgesamt kann sie als überflüssig weil nicht abschließend eingrenzbar qualifiziert werden. Außerdem fragt sich, in welcher denkbaren Fallkonstellation der Wesensgehalt überhaupt verletzt sein soll, wenn doch die Verhältnismäßigkeit gewahrt sowie angemessene und spezifische Maßnahmen zur Sicherung der Grundrechte und Interessen der betroffenen Person getroffen wurden.³⁷ Man wird bei Betrachten des Wortlautes von Art. 9 Abs. 2 lit. g DS-GVO sagen können, dass die Wesensgehaltsgarantie zwar vom Verhältnismäßigkeitsgrundsatz zu trennen ist, aber letztlich nicht mehr bedeutet, als dass der Gesetzgeber berechtigt ist, das Datenschutzrecht mit anderen Rechtsgütern abzuwägen, nur dass er eben dessen Kernbereich nicht preisgeben darf, was aber wohl nur dann der Fall wäre, wenn er eine Datenverarbeitung ohne auch nur eine einzige Beschränkung als zulässig erklärte.³⁸

Unabhängig von dieser Kritik an der gebrauchten Begrifflichkeit sowie der Ausgestaltung der Norm³⁹ muss aber nach diesen Grenzlinien jedenfalls in der hier gegebenen Konstellation der Wesensgehalt des Datenschutzrechts als gewahrt angesehen werden. Die Mindestrechte des Betroffenen aus

32 Vgl. EuGH v. 21.07.2011 – C-2/10, NVwZ 2011, 1057 Rn. 73 (Franchini); EuGH v. 09.03.2010, C-379/08, EuZW 2010, 388 Rn. 86 (ERG); s. auch Jarass, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 52 Rn. 36.

33 Dazu näher Jarass, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 52 Rn. 36; s. auch Grabitz/Hilf/Nettesheim/Leible/T. Streinz, Das Recht der EU, 62. EL Juli 2017, Art. 34 Rn. 123 ff. die darauf hinweisen, dass der EuGH keine dem deutschen Recht ähnelnde dreistufige Verhältnismäßigkeitsprüfung durchführt; anders dagegen GA Trstenjak, SchLA C-10/10 Rn. 67 ff. – Kom./Österreich.

34 Deswegen könnte man auch von einem *Dis legomenon* sprechen.

35 Selbst in der viel beachteten EuGH-Entscheidung v. 06.10.2015, C-362/14, EuZW 2015, 881 Rn. 94 in der Rechtssache Schrems hat der EuGH einen Verstoß gegen den Wesensgehalt des Art. 7 GrCh angenommen, ohne jedoch zu definieren, worin dieser genau liegt; vertiefend Sydow/Peuker, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 23 Rn. 39 m.w.N.

36 Schon früh hat Scheuerle in seinem Aufsatz „Das Wesen des Wesens“ darauf hingewiesen, dass das Wesensargument nichts weiter ist als ein Kryptoargument, das nur gebraucht wird, um anderes zu verschleiern, und dass es wegen seiner fehlenden Klarheit nicht geeignet ist, rechtlich belastbare Begründungen zu liefern; Scheuerle, AcP 163 (1964), 429 ff.

37 Dieselbe Frage stellen sich auch Sydow/Kampert, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9 Rn. 40, die deshalb auch eine eigenständige Bedeutung der Wesensgehaltsgarantie zu Recht verneinen.

38 Sydow/Peuker, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 23 Rn. 41; lesenswert auch Bock/Engeler, DVBL. 2016, 593, 596.

39 Vgl. tiefergehend auch Stern/Sachs/Johlen, Europäische Grundrechte-Charta, 1. Aufl. 2016, Art. 8 Rn. 38 ff.

§ 37 Abs. 1 Nr. 2 BDSG n.F. garantieren nicht nur die Grundprinzipien des Datenschutzrechts und verhindern es in effektiver Art und Weise, dass die Gesundheitsdaten des von der Verarbeitung Betroffenen ausschließlich schwer nachvollziehbaren automatisierten Einzelentscheidungen überlassen werden, sondern ermöglichen auf Tätigwerden des Betroffenen hin eine Überprüfung durch Mitarbeiter des privaten Krankenversicherers. Dass der Betroffene auf seine eigene Initiative hin eine Revision der ablehnenden oder nicht vollumfänglich dem Begehren des Versicherten stattgebenden Entscheidung erreichen kann, entspricht auch der Konzeption der DS-GVO selbst, wie ein Blick auf das in Art. 21 Abs. 1 DS-GVO verankerte Widerspruchsrecht zeigt. Auch dort hat die betroffene Person das Recht, gegen die an sich erlaubte Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen, aus Gründen, die sich aus ihrer besonderen Situation ergeben.⁴⁰ Deshalb kann ein Verarbeitungsverfahren, das europäischen Vorgabebestimmungen jedenfalls von der dahinterstehenden Konzeption her gleicht (auch wenn Widerspruchs- und Überprüfungsrecht für den Fall, dass dem Antrag nicht stattgegeben wird, dogmatisch etwas anderes sind), wohl kaum europarechtswidrig sein – das wäre mehr als widersprüchlich.

IV. Summa

Es hat sich gezeigt, dass § 37 Abs. 1 Nr. 2 BDSG n.F. im Einklang mit Art. 9 Abs. 2 lit. g), 22 Abs. 4 DS-GVO steht und damit europarechtskonform ist – genauso wie seine noch gültige Vorgängerregelung in § 6a Abs. 2 Nr. 2 BDSG mit Art. 8 Abs. 4, 15 Abs. 2 DSRL vereinbar ist. Denn: Die marginalen Wortlautänderungen der europäischen Vorgaben fallen unter der DS-GVO im Vergleich zur aktuell noch gültigen Rechtslage leicht ab. Die vormals „wichtigen“ werden zu „erheblichen“ öffentlichen Interessen, die angemessenen „Garantien“ werden zu angemessenen „Maßnahmen“.

Daraus folgt: Wer die künftige Regelung für europarechtswidrig hält, hält auch den *status quo* für europarechtswidrig. Das aber vermag nicht zu überzeugen. Denn parallel zu den abfallenden europarechtlichen Vorgaben werden die Rechte des von der automatisierten Einzelentscheidung Betroffenen in § 37 Abs. 1 Nr. 2 BDSG n.F. mutiger formuliert als in § 6a Abs. 2 Nr. 2 BDSG und steigen damit leicht an. Dem hinter dem grundsätzlichen Verbot automatisierter Einzelentscheidungen und deren Zulässigkeit im Ausnahmefall stehende Gedanken, auf Grund der besonderen Sensibilität von Gesundheitsdaten im Hinblick auf die Persönlichkeit des Betroffenen eine personale Verantwortung für die Einzelentscheidung sicherstellen zu wollen, wird durch die explizit von § 37 Abs. 1 Nr. 2 BDSG n.F. genannten Mindestrechte des Betroffenen Rechnung getragen. Deshalb lässt sich die Europarechtskonformität der auf der europäischen Öffnungsklausel beruhenden nationalen Norm wohl kaum ernsthaft bestreiten. Alles in allem lässt sich also festhalten, dass die eingangs geäußerte Vermutung zutrifft: Bloß viel Lärm um nichts!



Prof. Dr. Gregor Thüsing

ist Direktor des Instituts für Arbeitsrecht und Recht der sozialen Sicherheit der Universität Bonn und Vorstandsmitglied der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn.

⁴⁰ Dazu Auernhammer/Kramer, DS-GVO und BDSG, 5. Aufl. 2017, Art. 21 Rn. 1 f.

Update-Workshop zur Datenschutz-Grundverordnung

UPDATE-
WORKSHOP



24.–25. April 2018
in Köln

Sichern Sie sich Ihren fachlichen Vorsprung!

Informationen und Anmeldung auf www.datakontext.com

GDD

Gesellschaft für Datenschutz
und Datensicherheit e.V.

DATAKONTEXT

Kurzbeiträge

Betriebliche Hausverbote und Datenschutz

RA Dr. Georg Wronka, Bonn*

I. Berechtigung des Arbeitgebers zur Erteilung von Hausverboten

Die grundrechtliche Eigentumsgarantie (Art. 14 GG) enthält die Befugnis des Eigentümers, mit der ihm gehörenden Sache grundsätzlich nach Belieben zu verfahren und andere von der Einwirkung auszuschließen (§ 903 S. 1 BGB). Das gilt auch hinsichtlich eines Gebäudes oder eines Grundstücks, d.h. der Grundstückseigentümer oder -besitzer (§§ 858 ff, 903, 1004 BGB) besitzt das Hausrecht, das es ihm in der Regel gestattet, frei darüber zu entscheiden, wem er den Zutritt gestattet und wem er ihn verwehrt.

Darüber hinaus ist das Hausrecht Ausdruck der durch Art. 2 Abs. 1 GG gewährleisteten Privatautonomie, die die Selbstbestimmung des Einzelnen im Rechtsleben schützt. Das gilt auch für die Entscheidung, ob und in welchem Umfang einem Dritten der Zugang zu einer bestimmten Örtlichkeit gestattet wird.

Durch das Hausrecht geschützte Bereiche sind u.a. die Geschäfts- und Betriebsräume oder sonstiges befriedetes Eigentum. Es kann nicht nur dem Eigentümer, sondern auch anderen Personen zustehen, insbesondere dem unmittelbar über die Einrichtung verfügungsberechtigten unmittelbaren Besitzer, der nicht Eigentümer sein muss. Strafrechtlich flankiert wird es durch den Straftatbestand des Hausfriedensbruchs (§ 123 StGB).

Das Hausrecht steht auch einem Betriebsinhaber hinsichtlich der seinen Betrieb betretenden Personen zu, wobei jedoch Einschränkungen gelten, soweit diese Personen in einem Arbeitsverhältnis mit dem Hausrechtsinhaber stehen.

II. Beschränkung des Hausrechts bei bestehendem Arbeitsvertrag

1. Die arbeitsrechtliche Beschäftigungspflicht

Im bestehenden Arbeitsverhältnis ist das Hausrecht des Arbeitgebers auf Grund der ihm obliegenden Beschäftigungspflicht eingegrenzt. Der Arbeitnehmer hat in einem ungekündigten Arbeitsverhältnis einen Anspruch darauf, dass das Unternehmen seine Arbeitsleistung entgegennimmt. Das Bundesarbeitsgericht¹ leitet diesen Anspruch aus dem sich aus dem Persönlichkeitsrecht ergebenden Beschäftigungsanspruch ab. Der Mitarbeiter muss die für seine Arbeit notwendigen Betriebsräume aufsuchen dürfen. Demgemäß überwiegt die Beschäftigungspflicht regelmäßig gegenüber einer ihr entgegen stehenden Ausübung des Hausrechts.

2. Hausverbot im Zusammenhang mit der bevorstehenden Beendigung des Beschäftigungsverhältnisses

Somit kann dem Mitarbeiter vor Beendigung des Arbeitsverhältnisses das weitere Betreten des Betriebes nur in besonderen Fällen verweigert werden, die in der Regel im Zusammenhang mit der nachfolgenden Beendigung des Beschäftigungsverhältnisses stehen müssen.²

Berechtigt ist der Arbeitgeber zu einer sofortigen Freistellung nach Ausspruch einer verhaltensbedingten Kündigung, wenn der Kündigungsgrund das sofortige Verweisen vom Betriebsgelände rechtfertigt. Ein solcher Verweis könnte z.B. notwendig sein, um sicherzustellen, dass der Gekündigte keine Daten vom Rechner löscht oder Unterlagen aus dem Büro entfernt. Das gilt unabhängig davon, ob die Beendigung befristet, fristlos oder einvernehmlich erfolgt.

Ein besonderes berechtigtes Interesse des Arbeitgebers an der sofortigen Freistellung kann auch bereits vor einer eventuellen Kündigung gerechtfertigt sein, wenn ein konkreter Verdacht gegen den Mitarbeiter besteht, der aufgeklärt werden muss.

3. Fortbestehende spezielle Zutrittsrechte

Der Arbeitgeber hat jedoch zu berücksichtigen, dass im Zusammenhang mit der (faktischen) Beendigung des Beschäftigungsverhältnisses beiderseitige Rechte und Pflichten bestehen können, die ein – ggf. abgestimmtes – Betreten des Betriebes bedingen. Dies kann erforderlich sein, weil noch zum Eigentum des Arbeitgebers gehörende Arbeitsmittel abzugeben sind oder der Arbeitnehmer noch persönliche Gegenstände in dem Unternehmen hat.

Auch aus anderen Gesichtspunkten kann ggf. nur ein eingeschränktes Hausverbot erfolgen. Einem Mitarbeiter, dessen Freistellung bis zum Renteneintritt vereinbart wurde, kann aufgrund des arbeitsrechtlichen Gleichbehandlungsgrundsatzes nicht die Teilnahme an betrieblichen Veranstaltungen wie Weihnachtsfeiern oder Betriebsausflügen untersagt werden, soweit der Arbeitgeber die Teilnahme betriebsöffentlich den bei ihm beschäftigten Arbeitnehmern anbietet. Will er einzelne Arbeitnehmer von der Teilnahme ausschließen

* Der Autor ist Rechtsanwalt in Bonn mit den Arbeitsschwerpunkten Datenschutz- und Wettbewerbsrecht.

¹ Vgl. zur Nichtheranziehung des Hausrechts im Rahmen der Videoüberwachung am Arbeitsplatz: BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03.

² LAG Rheinland-Pfalz, Urt. v. 25.08.2015 – 6 Sa 30/15.

ßen, bedarf er eines sachlichen Grundes. Eine vorausgegangene einvernehmliche Freistellung ist jedenfalls kein solcher Sachgrund.³

Inbesondere gelten Besonderheiten bei Betriebsratsmitgliedern. Einem Betriebsratsmitglied kann die Ausübung seines Amtes regelmäßig nicht durch ein absolutes Hausverbot unmöglich gemacht werden.⁴ Dies würde einen Verstoß gegen das Behinderungsverbot des § 78 S. 1 BetrVG darstellen, das auch besteht, wenn die Kündigung beabsichtigt ist bzw. im Rahmen eines Zustimmungseretzungsverfahrens nach § 103 Abs. 2 betrieben wird.⁵

Ein generelles Hausverbot gegenüber einem Mitglied des Betriebsrats darf daher nur ausnahmsweise erfolgen, wenn mit an Sicherheit grenzender Wahrscheinlichkeit feststeht, dass eine strafbare Handlung gegenüber dem Arbeitgeber vorliegt.

III. Hausverbot nach Beendigung des Arbeitsverhältnisses

1. Freie Ausübung des Hausrechts

Für die Zeit nach der Beendigung des Arbeitsverhältnisses ist ein Arbeitgeber frei in seiner Entscheidung, sein Hausrecht gegenüber einem früheren Arbeitnehmer durch Ausspruch eines Hausverbots auszuüben, d.h. das Hausverbot kann unmittelbar mit der Kündigung erfolgen. Das zwischenzeitlich beendete Arbeitsverhältnis schränkt die verfassungsrechtlich verankerte Verfügungsbefugnis des Eigentümers/Besitzers nicht mehr ein. Grundsätzlich bedarf es für die Ausübung des Hausrechts auch keines rechtfertigenden Grundes.

2. Einschränkung der Berufsfreiheit

Eine Beschränkung des Hausrechts, die das Vorliegen sachlicher Gründe zum Ausschluss eines Hausverbots erfordert, kann sich allerdings aus einer marktbeherrschenden Stellung des früheren Arbeitgebers ergeben⁶.

Eine missbräuchliche Ausnutzung eines Machtverhältnisses liegt aber nicht vor, wenn das Hausverbot ausgesprochen wurde, weil der durch Tatsachen begründete Verdacht bestand, der Arbeitnehmer habe gegen die Geschäftsinteressen seines Arbeitgebers in erheblicher Weise verstoßen. Dabei kommt es weder auf eine strafrechtliche Bewertung noch darauf an, ob Gründe vorliegen, die den Ausspruch einer Kündigung rechtfertigen. Auch ein Vergleich der Parteien, wonach das Arbeitsverhältnis durch ordentliche Kündigung geendet hat, steht der Wirksamkeit eines Hausverbots nicht entgegen.

IV. Hausverbote gegenüber Dritten

Das Hausrecht gestattet es auch, gegenüber Dritten ein Hausverbot zu erteilen, z.B. wenn diese als Mitarbeiter eines externen Dienstleisters im Betrieb Arbeitsleistungen erbringen, mag das auch dazu führen, dass sie in Ausübung ihrer beruflichen Tätigkeit beeinträchtigt sind bzw. ihr Ar-

beitgeber sich zur Kündigung des Arbeitsverhältnisses entschließt⁷.

Wird der Kraftfahrer eines für den Betrieb tätigen Transportunternehmens in eine körperliche Auseinandersetzung mit Mitarbeitern des Betriebs verwickelt und beleidigt er den Betriebsleiter, kann das Hausverbot ggf. zum Verlust seines Entgeltanspruchs gegenüber seinem Arbeitgeber und zur Gefährdung seines Arbeitsverhältnisses führen, wenn der Kraftfahrer nur für Fahrten für den das Hausverbot aussprechenden Betrieb eingesetzt wurde und werden konnte⁸.

V. Datenverarbeitungen zur Umsetzung des Hausverbots im verfügbaren Betrieb

1. Allgemeines

Eine Form ist für die Erteilung des Hausverbots nicht vorgesehen. Auch der bei einem noch bestehenden Arbeitsverhältnis mit dem Hausverbot verbundene Verzicht auf die Arbeitsleistung muss nicht schriftlich erklärt werden⁹, mag der Arbeitnehmer auch daran aus Beweisführungsgründen im Hinblick auf seinen infolge Annahmeverzugs des Arbeitgebers (§ 615 BGB) bestehenden Vergütungsanspruch ein gewichtiges Interesse haben.

Erfolgt die Erklärung schriftlich oder wird sie nachträglich schriftlich dokumentiert – sei es als Vorgang in der Personalakte oder sei es ggf. in einer in digitalisierter Form geführten Hausverbots-Datei –, so sind die hierbei zu beachtenden datenschutzrechtlichen Anforderungen in Betracht zu ziehen.

2. Gesetzliche Erlaubnisnormen

a. Allgemeines

Zu beachten ist das nunmehr in Art. 6 Abs. 1 DS-GVO statuierte und in § 26 Abs. 5 und 1 BDSG n.F. auf alle Arten der Verarbeitung von Beschäftigtendaten ausgedehnte Verbot mit Erlaubnisvorbehalt. Wegen der in diesem Fall nicht in Betracht kommenden Einwilligung des Beschäftigten ist für die Verarbeitung des Datums „Hausverbot“ vorrangig § 26 Abs. 1 S. 1 BDSG n.F. als Gestattungsnorm in Erwägung zu ziehen. Danach ist es dem Arbeitgeber erlaubt, personenbezogene Daten von Beschäftigten zu verarbeiten, wenn dies im Zusammenhang mit der Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

Dabei ist nach dem Zeitraum des Hausverbots zu unterscheiden.

3 ArbG Köln, Urt. vom 22.06.2017 – 8 Ca 5233/16.

4 Vgl. LAG Berlin-Brandenburg, Beschl. vom 02.09.2009 – 17 TaBVGA 1372/09.

5 AG München, Beschl. vom 16.07.2009 – 32 BVGA 30/09, LAG München, Beschl. vom 18.11.2009 – 11 TaBVGA 16/09.

6 Vgl. zur Problematik BAG, Urteil v. 28.09.2016 – 5 AZR 224/16.

7 Vgl. BAG, Urteil v. 18.09.2008 – 2 AZR 1060/06 für den Luftfrachtabfertiger einer Drittfirma, dem wegen körperlicher Auseinandersetzungen mit Beschäftigten von dem Betrieb, in dem er eingesetzt war, ein Hausverbot erteilt wurde.

8 BAG, Urteil v. 28.09.2016 – 5 AZR 224/15.

9 LAG Rheinland-Pfalz, Urteil v. 25.08.2015 – 6 Sa 30/15.

b. Betriebsbezogenes Hausverbot im (noch) laufenden Arbeitsverhältnis

Erfolgt das Hausverbot im Rahmen eines (noch) laufenden Arbeitsverhältnisses, um dieses jedenfalls faktisch sofort zu beenden, kommt eine Speicherung und eine ggf. betriebsinterne Weitergabe des Vorgangs im Rahmen der Erforderlichkeit der Durchführung bzw. sogar der Beendigung des Beschäftigungsverhältnisses in Betracht (§ 26 Abs. 1 S. 1 BDSG n.F.). Relevant ist, ob und welche Datenverarbeitungen im Rahmen ordnungsgemäßer Personalaktenführung und zur Umsetzung des Hausverbots erforderlich sind.

§ 26 beschreibt den Begriff der Erforderlichkeit nicht näher. Jedoch enthält die Gesetzesbegründung¹⁰ Hinweise, die die diesbezügliche Rechtsprechung des BAG aufgreifen. „Im Rahmen der Erforderlichkeitsprüfung sind die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen. Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.“ Bekräftigt wird damit, dass auch die Erforderlichkeit an Hand einer am Verhältnismäßigkeitsgrundsatz ausgerichteten Interessenabwägung zu ermitteln ist¹¹.

3. Erforderlichkeit der Verarbeitung

Betrachtet man die Zweckbestimmungen der Speicherung des Hausverbots zunächst bis zum rechtlichen Ende des Beschäftigungsverhältnisses, so ergeben sich zumindest zwei „Erforderlichkeiten“, und zwar einmal, dass das Hausverbot zu Beweis Zwecken dokumentiert werden muss, und zum anderen, dass – je nach der Größe und Organisation des Betriebes – die mit der Umsetzung des Hausverbots beauftragten Stellen (z.B. Pförtner, Werksschutz) informiert werden. Nur ausnahmsweise zulässig wäre es dagegen, die Gesamtleitung zu unterrichten, was z.B. der Fall in einem kleinen Betrieb sein könnte, in dem eine Einlasskontrolle nicht besteht. Regelmäßig wird es jedoch nicht erforderlich sein, z.B. durch Aushang die gesamte Belegschaft in Kenntnis zu setzen. Generell scheidet das Verfahren wegen der mit dem Aushang des Hausverbots zudem verbundenen Prangerwirkung aus, wenn auch Publikumsverkehr bestünde¹².

In jedem Fall ist nur das Hausverbot als solches mitzuteilen, nicht aber dessen Gründe.

VI. Löschungspflicht

1. Geltung bis zur Beendigung des Beschäftigungsverhältnisses

Soll das Hausverbot nur bis zu dem per Kündigung oder per Auflösungsvereinbarung bewirkten rechtlichen Ende des Arbeitsverhältnisses wirken, stellt sich die Frage, ob es, sofern es gespeichert wurde, anschließend unverzüglich zu löschen ist, da die Zwecke, für die es verarbeitet wurde, ja an sich entfallen sind (Art. 17 Abs. 1 lit. a DS-GVO). Eine Zweckbestimmung ist jedenfalls dann nicht mehr erkennbar,

wenn es den Vergütungsanspruch des Betroffenen nicht tangierte und es nicht befristet als Beweis für den Fortfall der Entgeltzahlung weiterhin gespeichert werden durfte (Art. 17 Abs. 3 lit. e DS-GVO).

Sollte das Hausverbot jedoch auch über das rechtliche Ende des Arbeitsverhältnisses hinaus gelten, so greifen für diesen Zeitraum die nachfolgenden Überlegungen.

2. Betriebsbezogenes Hausverbot nach Ende des Beschäftigungsverhältnisses

Wird das Hausverbot für die Zeit nach Beendigung des Beschäftigungsverhältnisses ausgesprochen, so ist zwar ein gewisser Zusammenhang des Geschehens nicht zu verkennen. Gleichwohl dient die Verarbeitung des Datums nicht der „Zweckbestimmung“ Beendigung. Gleiches gilt für den Fall einer erneuten Begründung des Beschäftigungsverhältnisses, mag das Hausverbot auch den Willen zum Ausdruck bringen – jedenfalls für die Dauer seiner Geltung –, kein erneutes Beschäftigungsverhältnis mit dem Betroffenen abschließen zu wollen.

§ 26 Abs. 1 S. 1 BDSG n.F. gilt hier somit nicht; andererseits ist die Norm keine abschließende Regelung der Zulässigkeit der Verarbeitung von Arbeitnehmerdaten durch den Arbeitgeber. Er verdrängt die DS-GVO nur mit seiner parallelen Regelung in Art. 6 Abs. 1 lit. b (§ 1 Abs. 5 BDSG n.F.). Die übrigen Zulässigkeitsstatbestände des DS-GVO gelten weiter¹³.

Zu prüfen ist daher, ob die sich über das Ende des Beschäftigungsverhältnisses erstreckende Verarbeitung des Datums „Hausverbot“ im Rahmen der Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO gerechtfertigt sein kann, wobei anzumerken ist, dass diese bei herkömmlicher Speicherung in der nicht dateimäßig organisierten Personalakte nicht greift, d.h. die DS-GVO keine Anwendung findet (Art. 2 Abs. 1 DS-GVO), so dass die Zulässigkeit der Verarbeitung nach persönlichkeitsrechtlichen Gesichtspunkten der Personalaktenführung zu beurteilen wäre¹⁴.

Im Rahmen der zentralen Abwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO können berechnete Interessen des für die Verarbeitung Verantwortlichen eine Verarbeitung rechtfertigen, wenn nicht gegen die Verarbeitung gerichtete Interessen der betroffenen Person Vorrang haben, wobei auch hier die aufgezeigten Anforderungen an die Erforderlichkeit der Maßnahme gelten.

Das berechnete Interesse ist nach Maßgabe der Zweckbestimmung der Verarbeitung zu bestimmen. Liegen die Voraussetzungen für die Verfügung eines Hausverbots vor, so sind die berechtigten Interessen des Arbeitgebers an der Verarbeitung der Information im Rahmen der Notwendigkeiten der betrieblichen Organisation ohne weiteres zu bejahen.

10 Bundestags-Drucksache 18/11325, S. 97.

11 Zu den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit vgl. ausführlich Wolff, in: Wolff/Brink, DSR-Syst. A Rn. 23 ff.

12 Vgl. 8. Tätigkeitsbericht (04/2015 – 03/2017) Datenschutz im nicht-öffentlichen Bereich in Sachsen, Ziff. 8.3.0 und 8.3.2.

13 Vgl. Gola, in: Gola (Hrsg.), DS-GVO Art. 6 Rn. 123; Kort, ZD 2017, S. 319 (323).

14 Vgl. Gola, in: Gola (Hrsg.), DS-GVO Art. 2 Rn. 5 f.

Gleichwohl dürfen diesen nach Art. 6 Abs. lit. f DS-GVO keine überwiegenden Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person entgegenstehen, d.h. die beiderseitigen Interessen sind nunmehr zu gewichten¹⁵. Derartige vorrangige entgegenstehende Interessen kann der ehemalige Beschäftigte oder ein mit einem (berechtigten) Hausverbot belegter Dritter gegenüber der Ver-

arbeitung dieses Datums jedoch nicht geltend machen, wenn sie in zu seiner Durchsetzung notwendigem Umfang als betriebsinterne Maßnahme erfolgt.

¹⁵ Vgl. zum bislang geltenden Recht schon BGH, Urteil v. 17.12.1985 – VI ZR 244/84; Art. 29-Datenschutzgruppe, WP 217 v. 09.04.2014, S. 3 f.

Aus den aktuellen Berichten der Aufsichtsbehörden (33): Die Digitalisierung des Bewerbermanagements – Videointerviews bei der Bewerbung

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter*

I. Vorbemerkung

Schritt für Schritt wird auch das Bewerbermanagement unter dem Stichwort des E-Recruitings digitalisiert. Ggf. startet der Bewerbungsprozess mit der Nutzung von vom Arbeitgeber angebotenen chatbots, d.h. computergesteuerter Dialogsoftware, mit der sich der Bewerber über das Unternehmen und die angebotenen Arbeitsbedingungen unterhält. Die aufgerufene Karrierewebsite lädt ein zum Abrufen des Online Bewerbungsformulars und zur Teilnahme an einer IT-gestützten Eignungsdiagnose. Unter Bezugnahme auf Vergleichswerte früherer bzw. vorhandener Mitarbeiter können bereits aus den Bewerbungsdaten Erkenntnisse „analysiert“ werden, wie lange der Mitarbeiter vermutlich im Unternehmen bleiben werde und ob sich die Investitionen in seine Ausbildung lohnen. Schlusspunkt ist eine auf Grund eines Profiling erstellt Auswahlempfehlung. Die Akzeptanz bzw. Präferenz des Bewerbers für die Wahl des digitalen Kommunikationswegs hängt von diversen Faktoren ab, wie u.a. seinem Alter, der Ausbildung und der Art der Tätigkeit. Ist dem Unternehmen daran gelegen, nachgefragtes Personal zur Bewerbung zu motivieren, sollte dies entsprechend beachtet werden. Gleichzeitig muss aber vorab ermittelt werden, ob die Digitalisierung des Bewerbermanagement auf datenschutzrechtliche Grenzen stößt. Das Online-Bewerbungsformular muss den datenschutzrechtlichen Vorgaben der Erhebung von Bewerberdatendaten entsprechen, wobei ggf. Informationen dem Stand der Bewerbung entsprechend nur sukzessive abgefragt werden dürfen. Insbesondere unter dem Gesichtspunkt, dass die Datenübertragung via Internet ohne dem Stand der Technik entsprechende Datensicherheitsmaßnahmen nicht geschützt ist und mit dem entsprechenden Wissen weltweit eingesehen und vielfältig ausgewertet werden kann, muss z.B. das elek-

tronische Recruiting regelmäßig verschlüsselt erfolgen (Lorenz, Datensicherheit von E-Mails, DuD 2017, 757). Des Weiteren hat die Transparenz der Verfahren besonderes Gewicht für seine Rechtmäßigkeit (Art. 5, 13 DS-GVO).

In jüngster Zeit speziell in die Kritik geraten sind Videointerviews und Analyseprogramme zur Auswertung eines in Bild und Ton aufgezeichneten Videogesprächs. Ziel ist die Verbesserung der Nachwuchsgewinnung durch sorgfältigere und Ressourcen schonende Vorauswahl. Verfahren und Zulässigkeit werden betrachtet in Anwendung der DS-GVO und der BDSG-Neufassung.

II. Arten von Videointerviews

1. Erhebung, Aufzeichnung, Analyse

Ein Aspekt der Digitalisierung des Bewerbungsverfahrens ist, dass Arbeitgeber Bewerbern statt oder vor dem mündlichen Vorstellungsgespräch die Durchführung eines Videointerviews anbieten. In Betracht kommen im wesentliche folgende drei Varianten des Bewerberinterviews, nämlich

- das reine Live-Interview ohne Aufzeichnung,
- das zeitversetzten Interview mit Aufzeichnung ohne Auswertungsprogramm,
- das aufgezeichneten Interview mit automatisierter Sprach- und Bildanalyse zwecks Profiling des Bewerbers.

Maßstab für die Zulässigkeit der Verarbeitung der Gesprächsdaten, d.h. der Erhebung und der ggf. nachfolgenden Speicherung und Auswertung ist ab dem 25.05.2018 die spezielle Norm des Beschäftigtendatenschutzes in § 26 BDSG n.F. Danach ist Voraussetzung, dass die Verarbeitung der Beschäftigtendaten für die Entscheidung über die Be-

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

gründung eines Beschäftigungsverhältnisses erforderlich ist. Der Begriff beinhaltet, dass die Maßnahme geeignet, angemessen und verhältnismäßig ist, was insbesondere bedeutet, dass mildere Mittel mit gleicher Zweckerreichung nicht zur Verfügung stehen. Dies wird von zumindest zwei Aufsichtsbehörden (LDI NW, 23. Datenschutz- und Informationsfreiheitsbericht (2017), S. 53 und 61; LfDI Berlin, Jahresbericht 2016, S. 114 ff) verneint, wobei dies insbesondere bei zeitversetzten Videointerviews der Fall sein soll. Krause betont in dem 2016 vorgelegten BMAS-Forschungsbericht 482 zum Thema „Digitalisierung und Beschäftigten-datenschutz“ persönlichkeitsrechtswidriges Vorgehen insbesondere in der Durchleuchtung der Persönlichkeit durch die Auswertung der aufgezeichneten Interviews mittels Sprachanalyseverfahren. Aufgabe des Gesetzgebers sei es, psychologische Untersuchungsmethoden klar im Hinblick auf strenge Wissenschaftlichkeit und das Verbot der Gesamtbetrachtung der Persönlichkeit einzuschränken.

Andererseits müssen Unternehmen angesichts der Arbeitsmarktsituation Auswahlverfahren anbieten, die sowohl von Bewerbern akzeptiert werden als auch ein hohes Maß an Eignungsdiagnostik haben, was wiederum für Datenschutzaspekte beachtende digitalisierte Verfahren spricht (vgl. Dierks, Videointerviews im Personalauswahlverfahren, DuD 2017, S. 750 ff).

2. Kommunikationsnutzenderdaten

Ein mit dem Verfahren der Informationsgewinnung über den Bewerber nicht unmittelbar zusammenhängender Datenschutzaspekt kann sich aus der technischen Lösung der Videotelefonie, d.h. speziell eines hierbei ggf. eingesetzten Dienstleisters ergeben, was die Aufsichtsbehörde Berlin im Hinblick auf die Nutzung von Skype und die von Skype in der USA gespeicherten Kommunikationsdaten problematisiert. Bei der Nutzung von Skype werden Chat-Protokolle auf den Servern von Microsoft in den USA bis zu 90 Tage zwischengespeichert und damit für Microsoft der Zugriff auf die Kommunikationsnutzenderdaten eröffnet. Die Verarbeitung der Daten bedarf, da dieser Vorgang nicht zur Begründung des Beschäftigungsverhältnisses erforderlich ist, der Einwilligung. Jedenfalls ist die Nutzung von Skype aus Sicht des Bewerbers u.a. freiwillig, wenn er z.B. den digitalisierten Kontakt zur Ersparnis der persönlichen Anreise selber wünscht und auch die Verarbeitungen von Skype akzeptiert. Diese Freiwilligkeit kann aber auch – entgegen der Meinung der LfDI Berlin (Jahresbericht 2016, Ziff. 7.2) – bei dem betrieblichen oder behördlichen Gesprächspartner bestehen, wenn er in der Position ist, selbst über den Einsatz der Gesprächstechnik zu entscheiden.

3. Sprachaufzeichnung

Bereichsspezifischer Datenschutz gilt zudem für das Recht am eigenen Wort. § 201 StGB schützt dieses Recht auch vor Aufzeichnungen, bei denen nicht der aufgezeichnete Inhalt, sondern die Sprechweise und Stimme zur Ermittlung

von Persönlichkeitsmerkmalen untersucht werden sollen. Daher ist unabhängig von der datenschutzrechtlichen Regelung bereits nach § 201 Strafgesetzbuch die Aufzeichnung der Interviewgespräche ohne Einwilligung der Betroffenen regelmäßig unzulässig. Der Bewerber muss vor Durchführung des Interviews über die Aufzeichnung informiert sein. Auf die daneben ggf. erforderlichen Anforderungen einer datenschutzrechtlichen Einwilligung nach Art. 7 DS-GVO und § 26 Abs. 2 BDSG n.F. ist nachfolgend einzugehen.

III. Video-Live-Interview ohne Aufzeichnung

Eine Form des Videointerviews ist, dass das Gespräch mit dem Bewerber live erfolgt und Bild und Ton nicht aufgezeichnet werden. Gleichwohl muss auch diese Art der Erhebung der Daten dem Grundsatz der Erforderlichkeit genügen. Sie muss zunächst zur Erreichung des legitimen Zwecks geeignet sein. Sodann dürfen mildere, d.h. gleich geeignete, weniger eingriffsintensive Mittel nicht zur Verfügung stehen. Nicht erkennbar ist insoweit jedoch, dass vor Ort geführte „analoge“, frontal zu einem Auswahlgremium abverlangte persönliche Präsentationen ein milderes Mittel, also eine einen geringeren Eingriff in das Persönlichkeitsrecht des Bewerbers beinhaltende Datenerhebung sein soll als ein per Video als Momentaufnahme geführtes Interview. In beiden Fällen kann der Arbeitgeber sein Fragerecht ausüben und neben den mitgeteilten Informationen auch die Art von deren Wiedergabe, d.h. die Gestik, Mimik und das sonstige persönliche Verhalten des Bewerbers beobachten und bewerten.

Zu beachten ist auch, dass für den Arbeitgeber (vgl. ausführlich bei Dierks, DuD 2017, S. 752 ff) und auch für den Bewerber zwischen einem Vorstellungsgespräch und einem Videointerview für letzteres durchaus positive Unterschiede bestehen. Das mit Hilfe automatisierter Kommunikation geführte Gespräch ist somit bei einem dem Bewerber zuvor transparent gemachten Verfahren als zulässig anzusehen.

Einer Einwilligung bedarf es jedoch hinsichtlich des § 201 StGB. Sofern diese auch (so offenbar LfDI Berlin, Jahresbericht 2016, Ziff.) dem § 26 Abs. 2 BDSG n.F. genügen muss, so ist deren Freiwilligkeit nicht in Frage zu stellen, wenn der Bewerber neben der weiterhin bestehenden Möglichkeit eines nachfolgenden persönlichen Gesprächs das Videointerview selber wünscht bzw. akzeptiert.

IV. Zeitversetztes, automatisiert geführtes Interview mit Aufzeichnung

1. Das Verfahren

Eine anders gelagerte Problematik besteht jedoch bei automatisierten zeitversetzten Videointerviews (vgl. z.B. das Produkt <https://www.viasto.com>). In diesem Falle werden dem Bewerber automatisiert eingeblendete Fragen ohne die Beteiligung eines präsenten Gesprächspartners gestellt. Das

Programm ermöglicht es, diese Fragen nach den zuvor gegebenen Antworten zu strukturieren. Die nach einer Vorbereitungszeit gegebenen Antworten werden in Bild und Ton aufgezeichnet und können nicht korrigiert oder wiederholt werden.

In einem von der LDI NW bewerteten diesbezüglichen Verfahren einer Kommune sollte das Interview als dritter Schritt nach positiver Sichtung der Bewerbungsunterlagen und erfolgreichem Eignungstest obligatorisch vor der Entscheidung über die Einladung zu dem Vorstellungsgespräch stattfinden. Die Notwendigkeit des Interviewaufzeichnung wurde damit begründet, dass die hohe Bewerberzahl und die für die Auswahl verfügbare Zeit es nicht zuließen, alle nach schriftlicher Bewerbung und Eignungstest grundsätzlich geeigneten Bewerberinnen und Bewerber auch zu einem persönlichen Gespräch einzuladen. Mit dem Einsatz der Interview-Software könne die Anzahl der zu einem Auswahlgespräch einzuladenden Personen auf ein zu bewältigendes Maß begrenzt werden.

2. Manuelle Auswertung der Aufzeichnung

Die LDI NRW beurteilt das Verfahren als im Regelfall unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht der Bewerber, und zwar auch für den Fall, dass es nur in der Absicht der nicht automatisierten Auswertung der an sich zulässig gestellten Fragen erfolge. Im Wortlaut noch eindeutiger entscheidet die LfDI Berlin, nach der eine zeitversetzte Auswertung der Videointerviews für eine Bewerberauswahl „in keiner Hinsicht notwendig“ und damit rechtswidrig sei. Die LDI NW stellt darauf ab, dass im Unterschied zu flüchtigen, weil nicht reproduzierbaren Wahrnehmungen in einem herkömmlichen Vorstellungsgespräch die Aufzeichnung in Ton und Bild eine detaillierte und intensive Auswertung auch des nonverbalen Verhaltens (etwa Mimik, Gestik, Tonfall) ermögliche. Dies könne für die Auswahl für Berufe mit starkem Öffentlichkeitsbezug – etwa bei Fernsehsendern – erforderlich und daher ggf. zulässig sein; für künftige Beschäftigte in der Verwaltung jedoch nicht. Ob das so generell gilt, mag einmal dahinstehen. Mit anderen Worten: Auch wenn derartige intensivere „manuellen“ Auswertungen nicht vorgesehen sind, soll allein ihre Möglichkeit die Rechtswidrigkeit des Verfahrens begründen. Verwiesen wird auf den hier einschlägigen § 29 Abs. 1 DSGVO NRW, der verlangt, dass eine Aufzeichnung und Auswertung zur Eingehung eines Dienst- oder Arbeitsverhältnisses erforderlich sein muss, wobei das Prinzip für die öffentliche Verwaltung in stringenter Weise dahingehend ausgelegt wird, dass sie sich auf die Datenverarbeitungen und -erhebungen beschränken müsse, die für die rechtmäßige Aufgabenerledigung unerlässlich sind.

Ob diese Aussage der Unzulässigkeit einer Gesprächsaufzeichnung auch für den privaten Arbeitgeber gilt, erscheint jedenfalls dann fraglich, wenn im Rahmen der notwendigen Mitbestimmung (§ 87 Abs. 1 Nr. 6 BetrVG) nur definierte, d.h. arbeitsplatzbezogene, manuelle Auswertungen zugelassen sind (vgl. § 26 Abs. 1 S. 1 BDSG n.F.) und die Rege-

lung hinreichende Garantien für die Betroffenenrechte vorsieht.

Die von der LDI NW an Stelle des aufgezeichneten Interviews empfohlene Konkretisierung des Anforderungsprofils oder eine stellenspezifische Ausweitung kognitiver Eignungstests sind keine gleichwertigen mildereren Mittel, kommen aber als ebenfalls für die Entscheidung zur Einladung zum Vorstellungsgespräch mit entscheidende zulässige Maßnahmen auch unter den Anforderungen des künftig für private Arbeitgeber geltenden § 26 Abs. 1 S. 1 BDSG n.F. in Betracht. Die geforderte Erforderlichkeit rechtfertigt auch hier eine Digitalisierung der Verfahren, so dass z.B. die Angaben auf dem mit dem Anforderungsprofil abgestimmten elektronischen Fragebogen mit den Kriterien des Anforderungsprofils in einen Scoringverfahren abgeglichen werden können.

3. Sprachgebrauchsanalyse (Keywordspotting)

Wie aufgezeigt, kann die Aufzeichnung und ggf. auch deren automatisierte Auswertung arbeitsplatzbezogen zulässig sein. Ein Beispiel bilden die von der LfDI NW erwähnten Fernsehmoderatoren. Ein anderes Beispiel bilden zur Sprachgebrauchsanalyse verwendete Aufzeichnungen, wie sie u.a. zum Monitoring von sog. Call Center-Agenten Verwendung finden. Derartige Analysen sind auch bei einem Bewerbungsgespräch möglich. Ermittelt werden kann ähnlich dem sog. Keywordspotting, ob der Bewerber bestimmte Begriffe und Formulierungen verwendet oder vermeidet, d.h. ein zulässiges Kontrollziel kann in der Feststellung des für den Beruf erforderlichen „Sprachniveaus“ liegen. Gleiches gilt für benötigte, insbesondere fachspezifische Fremdsprachenkenntnisse.

4. Profiling per Sprachanalyse

Anders gelagert und gravierender ist der Eingriff in das Persönlichkeitsrecht des Bewerbers, wenn der Arbeitgeber oder ein damit beauftragter Dienstleister aus dem Inhalt und der Gestaltung des Gesprächs auch Erkenntnisse über Persönlichkeitsmerkmale des Bewerbers zu gewinnen versucht. Diesbezüglich bereits eingesetzte Analyseprogramme (<https://www.psyware.de>) basieren auf der Erkenntnis, dass sich unter Heranziehung linguistischer, psychologischer und kommunikationsbezogener Merkmale für jeden Menschen gewisse Verhaltensmuster identifizieren lassen, in denen bestimmte Persönlichkeitsmerkmale zum Ausdruck kommen (zur auf künstlicher Intelligenz basierter Verhaltensanalyse an Hand von Bild- und Tonaufnahmen vgl. bei Conrad, DuD 2017, S.740 (742)). So soll aus dem Gesprächsverhalten herausgelesen können, wie einsatzbereit, wie belastbar, wie kommunikativ, wie teamfähig, wie charismatisch zielorientiert, ausgeglichen und verantwortungsbereit ein Bewerber ist. Die Software analysiert nicht, was die Person sagt, sondern ausschließlich, wie sie es sagt: die Sprache und die Sprechweise – zum Beispiel die sprachliche Vielfalt, die Wortwahl, die Satzlängen, die Anzahl der Füllwörter und Pausen, aber auch die Sprachmelodie und stimmliche Eigen-

schaften wie Lautstärke und Monotonie sind die Grundlage der Bewertung (vgl. zu Verhaltensweisen bei Videointerviews; <http://www.focus.de/finanzen/partner/cv-coach/bewerbung-was-beim-video-interview-zu-beachten-ist>). Das individuelle Ergebnis wird verglichen mit einer Referenzdatei von Vergleichspersonen, wobei als Resultat eine Wahrscheinlichkeitsaussage über das Persönlichkeitsprofil des Bewerbers erstellt wird.

Die DS-GVO erfasst den Vorgang mit dem in Art. 4 Nr. 4 definierten Begriff des Profilings, das darin besteht, „bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“.

Zur Zulässigkeit eines solchen Profilings äußert sich die DS-GVO jedoch nicht speziell. Es ist einmal im Zusammenhang mit automatisierten Einzelentscheidungen gemäß Art. 22 DS-GVO und zum anderen im Rahmen der im Bewertungsverfahren benötigten Erforderlichkeitsaspekte (§ 26 Abs. 1 S. 1 BDSG n.F.) zu betrachten.

5. Automatisierte Einzelentscheidungen und Profiling

Nach Art. 22 Abs. 1 DS-GVO sind Entscheidungen mit rechtlichen Folgen oder erheblichen Beeinträchtigungen für die Betroffenen grundsätzlich unzulässig, soweit sie sich ausschließlich auf automatisierte Bewertungen von Persönlichkeitsmerkmalen stützen, ohne dass eine natürliche Person die entscheidungserheblichen Sachverhalte prüft und auf dieser Basis eigenständige Entscheidungen trifft. Daraus folgt zumindest, dass auch Bewerber mit ungünstiger Bewertung ggf. noch bei einem mündlichen Auswahlgespräch eine Chance auf eine positive Auswahlentscheidung haben müssen und dass die für die Personalauswahl Verantwortlichen sich über die Softwareentscheidung hinwegsetzen können. Um nicht schon bereits unter das Verbot automatisierter Einzelfallentscheidungen zu fallen, sind daher mindestens folgende Voraussetzungen bei der Auswertung von Videointerviews zu beachten (LDI NW, 23. Datenschutz- und Informationsfreiheitsbericht 2017, S. 62): Alle Bewerberinnen und Bewerber, deren Persönlichkeit mit der Software bewertet wurde, müssen zu einem Vorstellungsgespräch eingeladen werden, in dem trotz einer ungünstigen automatisierten Bewertung eine reale Chance auf eine positive Auswahlentscheidung besteht. Dafür benötigen die Personalverantwortlichen zum einen hinreichende Kenntnisse über die Funktionsweise des Verfahrens und zum anderen eine diesbezügliche Entscheidungskompetenz.

6. Erforderlichkeit nach § 26 Abs. 1 S. 1 BDSG n.F.

Zuvor stellt sich – abgesehen von der wissenschaftlich zu belegenden Treffsicherheit dieser Methode der Profilermittlung – jedoch die allgemeine Frage nach der datenschutzrechtlichen Zulässigkeit eines solchen Personalauswahlpro-

gramms. Den Bewerbern werden allein auf Grundlage der Sprachprobe charakterliche Eigenschaften und Kompetenzen zugewiesen oder abgesprochen, ohne dass sie durch eigene Leistungen und Darstellung ihrer Fähigkeiten einen Einfluss darauf haben. Es ist eindeutig, dass eine auf diesem Wege angestrebte Registrierung und Katalogisierung der individuellen Persönlichkeit mit der Menschenwürde und dem Schutz des Persönlichkeitsrechts auch bei „Wissenschaftlichkeit“ des Verfahrens nicht vereinbar sein kann. Die mit dieser Zielrichtung geführte automatisierte Verarbeitung von Gesprächsmerkmalen kann nicht als zur Begründung des Beschäftigungsverhältnisses erforderlich bewertet werden (§ 26 Abs. 1 S. 1 BDSG n.F.). Gravierend verletzt wird das den Erforderlichkeitsgrundsatz bestimmende Verhältnismäßigkeitsprinzip.

7. Gestattung der Gesprächsaufzeichnung und -auswertung per Einwilligung

Kommt man zu dem zutreffenden Ergebnis, dass § 26 Abs. 1 S. 1 BDSG n.F. bzw. die entsprechenden Normen für den öffentlichen Dienst nicht die Grundlage für die Sprachanalyse des aufgezeichneten Interviews geben, verbleibt die Frage, ob der Bewerber in eine ihm nach Art. 13 Abs. 1 DS-GVO offenzulegende Absicht der analytischen Verarbeitung der „Interviewdaten“ gestatten kann. Erste Voraussetzung wäre, dass die Betroffenen umfassend über die angestrebten Auswirkungen und die Tragweite des Verfahrens informiert werden und dass auch weitergehende Informationen, etwa zu den verwendeten Analyse-Algorithmen, bereitgestellt werden. Dass auch Einwilligungen nach dem neuen Datenschutzrecht im Beschäftigungsverhältnis zulässig bleiben, ist in § 26 Abs. 2 BDSG n.F. klargestellt, wobei die Vorgaben des Art. 7 DS-GVO für die Informiertheit und Freiwilligkeit der Erklärung für das Beschäftigungsverhältnis verdeutlicht werden (vgl. Erwägungsgrund 155). An der Freiwilligkeit fehlt es jedenfalls zunächst dann, wenn die Einladung zu dem persönlichen Vorstellungsgespräch von einem erfolgreichen Analyseergebnis abhängig gemacht wird. Eine freiwillige Teilnahme wäre daher nur gewährleistet, wenn die Bewerber auch bei einer verweigten Sprachanalyse ungeschmälertere Chancen auf die ausgeschriebene Stelle hätten (LDI NW, 23. Datenschutz- und Informationsfreiheitsbericht 2017, Ziff. S. 64)

Im öffentlichen Dienst ist ein unabdingbares zeitversetztes Videointerviewverfahren zudem auch nicht mit Art. 33 Abs. 2 Grundgesetz (GG) vereinbar, nach dem über Anträge auf Zugang zu öffentlichen Ämtern nur nach Maßgabe von Eignung, Befähigung und fachlicher Leistung entschieden werden darf. Würden Personen, die nach den vorliegenden Bewerbungsunterlagen zwar grundsätzlich geeignet sind, aber ihr Recht am eigenen Bild und am gesprochenen Wort nicht preisgeben und damit ihr Recht auf informationelle Selbstbestimmung geltend machen wollen, vom weiteren Bewerbungsverfahren ausgeschlossen, würde dies Art. 33 Abs. 2 GG zuwiderlaufen. Auch eine Einwilligung würde das rechtswidrige Verfahren nicht legitimieren.

Ferner sind bei in einem strukturierten Verfahren vorgegebenen Einwilligungen die in den §§ 307, 309 BGB vorgegebenen AGB-Anforderungen zu beachten, d.h. es ist zu fragen, ob der Bewerber nach Treu und Glauben unangemessen benachteiligt wird.

Für den Arbeitgeber stellt sich nämlich die grundsätzliche Frage, ob er die ihm im Hinblick auf die Wahrung des Persönlichkeitsrechts des Beschäftigten gezogenen Grenzen nicht durch die Einholung von Einwilligungen durchbrechen kann, um auf diesem Wege Informationen zu verarbeiten, die ihm nach dem für das Arbeitsrecht geltenden Grundsätzen unzugänglich sein sollen (Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn.). Die die Rechtsbeziehungen der Vertragsparteien gestaltenden Rücksichtnahmepflichten des § 241 BGB verlangen „dass in die Privatsphäre des Arbeitnehmers nicht tiefer eingegriffen werden darf, als es der Zweck des Arbeitsverhältnisses unbedingt erfordert“ (BAG, Beschl. v. 11.5.1986 – 1 ABP 12/84). Zur Sicherstellung

dieses Gebots und des dabei geltenden Verhältnismäßigkeitsprinzips hat der Gesetzgeber auch fallbezogene konkrete Verarbeitungsverbote aufgestellt. Krause (in BMAS-Forschungsbericht 482, Ziff. 3.2.6) verweist auf das generelle Verbot des § 19 GenDG, die Vornahme genetischer Untersuchungen oder Analysen zu verlangen. Die LDI NW zieht die Parallele zur Nicht-Anwendung von Lügendetektoren.

Ferner weist die LDI NW jedenfalls darauf hin, dass wie bei allen Wahrscheinlichkeitsaussagen treffsichere Feststellungen bestenfalls als Durchschnittswert für eine Gesamtgruppe, nicht aber für eine konkrete Person möglich sind. Der Einzelfall kann stets von der statistischen Regel abweichen. Der Betroffene müsse aber als individuelle Persönlichkeit und nicht als Mitglied einer statistischen Vergleichsgruppe wahrgenommen und beurteilt werden. Nicht das Einsortieren in Schubladen durch einen undurchschaubaren Algorithmus, sondern ihre tatsächlichen Fähigkeiten sollen ausschlaggebend für ihre Eignung und Befähigung sein.

Rechtsprechung

Zur Einwilligungserklärung in die Nutzung von Cookies (Ls)

(Bundesgerichtshof, Beschluss vom 5. Oktober 2017 – I ZR 7/16 –)

Dem Europäischen Gerichtshof werden folgende Fragen zur Vorabentscheidung vorgelegt:

1. a) Handelt es sich um eine wirksame Einwilligung im Sinne des Art. 5 Abs. 3 und des Art. 2 Buchst. f der Richtlinie 2002/58/EG in Verbindung mit Art. 2 Buchst. h der Richtlinie 95/46/EG, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers gespeichert sind, durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss?
- b) Macht es bei der Anwendung des Art. 5 Abs. 3 und des Art. 2 Buchst. f der Richtlinie 2002/58/EG in Verbindung mit Art. 2 Buchst. h der Richtlinie 95/46/EG einen Unterschied, ob es sich bei den gespeicherten oder abgerufenen Informationen um personenbezogene Daten handelt?
- c) Liegt unter den in Vorlagefrage 1. a) genannten Umständen eine wirksame Einwilligung im Sinne

des Art. 6 Abs. 1 Buchst. a der Verordnung (EU) 2016/679 vor?

2. Welche Informationen hat der Diensteanbieter im Rahmen der nach Art. 5 Abs. 3 der Richtlinie 2002/58/EG vorzunehmenden klaren und umfassenden Information dem Nutzer zu erteilen? Zählen hierzu auch die Funktionsdauer der Cookies und die Frage, ob Dritte auf die Cookies Zugriff erhalten?

Zum Auskunftsanspruch nach § 101 Abs. 2 S. 1 Nr. 3 UrhG gegen den Internet-Provider (Ls)

(Bundesgerichtshof, Urteil vom 21. September 2017 – I ZR 58/16 –)

- a) Begehrt der Rechtsinhaber, es dem Internet-Provider zu untersagen, diejenigen Daten zu löschen, die für die Erteilung der Auskunft gemäß § 101 Abs. 2 Satz 1 Nr. 3 UrhG über Name und Anschrift von Personen erforderlich sind, denen dynamische IP-Adressen zugeteilt waren, unter denen urheberrechtsverletzende Handlungen im Internet vorgenommen wurden, ist der

Rechtsweg zur streitigen ordentlichen Gerichtsbarkeit eröffnet. Dieses Begehren ist nicht nach den Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit geltend zu machen.

- b) Der Internet-Provider ist in Fällen offensichtlicher Rechtsverletzungen bis zum Abschluss des Gestattungsverfahrens nach § 101 Abs. 9 UrhG verpflichtet, die Löschung der von ihm nach § 96 Abs. 1 Satz 1 TKG erhobenen Verkehrsdaten zu unterlassen, die die Auskunftserteilung nach § 101 Abs. 2 Satz 1 Nr. 3 UrhG gegenüber dem Rechtsinhaber ermöglichen.

Influencer Marketing (Ls)

(Kammergericht Berlin, Beschluss vom 11. Oktober 2017 – 5 W 221/17 –)

Wer in seinem Instagram-Auftritt Modeartikel und Kosmetika präsentiert, hierbei „sprechende“ Links unmittelbar zu Internetauftritten der betreffenden Unternehmen setzt und dafür nach Lage der Dinge Entgelte oder sonstige Vorteile, wie z.B. Rabatte oder Zugaben erhält (wie etwa auch die kostenlose Überlassung der präsentierten Produkte), kann lauterkeitsrechtlich dazu verpflichtet sein, den kommerziellen Zweck in dem Auftritt ausreichend kenntlich zu machen (Anschluss OLG Celle WRP 2017, 1236).

Bußgeld wegen Dashcam-Aufzeichnungen zwecks Anzeige von Verkehrsordnungswidrigkeiten

(Oberlandesgericht Celle, Beschluss vom 4. Oktober 2017 – 3 Ss OWi 163/17 –)

Die Aufzeichnung mutmaßlich verkehrsordnungswidriger Verhaltensweisen Dritter im öffentlichen Straßenverkehr mittels einer sogenannten Dash-Cam (Onboard-Kamera) und die anschließende Übermittlung der dergestalt erhobenen Daten an die zuständige Bußgeldbehörde zwecks Ahndung ev. begangener Verkehrsordnungswidrigkeiten verstößt gegen § 1 Abs. 1 Bundesdatenschutzgesetz (BDSG) und stellt somit eine unzulässige Beeinträchtigung des Persönlichkeitsrechts der betroffenen Verkehrsteilnehmer dar. Derartige Handlungen werden vom personalen und sachlichen Anwendungsbereich der entsprechenden Schutzvorschriften des Bundesdatenschutzgesetzes, u.a. von § 1 Abs. 2 Nr. 3 BDSG, erfasst und durch § 43 Abs. 2 Nr. 1 BDSG als Ordnungswidrigkeit sanktioniert.

Aus den Gründen:

I. 1.) Das Amtsgericht Hannover hat den Betroffenen durch Urteil vom 10. April 2017 wegen fahrlässiger unbefugter Erhebung

und Verarbeitung nicht allgemein zugänglicher personenbezogener Daten zu einer Geldbuße von 250 € sowie zur Tragung der Kosten des Verfahrens verurteilt. Nachdem das Amtsgericht im Rahmen der Hauptverhandlung nach durchgeführter Beweisaufnahme von der Verfolgung fünf gleich gelagerter Tatvorwürfe abgesehen und das Verfahren insoweit gemäß § 47 Abs. 2 OWiG eingestellt hat, hat dieses lediglich noch einen Tatvorwurf zum Gegenstand. Zu diesem hat das Amtsgericht u.a. folgende Feststellungen getroffen:

Im Jahre 2004 hat der Betroffene damit begonnen, Verstöße gegen die Straßenverkehrsordnung zu dokumentieren und zur Anzeige zu bringen. Bis zum Zeitpunkt der Hauptverhandlung tat er dies in etwa 56.000 Fällen. Anlass hierfür war ursprünglich ein Gespräch mit dem Leiter der für die Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten zuständigen örtlichen Bußgeldbehörde. Dieser soll den Betroffenen zur Anzeigenerstattung ermuntert haben, nachdem der Betroffene jenem gegenüber seine Verwunderung darüber zum Ausdruck gebracht hatte, dass Verkehrsverstöße nicht konsequent geahndet würden. Als Beweismittel hat der Betroffene Fotografien oder Videoaufzeichnungen von den von ihm wahrgenommenen mutmaßlichen Verkehrsverstößen gefertigt und sich ergänzend als Zeuge zur Verfügung gestellt. Anfang des Jahres 2014 stattete der Betroffene sein Fahrzeug mit einer sogenannten „Onboard-Kamera“ bzw. „Dash-Cam“ aus, Mitte 2014 installierte er in seinem Wagen ein modifiziertes System mit zwei Kameras – eine vorne und eine hinten. Diese Kameras waren sowohl fernbedienbar als auch in der Lage, mittels eingebauter Infrarotsensoren Aufnahmen selbst in der Dunkelheit zu fertigen. Die Anlage ermöglichte zudem sowohl die Aufnahme von Einzelbildern als auch von Videos und war mit einem sogenannten Global Positioning System (GPS) ausgestattet, mit welchem satellitenbasiert u.a. die gefahrene Geschwindigkeit als auch der genaue Standort bestimmt werden konnte.

Die massenhafte Fertigung derartiger Videoaufzeichnungen von Verkehrsteilnehmern durch den Betroffenen aus Anlass der von den Verkehrsteilnehmern mutmaßlich begangenen Verkehrsverstöße gab dem durch die Bußgeldbehörde unterrichteten Landesbeauftragten für Datenschutz Niedersachsen Veranlassung, gegen den Betroffenen am 4. Juni 2014 einen Bußgeldbescheid wegen unbefugter Datenerhebung mittels Verwendung einer Onboard-Kamera im öffentlichen Straßenverkehr zu erlassen. Das Ordnungswidrigkeitenverfahren wurde indes im September 2014 durch das zuständige Gericht gemäß § 206a StPO eingestellt, weil der Bußgeldbescheid nicht den Anforderungen des § 66 OWiG entsprochen hatte. Der Landesbeauftragte für den Datenschutz Niedersachsen hat dieses Verfahren sodann nicht weiter betrieben, den Betroffenen indes mit Schreiben vom 29. Oktober 2014 unter Hinweis auf das Urteil des Verwaltungsgerichts Ansbach vom 12. August 2014 darauf hingewiesen, dass der Einsatz derartiger Onboard-Kameras in Form einer Videoüberwachung im Straßenverkehr unzulässig sei. Für den Fall der Wiederholung kündigte der Landesbeauftragte für den Datenschutz Niedersachsen die Einleitung eines neuen Bußgeldverfahrens an.

Gleichwohl setzte der Betroffene seine Tätigkeit fort und zeigte weitere von ihm mit seiner Onboard-Kamera dokumentierte mutmaßliche Verkehrsverstöße dem Landkreis O. als zuständiger Bußgeldbehörde an. Als Beweismittel übermittelte er dabei jeweils Digitalfotos bzw. Screenshots; wobei er letztere von den jeweiligen Videosequenzen gefertigt hatte. Auf diese Weise wurden dem Landkreis O. durch den Betroffenen am 1. November 2014 sieben, am 14. November 2014 neun, mit

Schreiben des Betroffenen vom 10. November 2014 eine, mit weiterem Schreiben vom 19. November 2014 fünf und mit Schreiben vom 26. November 2014 schließlich zehn Anzeigen mutmaßlicher Verkehrsverstöße übermittelt.

Mit Schreiben vom 1. Dezember 2014 wurde dem Betroffenen durch den abermals von der Bußgeldbehörde unterrichteten Landesbeauftragten für Datenschutz Niedersachsen die Einleitung eines aufsichtsbehördlichen Kontrollverfahrens gemäß § 38 BDSG mitgeteilt. Der Betroffene wurde zur Auskunftserteilung über die Erhebung, Speicherung und Löschung der mittels seiner Onboard-Kameras gefertigten Videoaufzeichnungen aufgefordert. Nachdem der Betroffene dieses Auskunftersuchen nur unzureichend beantwortet hatte, wurde ihm mit weiteren Schreiben vom 9. Januar 2015 durch den Landesbeauftragten für Datenschutz Niedersachsen eine letzte Frist gesetzt, zugleich wurde der Betroffene wiederum darauf hingewiesen, dass der Einsatz seiner Onboard-Kameras datenschutzwidrig sei.

Mit einer E-Mail vom 2. Mai 2016 zeigte der Betroffene dem Landkreis O. wiederum einen und mit einem Schreiben vom 22. Juni 2016 abermals einen mutmaßlichen Verstoß gegen Straßenverkehrsvorschriften an. Die E-Mail vom 2. Mai 2016 betraf den einzig noch verfahrensgegenständlichen Sachverhalt. Zusammen mit dieser E-Mail übermittelte der Betroffene drei Fotodateien von Screenshots, die ausweislich der darin enthaltenen und auf den papiernen Ausdrucken sichtbaren Daten betreffend Tag und Uhrzeit am 2. Mai 2016 um 15:09:42 Uhr gefertigt wurden und auf denen darüber hinaus neben diesem Zeitpunkt auch die GPS-Längen- und Breitengrade sichtbar sind. Das Amtsgericht nahm die von dem Betroffenen am 2. Mai 2016 übersandten und zwischenzeitlich ausgedruckten und zu den Akten genommenen Lichtbilder in Augenschein und wegen der darauf abgebildeten weiteren Einzelheiten gemäß § 267 Abs. 1 S. 3 StPO in Verbindung mit § 71 Abs. 1 OWiG auf die Lichtbilder Bezug.

Mit sofort vollziehbarem Verwaltungsakt vom 24. Juni 2016 untersagte der Landesbeauftragte für Datenschutz Niedersachsen dem Betroffenen die weitere Verwendung der Onboard-Kameras in der von diesem praktizierten Art und Weise und gab dem Betroffenen auf, die gespeicherten Daten der im öffentlichen Straßenverkehr gefertigten Videosequenzen bzw. Lichtbilder zu löschen. Zugleich verpflichtete er den Betroffenen, diese Löschung innerhalb von zwei Wochen nach Unanfechtbarkeit seiner Verfügung zu bestätigen. Der Betroffene erhob hiergegen Klage vor dem Verwaltungsgericht Göttingen und beantragte, die „Wiederherstellung der aufschiebenden Wirkung der Klage“. Mit Beschluss vom 12. Oktober 2016 lehnte das Verwaltungsgericht Göttingen dies ab.

Mit Schreiben seiner Verfahrensbevollmächtigten vom 8. November 2016 bestätigte der Betroffene die ordnungsgemäße Gestaltung der künftigen Verwendung seiner Onboard-Kameras sowie die Löschung der von ihm gespeicherten Dateien.

2.) Gegen das Urteil des Amtsgerichts Hannover vom 10. April 2017 hat der Betroffene form- und fristgerecht Rechtsbeschwerde eingelegt. Er begründet diese (zulässig allein) mit der Verletzung materiellen Rechts und vertritt u.a. die Auffassung, die Verwendung einer Onboard-Kamera auf dem Armaturenbrett sei im Gegensatz zu Blitzer- und Radarwarnern grundsätzlich mangels anderslautender Vorschriften oder Gesetze zulässig. Insbesondere werde der Sachverhalt nicht durch die Vorschriften des Bundesdatenschutzgesetzes (BDSG) erfasst. Die Nutzung von Onboard-Kameras zu familiären und persönlichen Zwecken sei zulässig. Sofern auf einem der drei von ihm am 2. Mai 2016 gefertigten Bilddateien das Kfz-Kennzeichen des von ihm

abgelichteten Mercedes-Cabriolet zu sehen sei, handele es sich nicht um personenbezogene Daten. Schließlich könne er sich auf § 6b Abs. 3 des BDSG berufen, welcher Videoaufzeichnungen der von ihm gefertigten Art gestatte.

3.) Die Generalstaatsanwaltschaft hat beantragt, den Antrag auf Zulassung der Rechtsbeschwerde als unbegründet zu verwerfen. Es sei offensichtlich nicht geboten, die Nachprüfung der Entscheidung zur Fortbildung des Rechts oder zur Sicherung einer einheitlichen Rechtsprechung zu ermöglichen oder das Urteil wegen Versagung des rechtlichen Gehörs aufzuheben. Die Feststellungen der angefochtenen Entscheidung hielten rechtlicher Überprüfung stand und würden eine Verurteilung wegen einer fahrlässig begangenen Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG tragen.

4.) Durch Beschluss des Senats ist die Rechtsbeschwerde zugelassen und das Verfahren gemäß § 80a Absatz 3 OWiG dem Bußgeldsenat in der Besetzung mit drei Richtern übertragen worden. Die Rechtsbeschwerde war gemäß § 80 Abs. 1 Nr. 1 OWiG zuzulassen. Es ist geboten, die Nachprüfung des Urteils zur Fortbildung des Rechts zu ermöglichen. Die Frage, ob Fälle der vorliegenden Art als Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch nicht-öffentliche Stellen unter Einsatz von Datenverarbeitungsanlagen zu nicht ausschließlich persönlichen oder familiären Tätigkeiten anzusehen sind und mithin von der entsprechenden Regelung des § 1 Abs. 2 Nr. 3 BDSG erfasst werden, wodurch dessen Anwendungsbereich eröffnet würde und sich in Konsequenz dessen eine solche Handlung als Verstoß gegen § 43 Abs. 2 Nr. 1 BDSG darstellen könnte, ist bislang weder durch die Bußgeldsenate des hiesigen Oberlandesgerichts noch – soweit erkennbar – durch die anderen Oberlandesgerichte entschieden worden.

II. Die Rechtsbeschwerde ist zulässig, indes unbegründet. Das Urteil des Amtsgerichts Hannover weist keinen durchgreifenden Rechtsfehler zum Nachteil des Betroffenen auf. Der Senat sah allein Veranlassung, den Schuldspruch abzuändern und auf eine vorsätzliche Tatbegehung zu erkennen.

1. Das Bundesdatenschutzgesetz dient gemäß § 1 Abs. 1 BDSG dem Zweck, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Der Umstand, dass der Betroffene am 2. Mai 2016 um 15:09:42 Uhr mit der im Heck seines Fahrzeuges montierten Onboard-Kamera den Fahrer eines Mercedes-Cabriolet und damit einen anderen Verkehrsteilnehmer dabei filmte, wie dieser im öffentlichen Straßenraum ein Fahrzeug führte und dabei zugleich möglicherweise sein Mobiltelefon nutzte, um diesen Sachverhalt sodann beim Landkreis O. als zuständiger Bußgeldbehörde unter Übermittlung dreier anhand der Videodatei gefertigter Screenshots anzuzeigen, stellt eine solch unzulässige Beeinträchtigung des Persönlichkeitsrechts dieses Verkehrsteilnehmers dar. Die Handlungen des Betroffenen werden mithin vom personalen und sachlichen Anwendungsbereich der entsprechenden Schutzvorschriften des Bundesdatenschutzgesetzes, nämlich von § 1 Abs. 2 Nr. 3 BDSG erfasst (nachfolgend a) und durch § 43 Abs. 2 Nr. 1 BDSG als Ordnungswidrigkeit sanktioniert (nachfolgend b).

a) Gemäß § 1 Abs. 2 Nr. 3 findet das BDSG auch für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen Anwendung, soweit diese Stellen die Daten unter Einsatz von Datenverarbeitungsanlagen erheben und die Tätigkeit nicht ausschließlich für persönliche oder familiäre Zwecke erfolgt.

aa) Der Betroffene ist gemäß der Legaldefinition in § 2 Abs. 4 S. 1 BDSG als natürliche Person eine solch nicht-öffentli-

che Stelle im Sinne des § 1 Abs. 2 Nr. 3 BGSg. Der Begriff „nicht-öffentlichen Stelle“ ist als Komplementärbegriff zu dem der öffentlichen Stelle zu verstehen und erfasst alle natürlichen Personen, die juristischen Personen des Privatrechts sowie Personenvereinigungen (vgl. BeckOK-DatenSR/Hanloser BDSg, 21. Edition § 2 Rn. 46). Als solche natürliche Person unterfällt der Betroffene schließlich auch nicht der Ausnahmeregelung des § 2 Abs. 4 S. 1 HS. 2 BGSg, wonach natürliche Personen dann als öffentliche Stellen anzusehen sind, wenn sie Aufgaben der öffentlichen Verwaltung wahrnehmen. Gemäß § 35 OWiG obliegt die Verfolgung und Ahndung von Ordnungswidrigkeiten der Verwaltungsbehörde. Die Feststellung und Ahndung von Ordnungswidrigkeiten ist eine typisch hoheitliche Aufgabe aus dem Kernbereich staatlichen Handelns, weshalb eine Mitwirkung von Privatpersonen grundsätzlich nicht möglich ist. Die Übertragung derartiger Verfolgungsaufgaben auf Dritte würde deren Beleihung bzw. eine hierfür erforderliche gesetzliche Ermächtigung voraussetzen, die es indes im Bereich des Gesetzes über Ordnungswidrigkeiten nicht gibt (vgl. KK-OWiG/Lampe, 4. Aufl. § 35 Rn. 6). Der Betroffene nahm durch seine Anzeigetätigkeit indes keine Aufgabe der öffentlichen Verwaltung wahr. Die von ihm exzessiv ausgeübte Anzeigetätigkeit bezüglich der von ihm wahrgenommen und als Ordnungswidrigkeiten bewerteten Sachverhalte erfolgte einzig und allein aus persönlichem bzw. privatem Antrieb. Der objektiv-rechtlichen Verpflichtung der Bußgeldbehörde, bei Eingang einer Anzeige tätig zu werden und zu prüfen, ob eine Ordnungswidrigkeit vorliegt und ob sie diese entsprechend den Opportunitätsprinzip verfolgt, korrespondiert auch kein subjektives Recht des Betroffenen auf ein entsprechendes Tätigwerden (grds. hierzu OVG Lüneburg v. 23.09.2013 – 13 LA 144712; NJW 2013, 3595). Das Ordnungswidrigkeitenrecht kennt anders als das Strafverfahren keine subjektiven Rechtspositionen von Anzeigerstattem auf Durchführung eines Verfahrens bzw. auf Ahndung eventuell festgestellter Verkehrsverstöße. Es enthält insbesondere keine dem Klageerzwingungsverfahren der §§ 172 ff. StPO vergleichbare Regelungen.

bb) Durch die Aufnahme des Videos am 2. Mai 2016 von dem betroffenen Mercedes Cabriolet-Fahrer und die anschließende Fertigung dreier Screenshots/Lichtbilder erhob und verarbeitete der Betroffene personenbezogene Daten. Gemäß § 3 Abs. 1 BDSg sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person. Bestimmbar in diesem Sinne ist eine natürliche Person, wenn grundsätzlich die auch nur abstrakte Möglichkeit besteht, ihre Identität festzustellen (BeckOK-DatenSR/Schild aaO § 3 Rn. 17). Anders formuliert hängt die Grenze zwischen Bestimmbarkeit und Nichtbestimmbarkeit davon ab, ob die Bestimmbarkeit absolut oder nur praktisch ausgeschlossen ist. Praktisch ausgeschlossen ist die Bestimmbarkeit, wenn die Wahrscheinlichkeit einer erfolgreichen Bestimmung so gering ist, dass das Risiko praktisch vernachlässigt werden kann (so Simitis/Dammann, Bundesdatenschutzgesetz, 8. Aufl., § 3 Rn. 23). Durch die wirksame Bezugnahme des Amtsgerichts gemäß §§ 267 Abs. 1 S. 3 StPO iVm § 71 Abs. 1 OWiG auf diese drei Lichtbilder (vgl. zur Zulässigkeit der Bezugnahme auf Ausdrucke von Videodateien BeckOK-StPO/Peglau, 27. Edition, § 267 Rn. 5; OLG Zweibrücken v. 20.11.2001 – 1 Ss 242/01, VRS 102 (103)), wurden diese Abbildungen als Ganzes Bestandteil der Urteilsgründe und können durch den Senat aus eigener Anschauung gewürdigt werden. Diese bilden jeweils dieselbe Situation ab, nämlich ein Mercedes Cabriolet der E-Klasse mit offenem Verdeck, dessen Fahrer mit seiner rechten

Hand einen Gegenstand, bei dem es sich um ein Mobiltelefon handeln könnte, an sein rechtes Ohr hält. Das amtliche Kennzeichen des Fahrzeuges ist deutlich und vollständig ablesbar. Mittels seines Autokennzeichens (ebenso BeckOK-DatenSR/Schild aaO Rn. 19) ist jeder Kraftfahrer und hier konkret die auf dem Video bzw. die auf dem davon gefertigten Lichtbild abgebildete Person zweifelsfrei bestimmbar. Es ist naheliegend, dass es sich bei dem Fahrer um den über die Zulassungsstelle identifizierbaren Halter des Mercedes Cabriolet handelt bzw. der Fahrer jedenfalls über den Halter namhaft gemacht werden könnte.

Die von dem Betroffenen erhobenen Daten enthalten schließlich auch Einzelangaben über persönliche oder sachliche Verhältnisse dieser Person. In diesem Sinne sind Einzelangaben solche Informationen, die sich auf die persönlichen Verhältnisse wie Name, Anschrift, Familienstand, Beruf etc. oder – wie hier – auf sachliche Verhältnisse, mithin auf einen auf eine bestimmte Person beziehbaren Sachverhalt wie etwa das Führen eines Telefongesprächs (vgl. Erfurter Kommentar Arbeitsrecht/Franzen, 17. Aufl. § 3 BDSg Rn. 2) beziehen. Die von dem Betroffenen erhobenen Daten ermöglichen eine solche Feststellung, nämlich dass eine bestimmte und bestimmbar Person am 2. Mai 2016 um 15:09 Uhr an einem mittels der GPS-Daten konkret bestimmbar Ort und an einer mittels des Lichtbildes sodann exakt bestimmbar Stelle auf der Straße nicht nur – augenfällig – mutmaßlich ein Mobiltelefon an ihr Ohr gehalten und dieses damit genutzt hat, sondern zugleich mit seinem Mercedes Cabriolet im öffentlichen Straßenverkehr fuhr.

Indem der Betroffene diese Person beim Führen ihres PKWs unter gleichzeitigem mutmaßlichen Telefonieren anlässlich deren mutmaßlichen Verstoßes gegen § 23 Abs. 1a StVO zielgerichtet mit seiner Videokamera gefilmt hat, erhob er zugleich deren personenbezogene Daten im Sinne von § 3 Abs. 3 BDSg. Diese Vorschrift definiert die Erhebung von Daten als das Beschaffen von Daten über den Betroffenen, mithin als jede Form gezielt betriebener Gewinnung personenbezogener Daten, sei dies unter Mitwirkung des Betroffenen, der Behörden oder privater Dritter (BeckOK-DatenSR/Schild § 3 Rn. 51). Hierunter fällt insbesondere die zweckgerichtete Beobachtung mittels Videoüberwachung (BeckOK-DatenSR/Schild aaO).

cc) Der Betroffene erhob diese personenbezogenen Daten schließlich auch unter Einsatz einer Datenverarbeitungsanlage im Sinne des § 1 Abs. 2 Nr. 3 BDSg. Der Begriff „unter Einsatz von Datenverarbeitungsanlagen“ ist dabei weit auszulegen (BeckOK-DatenSR/Gusy aaO § 1 Rn. 74; Simitis, Bundesdatenschutzgesetz, aaO, § 1 Rn. 140) und hat sich an § 3 Abs. 2 S. 1 BDSg zu orientieren (BeckOK-DatenSR/Gusy aaO § 1 Rn. 74; Simitis, Bundesdatenschutzgesetz, aaO § 1 Rn. 140; OVG Berlin-Brandenburg v. 06.04.2017 – OVG 12 B 7.16, juris), der die automatisierte Verarbeitung als „Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen“ legaldefiniert. Es kommt somit „nur und ausschließlich“ darauf an, ob die Daten automatisiert erhoben, verarbeitet oder genutzt (BT-Drs. 14/4329, S. 32) werden. Die automatisierte Verarbeitung mit Datenverarbeitungsanlagen umfasst dabei die Gesamtheit aller automatisierten Verarbeitungsschritte (OVG Berlin-Brandenburg, aaO unter Verweis auf BeckOK-DatenSR/Schild aaO § 3 Rn. 33). Der Begriff der automatisierten Verarbeitung ist angesichts der heutigen Vielfalt der technischen Geräte und ihrer jeweiligen Datenverarbeitungsprogramme außerordentlich vielfältig. Die verschiedenen von § 1 Abs. 2 Nr. 3 BGSg erfassten Formen des Datenumgangs müssen entweder „unter Einsatz von Datenverarbeitungsanlagen“ erfolgen oder aber „dafür erheben“, sprich dafür erhoben

werden, weshalb es bei der Erhebung entscheidend darauf ankommt, dass die Daten „dafür“, also für eine spätere automatische Nutzung oder Verarbeitung, erhoben werden. Die Erhebung selbst muss noch nicht automatisch erfolgen. Die Fixierung personenbezogener Daten auf Papier unterfällt mithin bereits dem BDSG, sofern die Daten nur für eine spätere automatische Verarbeitung erhoben werden. Gleichgültig ist weiter, ob es tatsächlich zu der beabsichtigten automatisierten Verarbeitung kommt. Entscheidend ist vielmehr der objektiv zu beurteilende, im Zeitpunkt der Erhebung bestehende Zweck einer späteren automatisierten Verarbeitung. Die Gesetzesanwendung steht also nicht etwa unter dem Vorbehalt, dass es später tatsächlich zu einer automatischen Verarbeitung oder Nutzung der Daten kommt, noch entfällt sie rückwirkend, wenn der Verarbeitungszweck endgültig entfällt, etwa weil eine nur manuelle Verarbeitung beschlossen wurde oder die Daten (genutzt oder ungenutzt) vernichtet oder vergessen wurden (so zutreffend Simitis, Bundesdatenschutzgesetz, aaO; im Ergebnis ebenso Erbs/Kohlhaas, Strafrechtliche Nebengesetze – BDSG/AmbS, Stand Mai 2017, § 3 Rn. 8 ff.).

Dies bedenkend, kann es vorliegend dahingestellt bleiben, ob sich aus dem Gesamtzusammenhang der Urteilsgründe noch ergibt, dass der Betroffene auch die Videosequenz am 2. Mai 2016 im Wissen darum erstellte bzw. die entsprechenden personenbezogenen Daten „dafür erhob“, dass die von ihm sodann der Bußgeldbehörde übersandten Daten dort „unter Einsatz von Datenverarbeitungsanlagen verarbeitet“ werden würden. So teilen die Urteilsgründe u.a. mit, dass der Betroffene bis zum Zeitpunkt der Hauptverhandlung vor dem Amtsgericht Hannover bereits in circa 56.000 Fällen mutmaßliche Verstöße gegen die StVO dokumentierte und zur Anzeige brachte und der Landesbeauftragte für den Datenschutz Niedersachsen dem Betroffenen bereits mit Schreiben vom 1. Dezember 2014 mitgeteilt hatte, dass gegen diesen (deshalb) ein aufsichtsbehördliches Kontrollverfahren gemäß § 38 BDSG eingeleitet worden und dem Betroffenen mit Verwaltungsakt vom 24. Juni 2016 als Maßnahme zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten gemäß § 38 Abs. 5 S. 1 BDSG aufgegeben worden war, seine Onboard-Kamera in der bisherigen Weise nicht mehr weiter zu betreiben und die von ihm erhobenen Videosequenzen zu löschen.

Mit der Erstellung des Videos am 2. Mai 2016 mittels seiner Onboard-Kamera und der anschließenden Fertigung von „drei Fotos/Screenshots Bl. 15–17 der Akte, laut Datumstempel sämtlich gefertigt an 02.05.2016“ (S. 5 UA), führte der Betroffene selbst bereits eine Datenverarbeitung und Nutzung „unter Einsatz von Datenverarbeitungsanlagen“ im Sinne von § 1 Abs. 2 Nr. 3 BDSG durch. Ungeachtet der Tatsache, dass Rechtsprechung und Kommentarliteratur bereits den bloßen Einsatz von digitalerameratechnik ohne weitergehende Differenzierung unter den Begriff „unter Einsatz von Datenverarbeitungsanlagen“ im Sinne von § 1 Abs. 2 Nr. 3 BDSG subsumieren (vgl. u.a. VG Saarlouis v. 18.05.2016 – 1 K 2102/14, BeckRS 2016, 47657; VG Göttingen v. 12.10.2016 – 1 B 171/16, NJW 2017, 1336; OVG Berlin-Brandenburg v. 06.04.2017 – OVG 12 B 7.16, juris) lässt sich den Feststellungen des angefochtenen Urteils der Einsatz einer Datenverarbeitungsanlage bzw. eine automatisierte Datenverarbeitung konkret entnehmen. So hat nach den weiteren Feststellungen des Amtsgerichts die Inaugenscheinnahme der Lichtbilder zum Tatgeschehen u.a. ergeben, dass auf diesen neben dem Kfz-Kennzeichen auch die GPS-Standortdaten abge-

bildet sind, und hat die Mitarbeiterin des Landesbeauftragten für den Datenschutz Niedersachsen, die Zeugin H., bekundet, der Betroffene habe auch in den weiteren von ihm zur Anzeige gebrachten (und nicht mehr verfahrensgegenständlichen) Fällen vom 31. Oktober 2016, 4., 10. und 26. November 2014 sowie vom 22. Juni 2016 jeweils die GPS-Standortdaten übermittelt. Da das Amtsgericht wegen der weiteren Einzelheiten der drei bildlichen Darstellungen wirksam auf die drei Lichtbilder vom 2. Mai 2016 Bezug genommen hat, vermag der Senat aus eigener Anschauung festzustellen, dass auf den Lichtbildern „49 km/h“ sowie GPS-Standortdaten angegeben sind. Der Betroffene hat mithin eine Videokamera mit GPS-Funktion bzw. GPS-Empfänger verwendet, die nicht nur die jeweilige Position des Betroffenen, sondern auch die von diesem selbst gefahrene Geschwindigkeit anzeigt. Neben diesen in der Urteilsurkunde unmittelbar bzw. durch Bezugnahmen dargelegten tatsächlichen Feststellungen des Amtsgerichts kann der Senat auch auf allgemeinkundige Tatsachen zurückgreifen, um als Rechtsbeschwerdegericht Lücken in den Urteilsfeststellungen zu schließen (vgl. Meyer-Goßner/Schmitt StPO 60. Aufl., § 337 Rn. 25; KG v. 22.07.2009 – (4) 1 Ss 181/09 (130/09), BeckRS 2009, 25371). Dies hat der Senat getan und als allgemein- und damit offenkundige Tatsachen weiter berücksichtigt, dass unbeachtet möglicher weiterer automatisierter Datenverarbeitungsvorgänge bereits die Einblendung derartiger GPS-Standortdaten und Geschwindigkeitsangaben in elektronische Bilddateien – deren Ausdrücke in Form dreier Lichtbilder bezüglich der von der Videosequenz gefertigten Screenshots hinsichtlich des Vorfalls vom 2. Mai 2016 dem Amtsgericht vorlagen – durch einen automatisierten Datenverarbeitungsprozess der betreffenden personenbezogenen Daten erfolgte. Die mittels GPS ermittelten Daten wie Position und Geschwindigkeit werden im Rahmen der digitalen Videografie im Rahmen eines automatisierten Datenverarbeitungsprozesses ebenso wie das Aufnahmedatum nach Tag, Monat und Jahr bzw. die Aufnahmezeit nach Stunde, Minute und Sekunde wie andere, kameraspezifische Daten wie etwa Blende und Verschlusszeit in die jeweiligen Bilddateien integriert und zusammen mit diesen abgespeichert (Wikipedia). Dieser automatisierte Datenverarbeitungsvorgang ermöglichte es dem Betroffenen, was die weiteren tatrichterlichen Feststellungen belegen, in jede einzelne der drei nachträglich von der Videosequenz gefertigten Kopien der Bilddateien, den Screenshots, die er als Anlage mittels E-Mail der Bußgeldbehörde übersandte hatte und die dem Amtsgericht in Form von papiernen Lichtbildern vorlagen, u.a. die geografische Position seines Fahrzeuges nebst Uhrzeit und Geschwindigkeit derart einzublenden, dass diese wie die eigentliche bildliche Darstellung selbst bei deren Betrachtung offen zu sehen sind und damit zugleich auch belegen, zu welcher Zeit sich der abgelichtete Mercedes Cabriolet-Fahrer an diesem Ort befand. Ob der Betroffene die Datenverarbeitungssoftware seiner Videokamera dabei so programmiert hatte, dass die Positionsdaten nebst Geschwindigkeit bereits offen ablesbar in das Video einblendet wurden, oder ob er diese Daten erst bei Erstellung der Screenshots in diese einblendete und abgespeichert hat, geht aus den tatrichterlichen Feststellungen nicht hervor, ist indes für die Entscheidung auch tatsächlich wie rechtlich ohne Bedeutung.

dd) Die Erhebung der Daten erfolgte schließlich auch nicht ausschließlich für persönliche oder familiäre Tätigkeiten. In rechtsbeschwerderechtlich nicht zu beanstandender Weise hat das Amtsgericht auf der Grundlage der von ihm getroffenen

Feststellungen, wonach der Betroffene bis zum Zeitpunkt der Hauptverhandlung in ca. 56.000 Fällen Verstöße Dritter gegen die Straßenverkehrsordnung dokumentiert und angezeigt und auch den verfahrensgegenständlichen Fall mit einer E-Mail am 2. Mai 2016 beim Landkreis O. als zuständiger Bußgeldbehörde zur Anzeige gebracht hat, die Einlassung des Betroffenen, der Einsatz der Onboard-Kamera habe auch an diesem Tage zunächst allein der Aufzeichnung von Fahrstrecken für spätere Motorradfahrten bzw. zur Abschreckung und zum Schutz vor möglichen Beschädigungen seines Fahrzeuges gedient, als Schutzbehauptung bewertet. Es ist zu der sich hier förmlich aufdrängenden Überzeugung gelangt, die verfahrensgegenständliche Videoaufnahme bzw. die davon gefertigten Screenshots hätten einzig dem Zweck gedient, „Verkehrsverstöße im Bild oder im Video festzuhalten und nach anschließender Auswertung die Videos bzw. die aus Videosequenzen stammenden Einzelbilder zwecks Erstattung von Ordnungswidrigkeiten als Beweismittel vorzuhalten bzw. den Ordnungsämtern zur Verfügung zu stellen“.

Als Ausnahmeregelung ist § 1 Abs. 2 Nr. 3 BDSG ebenso wie die insoweit inhaltsgleiche Regelung in § 27 Abs. 1 S. 2 BDSG restriktiv auszulegen (Simitis, Bundesdatenschutzgesetz, aaO § 1 Rn. 148). Mit der Wendung „für persönliche oder familiäre Tätigkeiten“ grenzt das Gesetz einen Bereich persönlicher Lebensführung ab von der beruflichen oder geschäftlichen Sphäre. Entscheidend ist mithin, dass der Datenumgang im privaten Aktionskreis stattfindet und mit all seinen Bestandteilen und während der gesamten Dauer ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Die Frage, was dabei als persönlich oder familiär einerseits oder als beruflich bzw. geschäftlich andererseits anzusehen ist, richtet sich nach der Verkehrsanschauung (vgl. Simitis, Bundesdatenschutzgesetz, aaO Rn. 150, 151). Vorliegend nutzte der Betroffene die Onboard-Kamera ausschließlich, um Verkehrsordnungswidrigkeiten anderer Verkehrsteilnehmer und damit das Verhalten Dritter zu dokumentieren. Schon der dadurch betroffene Personenkreis spiegelt keinerlei persönlichen oder familiären Bezug wider. Die Erhebung dieser personenbezogenen Daten erfolgte zudem ausschließlich zu dem Zweck, sich Beweismittel für mögliche Bußgeld- oder Strafverfahren zu beschaffen und die Aufnahmen bei den für die Ahndung derartige Verstöße zuständigen Behörde vorzulegen. Werden personenbezogene Daten zu einem solchen Zweck erhoben, wird dadurch der persönliche bzw. familiäre Bereich evident verlassen (ebenso VG Göttingen a.a.O., Rn. 29; VG Ansbach, Urteil vom 12.08.2014 – AN 4 K 13.01634, Rn. 44, juris).

b) Der Betroffene hat die personenbezogenen Daten, die nicht allgemein zugänglich waren, auch unbefugt im Sinne von § 43 Abs. 2 Nr. 1 BDSG erhoben bzw. verarbeitet.

aa) Die von dem Betroffenen erhobenen personenbezogenen Daten enthielten nicht allgemein zugängliche Informationen über die abgebildete, mithin eine andere Person. Der Begriff „allgemein zugänglich“ bezieht sich weniger auf das personenbezogene Datum selbst, als auf die durch diese dargestellte Information über die betroffene Person (vgl. Simitis/Eugen/Ehmann, Bundesdatenschutzgesetz, 8. Aufl., § 43 Rn. 54). Nicht allgemein zugänglich ist eine Information immer dann, wenn sie nicht aus allgemein zugänglichen Quellen entnommen werden kann (vgl. BeckOK-Wolff/Brink, Datenschutzrecht, § 28 Rn. 78). Im Übrigen kommt es weder auf den Inhalt noch auf die Aktualität der Angaben noch auf das Schutzbedürfnis der betroffenen Person an.

Die Information, dass die von dem Betroffenen am 2. Mai 2016 um 15:09:42 Uhr an einem bestimmten, durch die GPS-Daten genau bestimmbar Ort aufgenommene Person ein Mercedes-Benz Cabriolet auf öffentlichen Straßen steuerte und dabei mit der rechten Hand ein Gegenstand, mutmaßlich ein Mobiltelefon, ans rechte Ohr hielt, kann nicht aus allgemein zugänglichen Quellen entnommen werden.

bb) Der Betroffene erhob diese Daten auch unbefugt. Er verstieß gegen § 4 Abs. 1 BDSG, wonach die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig ist, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet bzw. der Betroffene in die Erhebung der Daten eingewilligt hat. Hier lag weder eine Einwilligung der abgebildeten Person vor, noch ergibt sich die Zulässigkeit der Datenerhebung aus dem Gesetz.

Die durch den Betroffenen durchgeführte Beobachtung kann insbesondere auch nicht auf die Vorschrift des § 6b BDSG gestützt werden, die als *lex specialis* für die hier zu beurteilende Videoüberwachung öffentlich zugänglicher Räume eine abschließende Regelung enthält und als solche auch den allgemeineren Vorschriften der §§ 28 ff. BDSG vorgeht (vgl. OVG Lüneburg v. 29.09.2014 – 11 LC 114/13, Rn. 39 juris). Nach dieser Vorschrift ist die Beobachtung öffentlich zugänglicher Räume mittels optisch-elektronischer Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der von der Datenerhebung Betroffenen überwiegen.

Die von dem Betroffenen am 2. Mai 2016 durchgeführte Videoaufnahme mittels der von ihm verwendeten Onboard-Kamera stellt sich als Beobachtung öffentlich zugänglicher Räume mit einer optisch-elektronischen Einrichtung im Sinne des § 6b Abs. 1 BDSG dar.

aaa) Der Betroffene hat öffentlich zugängliche Räume im Sinne von § 6b Abs. 1 BDSG überwacht. Hierunter fallen alle allgemein zugänglichen Bereiche innerhalb wie außerhalb von Gebäuden, die von einem unbestimmten bzw. nur nach allgemeinen Merkmalen abgrenzbaren Personenkreis betreten bzw. benutzt werden können und ihrem Zweck nach auch hierzu bestimmt sind. Hierzu zählen insbesondere Geschäfte, Kaufhäuser, Einkaufspassagen, Bahnhofshallen, Parks, Wege und – wie hier – öffentliche Straßen (Erfurter Kommentar Arbeitsrecht/Franzen aaO § 6b Rn. 3, VG Göttingen v. 31.05.2017 1 A 170/16, Rn. 34).

bbb) Der Betroffene verwendete hierzu optisch-elektronische Einrichtungen im Sinne von § 6b Abs. 1 BDSG. Mit dem unspezifischen Begriff der Einrichtung hat der Gesetzgeber bewusst keine Festlegung im Hinblick auf Größe, Funktionalität oder örtliche Gebundenheit getroffen, sondern vielmehr eine technikneutrale Formulierung gewählt, die Geräte jeglicher Art und Gestaltung erfasst, sofern diese nur zur Beobachtung geeignet sind. Einrichtungen in diesem Sinne erfassen daher sowohl stationäre wie mobile Geräte. Eine Festlegung auf stationäre Einrichtungen ergibt sich weder aus dem Gesetzeswortlaut noch aus den Materialien (vgl. Simitis/Philip/Scholz, Bundesdatenschutzgesetz, aaO, § 6b Rn. 37; VG Göttingen vom 31.05.2017, aaO. Rn. 34 mit Verweis auf Becker, in: Plath, BDSG/DS-GVO, 2. Aufl. 2016, § 6b Rn. 1; Bergmann/Möhrle/Herb, Datenschutzrecht, Loseblattsammlung, Stand September 2016, § 3 Rn. 62 ff.). Da der Betroffene die entsprechenden Dateien zudem ab-

gespeichert hat, kommt es auf den Streit, ob unter optisch-elektronische Einrichtungen im Sinne von § 6b Abs. 1 BDSG auch bloße Kamera-Monitor-Systeme als gleichsam „verlängertes Auge“ ohne nachfolgende Aufzeichnung und Auswertung fallen, nicht an (so zutreffend bereits VG Göttingen v. 31.05.2017, aaO Rn. 35).

ccc) Das Filmen des Fahrers des Mercedes-Cabriolets am 2. Mai 2016 stellt sich schließlich auch als Beobachtung dar. Unter Beobachtung ist die Sichtbarmachung von Geschehnissen und Personen mithilfe dazu geeigneter technischer Einrichtungen zu verstehen. Sie kann durch aktives und gezieltes Handeln aber auch aus einer abwartenden, passiven Handlung heraus erfolgen (Simitis/Philip/Scholz, Bundesdatenschutzgesetz aaO, § 6b Rn. 63). Der Betroffene hat den Mercedes-Fahrer während dessen Fahrt und während dessen mutmaßlicher verkehrsordnungswidriger Telefonie durch gezieltes Handeln mittels seiner Onboard-Kamera aufgenommen und dadurch sowohl eine Person als auch ein Geschehnis sichtbar gemacht.

ddd) Der Betroffene war zu dieser Beobachtung auch nicht berechtigt. Er führte diese weder zur Wahrnehmung eines etwaigen Hausrechts (§ 6b Abs. 1 Satz 1 Nr. 2 BDSG) bzw. zur Aufgabenerfüllung öffentlicher Stellen (§ 6b Abs. 1 Satz 1 Nr. 1 BDSG) durch – er handelte vielmehr als natürliche Person (vgl. oben a) aa)) –, noch diente die Beobachtung zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Satz 1 Nr. 3 BDSG).

Der Zweck der Wahrnehmung berechtigter Interessen kommt nur als Ermächtigung für – wie hier – nicht öffentliche Stellen in Betracht (vgl. BT-Drs. 14/5793 S. 61) und ist in Anbetracht der Tatsache, dass eine Datenerhebung aufgrund des in § 4 Abs. 1 Satz 1 BDSG enthaltenen Gesetzesvorbehalts grundsätzlich verboten ist, sofern sie nicht ausnahmsweise erlaubt ist, restriktiv auszulegen (so auch BeckOK DatenSR /Wolf/Brink, aaO § 6b Rn. 47). Als berechtigt im Sinne von § 6b Abs. 1 Satz 1 Nr. 3 BDSG gilt nicht nur ein rechtliches, sondern jedes tatsächliche Interesse etwa wirtschaftlicher, aber auch ideeller Natur. Berechtigt ist insbesondere das Interesse an der Abwehr drohender Gefahren und die Dokumentation der Verletzung eigener Rechte etwa durch Vandalismus oder Eigentumsdelikte (Simitis/Philip/Scholz, Bundesdatenschutzgesetz, aaO § 6b Rn. 77 ff.). Neben der Abschreckung möglicher Straftäter kommt daher auch die Sicherung von Beweismaterial für den Fall einer versuchten oder vollendeten Straftat zulasten der Verantwortlichen, d.h. der die Daten erhebenden Stelle, als berechtigtes Interesse in Betracht. Das Interesse an der Verfolgung von Straftaten oder, wie hier, von Ordnungswidrigkeiten ist ein rein staatliches. Es kann allenfalls mittelbar, etwa hinsichtlich zivilrechtlicher Ersatzansprüche, auch ein berechtigtes privates Interesse sein (vgl. BeckOK DatenSR/Wolf/Brink, aaO Rn. 48). Entsprechendes gilt für das Interesse an der Abwehr drohender Gefahren bzgl. möglicher Beschädigungen von Hausfassaden bzw. von Geschäfts- und Wohnhäusern im Rahmen von Veranstaltungen (vgl. AG Berlin-Mitte v. 18.12.2003 – 16 C 427/02, NJW-RR 2004, 531, 532) bzw. von sonstigen Gegenständen wie etwa PKWs oder Geldausgabeautomaten (bzgl. letzterer vgl. Simitis/Philip/Scholz, Bundesdatenschutzgesetz, aaO Rn. 79). Voraussetzung für die Annahme einer solchen Gefahrenlage ist indes mit Blick auf die gebotene, restriktive Auslegung regelmäßig eine auf konkrete, mithin einzelfallbezogene Tatsachen gestützte Gefahrenprognose, aus der sich der zu erwartende Eintritt einer Gefahr ergibt (Simitis/Philip/Scholz, Bundesdatenschutzgesetz, aaO).

Vorliegend hat das Amtsgericht die Einlassung des Betroffenen, der Betrieb der On-board-Kamera am 2. Mai 2016 habe allein der Aufzeichnung von Fahrstrecken für spätere Motorradtouren bzw. der Abschreckung vor möglichen Sachbeschädigungen gedient, rechtsfehlerfrei als Schutzbehauptung bewertet und damit festgestellt, dass der Zweck der Datenerhebung und -verarbeitung einzig der Dokumentation möglicher Ordnungswidrigkeiten und deren anschließender Anzeige bei der zuständigen Bußgeldbehörde diene. Die Feststellungen des angegriffenen Urteils enthalten keinerlei Hinweise auf konkrete Gefahrensituationen für Rechtsgüter des Betroffenen bzw. darauf, dass der Betroffene etwa durch die Handlungsweise des von der Datenerhebung betroffenen Mercedes-Fahrers in seinen Rechten verletzt worden sein könnte und sich aus einer etwaigen Rechtsgutverletzung zivilrechtliche Schadensersatzansprüche ergeben könnten.

Soweit der Betroffene danach die Onboard-Kamera einzig zu dem Zweck genutzt hat, die mutmaßlich verkehrsordnungswidrige Handlungsweise des Mercedes-Fahrers zu Beweiszwecken in einem Bußgeldverfahren zu dokumentieren, liegt hierin keine Wahrnehmung berechtigter Interessen. Der Betroffene geriert sich vielmehr zum Sachwalter öffentlicher Interessen. Im Bereich der Verkehrsordnungswidrigkeiten liegt die Entscheidung, ob eine Ahndung zu erfolgen hat, indes – wie vorstehend dargelegt – allein in staatlichen und nicht in privaten Händen. Danach hat der Betroffene mit der Anzeigenerstattung hinsichtlich des Geschehens vom 2. Mai 2016 bereits keine schützenswerten eigenen Interessen wahrgenommen.

Selbst wenn vorliegend von schutzwürdigen Interessen des Betroffenen auszugehen wäre, würden die schutzwürdigen Interessen des Mercedes-Fahrers das Interesse des Betroffenen an der Verkehrsüberwachung überwiegen. Das Interesse des Betroffenen an der Datenerhebung und Verarbeitung ist im Hinblick auf den von ihm beabsichtigten Zweck und damit im Hinblick auf die konkrete Nutzung aus den vorstehend dargelegten Gründen bereits nicht schützenswert und unterliegt im Rahmen der nach § 6b Abs. 1 Satz 1 Nr. 3 BDSG vorzunehmenden Güterabwägung dem Interesse des von der Datenerhebung betroffenen Mercedes-Fahrers, nicht Ziel einer heimlichen Videoüberwachung und Eingriffen in sein Recht auf informationelle Selbstbestimmung zu sein.

Schließlich hat der Betroffene seine Person als verantwortliche Daten erhebende Stelle sowie den Umstand der Beobachtung entgegen § 6b Abs. 1 Satz 2 BDSG auch nicht durch geeignete Maßnahmen erkennbar gemacht.

2. Der Betroffene hat den Verstoß gegen § 43 Abs. 2 Nr. 1 BDSG nach den Feststellungen im Urteil des Amtsgerichts Hannover vom 10. April 2014 im Wissen und Wollen um dessen vorstehend dargelegten objektiven Tatbestandsmerkmale begangen und damit vorsätzlich im Sinne von § 10 OWiG gehandelt. Der Betroffene wusste, dass er am 2. Mai 2016 um 15:09 Uhr, als er den Mercedes-Fahrer mit seiner Onboard-Kamera aufnahm, als natürliche Person und nicht-öffentliche Stelle personenbezogene Daten, mithin Einzelangaben über die persönlichen bzw. sachlichen Verhältnisse des Fahrers erhob und diese Datenerhebung mittels einer Datenverarbeitungsanlage, nämlich seiner Onboard-Kamera, durchführte und dass diese Datenerhebung auch nicht ausschließlich persönlichen oder familiären Zwecken diene. Des Weiteren war dem Betroffenen bewusst, dass es sich dabei um Daten aus nicht allgemein zugänglichen Quellen, mithin nicht allgemein zugängliche Daten handelte und er nicht berechtigt war, das Verhalten des Mercedes-Fahrers mit seiner Kamera zu filmen. Der Betroffene wusste schließlich auch, dass der Merce-

des-Fahrer anhand der von dem Betroffenen erhobenen Daten wie etwa dem abgelichteten Kfz-Kennzeichen bzw. der Abbildung seiner Person identifizierbar war. Der Betroffene handelte dabei einzig in der Absicht, die Daten dem Landkreis O. als zuständiger Bußgeldbehörde zu übersenden, verbunden mit dem Antrag, gegen den Mercedes-Fahrer ein Bußgeldverfahren einzuleiten.

Dass der Betroffene um die Rechtswidrigkeit seiner Handlung wusste, ergibt sich aus den weiteren Urteilsfeststellungen, wonach der Landesbeauftragte für Datenschutz Niedersachsen bereits am 4. Juni 2014 einen Bußgeldbescheid wegen unbefugter Datenerhebung mittels Verwendung einer Onboard-Kamera gegen den Betroffenen erließ und diesem mit weiterem Schreiben vom 29. Oktober 2014 unter Hinweis auf ein entsprechendes Urteil des Verwaltungsgerichts Ansbach darauf hinwies, dass der Einsatz von Onboard-Kameras unzulässig sei. Schließlich wurde dem Betroffenen durch Schreiben des Landesbeauftragten für Datenschutz Niedersachsen vom 1. Dezember 2014 mitgeteilt, dass gegen ihn ein aufsichtsbehördliches Kontrollverfahren gemäß § 38 BDSG eingeleitet wurde.

3. An der Änderung des Schuldspruchs, wonach der Betroffene einer vorsätzlichen unbefugten Erhebung und Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind, schuldig ist, war der Senat nicht gehindert. Dem Betroffenen wurde im Bußgeldbescheid des Landesbeauftragten für den Datenschutz Niedersachsen vom 11. November 2016 auch bezüglich der verfahrensgegenständlichen Tat bereits eine vorsätzliche Begehung zur Last gelegt, sodass es eines rechtlichen Hinweises nach § 71 Abs. 1 OWiG iVm § 265 Abs. 1 StPO bzw. der Klärung der Frage, ob sich der Betroffene im Falle des Fehlens eines solchen auch hätte anders verteidigen können, nicht bedurfte. Der Betroffene wird hierdurch auch nicht beschwert.

Die Korrektur des Schuldspruchs war geboten, weil die diesbezüglichen tatsächlichen Feststellungen im Urteil des Amtsgerichts Hannover vom 10. April 2017 allein diese Schuldform tragen. Danach war der Betroffene durch mehrere Schreiben des Landesbeauftragten für den Datenschutz Niedersachsen, u.a. durch Schreiben vom 29. Oktober 2014, 1. Dezember 2014 und 9. Januar 2015, auf die Rechtswidrigkeit vorheriger, gleichartiger Datenerhebungen hingewiesen worden und hat der Betroffene auch die verfahrensgegenständliche Datenerhebung danach, am 2. Mai 2016, zielgerichtet und einzig zu dem Zweck durchgeführt, die hierdurch dokumentierten Verstöße gegen verkehrsrechtliche Vorschriften zum Zwecke der Beweissicherung und anschließender Anzeige bei der zuständigen Bußgeldbehörde zu dokumentieren bzw. zu speichern. Zudem hat sich der Betroffene gegenüber dem Amtsgericht dahingehend eingelassen, er habe „eine längere Videosequenz gefilmt, nachdem ihm aufgefallen“ sei, dass der PKW-Führer während der Fahrt mit einem Mobiltelefon telefoniert habe.

4. Auch gegen die Höhe der festgesetzten Geldbuße, nämlich 250 €, ist nichts zu erinnern. § 43 Abs. 3 BDSG sieht für Ordnungswidrigkeiten in den Fällen des hier einschlägigen Abs. 2 eine Geldbuße bis zu 300.000 € vor. Das Amtsgericht, welches von einer fahrlässigen Begehungsweise und damit von einem oberen Rahmen der Geldbuße von 150.000 € ausgegangen ist, hat bei der Bemessung der Geldbuße rechtsfehlerfrei entsprechend § 17 Abs. 3 OWiG u.a. die Bedeutung der verletzten Vorschrift und den den Betroffenen treffenden Vorwurf und in diesem Zusammenhang u.a. den „relativ geringen Umfang der erhobenen personenbezogenen Daten sowie weiter berücksichtigt, dass der Betroffenen den objektiven Sachverhalt eingeräumt hat und unbestraft ist“.

Für Facebook gilt deutsches Datenschutzrecht – Datenweitergabe bedarf wirksamer Einwilligung (Ls)

(Kammergericht Berlin, Urteil vom 22. September 2017 – 5 U 155/14 –)

1. Facebook Deutschland unterliegt als eine Niederlassung von Facebook Irland deutschen Datenschutzrecht. Datenverarbeitung von Facebook Irland sind der Tätigkeit der Zweigniederlassung Facebook Deutschland selbst dann zuzurechnen, wenn die Daten nicht von der deutschen Niederlassung verarbeitet werden.
2. Facebook (Irland) ist es untersagt, Spiele so zu präsentieren, dass der Nutzer mit dem bloßem Betätigen des Buttons „Spiel spielen“ die Erklärung abgibt, einer Übermittlung personenbezogener Daten an den (externen) Betreiber des Spiels zuzustimmen.
3. Unwirksam ist mangels hinreichender Einwilligungserklärung auch eine Klausel, die es dem Betreiber des Spiels gestattet, im Namen des Nutzers auf Facebook zu posten.

(Nicht amtliche Leitsätze)

Voraussetzungen zur Verwertbarkeit von Dashcam-Aufzeichnungen im Zivilprozess

(Oberlandesgericht Nürnberg, Beschluss vom 10. August 2017 – 13 U 851/17 –)

1. Die Verwertung von sog. Dash-Cam-Aufzeichnungen zur Beweisführung über Verkehrsunfälle ist im Zivilprozess jedenfalls dann zulässig, wenn im Fahrzeug auf dem Armaturenbrett fest installierte Kameras, die in Fahrtrichtung, also nach vorne, ausgerichtet sind, auf Autobahnfahrten anlassbezogen betrieben werden.
2. Persönlichkeitsrechte des Unfallgegners sind durch diese Art von Aufzeichnungen, auf welchen konkrete Personen typischerweise nicht, sondern nur ihr Fehlverhalten zu erkennen sind, üblicherweise in so geringem Ausmaß betroffen, dass bei der gebotenen Abwägung zwischen beeinträchtigten Persönlichkeitsrechten einerseits und dem Anspruch auf rechtliches Gehör sowie dem Gebot des effektiven Rechtsschutzes andererseits letztere regelmäßig überwiegen. Dies gilt insbesondere dann, wenn andere zuverlässige Beweismittel im konkreten Fall nicht zur Verfügung stehen.
3. Darauf, ob die Aufnahmen unter Verstoß gegen § 6b BDSG erstellt wurden, kommt es in diesem Zusammenhang nicht an.

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien streiten um Schadensersatzansprüche aus einem Verkehrsunfall auf einer Autobahn.

Der Kläger fuhr am 18. März 2016 mit dem in seinem Eigentum stehenden Pkw, auf der BAB A 5, Kilometer 626 Nord. Hinter dem klägerischen Fahrzeug fuhr der Beklagte zu 2) mit einem Lkw, DAF, a. K., dessen Halterin die Beklagte zu 1) war. Der Lkw der Beklagten zu 1) fuhr dem klägerischen Fahrzeug heckseitig links auf, wodurch das klägerische Fahrzeug beschädigt wurde. Im Fahrzeug des Beklagten befand sich eine sog. Dashcam, mit der das Unfallgeschehen aufgezeichnet wurde.

Der Kläger hat in erster Instanz Schadensersatz in Höhe von 14.941,77 € nebst Zinsen geltend gemacht. Er hat behauptet, er sei bereits geraume Zeit auf der rechten Fahrspur der Autobahn gefahren, als er „verkehrsbedingt seine Geschwindigkeit reduzieren“ habe müssen, wobei er „aber keinesfalls abrupt und auch nicht bis zum Stillstand“ abgebremst habe. Er wisse nicht, „was der Grund für das Abbremsen der Vorderleute des Klägers“ gewesen sei. Der Beklagte zu 2) sei „alleinschuldhaft“ dem klägerischen Fahrzeug „aufgrund von Unaufmerksamkeit und/oder überhöhter, nicht angepasster Geschwindigkeit sowie insbesondere aufgrund von nicht eingehaltenem Sicherheitsabstand“ heckseitig aufgefahren. Für das alleinige Verschulden des Beklagten zu 2) an dem Unfallgeschehen spreche bereits der Beweis des ersten Anscheins. Deshalb habe der Kläger Anspruch darauf, dass ihm sein Schaden zu 100% von den Beklagten ersetzt werde.

Der Kläger hat die Auffassung vertreten, die von den Beklagten als Beweismittel angebotene Aufzeichnung der im Beklagten-Lkw installierten Dashcam sei nicht verwertbar. Wegen des mit der Dashcam verbundenen „unkonkreten, unspezifischen und permanenten, willkürlichen Eingriffs in die Persönlichkeitsrechte der aufgenommenen Personen“ würden „die schützenswerten Interessen des Klägers im konkreten Fall überwiegen“. Eine Beweisaufnahme dazu, dass die Kamera nur bei taktilem Erschütterung die aufgenommenen Sequenzen endgültig speichert, habe zu unterbleiben.

Die Beklagten haben in erster Instanz vorgetragen, der Kläger habe kurze Zeit vor dem Unfall den Lastwagen der Beklagten zu 1) überholt und sei dann von der äußersten linken Spur über die mittlere auf die ganz rechte Spur gewechselt. Sodann habe er abrupt bis zum Stillstand abgebremst. Der Unfall sei für den Beklagten zu 2) unvermeidbar gewesen. Die Beklagten haben die Auffassung vertreten, die Dashcam-Aufzeichnung sei verwertbar. Die Kamera zeichne auch nicht permanent, sondern nur anlassbezogen auf.

Das Landgericht hat eine Beweisaufnahme durchgeführt. Neben einer Zeugenvernehmung zur Frage des Aufzeichnens und Speicherns der Dashcam hat das Landgericht ein mündlich erstattetes unfallanalytisches Sachverständigengutachten des öffentlich bestellten und vereidigten Sachverständigen Dipl.-Ing. (FH) H. R. zur Rekonstruktion des Unfalls eingeholt. Im Zusammenhang damit wurden auch die vom Sachverständigen ausgedruckten Lichtbilder aus der Dashcam-Aufzeichnung in Augenschein genommen. Das Landgericht hatte den Sachverständigen gebeten, im Rahmen der Gutachtenserstattung alternativ darzustellen, mit welchem Ergebnis der Unfall einerseits ohne und andererseits mit Berücksichtigung der Dashcam-Aufzeichnungen zu rekonstruieren ist. Ergebnis der Begutachtung war:

- Ohne Berücksichtigung der Dashcam-Aufzeichnungen stehen als objektive Anknüpfungstatsachen nur die Schadensbilder an den Fahrzeugen zur Verfügung. Es ist dann lediglich feststellbar, dass ein Geschwindigkeitsüberschuss des Beklagten-Lkw gegenüber Kläger-Pkw dem bestand. Auf dieser Grundlage wäre keine der beiden behaupteten Unfallversionen auszuschließen.
- Dagegen ist bei Berücksichtigung der Dashcam-Aufzeichnungen klar feststellbar, dass die Unfalldarstellung der Beklagten unein-

geschränkt zutrifft und diejenige des Klägers nicht der Wahrheit entspricht. Es lässt sich dann nachvollziehen, dass der Kläger „ein höchst gefährliches Fahrmanöver durchgeführt“ hat, indem er von der linken Fahrspur der dort dreispurigen Autobahn auf die äußerst rechte Fahrspur gewechselt hat, vor dem Beklagten-Lkw einscherend, und dort „eine starke, wahrscheinlich eine Vollbremsung eingeleitet“ hat, mit der er das Fahrzeug „fast bis zum Stillstand abgebremst“ hat. Aus den in der Akte befindlichen Lichtbildern der Dashcam-Auswertung (Bl. 40 bis 43 der Akte) ist darüber hinaus schon im Wege des Augenscheins ersichtlich, dass sich vor dem klägerischen Fahrzeug auf der rechten Spur keine abbremsenden Fahrzeuge befanden, die dem Kläger seinerseits Anlass für eine Bremsung hätten geben können.

Demgegenüber hat der Fahrzeugführer des Beklagten-Lkw als Reaktion auf die erkennbare starke Abbremsung des klägerischen Fahrzeugs aus technischer Sicht keine Möglichkeit gehabt, den Unfall zu vermeiden. Der kurz vorher über zwei Fahrspuren hinweg vor dem Beklagten-Lkw einscherende Pkw des Klägers befand sich bei Beginn der klägerischen Bremsung nur 36 Meter vor dem Beklagten-Lkw. Selbst bei unverzüglicher Reaktion des Fahrers des Beklagten-Lkw, der vor der Bremsung mit 78 bis 80 km/h gefahren sei, sei der Lkw nicht mehr hinter dem sehr stark bremsenden Kläger-Pkw zum Halten zu bringen gewesen. Tatsächlich war anhand des Videomaterials auch die unverzügliche Abwehrreaktion seitens des Beklagtenfahrzeugführers beim Erkennen der starken Bremsung des vorausfahrenden Klägerfahrzeugs nach dem Spurwechsel festzustellen. Weiter war festzustellen, dass die mittlere Fahrspur neben dem Lkw durch einen weißen Audi besetzt war und daher dem Fahrer des Beklagten-Lkw auch ein Ausscheren auf die mittlere Spur nicht möglich war.

Das Landgericht hat mit Endurteil vom 28. März 2017 die Klage abgewiesen. Dabei hat es im Wesentlichen ausgeführt, es sei aufgrund des Sachverständigengutachtens davon überzeugt, dass das Unfallgeschehen für den Beklagten zu 2) unvermeidbar gewesen sei. Dabei seien die Dashcam-Aufzeichnung und auch die darauf gestützten Feststellungen des Sachverständigen verwertbar. Nach dem Ergebnis der Beweisaufnahme stehe außerdem fest, dass die Kamera nicht permanent, sondern nur anlassbezogen aufzeichne.

Mit der gegen das Urteil des Landgerichts eingelegten Berufung verfolgt der Kläger sein erstinstanzliches Ziel auf Verurteilung der Beklagten zur Zahlung von vollem Schadensersatz in Höhe von 14.941,77 € weiter.

Aus den Gründen:

Die Berufung hat offensichtlich keine Aussicht auf Erfolg.

Der Kläger hat weder neue berücksichtigungsfähige Tatsachen vorgetragen (§ 529 Abs. 1 Nr. 2 ZPO) noch konkrete Anhaltspunkte dargelegt, die Zweifel an der Richtigkeit und Vollständigkeit der entscheidungserheblichen Tatsachenfeststellungen des Landgerichts begründen würden (§ 529 Abs. 1 Nr. 1 ZPO).

In zutreffender Weise hat das Landgericht festgestellt, dass dem Kläger gegen die Beklagten aufgrund des Unfallereignisses vom 18. März 2016 kein Schadensersatzanspruch zusteht.

1. Das Erstgericht hat sich zutreffend die Überzeugung gebildet, dass die im Beklagten-Lkw installierte Dashcam so konfiguriert war, dass sie nur bei starker Erschütterung ein insgesamt 30 Sekunden langes Aufzeichnungssegment aus dem Zwischenspeicher dauerhaft auf die eingesetzte SD-Karte speichert, jedoch keine permanente Aufzeichnungsspeicherung erfolgt. Diese Feststellung konnte das Landgericht aufgrund der Aussage des Zeugen F. treffen, an deren Glaubhaftigkeit auch der Senat keine Zweifel hat.

a) Das Berufungsgericht, dessen Aufgabe die Fehlerkontrolle und Fehlerbeseitigung ist, hat gemäß § 529 Abs. 1 Nr. 1 ZPO

seiner Verhandlung und Entscheidung die vom Gericht des ersten Rechtszuges festgestellten Tatsachen zugrunde zu legen, soweit nicht konkrete Anhaltspunkte Zweifel an der Richtigkeit oder Vollständigkeit der entscheidungserheblichen Feststellungen begründen und deshalb eine erneute Feststellung gebieten. Fehler in der Beweiserhebung oder Beweiswürdigung sind hier allerdings nicht erkennbar.

Hat sich das Erstgericht – wie es hier der Fall ist – mit den Beweisergebnissen umfassend und widerspruchsfrei auseinandergesetzt – ist die Würdigung also vollständig und rechtlich möglich und verstößt sie nicht gegen Denkgesetze oder Erfahrungssätze – und ist auch das Berufungsgericht von der Richtigkeit der erstinstanzlichen Beweiswürdigung überzeugt, so sind die Feststellungen bindend. Eine Partei kann dann nicht in zulässiger Weise ihre eigene Würdigung an die Stelle derjenigen des Erstgerichts setzen.

Einwände gegen die Glaubwürdigkeit des Zeugen F. hat der Kläger nicht erhoben und auch sind im Übrigen nicht ersichtlich. Insbesondere macht nicht allein der Umstand, dass es sich um den Sohn des Geschäftsführers der Beklagten zu 2) handelt, macht den Zeugen nicht ungläubwürdig. Der Zeuge hat detailliert, differenziert und erkennbar um wahrheitsgemäße Angaben bemüht ausgesagt.

b) Entgegen dem Vorbringen des Klägers hat der Zeuge F. nicht bestätigt, dass eine anlasslose und permanente Aufzeichnung stattfindet. Zwar hat der Zeuge laut Protokoll der mündlichen Verhandlung angegeben, „Die Aufnahmen laufen immer...“ (Protokoll der mündlichen Verhandlung vom 21. Februar 2017, dort Seite 4 oben, Blatt 62 d. A.). Diese Aussage kann aber in Zusammenschau mit seinen weiteren Angaben nur dahin verstanden werden, dass es zunächst (immer) zu Aufnahmen in den flüchtigen Zwischenspeicher kommt und auch kommen muss, da andernfalls nicht auch das Geschehen vor der Erschütterung längerfristig aufgezeichnet werden kann, die – zunächst – endgültige Speicherung eines Segments von insgesamt 30 Sekunden aber erst durch eine erhebliche Erschütterung erfolgt, die einer stärkeren Bremsung entspricht, für die man „praktisch schon in den Gurten hängen“ muss. Nur dann werde aus dem flüchtig aufgezeichneten Material im Zwischenspeicher eine Sequenz von 20 Sekunden vor dem auslösenden Ereignis bis 10 Sekunden danach auf der eingesetzten SD-Karte abgespeichert. Damit deckt diese Aussage die Feststellung des Erstgerichts, dass eine permanente und anlasslose Aufzeichnung nicht erfolgte.

c) Unzutreffend ist auch die Behauptung des Klägers, der Zeuge F. habe nichts dazu sagen können, welche konkrete Einstellung die Dashcam zum Unfallzeitpunkt gehabt habe. Der Zeuge F. hat zwar angegeben, dass nach seinen Kenntnissen die Dashcams seit 2011 verbaut gewesen und auch schon konfiguriert gewesen seien, als er 2013 im Betrieb der Beklagten zu 1) tätig wurde. Es seien aber danach für alle Kameras neue Speicherkarten mit einem höheren Speicherplatz angeschafft worden. Diese Speicherkarten habe der Zeuge in allen Fahrzeugen nachträglich händisch konfiguriert, und dies in der von ihm beschriebenen Weise einer permanenten Aufzeichnung nur im Fall einer Erschütterung (Protokoll der mündlichen Verhandlung vom 21.02.2017, dort Seite 4, 3. Absatz, Blatt 62 d. A.).

d) Das Erstgericht war auch nicht gehalten, ein Sachverständigengutachten zur Frage der Programmierung der SD-Karte einzuholen.

Zunächst ist festzustellen, dass der Kläger entgegen seinem Vorbringen in der Berufungsbegründung einen gegenbeweisli-

chen Antrag auf Einholung eines Sachverständigengutachtens zu dieser konkreten Beweisfrage nicht gestellt hat. Er hat vielmehr lediglich geltend gemacht, eine Beweisaufnahme hierzu habe insgesamt zu unterbleiben (Schriftsatz vom 7. Februar 2017, S. 1, Bl. 54 der Akte).

Auch von Amts wegen musste das Erstgericht kein Sachverständigengutachten einholen. Die Einholung eines Sachverständigengutachtens nach § 144 Abs. 1 Satz 1 ZPO steht im Ermessen des Gerichts (Zöller/Greger, ZPO, 31. Aufl., § 144 Rn. 2). Hier hat das Landgericht die von den Beklagten vorgetragene Behauptung einer anlassbezogenen, nicht permanenten Aufzeichnung durch die Aussage des Zeugen F. als erwiesen angesehen. Der Einholung eines Sachverständigengutachtens zu der gleichen Beweisfrage von Amts wegen war daher nicht veranlasst.

Nur am Rande sei ergänzt, dass die weitere Beweiserhebung dazu auch deshalb entbehrlich gewesen wäre, weil es für die Verwertbarkeit im vorliegenden Fall nicht darauf ankommt, wie lang der Aufzeichnungszeitraum vor dem Unfall über die vom Landgericht festgestellte Dauer hinaus war (dazu näher unten 2 b cc (2)).

2. Die Aufzeichnung der im Lastwagen der Beklagten zu 1) an der Frontscheibe installierten Dashcam ist verwertbar. Sie konnte daher Gegenstand einer Inaugenscheinnahme nach § 371 BGB und Grundlage des Sachverständigengutachtens sein. Auf die zutreffenden Ausführungen des Erstgerichts in seinem Urteil wird zur Vermeidung von Wiederholungen zunächst Bezug genommen.

Für den Senat sind die nachstehenden Überlegungen maßgeblich:

a) Beweisverwertungsverbote sind in der Zivilprozessordnung nicht ausdrücklich normiert. Ein Verstoß gegen ein Verbot der Beweisbeschaffung oder -erhebung hindert nicht stets deren Verwertung, sondern nur nach Maßgabe der verletzten Norm und ihres Schutzzwecks (Musielak/Voit, ZPO, 14. Aufl., § 286 Rn. 6). Die Gerichte sind nach § 286 ZPO i.V.m. Art. 103 Abs. 1 GG verpflichtet, den von den Parteien vorgetragene Sachverhalt und die von ihnen angebotenen Beweise vollständig zu berücksichtigen. Dabei kommt der Funktionsfähigkeit der Rechtspflege und deren Streben nach einer materiell richtigen Entscheidung als wichtigen Belang des Gemeinwohls erhebliches, aber nicht ausschlaggebendes Gewicht zu. Über die Verwertbarkeit von Beweismitteln, die unter Verstoß gegen gesetzliche Normen gewonnen wurden, ist daher stets aufgrund einer Interessen- und Güterabwägung nach dem im Einzelfall gegebenen Umständen zu entscheiden (BGH, Urteil vom 27. Januar 1994 – I ZR 326/91 –, juris-Rn. 61). Für die Zulässigkeit der Verwertung von rechtswidrig beschafften Beweisen kommt es im Zivilprozess vor allem auch auf die Bedeutung des Beweismittels für die Rechtsverwirklichung einer Partei an, ein (stets gegebenes) schlichtes Beweisinteresse reicht nicht (BVerfG NJW 2002, 3619, juris-Rn. 62-64; BGHZ 27, 284 <290>; BGH, NJW 1982, S. 277; NJW 1988, S. 1016 <1018>; jeweils für den Schutz des gesprochenen Worts am Telefon vor unerlaubtem Mithören oder Mitschneiden; Zöller/Greger, 31. Aufl. 2016, ZPO, § 286 Rn. 15a).

Die Behauptung des Klägers, „nach der gängigen Rechtsprechung“ sei die Verwertung von Dashcam-Aufnahmen „unzulässig bzw. unverwertbar“, findet bei Recherche der hierzu veröffentlichten Rechtsprechung keine Stütze. Zur Frage, inwieweit die Erstellung von Aufzeichnungen mittels einer Dashcam (oder auch on-board-Kamera genannt) und insbesondere deren Ver-

wertung für Beweis Zwecke im Zivilprozess bei Verkehrsunfällen zulässig ist, sind bislang – zumindest in veröffentlichter Form – soweit ersichtlich nur Entscheidungen von Amts- und Landgerichten ergangen. Diese bejahen die Verwertbarkeit mehrheitlich (LG Frankenthal MDR 2016, 791; LG Traunstein ZD 2017, 239; LG München ZD 2017, 36; AG Nürnberg MDR 2015, 977; AG München DAR 2016, 275; ebenso wohl das OLG München im Rahmen der Erörterung des schließlich mit Vergleich beendeten Verfahrens 10 U 795/12, Nachweis bei Greger, NZV 2015, 114 <116>, Fn. 23). Der Senat hat nur zwei gerichtliche Entscheidungen finden können, die die Verwertbarkeit verneinen (LG Heilbronn NJW-RR 2015, 1019, dort bei einem Kleinschaden mit 820,00 € Streitwert, bei Annahme einer dauerhaften anlasslosen Aufzeichnung und Speicherung, sowie AG München ZfSch 2014, 692; beide genannten Entscheidungen stützen sich jeweils nur auf allgemeine, eher generalpräventive Erwägungen, ohne Interessenabwägung im Einzelfall). Die vom Kläger als Beleg für seine Auffassung herangezogene Entscheidung des LG Memmingen DAR 2016, 143 betrifft einen anderen Fall; dort geht es um die Nutzung einer Dashcam zur permanenten Überwachung des Hauseingangs eines Nachbarn, nicht um die Nutzung der Kamera im Straßenverkehr im Hinblick auf die Rekonstruierbarkeit eines Unfalls und erst recht nicht um Fragen der Verwertbarkeit für die Beweisführung zu einem Unfall in einem konkreten Einzelfall.

Auch in der Literatur wird die Verwertung derartiger Videoaufzeichnungen im Unfallprozess ganz überwiegend bejaht (etwa jeweils ohne Einschränkung hinsichtlich der Aufzeichnungsdauer Zöller/Greger, ZPO, 31. Aufl., § 286 Rn. 15c und Greger, NZV 2015, 114 ff., MüKoBGB/Prütting, 5. Aufl., § 284 Rn. 70; ähnlich Ahrens, MDR 2015, 926 ff., wenn auch mit der Empfehlung, dass bei fehlendem Beweisverwendungsbedarf regelmäßig gelöscht werden sollte; differenzierend nach der Dauer der Aufzeichnung Balzer/Nugel, NJW 2014, 1623 ff., wobei diese allerdings die Vorstellung haben, es sei „der Regelfall“, dass die gegnerische Partei der Verwertung nicht widerspreche, weil „üblicherweise beide Parteien ein Interesse daran haben, das Unfallgeschehen weitestgehend und umfassend aufzuklären“, was „die Problematik in vielen Fällen entschärfe“; diese Überlegung hilft allerdings gerade in den Fällen nicht weiter, in denen eine Partei beispielsweise mit prozessbetrügerischer Absicht durch unwahren Tatsachenvortrag einen rechtswidrigen Vorteil zu erlangen versucht und dann typischerweise der Verwertung nicht zustimmen wird).

Im Rahmen der durchzuführenden Interessen- und Güterabwägung werden dabei das informationelle Selbstbestimmungsrecht, das Recht am eigenen Bild nach § 22 Satz 1 KunstUrhG und datenschutzrechtliche Normen (§ 6 b BDSG) angesprochen, wobei allerdings – mit guten Gründen – die Auffassung vertreten wird, dass die Argumentation mit Datenschutzrecht oder den Persönlichkeitsrechten Dritter für das Straf- und Bußgeldrecht eine Rolle spielen können, nicht aber für die Interessenabwägung zur Verwertbarkeit von Videoaufzeichnungen im durch das Verhältnis der Parteien zueinander geprägten Zivilprozess (so Zöller/Greger, ZPO, 31. Aufl., § 286 Rn. 15b).

b) Für den vorliegenden Fall gilt folgendes:

aa) Ein Verwertungsverbot ergibt sich vorliegend nicht aus dem Recht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 GG). Es umfasst das Recht am eigenen Bild und stellt eine Ausprägung des Schutzes der personenbezogenen Informationen dar (BVerfG, Beschluss vom 26. Februar 2008 – 1 BvR 1602/07, 1 BvR 1606/07, 1 BvR 1626/07 –, juris Rn. 44 ff).

Eine Aufzeichnung des Straßenverkehrs durch eine in einem Fahrzeug installierte Kamera kann zwar in den Schutzbereich des allgemeinen Persönlichkeitsrechts eingreifen. Für die Frage, ob dieses durch Bildaufzeichnungen verletzt wird und ob sich gegebenenfalls daraus im Einzelfall ein Verwertungsverbot ableitet, sind nach ständiger Rechtsprechung die jeweils schutzwürdigen Interessen beider Parteien gegeneinander abzuwägen (BVerfG, Beschluss vom 9. Oktober 2002 – 1 BvR 1611/96, 1 BvR 805/98 –, juris Rn. 59; BGH, Urteil vom 25. April 1995 – VI ZR 272/94 –, juris Rn. 15; OLG Düsseldorf, Urteil vom 5. Mai 1997 – 5 U 82/96 –, juris Rn. 3; Zöller/Greger, ZPO, 31. Aufl., 2016, § 286 Rn. 15, 15a, 15c).

(1) Nach den Lichtbildern, die der Sachverständige im Rahmen seiner Gutachtenserstattung vorgelegt hat, ist die Person des Klägers auf der Aufzeichnung selbst nicht erkennbar. Entsprechendes wird auch vom Kläger nicht vorgetragen. Das allgemeine Persönlichkeitsrecht des Klägers in seiner Ausprägung als Recht am eigenen Bild wird hier nicht berührt. Zur Frage eines etwaigen Verstoßes gegen § 22 KunstUrhG wird auf die nachfolgenden Ausführungen unter Ziffer 2c Bezug genommen.

(2) Betroffen durch die Aufnahme ist aber das allgemeine Recht des Klägers, über die Preisgabe und Verwendung von persönlichen Daten selbst bestimmen zu können.

Letztlich bedarf es für die Beurteilung, ob ein Eingriff in das allgemeine Persönlichkeitsrecht einer Person zulässig ist, und damit, ob vorliegend die Beschaffung des Beweises durch die Aufzeichnung unzulässig war, stets einer Interessen- und Güterabwägung. Diese wird strukturiert durch die sog. Sphärentheorie, nach der zunächst danach zu unterscheiden ist, ob der Eingriff die Intim-, Privat- oder Sozialsphäre betrifft. Die Intimsphäre umfasst den Kernbereich der höchstpersönlichen privaten Lebensgestaltung, z.B. die innere Gedanken und Gefühlswelt mit ihren äußeren Erscheinungsformen wie vertrauliche Briefe, Tagebuchaufzeichnungen sowie die Angelegenheiten, bei denen ihrer Natur nach Anspruch auf Geheimhaltung besteht wie Einzelheiten des Sexuallebens oder des Gesundheitszustands. Die Privatsphäre beschreibt den Lebensbereich, zu dem andere Menschen nach sozialer Anschauung nur mit Zustimmung der Betroffenen Zugang haben, also im Wesentlichen das Privatleben im eigenen häuslichen Bereich. Die Sozialsphäre (Individualsphäre) schützt und bewahrt die persönliche Eigenart des Menschen in seinen Beziehungen zur Umwelt sowie seinem öffentlichen, wirtschaftlichen und beruflichen Wirken. Sie betrifft den Bereich, in dem sich die persönliche Entfaltung von Vorneherein im Kontakt mit der Umwelt vollzieht (zum Ganzen Palandt/Sprau, BGB, 76. Aufl., § 823 Rn. 87 mit zahlreichen Einzelnachweisen zur Rechtsprechung).

In die Intimsphäre sind Eingriffe nahezu ausgeschlossen, in die Privatsphäre nur nach streng geregelten Vorgaben zulässig, wenn es um den Schutz entgegenstehender Interessen von hohem Gewicht geht. Die Sozial-/Individual-/Öffentlichkeitssphäre steht dagegen unter einem weit geringeren Schutz. Maßnahmen, die diesen Bereich betreffen, weisen von Vorneherein – wenn überhaupt – nur eine geringe Belastungsintensität auf. Hier bestehen unter Verhältnismäßigkeitsgesichtspunkten die geringsten Rechtfertigungsanforderungen (Di Fabio, in: Maunz/Dürig, GG, Lfg. 39, Art. 2 Abs. 1 Rn. 160).

(a) Die Dashcam-Aufzeichnung hält als auf den Kläger bezogene persönliche Daten allein sein konkretes Fahrverhalten auf einer öffentlichen Autobahn in einem Zeitraum von weniger als einer Minute fest – und dies unabhängig davon, ob die Dashcam für eine permanente Aufzeichnung konfiguriert war oder nur anlassbezogen; das klägerische Fahrzeug ist erst wenige Se-

kunden vor dem Unfall überhaupt in den „Sichtbereich“ der Kamera eingefahren. Dieses Geschehen ist in die sog. Individual-sphäre einzuordnen.

In der Abwägung ist diesem persönlichkeitsrechtlichen Interesse des Klägers kein hohes Gewicht beizumessen. Es geht allein um das Interesse des Klägers, dass sein ohnehin in der Öffentlichkeit stattfindendes Verkehrsverhalten nicht, auch nicht für einen sehr kurzen Zeitraum, dokumentiert wird. Der Kläger wird durch die Aufnahme weder zur Schau gestellt noch in anderer Weise herabgewürdigt, als Person ist er überhaupt nicht erkennbar. Erkennbar ist letztlich nur sein Fahrverhalten als solches. Er hat sich durch die Teilnahme am öffentlichen Verkehr selbst der Wahrnehmung und Beobachtung anderer Verkehrsteilnehmer ausgesetzt und ist selbst von der Aufzeichnung auch nur für einen ganz kurzen Zeitraum betroffen (vgl. dazu auch BVerfG, Beschluss vom 20. Mai 2011 – 2 BvR 2072/10 –, beck-online Rn. 17, für die Nutzung einer Dauervideoaufzeichnung zur Ahndung von Ordnungswidrigkeiten).

(b) Dem gegenüberzustellen ist das Interesse der Beklagten daran, für den konkreten Unfall die Dashcam-Aufzeichnung als Beweismittel zur Verfügung zu haben und im Verfahren zur Verteidigung gegen die Inanspruchnahme durch den Kläger verwerten zu können. Dieses wiegt im Verhältnis zu dem Interesse des Klägers schwer. Das in Art. 20 Abs. 3 GG verbürgte Rechtsstaatsprinzip sowie das Recht auf rechtliches Gehör nach Art. 103 Abs. 1 GG gebieten grundsätzlich, dass angebotene Beweise erhoben und verwertet werden. Auch wenn das Gemeinwohlinteresse auf effektiven Rechtsschutz nach Art. 19 Abs. 4 GG nicht von vorneherein das Recht des Einzelnen, auch im öffentlichen Raum nicht gefilmt zu werden, überwiegt (LG München, Urteil vom 14. Oktober 2016 – 17 S 6473/16 –, juris Rn 13), ist jedenfalls dann dem Interesse des Beweisführers besonderes Gewicht beizumessen, wenn keine anderen Beweismittel zur Verfügung stehen, er also auf der Verwertung für die Erreichung seines Rechtsschutzziels angewiesen ist, womit zugleich auch der materiellen Gerechtigkeit Genüge getan wird.

So liegt der Fall hier. Den Beklagten stehen keine Zeugen für das Fahrverhalten des Klägers vor dem Unfall zur Verfügung. Der Zeuge Sch. hat nur den unmittelbaren Zusammenstoß im Rückspiegel gesehen, nicht das Geschehen davor (vgl. Bl. 34 der Akte). Ohne die Dashcam-Aufzeichnungen fehlt es auch an aussagekräftigen objektiven Anknüpfungstatsachen, mit denen das tatsächliche Unfallgeschehen in seinen für die rechtliche Bewertung entscheidenden Teilen unfallanalytisch rekonstruiert werden könnte. Dürfte die Dashcam-Aufzeichnung nicht verwertet werden, könnte der Beklagte den grob wahrheitswidrigen Sachvortrag des Klägers nicht widerlegen. Die Folge wäre, dass der Kläger mit seinem unter massiver Verletzung nach § 138 Abs. 1 ZPO getätigten unwahren Sachvortrag, der sich auch noch auf Abläufe seiner eigenen Wahrnehmung bezieht, staatliche Gerichte zu einer ungerechtfertigten Verurteilung der Beklagten zwingen könnte, wobei es vorliegend nicht um einen Bagatellschaden, sondern um einen erheblichen Betrag geht.

Ohne Berücksichtigung der Anknüpfungstatsachen aus der Dashcam-Aufzeichnung wäre über die Anwendung eines Anscheinsbeweises eine Alleinhaftung der Beklagten in Betracht zu ziehen, zumindest aber aufgrund der Unaufklärbarkeit des Unfalls eine mehr als hälftige Mithaftung der Beklagten aufgrund erhöhter Betriebsgefahr des Beklagten-Lkw. Dies obwohl tatsächlich, wie bei Berücksichtigung der Dashcam-Aufzeichnung feststeht, der Kläger das Unfallgeschehen durch ein grob verkehrswidriges, rücksichtsloses und hoch gefährliches Verhalten allein zu verantworten hat und nur die schnelle richtige Reak-

tion des Beklagten zu 2 (sofortige Bremsung ohne Ausscheren auf die von einem anderen Fahrzeug befahrene Mittelspur) schlimmere Folgen verhindert hat. Insoweit schließt sich der Senat der Beurteilung des Erstgerichts vollumfänglich an.

(c) Insgesamt führt die Interessenabwägung hier zu einem eindeutigen Ergebnis. Das Interesse des Klägers, dass sein Fahrverhalten auf einer öffentlichen Autobahn überhaupt nicht durch Videoaufzeichnung dokumentiert wird, auch nicht für wenige Sekunden, steht weit hinter dem Interesse des Beklagten zurück, rechtliches Gehör zu erhalten und nicht zu Unrecht auf der Grundlage einer vom Kläger auf grob wahrheitswidrige Behauptungen gestützten Klage zu einer erheblichen Zahlung verurteilt zu werden. Zumindest in der vorliegenden Einzelfallkonstellation hält der Senat jedes andere Abwägungsergebnis für offenkundig nicht zu vertreten.

cc) Die Tatsache, dass nicht nur die Bewegung des Fahrzeugs des Klägers im Straßenverkehr dokumentiert wurde, sondern auch die weiterer Fahrzeuge Dritter, führt zu keinem anderen Abwägungsergebnis, ebensowenig der Umstand, dass nicht ausschließbar vereinzelt auch Personen sichtbar abgebildet sein könnten.

(1) Inwieweit bei der Güterabwägung zur Verwertung im Zivilprozess überhaupt das allgemeine Interesse Dritter einzustellen ist, nicht dem Risiko ausgesetzt zu werden, ohne Anlass aufgezeichnet und sich auf Speichermedien wiederfinden zu müssen, ist als solches bereits zweifelhaft (ablehnend wohl Zöller/Greger, ZPO, 31. Aufl., § 286 Rn. 15b).

(a) Bei unbeteiligten Personen, die als Passanten oder Teilnehmer am fließenden Verkehr mit auf das Bild geraten, zu denen nicht – etwa durch einen nachfolgenden Unfall – persönlicher Kontakt, verbunden mit der Identifizierung der Person, besteht, fehlt es schon wegen der Anonymität der betreffenden Personen an der Eingriffsqualität der Aufzeichnung (Greger NZV 215, 214 <215>). Dementsprechend sind Abbildungen von Passanten und Verkehrsteilnehmern auf öffentlichen Wegen und Plätzen, die nur als Beiwerk des Stadt- oder Straßenbildes miterfasst werden, von diesen ohnehin hinzunehmen (BGH, Urteil vom 25. April 1995 – VI ZR 272/94 –, juris Rn. 17). Im Vordergrund steht bei diesen Aufnahmen gerade nicht die Abbildung einer Persönlichkeit, sondern ein Verkehrsgeschehen. Bei Fahrten auf der Autobahn ist darüber hinaus die Wahrscheinlichkeit, dass Personen überhaupt – auch in nicht identifizierter Form – abgebildet werden, wegen der Kameraperspektive in Relation zu den gefilmten Fahrzeugen äußerst gering. Auch die Möglichkeit, Bewegungsbilder oder dergleichen zu erstellen, ist beim Einsatz einer Dashcam in der streitgegenständlichen Form, also ohne gezielte Verfolgung oder Observation eines bestimmten Fahrzeugs, ausgeschlossen; und zwar bei realistischer Bewertung selbst dann, wenn die Dashcam über eine lange Fahrtstrecke Aufzeichnungen speichert, nicht nur begrenzt auf das Unfallereignis. Insofern stellt sich bereits die Frage, ob der Persönlichkeitsschutz der Verkehrsteilnehmer überhaupt erfordert, mit technischen Vorkehrungen das Aufzeichnen auf das unmittelbare Unfallgeschehen begrenzen (dies verneinend Greger NZV 215, 214 <215>).

(b) Unabhängig davon würde aber das Fehlen einer technischen Einrichtung zur Begrenzung der Aufnahmedauer auf das Unfallereignis nach Auffassung des Senats nicht dazu zwingen, die Verwertbarkeit derjenigen Sequenz für die Beweisführung zu einem Unfall zu verneinen, die als solche auch bei einer Begrenzung auf das unmittelbare Unfallgeschehen dauerhaft gespeichert wäre.

Insofern unterscheidet sich die Beurteilung der Verwertbarkeit einer Dashcam-Aufzeichnung wie der vorliegenden ganz

wesentlich von den Fragen, die sich etwa bei der Verwertung unzulässiger Mitschnitte des gesprochenen Worts oder einer gezielten filmischen Überwachung eines Arbeitnehmers oder eines Nachbarn stellen. In den letztgenannten Fällen sind gerade auch die Sequenzen, um deren Verwertung es geht, selbst direkt persönlichkeitsrechtsverletzend erhoben, d.h. es sollen beispielsweise gerade Äußerungen verwertet werden, die als solche nicht hätten aufgenommen werden dürfen.

Die Fragen, welche von Gegnern der Verwertbarkeit von Dashcam-Aufzeichnungen aufgeworfen werden, insbesondere bei der Frage der Aufzeichnungsdauer insgesamt, betreffen dagegen solche Teile der Aufzeichnung, die als solche gar nicht verwertet werden sollen. Insoweit wird die These vertreten, die als solche auch unter Verhältnismäßigkeitsgesichtspunkten unproblematisch verwertbare, zeitlich kurze Unfallsequenz dürfe dann nicht verwertet werden, wenn vorher weitere Aufzeichnungen vom Verkehrsgeschehen gefertigt worden seien, die möglicherweise Dritte abbilden, ohne dass es hierfür eine hinreichende Notwendigkeit oder Rechtfertigung gibt. Eine derartige Ausdehnung der Beurteilungskriterien für die Verwertungsprüfung wird aber der Bedeutung und Funktion des Zivilprozesses nicht gerecht. Das Zivilprozessrecht hat nicht die Aufgabe, sonstiges Verhalten von Prozessbeteiligten, welches nicht die Beschaffung des konkret zu verwertenden Beweises selbst – hier also das Filmen und Speichern der unmittelbaren Unfallsituation – darstellt, zu sanktionieren.

Konsequent zu Ende gedacht müssten diejenigen, die Aufnahmezeitbegrenzungen als Voraussetzung für die Verwertung von Dashcam-Aufzeichnungen im Zivilprozess fordern, in Fällen, in welchen das Unfallgeschehen vom Beifahrer mit der Kamera eines Mobiltelefons gefilmt wurde, auch klären, wie lange und wie oft der Beifahrer vorher gefilmt hat und ob er dafür gute Gründe hatte. Hätte er „anlasslos“ bei früherer Gelegenheit gefilmt, dürfte die spätere zufällige Aufnahme vom Unfallgeschehen nicht verwendet werden, hätte er nur beim Unfall gefilmt oder schon vorher gute konkrete Gründe zum Filmen gehabt, wäre die Verwertung gestattet. Der Sinn einer derartigen Differenzierung zur Entscheidung über die Verwertbarkeit derjenigen Sequenz, die das unmittelbare Unfallgeschehen zeigt, erschließt sich dem Senat nicht, jedenfalls nicht für den Zivilprozess. Dies gilt zumindest dann, wenn – wie vorliegend – bei den unmittelbar vorgelagerten Bildaufnahmen nicht etwa schwerwiegende Eingriffe wie Filmen in der Privat- oder gar Intimsphäre im Raum stehen, sondern ebenfalls nur Aufnahmen, bei denen lediglich die Sozialsphäre betroffen sein kann, wobei selbst deren Schutzbereich eher tangiert wird, als dass man überhaupt von einem Eingriff sprechen kann (also: Erfassung einer Einzelperson – wenn überhaupt – oder eines Fahrzeugs nur für einen kurzen Zeitraum, dann wiederum in aller Regel ohne Individualisierung, keine Schaffung von Bewegungsbildern Einzelner).

(2) In jedem Fall führt aber auch die Berücksichtigung der genannten allgemeinen Drittinteressen bei der vorliegenden Fallgestaltung – nach vorne gerichtete Dashcam mit Weitwinkelleinstellung bei einer Autobahnfahrt – nicht dazu, dass die Verwertbarkeit zu verneinen ist.

(a) Soweit die höchstrichterliche Rechtsprechung eine permanente, verdachtslose Videoüberwachung als unzulässig bewertet, betrifft dies regelmäßig Fälle, bei denen sich die Überwachung gezielt auf bestimmte, individualisierbare Personen richtet und sich darüber hinaus auch auf einen längeren Zeitraum erstreckt.

So hat der BGH eine permanente, verdachtslose Überwachung des Zugangs zu einem Wohnhaus auch dann als Verletzung des allgemeinen Persönlichkeitsrechts angesehen, wenn die Aufzeichnung nicht verbreitet werden sollte. Ein derartiger Eingriff sei höchstens dann zulässig, wenn schwerwiegenden Beeinträchtigungen, wie etwa Angriffen auf Personen, nicht anderweitig zumutbar begegnet werden können (BGH, Urteil vom 25. April 1995 – VI ZR 272/94 –, juris Rn. 16 ff).

Im Fall einer verdeckten Videoüberwachung am Arbeitsplatz (BAG, Urteil vom 21. Juni 2012 – 2 AZR 153/11 –, juris Rn. 30) wurde eine Rechtfertigung nur bei Vorliegen eines konkreten Verdachts einer Straftat oder einer anderen schweren Verfehlung anerkannt.

(b) Beim Einsatz einer Dashcam in der vorliegenden Weise – nach vorne gerichtet bei der Autobahnfahrt in einem Lkw – sind dagegen die Grundrechte Dritter nur in äußerst geringfügiger Weise tangiert. In Fahrzeugen sitzende Personen sind praktisch nicht sichtbar, weil die Fahrzeuge von hinten aufgenommen werden. Köpfe sind damit wenn überhaupt, nur in Konturen und dann auch noch überwiegend durch Kopfstützen verdeckt zu sehen, soweit nicht – wie bei einem Großteil der Fahrzeuge – getönte Scheiben den Blick auf die Personen nicht ohnehin verwehren.

Die Kamera ist einem mit starkem Weitwinkelobjektiv ausgestattet. Dadurch sind die einzelnen Fahrzeuge überwiegend nur relativ klein abgebildet, eine kurzzeitig größere Abbildung erfolgt regelmäßig nur beim Auftauchen eines Fahrzeugs direkt nach einem Überholvorgang. Aufgrund der typischen Fahrdynamik der Fahrzeuge zueinander muss auch kein Verkehrsteilnehmer, abgesehen möglicherweise von in Kolonne fahrenden Lkws, befürchten, dass sein Fahrzeug länger als für einen ganz kurzen Zeitraum, der sich oft mehr nach Sekunden als Minuten bemessen wird, auf einer einzelnen Dashcam aufgezeichnet wird; und zwar sogar dann nicht, wenn eine Dashcam längere Sequenzen oder sogar permanent dauerhaft abspeichernd aufzeichnen würde. Die Gefahr, dass mit einzelnen Dashcams, die auf isolierte Speichermedien aufzeichnen, Bewegungsbilder von bestimmter Kraftfahrzeuge oder gar bestimmter Personen erstellt werden können, besteht nicht. Etwas anderes würde allenfalls bei einer gezielten Verfolgung und Observation eines bestimmten Fahrzeugs gelten. Dies steht aber vorliegend nicht im Raum. Selbst dann, wenn die Dashcam über längere Zeit oder gar während der Autobahnfahrt permanent aufzeichnen würde, bliebe die Eingriffsintensität bei der genannten Kameraverwendung bei jedem einzelnen Verkehrsteilnehmer äußerst gering.

Es geht eben – anders als bei der automatisierten Kennzeichenerfassung zu Fahndungszwecken, die das BVerfG unter einen strikten Gesetzesvorbehalt gestellt hat – nicht um das gezielte Aufspüren gesuchter Personen oder Fahrzeuge, und es besteht wegen der nur vorübergehenden, zufallsgesteuerten Abbildung in der Regel nicht identifizierbarer Verkehrsteilnehmer auch nicht die Möglichkeit, personenbezogene Bewegungsprofile oder dergleichen zu erstellen. Insoweit sind zur polizeilichen Verkehrskontrolle, automatisierten Kennzeichenerfassung, Rasterfahndung und behördlichen Überwachung öffentlicher Plätze getroffene Entscheidungen auf die hier zu beurteilenden Sachverhalte nicht übertragbar (Greger, NZV 2015, 114 <115>, mit Einzelnachweisen in Fn. 15).

Nochmals weitaus weniger tangiert sind die Rechte Dritter, wenn wie vorliegend vom Erstgericht in zutreffender Weise festgestellt, die Kamera so konfiguriert ist, dass eine dauerhafte

Speicherung nur bei einer sehr erheblichen Erschütterung erfolgt und dann auch nur mit einer Sequenz von insgesamt 30 Sekunden. Insofern ist das Risiko jedes Einzelnen, auch als Unbeteiligter aufgezeichnet zu werden, das in der konkreten Gestaltung ohnehin praktisch nur fahrzeug- und nicht personenbezogen in Betracht kommt, nochmals massiv reduziert. Die nur kurzzeitige Erfassung von Vorgängen im Straßenverkehr birgt erst recht eine gegen Null gehende Gefahr der Aufzeichnung von Bewegungsabläufen Unbeteiligter und deren Rekonstruierbarkeit. Sofern im Einzelfall aber zufällig einzelne Personen, die den Verkehrsraum nutzen, mitabgebildet werden sollten, ist dies von diesen ohnehin hinzunehmen (BGH, Urteil vom 25. April 1995 – VI ZR 272/94 –, juris Rn. 17).

Selbst wenn man also die Interessen unbeteiligter Dritter mit einbezieht, wäre es angesichts der geschilderten sehr geringen und eher theoretischen Betroffenheit unbeteiligter Dritter bei der Interessenabwägung im Rahmen der zivilprozessualen Verwertbarkeit von Dashcam-Aufzeichnungen der vorliegenden Art nicht zu rechtfertigen, einer andernfalls in Beweisnot befindlichen Partei den Rückgriff auf dieses Beweismittel mit dem Argument einer abstrakten Überwachungsbefürchtung Dritter zu verwehren und es damit einem Prozessgegner zu ermöglichen, mit grob unwahrem Sachvortrag eine materiell falsche Verurteilung zu erwirken. Auch hier spricht die Abwägungsergebnis – sehr deutlich – für die Verwertbarkeit der Aufzeichnungen, wobei es nach Auffassung des Senats – wie bereits ausgeführt – im vorliegenden Fall sogar hätte dahinstehen hätte können, ob und in welchem Maß die Dauer der endgültig abgespeicherten Aufnahme begrenzt wurde.

b) Auch datenschutzrechtliche Erwägungen stehen einer Verwertung der Dashcam-Aufzeichnung nicht entgegen.

aa) Dabei kann grundsätzlich bereits dahinstehen, ob die streitgegenständliche Aufzeichnung unter Verstoß gegen § 6b BDSG zustande gekommen ist. Die Frage, ob Aufnahmen einer Dashcam verwertet werden dürfen, betrifft ausschließlich die prozessrechtliche Ebene. Entscheidend ist dabei, ob durch die Verwertung eines unter Verstoß gegen datenschutzrechtliche Regelungen gewonnenen Beweismittels Grundrechte verletzt werden und ob diese ggf. hinter das öffentliche und individuelle Interesse an der Rechtsdurchsetzung und Wahrheitsermittlung zurücktreten müssen (Greger, NZV 2015, 114 f.). Letzteres ist nach Ansicht des Senats der Fall. Insofern wird auf die bereits gemachten Ausführungen Bezug genommen.

bb) Ein Verstoß gegen § 6b BDSG, der gemäß § 2 Abs. 4 Satz 1 BDSG auch an Privatpersonen adressiert ist, ist aber auch als solcher schon nicht zu bejahen. Die von der Beklagten zu 1) gefertigten Aufzeichnungen sind zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich. Weiter bestehen keine Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Erstellung der Aufzeichnung und deren Verwendung im Prozess war sowohl für die Beklagten im Rahmen ihrer Rechtsverfolgung oder – hier – der Rechtsverteidigung als auch für eine funktionstüchtigen Rechtspflege mit dem Streben nach einer materiell richtigen Entscheidung erforderlich, wie dieser Fall plastisch zeigt. Ohne Verwertung der Aufzeichnung wäre den Beklagten eine effektive Rechtsverteidigung abgeschnitten, da ihnen andere geeignete Beweismittel, z.B. Zeugen, nicht zur Verfügung standen und ihr Prozessgegner den objektiv wahren Sachvortrag der Beklagten – mit grob wahrheitswidrigen Behauptungen – streitig gestellt hatte.

Die Aufzeichnung diene der Wahrnehmung berechtigter Interessen der Beklagten wie auch desjenigen der Allgemeinheit an materiell richtigen Entscheidungen (vgl. oben, Ziffer 2 a, cc). Die Aufzeichnungen wurden für diese konkret festgelegten Zwecke der Beweisführung in Prozessen erstellt. Schon allgemein durch die Umstände der Verwendung der Dashcam, aber erst recht durch die Konfigurierung der Speicherkarte in der Weise, dass eine permanente Aufzeichnung nur in dem Fall erfolgt, in dem es innerhalb eines Zeitraums von 30 Sekunden zu einer Erschütterung entsprechend der Stärke 7 auf der Skala von 1 bis 10 kommt, bestehen keine Zweifel an diesem Verwendungszweck. Anhaltspunkte dafür, dass die schutzwürdigen Interessen des Klägers oder anderer theoretisch Betroffener überwiegen, sind nicht gegeben. Auch insoweit wird auf die obigen Ausführungen im Rahmen der Interessenabwägung verwiesen.

c) Die Einführung der Dashcam-Aufzeichnung in den Zivilprozess und deren Verwertung im Verfahren verstößt auch nicht gegen § 22 Satz 1 KunstUrhG. Insbesondere liegt kein öffentliches Verbreiten oder Zurschaustellen eines Bildnisses vor. Der Anwendungsbereich dieser Vorschrift ist bei der hier vorliegenden Art der Verwendung der Dashcam und auch bei der konkret in Streit stehenden Aufzeichnung nicht anwendbar.

aa) Es fehlt bereits an dem Merkmal eines „Bildnisses“. Ein Bildnis im Sinne des Kunsturhebergesetzes ist die Wiedergabe des äußeren Erscheinungsbildes einer Person in einer für Dritte erkennbaren Weise (BGH, Urteil vom 1. Dezember 1999 – I ZR 49/97 –, juris Rn. 71 – Marlene Dietrich).

Im konkreten Fall ist das Recht am eigenen Bild des Klägers überhaupt nicht berührt. Auf keinen der vom Sachverständigen überreichten Lichtbilder, die aus der Dashcam-Aufzeichnung gewonnen wurden, ist die Person des Klägers als Fahrer eines Fahrzeugs allenfalls nur schemenhaft zu sehen. Gleiches gilt für Insassen anderer auf der Aufzeichnung zu sehenden Personenkraftwagen. Allein wegen der Perspektive, der Entfernungen und des Umstands von Spiegelungen und etwaiger Tönungen der Fahrzeugscheiben hält es der Senat für nahezu ausgeschlossen, dass Personen in den Fahrzeugen überhaupt in personalisierter Weise abgebildet werden können. Die Rechte Dritter an ihrem eigenen Bild werden demnach ebenso wenig wie das des Klägers tangiert, womit auch unter diesem Aspekt ein Beweisverwertungsverbot nicht besteht. Der auf der Aufzeichnung sichtbare Pkw des Klägers hingegen scheidet als Sachdarstellung als geeignetes Objekt eines Bildnisses von vorne herein aus.

bb) Ohne dass es hierauf entscheidend ankommt, fehlt es auch tatbestandlich an der Verbreitung oder öffentlichen Zurschaustellung im Sinne des § 22 Satz 1 Kunst-UrhG. Auch wenn die Aufzeichnung in einer nach § 169 S. 1 GVG öffentlichen Gerichtsverhandlung angesehen wurde, liegt keine öffentliche Zurschaustellung vor. Nach einem Urteil des EGMR (Urteil vom 27. Mai 2014 – 10764/09 –, NJW 2015, 1079, beck-online Rn. 35, 36) liegt eine „Verbreitung“ in der öffentlichen Sitzung oder ihrer Weitergabe an die Prozessbeteiligten im Laufe des Verfahrens dann nicht vor, wenn Aufnahmen eines Privatdetektivs zum Zwecke der Beweissicherung und Beweisführung gefertigt wurden, sie nicht zur Veröffentlichung bestimmt sind und keine Veröffentlichungsgefahr besteht. Werden die allein zu diesem Zweck gefertigten Beweismittel in die Gerichtsakte aufgenommen und allein zu diesem Zweck benutzt, liegt kein Verbreiten vor (EGMR, Urteil vom 27. Mai 2014, Rn. 41). Nach die-

sen Maßstäben fehlt es an dem nach § 22 Satz 1 KunstUrhG erforderlichen Öffentlichkeitsbezug; der Begriff des „Verbreitens“ ist teleologisch zu reduzieren (LG München, Urteil vom 14. Oktober 2016 – 17 S 6473/16 -, juris Rn. 9). Diese Grundsätze gelten auch dann, wenn – wie hier – im konkreten Fall die Aufnahmen von einer Partei und nicht nach gesonderten Regeln gefertigt wurden (im Urteil des EGMR von einem Privatdetektiv in einem nach spanischem Recht geregelten Verfahren). Die Aufnahmen wurden auch hier allein zu Beweis Zwecken gefertigt. Ein anderweitiges Interesse der Beklagten zu 1), einer Transportfirma mit ca. 20 Fahrzeugen, ihre gesamte Flotte mit Dashcams auszustatten, als das, vor allem in Unfallsituationen über Aufnahmen zur Beweisführung zu verfügen, ist nicht ersichtlich. Für eine Veröffentlichungsgefahr bestehen auch im Übrigen keinerlei Anhaltspunkte.

cc) Ein Verwertungsverbot kann im Hinblick auf das Recht am eigenen Bild auch nicht daraus abgeleitet werden, dass durch Dashcams auch zufällige Aufnahmen von unbeteiligten Personen, mit denen diese individualisiert werden könnten, nicht in jeder Konstellation restlos auszuschließen sind. Abgesehen davon, dass für die Frage eines Verwertungsverbotes der Kläger sich nicht auf die Verletzung von Rechten Dritter berufen kann, bestehen seitens des Senats selbst, dann, wenn man diese in die Abwägung einstellen würde, keine durchgreifenden Bedenken gegen eine Beweisverwertung.

Wie bereits in anderem Zusammenhang angesprochen zielen Dashcam-Aufzeichnungen der konkret verfahrensgegenständlichen Art (Aufzeichnung während einer Fahrt, insbesondere einer solchen auf der Autobahn) weder darauf ab, noch eignen sie sich besonders dazu, Personen in identifizierbarer Weise abzubilden. Die Dashcam ist an der Windschutzscheibe des Lkw-Führerhauses installiert und zeichnet daher regelmäßig Verkehrsvorgänge im Straßenraum auf, die sich vor der Lkw-Front abspielen. Handelt es sich dabei, wie im vorliegenden Fall, um ein Verkehrsgeschehen auf der Autobahn, ist eine Aufzeichnung von Personen ohnehin weitestgehend ausgeschlossen. Die Fahrer und Beifahrer der aufgezeichneten Fahrzeuge sind schon allein wegen der Perspektive nicht oder kaum sichtbar und noch weniger individualisierbar, allenfalls können (Hinter-)Köpfe der im Fond des Fahrzeugs sitzenden Personen aufgezeichnet werden. Selbst wenn es insgesamt nicht ausgeschlossen sein wird, dass im Einzelfall – vorwiegend bei Aufnahmen in anderen Verkehrsräumen – auch Personen in erkennbarer Weise abgebildet werden, rechtfertigt das nicht, die Aufzeichnungen als generell unzulässig zu beurteilen. Abbildungen von Passanten und Verkehrsteilnehmern auf öffentlichen Wegen und Plätzen, die nur als Beiwerk des Stadt- oder Straßenbildes miterfasst werden, sind von diesen ohnehin hinzunehmen (BGH, Urteil vom 25. April 1995 – VI ZR 272/94 -, juris Rn. 17). Im Vordergrund steht bei diesen Aufnahmen gerade nicht die Abbildung einer Persönlichkeit, sondern ein Verkehrsgeschehen.

Zusammenfassend lässt sich feststellen, dass ein Beweisverwertungsverbot der streitgegenständlichen Dashcam-Aufzeichnung nicht besteht. Der rechtlichen Beurteilung des Erstgerichts, dass das Fahrverhalten des Klägers als grob verkehrswidrig und rücksichtslos einzustufen ist und für den Beklagten zu 2) das Unfallgeschehen unvermeidbar war, schließt sich der Senat an. Die Klage ist zu Recht abgewiesen worden.

III. Der Senat legt deshalb die Rücknahme der Berufung nahe.

Information des Betriebsrats über Schwangerschaften

(Landesarbeitsgericht München, Beschluss vom 27. September 2017 – 11 TaBV 36/17 –)

Der Arbeitgeber ist selbst bei ausdrücklichem Widerspruch der Arbeitnehmerin verpflichtet, dem Betriebsrat eine mitgeteilte Schwangerschaft unter namentlicher Nennung der Arbeitnehmerin mitzuteilen. Weder das Persönlichkeitsrecht, noch Datenschutzrecht steht dem entgegen (in Anlehnung an BAG, 1 ABR 6/67, entgegen BVerwG 6 P 30/87).

Sachverhalt:

I. Die Beteiligten streiten über die Verpflichtung, ob dem Beteiligten zu 1) durch die Beteiligte zu 2) bekanntwerdende Schwangerschaften von Arbeitnehmerinnen des Betriebes namentlich mitgeteilt werden müssen.

Der Beteiligte zu 1) ist der im Betrieb der Beteiligten zu 2) in A-Stadt gebildete Betriebsrat. Seit Mitte 2015 räumt die Beteiligte zu 2) im Falle der Anzeige einer Schwangerschaft durch eine Arbeitnehmerin dieser schriftlich die Möglichkeit ein, einer Information des Betriebsrates hierüber zu widersprechen. Die Schwangere erhält ein Musteranschreiben der Beteiligten zu 2) (ab Bl. 34 d. A.) mit folgendem Passus:

„Sollten wir bis (2-Wochen-Frist) von Ihnen keine Rückmeldung erhalten, werden wir den Betriebsrat über Ihre Schwangerschaft und die damit verbundenen Mutterschutzfristen informieren.“

Im Falle eines Widerspruchs durch die Schwangere wird der Betriebsrat nicht über die Schwangerschaft informiert.

Zeitgleich mit dem Brief an die Mitarbeiterin sendet die Entgeltabrechnung eine vorausgefüllte Gefährdungsbeurteilung an die Führungskraft, einschließlich eines Leitfadens für die Führungskräfte. Die Gefährdungsbeurteilung wird dann durch die Führungskraft durchgeführt, bzw. die Führungskraft organisiert und überwacht die Durchführung der Gefährdungsbeurteilung, wobei bei Bedarf der Werksarzt involviert wird.

Ist kein Widerspruch der Mitarbeiterin bzgl. der Mitteilung über die bestehende Schwangerschaft an den Antragsteller eingegangen, so werden der Beteiligte zu 1), der Werksarzt, das Gewerbeaufsichtsamt und der zuständige Personalreferent durch die Entgeltabrechnung über das Ergebnis der Gefährdungsbeurteilung und die Mutterschutzfristen schriftlich informiert. Liegt hingegen ein Widerspruch der Mitarbeiterin vor, so wird eine Mitteilung wie vorgenannt zum Ergebnis der Gefährdungsbeurteilung an den vorgenannten Adressatenkreis mit Ausnahme des Betriebsrats verschickt.

Soweit sich etwa nach dem Ergebnis der Gefährdungsbeurteilung herausstellen sollte, dass die Mitarbeiterin aufgrund der Schwangerschaft den Arbeitsplatz nicht mehr ausfüllen kann und auch der Arbeitsplatz nicht angepasst werden kann, wird der Beteiligte zu 1) spätestens im Rahmen einer Versetzungsmeldung nach § 99 BetrVG über die Schwangerschaft der Mitarbeiterin informiert.

Mit Beschluss vom 17.10.2016 hat der Betriebsrat die Einleitung des vorliegenden Verfahrens beschlossen.

Der Beteiligte zu 1) war erstinstanzlich der Auffassung, er habe Anspruch auf vollständige Unterrichtung über alle bekanntwerdenden Fälle der Schwangerschaft von Mitarbeiterinnen, auch für den Fall, dass die betroffene Mitarbeiterin einer Information des Betriebsrats widersprochen habe. Denn die Rechte des Betriebsrates stünden nicht zur Disposition der betroffenen Arbeitnehmerinnen. Der Betriebsrat sei zudem nicht Dritter im Sinne des § 28 Abs. 6 Nr.

3 BDSG. Vielmehr habe der Betriebsrat nach § 80 Abs. 1 Nr. 1 BetrVG generell darüber zu wachen, dass im Betrieb geltende Rechtsvorschriften eingehalten würden. Nach § 80 Abs. 2 BetrVG stehe dem Betriebsrat daher auch ein umfassender Informationsanspruch zu, wobei diesen Informations- und Kontrollrechten des Betriebsrates im konkreten Einzelfall auch Vorrang vor einem Vertraulichkeitsinteresse der Arbeitnehmerin zustünde. Nach der Rechtsprechung des Bundesarbeitsgerichts stünde ein entsprechender Unterrichtsanspruch auch in den Fällen zu, in denen die schwangere Mitarbeiterin der Weitergabe widersprochen habe. Der Schutz des Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung stünden dem auch nicht entgegen, da beide Rechte ihre Grenze durch bestehende Gesetze erfahren könnten. Insoweit sei die Grenze durch § 80 BetrVG gesetzt. Insbesondere stünden der schwangeren Mitarbeiterin auch keine überwiegenden schutzwürdigen Interessen zu, die gegen die Information sprechen würden. Zur Begründung des Informationsanspruches bedürfe es auch keiner Darlegung eines anlassbezogenen Sachgrundes für die Information. Es sei lediglich erforderlich, dass ein Aufgabenbezug zu den Aufgaben des Betriebsrats bestehe. Nur wenn dieser offenkundig auszuschießen sei, bestehe keine Unterrichtungspflicht. Ausreichend sei eine Wahrscheinlichkeit für das Bestehen einer Betriebsratsaufgabe. Die Rechte des Betriebsrats stünden gerade nicht zur Disposition des Arbeitnehmers, da insbesondere der Unterrichtsanspruch des Betriebsrats gerade auch der selbständigen Prüfung diene, ob zu Gunsten des Mitarbeiters Schutzmaßnahmen seitens des Betriebsrats angeregt werden müssten. Außerdem sei zu berücksichtigen, dass die Beteiligte zu 2) nach Mitteilung durch die schwangere Mitarbeiterin zudem auch andere Personen über die Schwangerschaft unterrichtete. Die Weitergabe an den Betriebsrat sei keine Weitergabe an einen Unbefugten.

Der Beteiligte zu 1) beantragte erstinstanzlich:

Der Beteiligten zu 2) wird aufgegeben, den Beteiligten zu 1) über alle bekanntwerdenden Fälle der Schwangerschaft von Arbeitnehmerinnen im Betrieb der Beteiligten zu 2) in A-Stadt unaufgefordert namentlich zu unterrichten, auch in den Fällen, in denen die betroffene Arbeitnehmerin einer Unterrichtung des Beteiligten zu 1) widersprochen hat.

Die Beteiligte zu 2) beantragte erstinstanzlich:

Abweisung des Antrages.

Die Beteiligte zu 2) war erstinstanzlich der Auffassung, dass der Betriebsrat bei Widerspruch durch die Schwangere nicht über die Mitteilung der Schwangerschaft der Mitarbeiterin zu informieren sei. Insoweit überwiege der Schutz des Persönlichkeitsrechts der betroffenen Arbeitnehmerin die Interessen des Betriebsrats an der Information. Der Betriebsrat könne, spätestens nachdem die Schwangerschaft offenkundig geworden sei, nachprüfen, ob Arbeitnehmerschutzvorschriften verletzt worden seien. Aufgrund des Eingriffes in das Persönlichkeitsrecht der Mitarbeiterin sei zu berücksichtigen, dass der Grundsatz der Verhältnismäßigkeit verlange, dass an die Erforderlichkeit der Unterrichtung im Hinblick auf einen sachlich berechtigten Anlass strenge Anforderungen zu stellen seien. Zudem sei es möglich, auch den Betriebsrat in einer allgemeineren Form über den betroffenen Arbeitsplatz der Mitarbeiterin zu informieren, ohne die Schwangere namentlich zu benennen.

Das Arbeitsgericht München hat mit dem angefochtenen Beschluss vom 08.03.2017 dem Antrag stattgegeben. Es hat dies damit begründet, dass der Betriebsrat gem. § 80 Abs. 2 i.V.m. § 80 Abs. 1 Nr. 1 BetrVG verlangen könne, dass ihm die Beteiligte zu 2) die ihr bekanntwerdenden Fälle von Schwangerschaften im Betrieb auch ohne Einwilligung der betroffenen Arbeitnehmerinnen mitteile. Auch ein Widerspruch der Schwangeren sei unbeachtlich. Denn der Arbeitgeber habe den Betriebsrat nach § 80 Abs. 2 Satz 1 BetrVG zur Durchführung seiner Aufgaben rechtzeitig umfassend zu

unterrichten und nach Satz 2 Hs. 1 nach Verlangen die zur Durchführung der Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen. Mit dieser Verpflichtung gehe ein entsprechender Anspruch des Betriebsrats einher, soweit die begehrte Information zur Aufgabenwahrnehmung erforderlich sei. Insoweit zähle es auch zu den Aufgaben des Betriebsrats i.S.v. § 80 Abs. 2 Satz 1 BetrVG, darüber zu wachen, dass die zu Gunsten der Arbeitnehmer geltenden Gesetze, Tarifverträge und Betriebsvereinbarungen durchgeführt würden. Diese Überwachungsaufgabe beziehe sich nicht nur auf Arbeitsschutzgesetze im rechtstechnischen Sinne, sondern auf alle Vorschriften, soweit sie zu Gunsten der Arbeitnehmer wirkten. Diese Überwachungsaufgabe sei auch weder von einer zu besorgenden Rechtsverletzung des Arbeitgebers beim Normvollzug noch vom Vorliegen besonderer Mitwirkungs- oder Mitbestimmungsrechte abhängig. Hieraus folge eine zweistufige Prüfung daraufhin, ob überhaupt eine Aufgabe des Betriebsrats gegeben sei und ob im Einzelfall die begehrte Information zu ihrer Wahrnehmung erforderlich sei. Der entsprechende Aufgabenbezug liege vor, da der Betriebsrat auch die Einhaltung der Bestimmungen des Mutterschutzgesetzes sowie sonstiger arbeitsschutzrechtlicher Vorschriften (u.a. auch MuSchArbV) im Betrieb zu überwachen habe. Zwar ergebe sich aus dem Mutterschutzgesetz selbst kein ausdrücklicher Unterrichtsanspruch, anders als etwa im Rahmen des betrieblichen Eingliederungsmanagements. Jedoch sei nach der Entscheidung des Bundesarbeitsgerichts vom 27.02.1968 (1 ABR 6/67) aus der Vorschrift in § 5 Abs. 1 Satz 4 MuSchG nicht abzulesen, dass der Gesetzgeber damit seinen Willen zum Ausdruck gebracht hätte, dem Betriebsrat das Auskunftsrecht zu versagen. Die Frage, ob dem Betriebsrat das Auskunftsrecht zustehe, sei nicht eine solche des Mutterschutzrechts, sondern betriebsverfassungsrechtlicher Natur. Es sei zwar nach dem Mutterschutzgesetz die Mitteilung der werdenden Mutter und des Bestehens der Schwangerschaft an unbefugte Dritte verboten. Jedoch stelle sich die Frage der Unbefugtheit nach dem Betriebsverfassungsgesetz. Aus diesem sei ein Verbot der Weitergabe an den Betriebsrat nicht abzuleiten. Der Aufgabenbezug nach § 80 Abs. 1 Nr. 1 BetrVG werde auch durch die Regelung in § 89 Abs. 1 BetrVG verstärkt. Nach dieser Vorschrift sei der Betriebsrat nicht nur berechtigt, sondern sogar verpflichtet, auf dem Gebiet des Mutterschutzgesetzes gleichberechtigt mit dem Arbeitgeber zusammen tätig zu werden. Zwar hätten die Gewerbeaufsichtsämter die entsprechende Aufsicht über die Ausführung der Vorschriften des Gesetzes und der danach erlassenen Vorschriften, nach der Fassung der § 89 Abs. 1 sei es aber eine selbständige Pflicht des Betriebsrats, auf die Bekämpfung der Gesundheitsgefahren zu achten. Die begehrte Auskunft sei auch zur Erfüllung dieser Aufgaben erforderlich. Insofern sei der Umfang der Information auch davon abhängig, in welchem Umfang der Betriebsrat bereits über Kenntnisse verfüge. Der Betriebsrat verfüge aber über keine anderweitigen Kenntnisse über das Vorliegen von Schwangerschaften im Betrieb. Insbesondere reiche es nicht aus, dass der Betriebsrat bis zur Offensichtlichkeit der Schwangerschaft keine Information erhalte. Denn der Zeitpunkt der Erkenntlichkeit der Schwangerschaft sei zudem unterschiedlich, darüber hinaus sei es dem Betriebsrat nicht zuzumuten, den Betrieb nach ersichtlich schwangeren Mitarbeiterinnen zu durchsuchen. Die eventuell im Zusammenhang mit § 99 BetrVG erfolgende Information reiche nicht aus, da die Überwachungsaufgabe des Betriebsrats schon früher greife. Die Wahrnehmung der Aufgaben des Betriebsrats stünde nach der Konzeption des BetrVG auch nicht zur Disposition des Arbeitnehmers. Daher stehe ein Widerspruch dieser Information auch nicht entgegen. Der Betriebsrat sei auch nicht Dritter i.S.d. § 5 Abs. 1 Satz 4 MuSchG. Dabei komme es auch nicht darauf an, ob die Arbeitnehmerin ihrerseits eine Verpflichtung habe, die Schwangerschaft dem Arbeitgeber mitzuteilen. Jedenfalls habe der Arbeitgeber die Angelegenheit

nach erfolgter Mitteilung dieser Information an den Betriebsrat weiterzugeben, weil hierdurch auch das Überwachungsrecht des Betriebsrats ausgelöst würde. Auch datenschutzrechtliche Gründe stünden der Information nicht entgegen. Denn nach § 28 Abs. 6 Nr. 3 BDSG sei das Erheben, Verarbeiten und Nutzen besonderer Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG für eigene Geschäftszwecke auch ohne Einwilligung des Betroffenen zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich sei und kein Grund zu der Annahme bestehe, dass schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiege. Es bestehe insbesondere kein Grund zur Annahme, dass das schutzwürdige Interesse der jeweilig betroffenen Arbeitnehmerin das Interesse des Arbeitgebers an der Datenerhebung überwiege. Denn hierdurch würden erhebliche Schutzmaßnahmen zu Gunsten der Schwangeren ausgelöst. Die Übermittlung der Daten an den Betriebsrat sei auch keine Datenübermittlung an einen Dritten, weil der Betriebsrat nicht Dritter i.S.d. § 3 Abs. 4 Nr. 3 BDSG sei. Überwiegend schutzwürdige Interessen stünden auch nicht der Bekanntgabe des Namens gegenüber dem Betriebsrat entgegen. Das durch Art. 8 Abs. 1 GRK gewährleistete Recht auf Schutz der eine Person betreffenden personenbezogenen Daten werde ausreichend dadurch gewahrt, dass der Betriebsrat in Bezug auf Gesundheitsdaten der Arbeitnehmer nicht nur dem Datengeheimnis, sondern auch einer strafbewehrten Verschwiegenheitspflicht unterliege gem. §§ 79 Abs. 1, 120 Abs. 2 BetrVG. Ebenso wie ein Arbeitnehmer aus datenschutzrechtlichen Gründen nicht beanspruchen könne, dass bestimmte Mitarbeiter im Rahmen ihrer Arbeitsaufgaben mit der Verarbeitung seiner persönlichen Daten nicht befasst würden, könne er nicht verlangen, dass eine ebensolche Übermittlung an den Betriebsrat unterbleibe. Dieses Ergebnis werde auch dadurch unterstützt, dass der Arbeitgeber gem. § 2 MuSchArbV verpflichtet sei, nicht nur die werdende Mutter, sondern auch den Betriebsrat über die Ergebnisse einer Gefährdungsbeurteilung gem. § 1 dieser Verordnung und über die zu ergreifenden Maßnahmen für Sicherheit und Gesundheitsschutz am Arbeitsplatz zu unterrichten, sobald dies möglich sei.

Gegen diesen, der Beteiligten zu 2) am 16.03.2017 zugestellten, Beschluss richtet sich die Beschwerde der Beteiligten zu 2) mit Schriftsatz vom 18.04.2017, am gleichen Tag beim Landesarbeitsgericht München eingegangen.

Die Beteiligte zu 2) ist auch im Rahmen der Beschwerde weiterhin der Auffassung, dass die vom Betriebsrat begehrte namentliche Benennung der schwangeren Mitarbeiterin bei erfolgtem Widerspruch nicht geschuldet sei. Die Beteiligte zu 2) stelle den Informationsanspruch des Betriebsrats nach § 80 Abs. 2 BetrVG nicht in Abrede. Dieser Informationsanspruch sei aber nicht unbegrenzt. Denn so wie die Mitarbeiterin schon nach § 5 nicht verpflichtet sei dem Arbeitgeber die Schwangerschaft mitzuteilen, da es sich hierbei um eine Sollvorschrift handle, müsse es der Mitarbeiterin auch freistehen zu bestimmen, ob die Weitergabe an den Betriebsrat erfolgen dürfe. Insoweit sei das Recht einer Schwangeren anzuerkennen, darüber zu bestimmen, wenn sie den Kreis der Kennnisträger möglichst klein halten wolle. Zudem habe sich auch die Rechtsgrundlage, die der Entscheidung des BAG aus dem Jahr 1968 zugrunde gelegen habe, geändert. Es sei nicht mehr von einer Bekämpfung von Unfall- und Gesundheitsgefahren durch den Betriebsrat die Rede, sondern nur noch von einem Einsetzen dafür, dass die Vorschriften eingehalten würden. Entsprechend habe das Bundesverwaltungsgericht den Vorrang des Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung bejaht, soweit kein konkreter Anlass für die Mitteilung des Namens bestehe. Insbesondere sei auch zu berücksichtigen, dass die Schwangere bereits hinreichenden Schutz durch die Mitteilung an die entsprechende Aufsichtsbehörde nach § 20 MuSchG genieße. Die umfas-

senden Befugnisse dieser Behörde würden schon eine ausreichende Überwachung gewährleisten. Des Weiteren sei auch eine Mitteilung des Namens an den Betriebsrat nicht zwingend erforderlich, damit dieser seine Aufgaben erfüllen könne. Denn dem Betriebsrat könne von Seiten des Arbeitgebers auch in einer allgemeineren Art und Weise die Abteilung oder der Bereich mitgeteilt werden, in welcher die Mitarbeiterin beschäftigt ist. Damit könne der Betriebsrat seine Überwachungsaufgabe auch ohne exakte Benennung der Mitarbeiterin erfüllen. Wenn im konkreten Fall dann Zweifel an der Einhaltung der Bestimmungen bestünden, wäre eine entsprechende Mitteilung immer noch möglich. Auch der Verweis auf § 2 MuSchArbV überzeuge nicht, da dieser selbst den Zusatz enthalte, dass die Information erst gegeben werden könne, sobald dies möglich ist. Solange aber die Schwangere der Information nicht zustimme, sei eine Informationsweitergabe nicht möglich. Des Weiteren würden auch datenschutzrechtliche Bestimmungen gegen die Information sprechen. Insoweit würde auch die interne Weitergabe der personenbezogenen Daten vom Arbeitgeber auf den Betriebsrat eine Nutzung personenbezogener Daten darstellen. Diese Informationsweitergabe unterfalle auch nicht § 28 Abs. 6 Nr. 3 BDSG, da es sich bei der Schwangerschaft nicht um ein Gesundheitsdatum und insoweit um kein sensibles Datum gem. § 3 Abs. 9 BDSG handle. Andere Erlaubnistatbestände würden ebenfalls nicht eingreifen. Insbesondere würden § 4 a und § 32 BDSG nicht eingreifen und eine Betriebsvereinbarung nicht vorliegen. Insofern verbliebe es beim Erlaubnistatbestand des § 28 BDSG, insbesondere des § 28 Abs. 1 Nr. 1 Satz 2 BDSG, dessen Interessenabwägung aufgrund des Persönlichkeitsrechts der Schwangeren zu Gunsten derer ausfalle. Bei einer Schwangerschaft handle es sich insbesondere nicht um ein der Geheimhaltungspflicht nach § 79 BetrVG unterfallendes Betriebs- und Geschäftsgeheimnis. Die Argumentation des BAG im Beschluss vom 07.02.2012 (1 ABR 46/10) greife hingegen nicht ein, da insbesondere die Betriebsöffentlichkeit der Schwangerschaft, anders als etwa einer krankheitsbedingten Abwesenheit, nicht gegeben sei.

Der Beteiligte zu 1) ist auch im Rahmen der Beschwerde weiterhin der Auffassung, dass ein entsprechender Unterrichtsanspruch bestehe. Ein überwiegendes schutzwürdiges Interesse der Schwangeren an der Nichtweitergabe der Information liege nicht vor, da die Schwangere sich durch Bekanntgabe der Schwangerschaft an den Arbeitgeber bereits entschlossen habe, die Information, zumindest teilweise, öffentlich zu machen. Die dem Betriebsrat nach dem Betriebsverfassungsgesetz eigens zustehenden Rechte könnten nicht durch einzelindividualrechtliche Ansprüche von Arbeitnehmern eingeschränkt werden. Insbesondere sei zu berücksichtigen, dass auch der Betriebsrat hinreichend zur Verschwiegenheit verpflichtet sei, sei es aus dem Betriebsverfassungsgesetz heraus oder auch aufgrund von § 5 BDSG. Der Betriebsrat sei nicht unbefugter Dritter i.S.d. § 5 Abs. 1 Satz 4 MuSchG. Die Rechtsprechung des Bundesarbeitsgerichts aus dem Jahr 1968 sei weiterhin gültig, insbesondere seien vielmehr die Aufgaben des Betriebsrats noch gegenüber dem damaligen Zustand erweitert worden. Vor allem müsse der Betriebsrat prüfen können, ob er tätig werden müsse. Ohne entsprechende Mitteilung würde dieses Recht dem Betriebsrat genommen. Die verfassungsrechtlich gewährleisteten Schutzbereiche des Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung würden ihre Grenzen in den Vorschriften der Gesetze finden, so dass § 80 BetrVG den entsprechenden Unterrichtsanspruch auch gegenüber den verfassungsrechtlich gewährleisteten Rechten durchsetzen könne. Zwar sei gegebenenfalls der Schutz der Schwangeren durch andere Stellen gewährleistet. Die Aufgabe des Betriebsrats bestehe aber gerade darin, die Einhaltung dieses Schutzes zu überwachen. Insofern sei es auch nicht ausreichend, wenn nur allgemeine Informationen über betroffene Arbeitsplätze weitergegeben würden, weil insbesondere in größeren Abteilungen möglicherweise der Betriebsrat dann darauf

angewiesen wäre, verschiedene Mitarbeiterinnen nach der Schwangerschaft zu fragen. Gerade das würde aber die Schwangerschaft noch weiter bekannt machen. Auch der Zusatz in § 2 MuSchArbV hindere nicht die Information, da der Zusatz „sobald es möglich ist“ auf die tatsächliche Möglichkeit abstelle und nicht etwa auf rechtliche Gründe. Auch datenschutzrechtliche Erwägungen stünden nicht entgegen, da der Betriebsrat verantwortlich i.S.d. § 3 Abs. 8 BDSG sei und insoweit auch eine Weitergabe an ihn unschädlich sei. Des Weiteren ermögliche § 32 Abs. 1 Satz 1 BDSG auch die Verarbeitung personenbezogener Daten, da diese für die Durchführung des Beschäftigungsverhältnisses erforderlich sei. Insoweit ergebe sich dies schon aus den dann entstehenden Schutzpflichten zu Gunsten der Schwangeren und der Nebenpflicht gegenüber dem Arbeitgeber, den Betriebsrat zu informieren. Auch unter Berücksichtigung von § 28 BDSG lägen jedenfalls keine überwiegend schutzwürdigen Interessen der Schwangeren vor.

Im Übrigen wird auf die Schriftsätze vom 18.04.2017, 10.05.2017, 16.06.2017, 18.07.2017 sowie auf die Sitzungsniederschrift Bezug genommen.

Aus den Gründen:

II. 2. Die Beschwerde ist unbegründet. Insoweit wird auf die absolut zutreffende und ausführliche Begründung des erstinstanzlichen Beschlusses Bezug genommen. Zu den näheren Ausführungen in der Beschwerdeinstanz sind folgende Anmerkungen veranlasst:

a) Zu Recht hat das Arbeitsgericht einen Informationsanspruch im Hinblick auf die namentliche Benennung von schwangeren Mitarbeitern aus § 80 Abs. 1 Nr. 1 i.V.m. mit Abs. 2 Satz 1 BetrVG angenommen. Insbesondere zur Überwachung der Einhaltung von Arbeitsschutzvorschriften, wie etwa des Mutterschutzgesetzes und der in diesem Zusammenhang ergangenen Verordnungen, besteht die Informationspflicht, auch im Zusammenhang mit den Aufgaben nach § 89 BetrVG.

Denn nach § 80 Abs. 2 Satz 1 BetrVG hat der Arbeitgeber den Betriebsrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten und nach Satz 2 Hs. 1 auf Verlangen die zur Durchführung der Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen. Dabei geht mit dieser Verpflichtung ein entsprechender Anspruch des Betriebsrats einher, soweit die begehrte Information zur Aufgabenwahrnehmung erforderlich ist (vgl. BAG Beschluss v. 07.02.2012 – 1 ABR 46/10; Beschluss v. 15.03.2011 – 1 ABR 112/09). Diese Überwachungsaufgabe nach § 80 Abs. 1 Nr. 1 BetrVG dahingehend, dass die zu Gunsten der Arbeitnehmer geltenden Gesetze, Tarifverträge und Betriebsvereinbarungen durchgeführt werden, ist weder von einer zu besorgenden Rechtsverletzung des Arbeitgebers beim Normvollzug noch vom Vorliegen besonderer Mitwirkungs- oder Mitbestimmungsrechte abhängig (vgl. BAG Beschluss v. 24.01.2006 – 1 ABR 60/04). Maßgeblich ist lediglich, im Sinne einer zweistufigen Prüfung, worauf bereits das Arbeitsgericht hingewiesen hat, ob überhaupt eine Aufgabe des Betriebsrats gegeben ist und ob im Einzelfall die begehrte Information zur Wahrnehmung erforderlich ist.

b) Der entsprechende Aufgabenbezug liegt unstreitig auch zwischen den Beteiligten vor. Auch die Beteiligte zu 2) bestreitet nicht, dass die entsprechende Information, d.h. die namentliche Benennung der Mitarbeiterin, Bezug zur wahrzunehmenden Aufgabe, der Überwachung, etwa des Mutterschutzgesetzes, hat. Die Beteiligte zu 2) ist lediglich der Auffassung, dass dieser Aufgabenbezug zum einen durch die verfassungsrechtlich gewährleisteten Rechte auf Schutz des Persönlichkeitsrechts und auf informationelle Selbstbestimmung eingeschränkt ist und zudem auch die namentliche Benennung nicht zwingend erforderlich sei.

Entgegen der Auffassung der Beteiligten zu 2) ist aber die Mitteilung der Schwangeren durchaus für die Wahrnehmung des Betriebsrats erforderlich. Ein etwa ebenso wirksamer und daher in die Rechte

der Schwangeren weniger eingreifender Schutzmechanismus und eine Möglichkeit, die Aufgabenerfüllung des Betriebsrats dennoch zu ermöglichen, liegt insbesondere nicht in der Möglichkeit der Aufsichtsbehörden, entsprechende Überwachungsaufgaben zu übernehmen, wie sie das Mutterschutzgesetz vorsieht, ebenso wenig in einer Mitteilung etwa nur der allgemeinen Abteilung oder des Arbeitsplatzes im Allgemeinen ohne namentliche Benennung der Mitarbeiterin.

aa) Zu Recht hat das Arbeitsgericht, ebenso wie auch der Beteiligte zu 1) darauf hingewiesen, dass grundsätzlich die Aufgaben des Betriebsrats nicht zur Disposition des Arbeitnehmers stehen (vgl. BAG Beschluss v. 07.02.2012 – 1 ABR 46/10, Rn. 17). Insoweit ist schon von Seiten der gesetzlichen Konzeption her eine Einwilligung oder etwa auch ein Widerspruch der Arbeitnehmerin nicht erforderlich bzw. maßgeblich.

bb) Darüber hinaus sind die Aufgaben des Betriebsrats auch nicht durchweg durch die Aufsichtsbehörden übernehmbar. Zum einen ist hier zu berücksichtigen, dass die Aufsichtsbehörde als außenstehende Einrichtung schon nicht die entsprechenden Einsichtsmöglichkeiten und Erkenntnisse haben wie der Betriebsrat, trotz aller Informationsmöglichkeiten, die etwa nach dem Mutterschutzgesetz bestehen, es zudem um Aufgaben des Betriebsrats geht und nicht um die Aufgaben der Aufsichtsbehörden – zumal schon fraglich ist, ob aufgrund der personellen Ausstattung der Aufsichtsbehörden überhaupt ein maßgeblicher Schutz der Mitarbeiter gewährleistet ist. Gerade in diesem Zusammenhang sieht auch § 89 Abs. 1 Satz 2 BetrVG vor, dass zur Bekämpfung von Unfall- und Gesundheitsgefahren die für den Arbeitsschutz zuständigen Behörden durch den Betriebsrat durch Anregung, Beratung und Auskunft zu unterstützen sind. Gerade der Punkt „Anregung“ zeigt, dass nicht erst etwa auf Initiative der Aufsichtsbehörde hin der Betriebsrat tätig werden kann und soll, sondern dieser schon von sich aus tätig werden darf. Denn § 89 Abs. 1 Satz 2 BetrVG begründet nicht nur ein Recht, sondern zugleich eine öffentlich rechtliche Pflicht des Betriebsrats, die zuständigen öffentlichen Stellen zu unterstützen (vgl. BAG Beschluss v. 03.06.2003 – 1 ABR 19/02, Rz. 33).

cc) Der Betriebsrat kann auch nicht mit einer „abgespeckten“ Information über die allgemeine Abteilung oder eine bestimmte Arbeitsgruppe oder allgemeine Beschreibung des Arbeitsplatzes seinen Schutzaufgaben hinreichend nachkommen. Dabei ist schon fraglich, ob nicht gerade etwa in kleineren Betrieben bereits die Information über den entsprechenden Arbeitsplatz letztlich einer namentlichen Benennung der Schwangeren Mitarbeiterin gleichkäme. Zu Recht verweist der Betriebsrat darauf, dass es bei einer relativ allgemeinen Benennung darauf hinauslaufen würde, dass der Betriebsrat in dem entsprechenden Bereich sich zum einen überlegen müsste, welcher Arbeitsplatz jetzt letztlich betroffen sein könnte, zudem auch nicht auf die gerade individuelle Position der Mitarbeiterin sein Augenmerk ausrichten kann. Die Situation der Schwangeren kann aber selbst bei gleichen Arbeitsplätzen eine ganz unterschiedliche sein, gerade im Hinblick etwa auf ihre persönlichen Verhältnisse oder ihre Konstitution. So könnten bei unterschiedlichem Alter oder unterschiedlicher gesundheitlicher Lage ganz unterschiedliche Schutzpflichten entstehen. Letztlich könnte es tatsächlich darauf hinauslaufen, dass der Betriebsrat durch eigene Ermittlungen herausfinden müsste, wer gegebenenfalls die Schwangere ist. Dies kann dem Betriebsrat aber nicht zugemutet werden, zumal der Erfolg zweifelhaft wäre. Hinzu kommt auch, dass die Einhaltung der Gesundheitsvorschriften nicht nur die Schwangere selbst betreffen, sondern etwa auch Mitarbeiter, die mit der Schwangeren zusammenarbeiten. Auch diese hätten gegebenenfalls Rücksicht zu nehmen auf den Zustand der Mitarbeiterin. Dies gilt insbesondere für Führungskräfte dahingehend, dass diese keine Arbeiten etwa zuweisen, die die Schwangere nicht ausüben darf. Insoweit besteht gerade die Überwachungsaufgabe des Betriebsrats, ganz unabhängig davon, ob der Arbeitgeber seiner Informations-

pflicht und seinem Informationsrecht gegenüber Führungskräften, wie etwa bei der Beteiligten zu 2), nachkommt. Es geht ja gerade darum, eine entsprechende Überwachung zu ermöglichen. Des Weiteren kann der Betriebsrat etwa auch im Rahmen der Schwangerschaft die Schwangere darüber informieren, welche Rechte und Pflichten sie hat, etwa über die Möglichkeit, einer Nacharbeit zu widersprechen oder sie gerade trotz der Schwangerschaft durchführen zu dürfen. Eine entsprechende Information ohne namentliche Benennung wäre insoweit gar nicht möglich. Daher erscheint es als nicht ausreichend, wenn etwa nur die Arbeitsplätze allgemein benannt würden oder auch etwa nur die Gefährdungsbeurteilung allgemein des Arbeitsplatzes ohne namentliche Konkretisierung an den Betriebsrat weitergegeben würde. Insbesondere wäre es auch Aufgabe des Betriebsrats, gerade zu überwachen, dass eine Gefährdungsbeurteilung durchgeführt wird. Wenn aber der Betriebsrat keinerlei Information über die Schwangere hat, kann er auch den entsprechenden Überwachungsaufgaben nicht nachkommen. Somit ergibt sich, dass jedenfalls ein Aufgabenbezug im Bezug auf die Mitteilung des Namens festzustellen ist und dass diese Information auch zur Durchführung der Aufgabe erforderlich ist.

c) Soweit die Beteiligte zu 2) sich auf die verfassungsmäßigen Rechte der Mitarbeiterin bezogen hat, insbesondere auf den Schutz ihres Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung, so bestehen diese nicht schrankenlos. Die Tatsache der Schwangerschaft ist zwar ein dieser Privatsphäre der Mitarbeiterin zuzuordnender Umstand, der insbesondere auch über das Recht auf informationelle Selbstbestimmung, d.h. welche Mitteilungen aus der Privatsphäre letzten Endes an die Öffentlichkeit gelangen, geschützt ist. Insoweit soll grundsätzlich der Inhaber dieses Rechts selbst darüber bestimmen können, welche Informationen an die Öffentlichkeit geraten (vgl. BAG Urt. v. 27.07.2017 – 2 AZR 681/16). Grundsätzlich schützen Art. 1 und Art. 2 GG das allgemeine Persönlichkeitsrecht und damit die Privatsphäre des Einzelnen. Davon umfasst wird auch der Schutz vor der Offenlegung personenbezogener Daten, und zwar auch solcher, die der betroffene Dritte bereits offenbart hat (BAG Urteil v. 06.06.1984 – 5 AZR 286/81). Es ist insbesondere auch zu beachten, dass die Tatsache der Schwangerschaft ein der Intimsphäre der Schwangeren zuzuordnender Umstand ist. Dieser ist auch grundsätzlich besonders geschützt.

Andererseits besteht dieser Schutz nicht schrankenlos, sondern insbesondere in Abwägung zu den Interessen, die etwa auch im Rahmen gesetzlicher Vorschriften, wie sie etwa in den §§ 80 und 89 BetrVG formuliert sind, vorliegen. Dabei sind insbesondere die Interessen, die hinter diesen gesetzlichen Normen stehen, im Hinblick auf Verhältnismäßigkeit, also Erforderlichkeit, Eignung und Angemessenheit zum Zweck dem Interesse des Arbeitnehmers am Schutz seiner Privatsphäre und informationeller Selbstbestimmung gegenüberzustellen. Letztlich ergibt die Interessenabwägung aber hier die Wahrung der Verhältnismäßigkeit unter Berücksichtigung der Interessen des Betriebsrates, wie sie ihm kraft Gesetzes zugewiesen werden.

Zur Erforderlichkeit kann auf das oben unter 2. B) cc) Dargelegte verwiesen werden. Die Mitteilung des Namens ist auch geeignet, den Zweck dieser Mitteilung, die Ausübung der Aufgaben des Betriebsrates zu ermöglichen, zu erfüllen.

Die namentliche Nennung ist schließlich auch angemessen. Sie geht nicht über das zur Erreichung des Zweckes Erforderliche hinaus. Denn ein milderer, die Schwangere weniger belastendes Mittel ist, wie oben dargelegt, gerade nicht gegeben. Des Weiteren ist zu berücksichtigen, dass der Betriebsrat gerade im Interesse der Mitarbeiterin tätig wird, indem zu Gunsten der betroffenen Mitarbeiterin die Einhaltung der Schutzvorschriften überprüft wird. Des Weiteren ist auch zu berücksichtigen, dass letztlich mit der Mitteilung

der Arbeitnehmerin an den Arbeitgeber und in Folge der damit verbundenen Mitteilungspflichten gegenüber der Aufsichtsbehörde oder auch gegenüber den Führungskräften eine gewisse Öffentlichkeit der Schwangerschaft ohnehin eintritt. Genauso wie also der Arbeitgeber gegenüber den Führungskräften die Schwangerschaft mitteilen darf, damit diese den gesetzlichen Schutzpflichten, etwa auch zur Erstellung einer Gefährdungsbeurteilung, nachkommen können, muss die entsprechende Verpflichtung auch gegenüber dem Betriebsrat bestehen, der gerade ja überwachen soll, ob der Arbeitgeber seine Schutzpflichten nachkommt. Dies vor allem auch im eigenen Interesse der Schwangeren. Wie bereits oben dargestellt, wäre dem Betriebsrat auch nicht durch eine etwas abgespeckte Version der Information gedient, so dass auch der Grundsatz der Verhältnismäßigkeit im Sinne einer fehlenden Erforderlichkeit der Information zur Aufgabenerfüllung der Mitteilung des Namens nicht entgegensteht.

d) Der Information über den Namen der Mitarbeiterin steht auch nicht etwa Datenschutzrecht entgegen.

aa) Bei der Mitteilung der Schwangerschaft handelt es sich um mitteilungssensitive Daten i.S.d. § 3 Abs. 9 BDSG. Denn hierbei handelt es sich um Angaben zur Gesundheit. Zwar mag die Schwangerschaft als solche keine Krankheit sein und insoweit sich die Frage stellen, ob es sich hier um ein Gesundheitsdatum handelt. Andererseits ist gerade der Schutz der Schwangeren und des ungeborenen Kindes darauf ausgerichtet, deren Gesundheit zu schützen. Insofern besteht durchaus eine erhebliche Verknüpfung zur Gesundheit der entsprechenden Mitarbeiterin und damit ein sensibles Datum im Sinne dieser Vorschrift (vgl. Seifert, in: Simitis BDSG, 8. Aufl. § 32, Rn. 63, 65). Abgesehen davon, dass Datenschutzrecht an und für sich im Verhältnis Arbeitgeber/Betriebsrat ohnehin nur eingeschränkt zum Tragen kommt, weil der Betriebsrat nicht Dritter i.S.d. § 3 Abs. 4 Nr. 3 BDSG anzusehen ist, sondern vielmehr selbst Teil dieser Stelle ist (vgl. BAG Beschluss v. 07.02.2012 – 1 ABR 46/10), ist jedenfalls die Übermittlung der Daten nach § 28 Abs. 6 Nr. 3 BDSG auch dann zulässig, wenn der Mitarbeiter der Weitergabe der Daten nicht zugestimmt hat, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt. Insofern ist auch nicht § 32 BDSG einschlägig, da § 28 Abs. 6 Nr. 3 BDSG als speziellere Regelung vorgeht.

bb) Abgesehen von der vorzunehmenden Interessenabwägung, die schon beim allgemeinen Persönlichkeitsrecht dargelegt wurde, ist auch im vorliegenden Fall zu berücksichtigen, dass entsprechend der in der Entscheidung vom 07.02.2012 (1 ABR 46/10) vorliegenden Fallgestaltung, auch hier das vorliegende Informationsrecht gerade dem Schutz des Arbeitnehmers, also insbesondere etwa der Erhaltung seines Arbeitsplatzes, insbesondere aber auch seiner Gesundheit und der Gesundheit des ungeborenen Kindes dient. Die namentliche Mitteilung der Mitarbeiterin dient gerade dazu, den besonderen Schutz etwa des Mutterschutzgesetzes, im Hinblick auf die Ausgestaltung ihres Arbeitsplatzes und im Hinblick auf ihre persönliche Situation zu überwachen. Der Schutz geht damit sogar noch über die wirtschaftliche Komponente des Schutzes des Arbeitsplatzes hinaus, weil hier gerade das Leben sowohl der Schwangeren wie deren Gesundheit und das des ungeborenen Kindes geschützt werden sollen. Daher ist auch der etwas gravierendere Eingriff in die Rechte der Mitarbeiterin, der darin liegt, dass die Schwangerschaft den Betriebsräten bekannt gegeben wird, gerechtfertigt, während etwa im Rahmen des betrieblichen Eingliederungsmanagements keine Krankheitsursachen, sondern nur die Krankheitszeiten an sich mitgeteilt werden. Neben der Tatsache, dass durch die Mitteilung der Mitarbeiterin an den Arbeitgeber oh-

nehin eine gewisse Öffentlichkeitswirkung der Schwangerschaft nach Außen verbunden ist, ist insbesondere auch zu berücksichtigen, dass gerade der Betriebsrat aufgrund der datenschutzrechtlichen Vorschriften und § 5 BDSG aber auch aufgrund der Verschwiegenheitspflichten im Zusammenhang mit dem Betriebsverfassungsgesetz, § 79 BetrVG, einer erheblichen Schweigepflicht unterliegt und insofern auch ein hinreichender Schutz der Daten der Schwangeren gewährleistet ist. Mag auch eine gewisse Skepsis im Hinblick auf diese Geheimhaltung gegeben sein, so wäre auch eine Weitergabe etwa an Mitarbeiter der Personalabteilung dann nicht möglich, weil für diese Gleiches gelten würde. Gerade aber zur Verrichtung der gesetzlichen Aufgaben, zur Durchführung des Arbeitsverhältnisses, wie auch zur Überwachung der Schutzmechanismen, muss aber der Schutz über die Verschwiegenheitspflicht als grundsätzlich ausreichend angesehen werden.

Da somit überwiegende Interessen der Schwangeren, sei es aufgrund des Persönlichkeitsrechts, oder etwa im datenschutzrechtlichen Sinne nicht ersichtlich sind, der Mitarbeiterin gegenüber den Aufgaben des Betriebsrats auch kein Dispositionsrecht zusteht, besteht der Anspruch des Betriebsrats auf Mitteilung des Namens der Mitarbeiterin, um den gesetzlichen Pflichten und Aufgaben des Betriebsrats nachkommen zu können.

e) Dem steht auch nicht die Entscheidung des Bundesverwaltungsgerichts vom 29.08.1990 – 6 P 30/87 entgegen. Zwar hat das Bundesverwaltungsgericht im Zusammenhang mit einer teilweise wortgleichen Vorschrift aus dem Personalvertretungsrecht nur im Falle eines konkreten Anlasses die Mitteilung des Namens der Schwangeren für zulässig erachtet. Es hat aber im Rahmen der Entscheidung insbesondere darauf abgestellt, auch in Abgrenzung zur Entscheidung des Bundesarbeitsgerichts aus dem Jahr 1968, inwieweit nach dem Betriebsverfassungsgesetz gegebenenfalls eine verschärfte Überwachungspflicht des Betriebsrats besteht. Das Bundesverwaltungsgericht hat eine allgemeine Kontrollfunktion des Personalrats verneint. Das Bundesarbeitsgericht hingegen sieht eine derartige Überwachungsfunktion völlig losgelöst von konkreten Ereignissen, Mitbestimmungsrechten und Vorfällen durchaus als gegeben an. Des Weiteren ist zu berücksichtigen, dass das Bundesverwaltungsgericht die Formulierung der „Bekämpfung von Gesundheits- und Unfallgefahren“ nach altem Recht als maßgebliches Abgrenzungskriterium herangezogen hat. Diese Formulierung findet sich aber nach wie vor in § 89 BetrVG im Zusammenhang mit der Zusammenarbeit des Betriebsrats und der jeweiligen Aufsichtsbehörden. Hier ist durchaus noch die Bekämpfung dieser Gefahren als eine Aufgabe des Betriebsrats vorgesehen.

f) Schließlich steht auch nicht die Formulierung in § 5 Abs. 1 Satz 4 MuSchG, wonach Dritten gegenüber die Mitteilung der werdenden Mutter nicht unbefugt bekanntgegeben werden darf, entgegen, weil der Betriebsrat gerade aufgrund der gesetzlich vorgesehenen Aufgaben nicht Dritter im Sinne dieser Vorschrift ist.

Des Weiteren spricht, wie bereits das Arbeitsgericht festgestellt hat, gerade auch § 2 MuSchArbV dafür, dass eine entsprechende Mitteilung an den Betriebsrat erfolgen darf. Denn die Gefährdungsmittelteilung ist an den Betriebsrat mitzuteilen. Damit dieser tatsächlich diese Gefährdungsbeurteilung vollständig überprüfen kann, ist auch eine Mitteilung des Namens erforderlich, um die Zuordnung des Arbeitsplatzes zum konkreten Mitarbeiter und die dabei bestehenden Gefahren beurteilen zu können.

Somit konnte die Beschwerde der Beteiligten zu 2) keinen Erfolg haben und war zurückzuweisen.

3. Da dem Rechtsstreit, insbesondere auch im Hinblick auf die Entscheidung des Bundesverwaltungsgerichts grundsätzliche Bedeutung zukommt, war die Rechtsbeschwerde zuzulassen. Insofern ist auf die anliegende Rechtsmittelbelehrung zu verweisen.

Ton- und Bildaufnahmen durch den Leistungsberechtigten im Jobcenter (Ls)

(Landessozialgericht München, Beschluss vom 17. Oktober 2017 – L 11 AS 589/17 –)

1. Eine Sozialleistungsbehörde muss sich nur im Rahmen des § 13 SGBX an einen Bevollmächtigten des Leistungsberechtigten wenden.
2. Ton- und Bildaufnahmen eines Leistungsberechtigten von Gesprächen zwischen Mitarbeitern eines Jobcenters und dem Leistungsberechtigten bedürfen wegen des allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) der Erlaubnis der betroffenen Mitarbeiter.

(Nicht amtliche Leitsätze)

Der Einsatz von Wildkameras unterliegt den BDSG-Regeln

(Oberverwaltungsgericht Saarlouis, Urteil vom 14. September 2017 – 2 A 197/16 –)

1. Der Einsatz von Wildbeobachtungskameras unterfällt dem Regelungsregime des Bundesdatenschutzgesetzes. Der Personenbezogenheit der Datenerhebung steht nicht entgegen, dass mit der Wildkamera nur die Aufnahme von Wildtieren beabsichtigt ist, denn es besteht die Möglichkeit, dass Waldbesucher, die nicht damit rechnen müssen, heimlich gefilmt zu werden, in den Fokus der Kamera geraten.
2. Es ist nicht auszuschließen, dass von dem Erfassungsbereich der Tierbeobachtungskamera nicht nur der unmittelbare Bereich der Kirtung erfasst wird, sondern darüber hinaus auch angrenzende Waldflächen. Die Unwägbarkeiten im Hinblick auf Ausrichtung und Erfassungsbereich der Kamera verdeutlichen die Notwendigkeit einer präventiven datenschutzrechtlichen Überprüfung, der die – nur geringfügig in Grundrechte des Klägers eingreifende – Meldepflicht Rechnung trägt.
3. Selbst wenn es sich bei der Kirtung um eine mit einem Betretungsverbot belegte jagdliche Einrichtung handelt, ist die Fläche faktisch für die Öffentlichkeit zugänglich.
4. In dem Beobachten von Kirtungen mittels Tierbeobachtungskameras liegt keine ausschließlich persönliche oder familiäre Tätigkeit des die Jagd als Hobby betreibenden Klägers.

Sachverhalt:

Der Kläger ist Jäger und Jagdpächter im Landkreis A-Stadt. Er begehrt die Feststellung, dass er den Betrieb von Tierbeobachtungs-

kameras, soweit diese zur Beobachtung von Kurrungen dienen, nicht dem Beklagten melden muss.

Das Unabhängige Datenschutzzentrum Saarland hat ein Merkblatt zum datenschutzkonformen Einsatz von Tierbeobachtungskameras in saarländischen Wäldern erstellt. Am Ende des beigefügten Meldebogens befindet sich der Hinweis, dass eine verantwortliche Stelle, wenn sie vorsätzlich oder fahrlässig entgegen § 4d Abs. 1 BDSG, auch in Verbindung mit § 4e Satz 2 BDSG, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht, gemäß § 43 Abs. 1 Nr. 1 BDSG eine Ordnungswidrigkeit begeht, die mit einer Geldbuße bis zu 50.000,- EUR geahndet werden kann.

Am 19.12.2014 hat der Kläger Klage erhoben mit dem Ziel festzustellen, dass er den Betrieb von Wildkameras, soweit diese zur Beobachtung von Kurrungen dienen, nicht dem Beklagten melden müsse. Zur Begründung hat er vorgetragen, dass es sich bei einer Kurrung nicht um einen öffentlichen Raum handle, was aus § 23 Abs. 3 SJK folge, wonach die Kurrung eine jagdliche Einrichtung sei. Gemäß § 49 Abs. 1 Nr. 6 SJK sei das Betreten einer Jagdeinrichtung eine Ordnungswidrigkeit. Daraus folge zwingend, dass das Betreten des Bereichs einer Kurrung verboten sei. Daher könne es sich nicht um einen öffentlichen Raum handeln. Seine Kameras sollten ausschließlich auf den Bereich der jagdlichen Einrichtung ausgerichtet sein. Die ortsübliche Bekanntmachung von Tierbeobachtungskameras sei nicht geboten, da diese keinen öffentlichen Raum filmten. Der Betrieb der Wildkameras sei auch nicht vor Inbetriebnahme anzuzeigen, da sich diese nicht im öffentlichen Raum befänden. Da die Erhebung, Verarbeitung und Nutzung der Daten ausschließlich zu jagdlichen Zwecken erfolge, handle es sich um eine Datenerhebung ausschließlich für persönliche Tätigkeiten. Insofern sei das Bundesdatenschutzgesetz überhaupt nicht anwendbar. Er jage Schwarzwild, das in der Regel an der Kurrung im Dunkeln gejagt werde. Da die Wildschweine regelmäßig die Kurrung aufsuchten, lasse sich über die Aufnahme überprüfen, ob es sich um eine führende Bache mit Frischlingen, die nicht beschossen werden dürfe, oder ob es sich um einen einzelnen Keiler handle. Streitbefangen sei vorliegend allein die Frage, ob mit der Kamera eine Kurrung und damit eine jagdliche Einrichtung beobachtet werden könne und ob es eine diesbezügliche Anzeigepflicht gebe. Eine weitere Funktion hätten diese Kameras nicht. Sie sollten nicht den Wald oder Wanderwege filmen, da sich auf Wanderwegen in der Regel auch keine Kurrungen befänden. Im Übrigen fänden sich Kurrungen in der Regel an Stellen, wo sich keine Personen aufhielten. Entgegen der Auffassung der Beklagten sei eine Kurrung auch problemlos erkennbar, da die Grasnarbe zerstört sei, weil die Wildschweine den Waldboden aufgewühlt hätten. Alle Kameras seien an Stellen angebracht, die sich abseits der öffentlichen Wege befänden, wo Personen üblicherweise nicht spazieren gingen. Da die Verbindung der Kameras nicht auf die Aufzeichnung von Personen oder deren Abschreckung abziele, sondern auf die Aufzeichnung von Wildtieren, fehle es bereits an dem subjektiven Element des „Erhebens“ der Daten. In subjektiver Hinsicht sei ein aktives, auf Datenerlangung gerichtetes Element erforderlich, d.h. ein zielgerichtetes Beschaffen von personenbezogenen Daten, wozu nicht die zufällige Beobachtung zähle. Bei den hier streitbefangenen Wildkameras würden schon nach dem Einsatzzweck keine personenbezogenen Daten zielgerichtet beschafft. Sollten versehentlich Personen aufgenommen werden und deren Daten nicht gleich gelöscht werden, so sei dies eine Frage der „Verarbeitung“ im Datenschutzrecht und keine Frage des „Erhebens“. Er nehme das Erfassen von Daten von Personen auch nicht billigend in Kauf, weil die Kameras an Stellen im Wald aufgehängt seien, an denen keine Personen herumliefen. Es fehle deshalb bereits an dem Anwendungsbereich des § 6b BDSG, da mit einer Wildkamera weder Personen erfasst werden sollten noch Räume, in denen sich Personen üblicherweise aufhielten. Fehle es bereits an einer „Erhebung“, finde bei Speicherung dieser Daten auch eine „Verarbeitung“ im Sinne des BDSG nur dann statt,

wenn die Speicherung zum Zwecke ihrer weiteren Verarbeitung oder Nutzung erfolge (§ 3 Abs. 4 Satz 2 Nr. 1 BDSG). Dies sei jedoch gerade bei dem Einsatz einer Wildkamera zum Zwecke der Jagd unter „Erstspeicherung“ in der Kamera selbst nicht anzunehmen, weil zufällig aufgenommene Personenaufnahmen eben nicht von Interesse seien und auch nicht verarbeitet werden sollten.

Der Beklagte hat beantragt, die Klage abzuweisen.

Er hat vorgetragen, eine gesetzliche Verpflichtung, den Betrieb von Tierbeobachtungskameras, soweit diese zur Beobachtung von Kurrungen dienen, der Beklagten zu melden, ergebe sich aus § 4d Abs. 1 BDSG. Diese Vorschrift verlange, dass Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme von nicht öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde nach Maßgabe von § 4e BDSG zu melden seien. Diese Voraussetzungen seien hier gegeben. Nach § 1 Abs. 2 Nr. 3 BDSG gelte das Gesetz für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie Daten und Einsatz von Datenverarbeitungsanlagen verarbeiteten, nutzten oder dafür erhoben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolge ausschließlich für persönliche oder familiäre Tätigkeiten. Der Kläger sei eine nicht-öffentliche verantwortliche Stelle im Sinne des Gesetzes. Bei der Videoüberwachung mittels Tierbeobachtungskameras handle es sich um eine Erhebung und Verarbeitung (Speicherung) personenbezogener Daten im Sinne des § 3 Abs. 1 BDSG. Die Bildaufnahmen von Personen, die zufällig den Aufnahmebereich der Kamera passierten, stellten personenbezogene Daten dar. Personenbezogene Daten seien nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person. Bestimmbar sei eine Person (nach dem Art. 2 Buchst. a der Richtlinie 95/46/EG), „die direkt oder indirekt identifiziert werden könne, insbesondere durch Zuordnung ... zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen ... Identität seien“. Die im Hinblick auf den Gesetzeszweck weit gefasste Formulierung umfasse jede Information im Sinne der Vermittlung oder des Verfügbarhaltens von Erkenntnissen über eine Person. Darunter falle auch die eine Person betreffende Bildaufnahme, da auch sie im Sinne des Gesetzes Angaben über die tatsächlichen oder persönlichen Verhältnisse der abgebildeten Person beinhalte. Durch das Anbringen und Inbetriebnehmen der Wildkamera eröffne der Kläger die Möglichkeit, dass ohne sein weiteres Zutun personenbezogene Daten bei ihm anfielen. Dabei sei es irrelevant, dass Anlass und Zweck der Kamerainstallation nicht in der Beobachtung von Personen bestünden. Genauso wenig müsse die Verwendung der erhaltenen Informationen beabsichtigt sein. Für das vom Begriff des Beschaffens geforderte aktive und subjektive Element reiche es bereits aus, wenn das Anfallen personenbezogener Daten als unvermeidliche Folge mitakzeptiert werde. Durch die Wahl von Wildkameras als Mittel zur Beobachtung der Gewohnheiten des Wildes an Kurrungen nehme der Kläger die Erfassung von Personen, die zufällig den Aufnahmebereich der Kamera passierten, zumindest billigend in Kauf. Gelangten Personen in den Aufnahmebereich, würden zweifelsfrei personenbezogene Daten gespeichert. Unter Speichern, als Unterfall der Verarbeitung, verstehe das Gesetz, das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung (§ 3 Abs. 4 Satz 1, 2 Nr. 1 BDSG). Sobald der Bewegungsmelder der Wildkameras auslöse, fertige er je nach Vorgabe des Klägers eine bestimmte Anzahl und Folge von Einzelbildern oder eine Videoaufnahme über einen vordefinierten Zeitraum. Auf den so erstellten Aufnahmen sei dann das Objekt zu erkennen, das den Bewegungsmelder auslöse. Die Wildkamera könne keine Unterscheidung vornehmen, ob es sich bei diesem Objekt um einen Menschen oder ein Tier handle, mit der Folge, dass sie unterschiedslos alles aufnehme, was ihren Aufnahmebereich passiere. Hierzu gehörten dann auch Abbildungen von natürlichen Personen, die sich – berechtigt oder unberechtigt

– im Aufnahmebereich der Kamera aufhielten oder diesen passieren. Der mit der Speicherung verfolgte Zweck liege hier in der Kenntnisnahmemöglichkeit für den Kläger, was als Nutzung personenbezogener Daten zu werten sei. Nutzung meine nach § 3 Abs. 5 BDSG jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handle. Es handle sich beim Begriff der Nutzung um einen Auffangtatbestand, der weit auszulegen sei. Die Kenntnisnahme personenbezogener Daten sei ein Fall des Nutzens, ohne dass es auf die Verwendung oder eine Verwendungsabsicht ankomme. Das Anfertigen der Aufnahmen durch die Wildkamera stelle keinen Selbstzweck dar, sondern diene dem Kläger gerade dazu, die Aufnahmen später sichten zu können, um die Gewohnheiten des Wildes zu beobachten. Soweit die Kamera aber anstatt Wild Personen aufgenommen habe – worauf der Kläger keinen Einfluss habe – bekomme er bei der Sichtung der Aufnahmen Kenntnis von personenbezogenen Daten der aufgenommenen Personen. Bei dem Betrieb der Tierbeobachtungskamera handle es sich zudem um ein automatisiertes Verfahren. Automatisiert sei ein Verfahren nach § 3 Abs. 2 BDSG dann, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen stattfinde. Jede Art von Digitalkamera, auch eine Tierbeobachtungskamera, stelle eine solche Datenverarbeitungsanlage dar. Der Betreiber der Wildkamera sei auch verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG, da er die Aufnahmen für eigene Zwecke anfertige. Er entscheide darüber, für welche Zwecke die Aufnahmen, die Ablichtungen von natürlichen Personen enthielten, verwendet würden. In dem Beobachten von Kurrungen mittels Tierbeobachtungskameras liege keine ausschließlich persönliche oder familiäre Tätigkeit, die vom Anwendungsbereich des BDSG ausgenommen wäre. Die Begrifflichkeit der „ausschließlich persönlichen oder familiären Tätigkeit“, sei eng auszulegen und daher restriktiv anzuwenden. Während familiäre Tätigkeiten mit dem Familienleben in Verbindung stünden – was hier offensichtlich nicht der Fall sei – erfasse der Begriff der persönlichen Tätigkeit solche Tätigkeiten, die in enger und objektiver Verbindung mit dem Privatleben einer Person stünden. Bei der hier in Frage stehenden Tätigkeit handle es sich um eine durchweg gesetzlich regulierte Tätigkeit, die über den privaten Aktionskreis hinausgehe. So definiere § 1 BJG das Jagdrecht als die Befugnis und gleichzeitig auch die Beschränkung, auf einem Gebiet wildlebende Tiere, die dem Jagdrecht unterliegen, zu hegen, auf sie die Jagd auszuüben und sie sich anzueignen. Das Aufstellen und Inbetriebnehmen der Tierbeobachtungskamera an einer Kurrung erfolge in Ausübung dieser Jagdtätigkeit mit dem Ziel, mehr über die Gewohnheiten und den Bestand der zu jagenden Wildtiere im eigenen Jagdbezirk zu erfahren. Bereits die Ausübung der Jagd sei von der Erteilung eines Jagdscheins abhängig. Auch in der Errichtung einer Kurrung sei der Jagdausübungsberechtigte nicht frei, sondern er dürfe nach § 23 Abs. 1 i.V.m. Abs. 3 Satz 2 Saarländisches Jagdgesetz (SJG) diese nur mit Einwilligung des Grundstückseigentümers oder Nutzungsberechtigten errichten. Durch die Meldepflicht werde die Aufsichtsbehörde in die Lage versetzt, bereits vorab Empfehlungen für einen datenschutzkonformen Einsatz zu geben – etwa im Hinblick auf die Ausrichtung der Kameras oder Transparenzanforderungen –, um so die Streubereite der Videoüberwachung und die Eingriffe in das Recht auf informationelle Selbstbestimmung zu minimieren oder ganz auszuschließen. Unter einem öffentlich zugänglichen Raum im Sinne des § 6b BDSG seien alle Bereiche – innerhalb und außerhalb von Gebäuden – zu verstehen, die dazu bestimmt seien, von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten oder genutzt werden zu können. Maßgeblich für die Bewertung der Kurrung als öffentlichen Raum sei zunächst die Regelung des § 11 Abs. 2 Satz 1 Saarländisches Naturschutzgesetz (SNG) bzw. § 25 Abs. 1 Landeswaldgesetz (LWaldG). Danach sei es jedermann zum Zwecke der Erholung gestattet, den Wald und die freie Landschaft zu betreten. Auch wenn es sich bei den zu betretenden Flä-

chen um solche handle, die im Privateigentum stünden, widmeten das SNG und das LWaldG diese Flächen der Öffentlichkeit. Der Jagdausübungsberechtigte als Betreiber der Wildkamera und als die Person, die die Kurrung errichte, habe nur eingeschränkt Einfluss darauf, wer die jagdliche Einrichtung zulässigerweise betreten dürfe, denn § 23 Abs. 3 Satz 1 SJG bestimme, dass neben dem Jagdausübungsberechtigten selbstverständlich auch der Eigentümer darüber entscheiden dürfe, wer sein Grundstück und die dort errichtete jagdliche Einrichtung in welchem Umfang betreten dürfe. Aus Sicht des Jagdausübungsberechtigten sei der Personenkreis damit unbestimmt, da er den Kreis der Zutrittsberechtigten nicht abschließend bestimmen könne. Entscheidend sei, dass die Kurrung trotz eines gesetzlich normierten Betretungsverbot faktisch zugänglich sei und bleibe. Die Kurrung sei gerade nicht eingefriedet oder eingegrenzt, da dies ihrem Zweck zuwiderlaufen würde und im Übrigen auch nach § 46a Abs. 1 Nr. 5 der Verordnung zur Durchführung des Saarländischen Jagdgesetzes (DV-SJG) untersagt sei. Eine faktische Zugangsmöglichkeit begründe aber nur dann keine Öffentlichkeit im Sinne des § 6b Abs. 1 BDSG, wenn der entgegenstehende Wille bzw. die Nichtöffentlichkeit aus den Umständen (etwa durch vorhandene Verbotsschilder) oder aus dem Kontext der Umgebung erkennbar werde. Das sei hier aber gerade nicht der Fall. Weder werde durch Anbringung von Hinweisschildern im Umfeld der Kurrung darauf hingewiesen, dass es sich um eine solche handle, noch sei der normale, mit der Jagd nicht vertraute Waldbesucher oder Spaziergänger in der Lage, eine Kurrung als solche zu erkennen bzw. deren flächenmäßige Ausdehnung zu bestimmen. Dies vor allem deshalb, weil § 46a Abs. 1 DV-SJG anordne, dass – vor dem Hintergrund, dass eine Kurrung keine Fütterung sein dürfe – lediglich 2 kg Getreide, Mais oder heimische Früchte (Schwarzwild) bzw. 2 l Trester (Rehwild) ausgebracht werden dürften und dies so, dass es für anderes Schalenwild unzugänglich bleibe. Die fehlende Möglichkeit, die flächenmäßige Begrenzung der Kurrung zu bestimmen, führe auch dazu, dass die Wildkameras durch die Kegelform des Aufnahmebereichs von bis zu 20 m zwingend auch solche Bereiche erfassen, die nicht mehr Teil der Kurrung seien und damit öffentlich zugänglich seien. So werde die Wildkamera regelmäßig nicht nur den engen Bereich der Kurrung erfassen, sondern auch die darüber hinausgehenden angrenzenden Waldflächen, die von Waldbesuchern uneingeschränkt frequentiert werden dürften. Der Waldbesucher gehe davon aus, dass er ein Recht habe, sich im Wald frei zu bewegen. Sollte dieses Recht räumlich eingeschränkt werden, so müsse der Umfang der Einschränkung klar erkennbar sein. Dies gelte umso mehr, wenn ein Verstoß mit einem Bußgeld sanktioniert werde.

Mit dem aufgrund der mündlichen Verhandlung vom 18.5.2016 – 1 K 2102/14 – ergangenen Urteil hat das Verwaltungsgericht des Saarlandes die Klage als unbegründet abgewiesen. Der Kläger unterliege der Meldepflicht nach § 4d Abs. 1 BDSG.

Aus den Gründen:

Die zulässige Berufung des Klägers ist unbegründet.

Mit Recht hat das Verwaltungsgericht die Klage als unbegründet abgewiesen. Der Kläger ist nach dem zum für die Beurteilung der Sach- und Rechtslage maßgeblichen Zeitpunkt der mündlichen Verhandlung geltenden § 4d Abs. 1 BDSG verpflichtet, den Betrieb von Tierbeobachtungskameras, soweit diese zur Beobachtung von Kurrungen dienen, zu melden. Nach der genannten Vorschrift sind Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde (vgl. § 28a Abs. 1 SDSG i.V.m. § 38 BDSG) nach Maßgabe von § 4e zu melden. Mit der Meldepflicht soll die Transparenz der Verarbeitung personenbezogener Daten erhöht werden.

Der Einsatz von Tierbeobachtungskameras an Kurrungen unterfällt dem Regelungsregime des Bundesdatenschutzgesetzes.

Das Bundesdatenschutzgesetz ist anwendbar, wenn personenbezogene Daten Gegenstand einer vom Gesetz geregelten Phase der Datenverarbeitung sind. Nach § 1 Abs. 2 Nr. 3 BDSG gilt dieses Gesetz für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person; letztere wird als Betroffener legaldefiniert. Automatisierte Verarbeitung wird in § 3 Abs. 2 BDSG als Erhebung, Verarbeitung oder Nutzung personenbezogener Dateien unter Einsatz von Datenverarbeitungsanlagen bezeichnet. Nicht-öffentliche Stellen sind gemäß § 2 Abs. 4 Satz 1 BDSG u.a. natürliche Personen.

Die Aufzeichnungen im Rahmen der Videoüberwachung einer Kirtung mit Wildkameras stellen eine Erhebung und Verarbeitung (Speicherung) personenbezogener Daten im Sinne des § 3 Abs. 1 BDSG dar.

Bei einer Wildkamera handelt es sich um eine Kameraeinheit, die mit einem elektronischen Sensor kombiniert wird, der in der Regel auf Wärme und Bewegung reagiert (Bewegungsmelder). (vgl. Dienstbühl, Der Einsatz von „Wildkameras“ durch Privatpersonen – Zur Frage der datenschutzrechtlichen Zulässigkeit der Videoüberwachung im Wald, NuR 2012, 395). Kommt ein Tier oder ein Mensch in den Erfassungsbereich des Bewegungsmelders, wird nach einer kurzen Zeitverzögerung ein elektronischer Impuls erzeugt, der wiederum – je nach Modell und Einstellung – einzelne Fotos oder eine Videosequenz auslöst. Eine Differenzierung des in den Erfassungsbereich eindringenden Objekts – Mensch oder Tier – kann das Gerät nicht vornehmen. Infrarottechnik ermöglicht Nachtaufnahmen ohne sichtbaren Blitz. Die digitalen Bilder und Videos, auf denen neben dem Datum auch die Uhrzeit der Aufnahme zu finden ist, werden auf einer herausnehmbaren Speicherkarte gespeichert und können auf dem PC gesichtet und bearbeitet werden. Das wetterfeste Gehäuse der Kamera ist farblich der Umgebung angepasst. Primärer Zweck der Wildkamera ist, dass der Jäger seine Ansitze gezielt planen kann (vgl. Dienstbühl, a.a.O.: „Eine Wildkamera ist der unsichtbare Jagdaufseher im Revier. Sie dokumentiert, welche Wildarten zu welcher Uhrzeit die Kirtungen aufsuchen und ob beispielsweise Trophäenträger dabei sind.). Daher finden sich solche Kameras für gewöhnlich direkt an Kirtungen, die mit einem Schirm (Erdsitz) oder Hochsitz ausgestattet sind, von dem aus das Wild erlegt werden kann. Mit Hilfe der Foto- und Videodateien kann der Jäger bestimmen, wo mit welchem Wild zu welcher Zeit zu rechnen ist und in welcher Konstellation es auftritt (Dienstbühl, a.a.O., S. 395). Als Kirtung wird ein Platz zum Ausbringen von Getreide oder Mais oder anderen nichtfleischlichen Stoffen, die von Wild als Nahrung gesucht werden, bezeichnet. Sinn einer Kirtung ist es, das Wild an einen bestimmten Platz zu locken und dort ausreichend lange zu beschäftigen, um es bejagen und/oder beobachten zu können. Kirtungen werden entsprechend der zu kirtenden Wildart offen ausgelegt, eingegraben oder durch Behälter gesichert, die bei Bewegung Kirrgut abgeben (zitiert nach: wikipedia).

Entgegen der Ansicht des Klägers steht der Personenbezogenheit der Datenerhebung nicht entgegen, dass er mit dem Einsatz der Wildkamera keine Daten von Personen, sondern ausschließlich von Wildtieren, die eine Kirtung aufsuchen, sam-

eln möchte, denn es besteht die Möglichkeit, dass Waldbesucher, die nicht damit rechnen müssen, heimlich gefilmt zu werden, in den Fokus der Tierbeobachtungskamera geraten können. Nach § 25 Abs. 1 Landeswaldgesetz (vom 26.10.1977, zuletzt geändert durch das Gesetz vom 26.6.2013; Amtsbl. I S. 268 – LwaldG –) ist das Betreten des Waldes jedermann zum Zweck der naturverträglichen Erholung gestattet. Beim Wald handelt es sich demzufolge um einen öffentlichen Raum, der für jedermann zu Erholungszwecken zugänglich ist. (Becker, in: Plath BDSG/DS-GVO, 2. Aufl. 2016, § 6 b; Scholz, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl. 2014 § 6 b Rdnr. 42). Aus dieser Zweckbestimmung folgt das Recht des Waldbesuchers, im Rahmen seiner privaten Freizeitgestaltung unbeobachtet zu bleiben, d.h. er muss nicht befürchten, Gegenstand einer Videoüberwachung zu werden. Das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG vermittelt jedem einen Anspruch auf Achtung und Entfaltung seiner Persönlichkeit und auf den Schutz seines Privatbereichs (BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 u.a. („Volkszählungsurteil“); juris; NJW 1984, 419). Es umfasst auch die Freiheit vor unerwünschten Videoaufnahmen (BVerfG, Beschluss vom 11.8.2009 – 2 BvR 941/08 –, juris). Da die Wildkamera keine Unterscheidung vornehmen kann, ob es sich bei dem Objekt, das den Bewegungsmelder auslöst, um einen Menschen oder ein Tier handelt, ermöglicht sie auch Abbildungen von Personen, die sich im näheren Umfeld der im öffentlichen Raum gelegenen Kirtung bewegen und von der Kameraperspektive noch erfasst werden. Der Kläger schafft daher durch das Anbringen, das Ausrichten und die Inbetriebnahme der Tierbeobachtungskamera die Voraussetzungen dafür, dass personenbezogene Daten bei ihm anfallen. Auf die tatsächliche Kenntnisnahme der Daten oder auf deren Speicherung kommt es nicht an, denn für das „Erheben“ i.S.v. § 3 Abs. 3 BDSG reicht es aus, dass die Zugriffsmöglichkeit besteht (vgl. Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 3, Rdnr. 106). Es muss nicht die Absicht bestehen, die Informationen personenbezogen zu verwenden (Dammann in: Simitis, BDSG, § 3 Rdnr. 105).

Der Einwand des Klägers, es gehe im vorliegenden Fall (allein) um die Meldepflicht von Beobachtungskameras, die ausschließlich auf den engen Bereich der Kirtung ausgerichtet seien, für die als jagdliche Einrichtung ein Betretungsverbot bestehe und die daher der Öffentlichkeit nicht zugänglich sei, steht der Anwendbarkeit der datenschutzrechtlichen Bestimmungen nicht entgegen. Es ist bereits fraglich, ob überhaupt die Möglichkeit besteht, den Aufnahmebereich der Kamera derart zu fokussieren, dass tatsächlich nur der Bereich der sich im öffentlichen Raum befindlichen und nicht eingefriedeten Kirtung aufgezeichnet wird. Zweifel daran bestehen deshalb, weil durch die Kegelform des Aufnahmebereichs von bis zu 20 m zwingend auch solche Bereiche erfasst werden, die nicht mehr Teil der Kirtung sind. Dies verdeutlichen im Übrigen anschaulich die von dem Kläger im erstinstanzlichen Verfahren vorgelegten Lichtbilder (vgl. S. 55–62 d. Gerichtsakte), denn darauf ist das Erfassungsspektrum der Wildkamera zu erkennen, das auch die nähere Umgebung und den Bereich zwischen dem Anbringungsort der Kamera und der Kirtung einschließt. Es ist daher nicht ausgeschlossen, dass von der Wildkamera nicht nur der unmittelbare Bereich der Kirtung erfasst wird, sondern auch die darüber hinaus gehenden angrenzenden Flächen, die von Waldbesuchern uneingeschränkt frequentiert werden dürfen. Allein diese Unwägbarkeiten im Hinblick auf die Ausrichtung und den Erfassungsbereich der Wildkamera vor Ort belegen bereits die Notwendigkeit einer präventiven datenschutzrechtlichen

Überprüfung, der die – nur geringfügig in die Grundrechte des Klägers eingreifende – Meldepflicht nach § 4d BDSG Rechnung trägt. Dies insbesondere auch vor dem Hintergrund, dass nach Aussage des Beklagten die bisherige Meldepraxis gezeigt habe, dass Jäger im Regelfall nicht nur eine Kamera, sondern oft zwei oder drei Kameras, manche sogar sechs bis acht Kameras in Betrieb hätten (der Kläger selbst habe am 22.8.2014 den Betrieb von sieben Wildkameras gemeldet), was einer Gesamtzahl von schätzungsweise 8.000 bis 10.000 Kameras in saarländischen Wäldern entsprechen würde.

Selbst wenn es sich bei der Kirtung um eine jagdliche Einrichtung handelt, die von dem allgemeinen Betretungsrecht ausgenommen ist (so Dienstbühl, aaO., S. 397 m.w.Nw.; ebenso LG Essen; Urteil vom 26.6.2014 – 10 S 37/14 – juris), hätte der Kläger die Vorschriften des BDSG zu beachten, weil diese Fläche des Waldes trotz eines Betretungsverbotes faktisch für die Öffentlichkeit zugänglich ist. Vom allgemeinen Betretungsrecht des Waldes ausgenommen sind nach § 25 Abs. 3 Nr. 2 LWaldG u.a. forst- und jagdwirtschaftliche Einrichtungen, die nur mit Zustimmung des Waldbesitzers betreten werden dürfen. Nach § 23 Abs. 3 Satz 1 des Saarländischen Jagdgesetzes (vom 27. Mai 1998, zuletzt geändert durch das Gesetz vom 13. Oktober 2015; Amtsbl. I S. 712; – SJG –) gehören zu den jagdlichen Einrichtungen insbesondere Ansitzeinrichtungen, Jagdschirme, Salzlecken und Einrichtungen, die zum Füttern gemäß § 25 Absatz 2 LWaldG oder Anlocken des Wildes dienen sowie vom Jagdausübungsberechtigten angelegte Wildäcker. Obwohl die Kirtung nicht ausdrücklich in der beispielhaften („insbesondere“) Aufzählung genannt ist, spricht einiges dafür, dass sie neben Fütterungen und Hochsitzen ebenfalls zu den jagdlichen Einrichtungen zählt, da sie dem Anlocken des Wildes dient. Maßgeblich für die datenschutzrechtliche Beurteilung ist indessen, dass die Kirtung faktisch für jedermann zugänglich und im öffentlichen Raum gelegen ist. Der (datenschutzrechtliche) Begriff des öffentlich zugänglichen Raums ist weit zu verstehen und erfasst jedenfalls alle räumlichen Bereiche, die der Öffentlichkeit ausdrücklich oder aufgrund einer nach außen erkennbaren Zweckbestimmung zugänglich gemacht werden. (Becker, in: Plath, BDSG/DS-GVO, 2. Aufl. 2016, § 6b BDSG). Nicht öffentlich sind hingegen Räume, die nur von einem bestimmten und abschließend definierten Personenkreis betreten werden können oder dürfen. Maßgebend sind insoweit die Vorgaben des Verfügungsberechtigten, d.h. dessen nach außen sichtbarer Wille (Scholz, in: Simitis, aaO. § 6b Rdnr. 48). Das gesetzliche Betretungsverbot der Kirtung ist für den Waldbesucher aber weder aufgrund von Hinweis- oder Verbotsschildern noch durch (bauliche) Abgrenzungen erkennbar. Die Kirtung ist weder eingefriedet noch eingegrenzt, da dies im Übrigen auch ihrem Zweck zuwiderlaufen würde und zudem nach § 46a Abs. 1 Nr. 5 der Verordnung zur Durchführung des Saarländischen Jagdgesetzes (DV-SJG) untersagt ist. Es ist auch nicht gewährleistet, dass diese Waldfläche aufgrund ihrer äußeren Gestaltung oder Beschaffenheit (vgl. Dienstbühl, aaO. S. 397) für den jagdunkundigen Waldbesucher erkennbar ist, da – was die vom Kläger präsentierten Ablichtungen veranschaulichen – örtlich vorhandene natürliche Materialien (Äste, Steine, Laub) zur Abdeckung verwendet werden. Die Behauptung des Klägers, die Fläche, auf der gekirt werde, sei anhand des aufgewühlten Bodens (sogenanntem Gebräch) selbst für den jagdlichen Laien erkennbar, lässt sich in dieser Allgemeingültigkeit daher nicht bestätigen. Aus Sicht des Senats hat der Beklagte außerdem zu Recht darauf hingewiesen, dass mit dem Verbrauch des Futtermittels die rechtliche Qualifikation der Kirtung als besondere jagdliche Einrichtung endet,

da ein Anlocken ohne Lockmittel nicht mehr möglich ist und damit ab diesem Zeitpunkt auch kein Betretungsverbot mehr besteht, obgleich die Kamera weiter aufzeichnet. Auch stellt sich in diesem Zusammenhang die Frage, welche räumliche Ausdehnung diese jagdliche Einrichtung zum Anlocken des Wildes hat. Von daher ist davon auszugehen, dass der Betrieb der Wildkameras regelmäßig in einem öffentlichen Raum stattfindet, der von Waldbesuchern frequentiert werden kann.

In dem Beobachten von Kirtungen mittels Tierbeobachtungskameras liegt keine ausschließlich persönliche oder familiäre Tätigkeit des Klägers, die vom Anwendungsbereich des BDSG ausgenommen wäre (vgl. § 1 Abs. 2 Nr. 3 a.E. BDSG). Ausdrücklich vom Anwendungsbereich der bestehenden Datenschutzgesetze ausgenommen bleibt die Datenverarbeitung im privaten und familiären Kontext (sog. Haushaltsausnahme) (von Lewinski, in: Auernhammer, DS-GVO/BDSG, a.a.O., § 1 Rdnr. 15). Während im BDSG von 1977 die Anwendung des Gesetzes noch auf den Datenumgang als „Hilfsmittel für die Erfüllung von Geschäftszwecken oder Zielen“ (vgl. § 22 Abs. 1 Satz 1 BDSG 1977) begrenzt war und dies im BDSG von 1990 nur redaktionell geändert wurde („geschäftsmäßig oder für berufliche oder gewerbliche Zwecke“, § 1 Abs. 2 Nr. 3 BDSG), wurde der Anwendungsbereich im BDSG 2001, europarechtliche Vorgaben aufgreifend (vgl. Art. 3 Abs. 2 2. Spiegelstrich der Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-DatSchRL); EuGH, Urteil vom 6.11.2003 – C-101/01 – („Lindquist“); juris), im Ergebnis erweitert, indem (nur) die Datenerhebung zu rein persönlichen und familiären Zwecken ausgenommen wurde.

Der Rechtsprechung des EuGH zufolge (Urteil vom 11.12.2014 – C-212/13 -, juris) verlangt der Schutz des in Art. 7 der Charta der Grundrechte der Europäischen Union (ABL. C 202 vom 07.06.2016, S. 395-395) garantierten Grundrechts auf Privatleben, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige beschränken müssen. § 1 Abs. 2 Nr. 3 BDSG grenzt damit die persönliche Lebensführung von der beruflichen und gesellschaftlichen Sphäre ab. Was familiär oder persönlich ist, richtet sich nach der Verkehrsanschauung; der Zweck muss objektiv als familiär oder persönlich erkennbar sein, was schon der Begriff „Haushaltsausnahme“ nahelegt. Zu den typischen persönlich-familiären Bereichen gehören Tätigkeiten im Rahmen der Familie und der Freizeit und die dazugehörige Datenverarbeitung wie z.B. private Korrespondenz, Tagebücher, Notizbücher, Adressverzeichnisse, Fotos, Videos u.ä. (von Lewinski, in: Auernhammer, DS-GVO/BDSG, § 1 Rdnr. 17 ff.). Der Gesetzgeber möchte damit Datenverarbeitungen, die im privaten Aktionskreis stattfinden, privilegieren. Voraussetzung ist aber, dass der Datenumgang mit all seinen Bestandteilen und während der gesamten Dauer im privaten Aktionskreis verbleibt bzw. zwischen den Teilhabern an der eigenen Privat- oder Familiensphäre untereinander erfolgt.

Hieran gemessen hat das Verwaltungsgericht zu Recht festgestellt, dass die Datenerhebung des Klägers mittels Einsatzes von Wildkameras nicht als ausschließlich persönliche oder familiäre Tätigkeit aufzufassen ist, auch wenn der Kläger die Jägerei als Hobby betreibt. Eine ausschließlich persönlich familiäre Tätigkeit liegt schon deshalb nicht vor, weil die Jagdausübung im Unterschied zu sonstigen Freizeitgestaltungen nicht nur im privaten Interesse des Jagdausübungsberechtigten sondern auch im öffentlichen Interesse liegt und die Jagdausübung darüber hinaus gesetzlichen Anforderungen unterliegt. Nach § 1 Abs. 2

BJagdG ist das Jagdrecht die ausschließliche Befugnis, auf einem bestimmten Gebiet wildlebende Tiere, die dem Jagdrecht unterliegen (Wild) zu hegen, auf sie die Jagd auszuüben und sie sich anzueignen. Mit dem Jagdrecht ist die Pflicht zur Hege verbunden. Die Ausübung der Jagd ist von der Erteilung eines Jagdscheins abhängig. Davon abgesehen ist der private Aktionskreis der Freizeitgestaltung des Klägers aber auch deshalb überschritten, weil mit der Wildkamera Abbildungen von Waldbesuchern (Spaziergänger, Wanderer, Freizeitsportler u.a.) erfolgen, die in keiner Verbindung oder Beziehung zu der als Freizeitbeschäftigung ausgeübten Betätigung des Klägers stehen. Es handelt sich dabei um einen unbestimmten Personenkreis, der nur zufällig in den Einflussbereich des Klägers gelangt ist und an dessen persönlichen Zweck in Gestalt der Jagdausübung nicht teilhat. Damit wird mit dem Einsatz der Wildkamera der Rahmen des § 1 Abs. 2 Nr. 3 BDSG überschritten. Personenbezogene Daten bzw. Bildaufzeichnungen von Dritten, die mit der Jagd nichts zu tun haben, unterliegen daher dem Schutz des BDSG (Dienstbühl, Der Einsatz von „Wildkameras“ durch Privatpersonen, a.a.O., S. 396).

Zum Recht auf Vergessenwerden (Ls)

(Landgericht Frankfurt/M., Urteil vom 26. Oktober 2017 – 2-03 0 190/16 –)

1. Der Betreiber einer Suchmaschine ist nicht als Access Provider gemäß § 8 TMG anzusehen, da er in der Regel den Suchergebnissen nicht neutral gegenüber steht.
2. Das Recht auf Vergessenwerden gebietet nicht die Entfernung eines Suchergebnisses zu 6 Jahre alten Berichten über die Geschäftsführertätigkeit des Betroffenen, wenn ein öffentliches Interesse an der Berichterstattung besteht.
3. Enthält der hinter dem Suchergebnis stehende Beitrag Gesundheitsdaten des Betroffenen, ist eine Abwägung im Einzelfall möglich und erforderlich. Hierbei kann es eine Rolle spielen, ob die Angaben konkret oder lediglich unkonkret und allgemein sind.
4. § 35 BDSG ist mit Blick auf das Recht auf Vergessenwerden nicht abschließend.

Unterlassung einer negativen Bewertung auf einer Internetplattform (Ls)

(Landgericht Augsburg, Urteil vom 17. August 2017 – 022 0 560/17 –)

Können auf einer Internetplattform Nutzer Erfahrungsberichte zu verschiedenen Einrichtungen abgeben, ist der Betreiber der Plattform nicht verpflichtet, die Bewertung einer Praxisklinik ohne Begründungstext mit (nur) einem von fünf Sternen deshalb zu löschen, weil der Nutzer nach dem Vortrag des Klinikbetreibers nicht in

der Klinik behandelt worden ist. Für die ihm zustehende Meinungsäußerung genüge es, dass der Nutzer in irgendeiner Art und Weise mit der Klinik in Berührung gekommen ist, die ihn veranlasst hat eine negative „Ein-Sternchen“-Bewertung abzugeben.

(Nicht amtlicher Leitsatz)

Zum Umfang des datenschutzrechtlichen Auskunftsrechts

(Amtsgericht Dortmund, Urteil von 29. August 2017 – 425 C 3489/17 –)

Nach § 34 Abs. 1 BDSG besteht nur ein sogenannter „Basisanspruch“ auf Auskunft über personenbezogene Daten. Die Auskunft ist

1. hinsichtlich der zur Person des Auskunftsberechtigten gespeicherten Daten einschließlich der Herkunft dieser Daten,
2. hinsichtlich etwaiger Empfänger oder der Kategorien von Empfängern (z.B. Adresshändler, Kreditinstitute), an die die Daten des anspruchsberechtigten weitergegeben werden, sowie
3. hinsichtlich des Zwecks der Speicherung zu erteilen.

Es besteht kein Anspruch auf Auskunft in einer bestimmten äußerlichen Form. Hat der Auskunftspflichtige zu allen Informationen Angaben gemacht, ist das Auskunftsbegehren erfüllt. Ob die Angaben richtig sind oder der Auskunftsberechtigte an der Vollständigkeit Zweifel hat ist unerheblich, wenn der Auskunftspflichtige angibt, keine weiteren Daten gespeichert zu haben.

Nach § 34 BDSG besteht kein Anspruch gegen einen Lebensversicherer hinsichtlich der in Abzug gebrachten Abschluss-/Storno-/Verwaltungs- und Risikokosten sowie der monatlich aufgeschlüsselten, während der Vertragslaufzeit aus dem Versicherungsvertrag gezogenen Nutzungen. Es handelt sich nicht um Daten, die „personenbezogen gespeichert“ sind.

Sachverhalt:

Der Kläger macht gegenüber der Beklagte Auskunfts- und Herausgabeansprüche bezüglich von Daten geltend, welche im Zusammenhang mit einem zwischen den Parteien begründeten und mittlerweile beendeten Versicherungsvertragsverhältnis durch die Beklagte gewonnen worden sein sollen.

Der Kläger hat bei der Beklagten unter der Versicherungsnummer ... eine Kapital-/Risikoversicherung mit Berufsunfähigkeitsschutz als Rentenversicherung mit einem Versicherungsbeginn am 01.10.2004 abgeschlossen. Wegen der Einzelheiten wird auf die bei den Akten befindlichen Antrag und die Versicherungsbedingungen usw Bezug genommen. Der Vertrag wurde auf Wunsch des Klägers ab 1.1.2012 beendet, die Beklagte rechnete den Vertrag mit Schreiben vom 9.1.2012 ab und zahlte an den Kläger 1140,12 € aus.

Mit Schreiben seines Prozessbevollmächtigten vom 30.6.2016 baten diese um Übersendung diverser Unterlagen, worauf hin die Beklagte diverse Schreiben, eine Kopie des Versicherungsantrags, eine Kopie der Kündigungsbestätigung, eine Kopie der Abrechnung und die Allgemeinen Versicherungsbedingungen an den Klägervertreter übersandte. Ferner teilte sie mit, welche Zahlungen der Kläger insgesamt an welchem Tag in welcher Höhe erbracht hatte. Es folgten dann auf Nachfrage noch weitere Angaben. Wegen des genauen Inhalts aller Schreiben wird auf die bei den Gerichtsakten befindlichen Kopien, die den Parteien sämtlichst bekannt sind, verwiesen.

Mit Schreiben seines Prozessbevollmächtigten vom 5.8.2016 erklärte der Kläger gegenüber der Beklagten den Widerspruch nach § 5a VVG sowie hilfsweise den Widerruf gemäß § 8 Abs. 4 VVG bzw. Rücktritt nach § 8 Abs. 5 VVG jeweils in der bis zum 31.12.2007 geltenden Fassung. Am 28.2.2017 listete die Beklagte noch einmal genau auf, welche Fragen ihr gestellt worden waren und wann und wie sie diese Fragen beantwortet hatte (B. 31. d.A.).

Der Kläger vertritt durch seinen Prozessbevollmächtigten die Ansicht, dass ihm weiterhin ein umfassender Auskunftsanspruch aufgrund der Vorschriften des Bundesdatenschutzgesetzes, des Versicherungsvertragsgesetzes und des Bürgerlichen Gesetzbuches zustehen würde. So könne er § 34 BDSG i.V.m. §§ 1, 2 BDSG Auskunft über folgende Umstände verlangen.

Aus den Gründen:

I. Ein etwaiger Auskunftsanspruch des Klägers gegenüber der Beklagten gemäß § 34 BDSG ist wegen der bereits erfolgten Erfüllung gemäß § 362 Abs. 1 BGB erloschen.

1. Nach § 34 Abs. 1 BDSG besteht ein sogenannter „Basisanspruch“ auf Auskunft über personenbezogene Daten (vgl. hierzu Schmidt-Wudy, in: Datenschutzrecht in Bund und Ländern, 2013, § 34 Rn. 41–44). Die Auskunft ist

(1.) hinsichtlich der zur Person des Auskunftsberechtigten gespeicherten Daten einschließlich der Herkunft dieser Daten,

(2.) hinsichtlich etwaiger Empfänger oder der Kategorien von Empfängern (z.B. Adresshändler, Kreditinstitute), an die die Daten des anspruchsberechtigten weitergegeben werden, sowie

(3.) hinsichtlich des Zwecks der Speicherung zu erteilen.

2. Das Auskunftsrecht besteht unabhängig von der Form der Speicherung. Auch über in schriftlichen Akten gespeicherte Daten ist gem. § 34 BDSG Auskunft zu erteilen (vgl. vgl. Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage 2015, § 34 Rn. 8 ff). Die Auskunft hat gemäß § 34 Abs. 6 BDSG grundsätzlich schriftlich – im Sinne des § 126b BGB zu erfolgen, eine Übermittlung über andere Kommunikationsmedien (z.B. per Email) ist zulässig (vgl. Gola/Schomerus, aaO, § 34 Rn. 9).

3. Unter Berücksichtigung der vorgenannten Anforderungen hat die Beklagte insbesondere durch Vorlage der „e-Auskunft“ vom 7.6.2017 (Anlage B 7 zur Klageerwiderung) ihre Auskunftspflicht umfassend erfüllt. Die Auskunft ist aus sich heraus verständlich und logisch aufgebaut. Insbesondere ist ihr zu entnehmen, zu welchen Oberbegriffen („Kunde“, „Versichert“, „Grundvertrag“, „Bezugsrechte“, etc.) die Daten gespeichert wurden. Darüber hinaus hat die Beklagte am 16.5.2017 mitgeteilt, dass die Daten an den vom Kläger beauftragten Vermittler weitergeleitet worden sind und den Zweck der Speicherung – vorliegend die Vertragsdurchführung – bekannt gegeben. Zudem ist dem Schreiben zu entnehmen, dass diese Daten sämtlichst vom Kläger selbst bei der Abgabe seines Versicherungsantrags der Beklagten gegenüber angegeben wurden.

Damit ist die erforderliche und verlangte Auskunft vollständig erteilt. Es ist nicht ersichtlich, welche weiteren nach § 34 Abs. 1 BDSG auskunftspflichtigen Daten bei der Beklagten noch vorhanden sein sollen. Die Beklagte hat nämlich angegeben, dass keine weite-

ren Daten dort vorhanden sind. Auch das ist eine umfassende und vollständige Auskunft. Eine Auskunftsklage ist das falsche Mittel, sich hier Gewissheit zu verschaffen. Auch die Information, dass keine – weiteren – Angaben gemacht werden können, ist eine Auskunft. Das ist nicht nur im Datenschutzrecht, sondern in allen Rechtsgebieten, z.B. auch im Familienrecht, wo Auskunftsansprüche regelmäßig geltend gemacht werden, so.

Dass andere Versicherer die Auskunft in anderer Form erteilen, ist unerheblich, da die Auskunft der Beklagten den gesetzlichen Anforderungen völlig genügt.

4. Soweit der Kläger Auskunft über den Beitragszahlungsverlauf des zwischen den Parteien bestehenden Vertrages begehrt, ist festzustellen, dass er auch diese Auskunft bereits erhalten hat. Diese Daten sind dem Kläger seitens der Beklagten in einem den gerichtlichen Schriftsätzen beigefügten Schreiben mitgeteilt worden. Die entsprechende Aufstellung schlüsselt die Fälligkeit und Abbuchung der seit Vertragsbeginn bis zur Vertragskündigung von der Beklagten vereinnahmten Beträge auf. Zwar enthält diese Aufstellung keine Gesamtsumme der insgesamt gezahlten/abgebuchten Beträge. Diese ist jedoch bestimmbar. Eine weitere Auskunft hinsichtlich dessen wäre bloße Förmerei, da hieraus kein zusätzlicher Erkenntnisgewinn für den Kläger generiert wird.

5. Weitergehende Auskunftsverpflichtungen bestehen – entgegen der Auffassung des Klägers – auch hinsichtlich (a) in Abzug gebrachter Abschluss-/Storno-/Verwaltungs- und Risikokosten, (b) der Summe der von der Beklagten gezogenen Nutzungen aus dem nutzbaren Kapital des Klägers einschließlich der Höhe der gezogenen Zinsen sowie (c) der monatlich aufgeschlüsselten, während der Vertragslaufzeit von der Beklagten aus dem Versicherungsvertrag gezogenen Nutzungen nicht. Mögen diese Daten ggf. auch zum Versicherungsvertrag des Klägers und damit „personenbezogen gespeichert“ sein, so handelt es sich hierbei gerade nicht um von § 34 Abs. 1 BDSG erfasste Daten.

a) Nach § 34 Abs. 1 sind nämlich nur solche Daten mitzuteilen, die zur Person des Betroffenen sind. D.h., „die Angaben über persönliche oder sachliche Verhältnisse, die auf eine Person bezogen oder beziehbar sind“ (vgl. vgl. Gola/Schomerus, aaO., § 34 Rn. 9). Persönliche und sachliche Verhältnisse einer Person beschreibt körperliche und geistige Eigenschaften, Verhaltensweisen und berufliche, wirtschaftliche, soziale oder private Beziehungen. Erfasst werden auch alle identifizierenden Angaben wie bspw. Personenkennzeichen, Arbeitszeiten, GPS-Standortdaten, Daten in rechtlichen Analysen und biometrische Daten, auf die Sensibilität oder Aussagekraft der Angaben kommt es für ihre Einordnung als „personenbezogene Daten“ nicht an (Plath/Schreiber, in: Plath, BDSG/DS-GVO, 2. Aufl. 2016, § 3 BDSG, Rn. 8). Den unter Punkt (a)–(c) bezeichneten, klägerseitig begehrten Angaben fehlt jedoch ein solcher Bezug, weil sie keine individualisierende, den Kläger in seinen Eigenschaften und Verhaltensweisen betreffende Informationen enthalten.

b) Der Kläger verkennt, dass § 34 Abs. 1 BDSG eben nicht zur umfassenden Auskunftserteilung über sämtliche Daten verpflichtet. Dass etwaige Kalkulationen, Gewinn- und Abschläge von § 34 Abs. 1 BDSG nicht erfasst sind, folgt jedenfalls auch aus der Systematik der Auskunftsansprüche gemäß § 34 BDSG. Entsprechend besteht nach § 34 Abs. 2 BDSG ein Anspruch auf Auskunft bei Verwendung eines sogenannten Scorings im Sinne des § 28b BDSG. Dies betreffend ist dem Auskunftsberechtigten einzelfallbezogen und in allgemeinverständlicher Form mitzuteilen und zu erläutern, „welche konkreten Faktoren (Lebenssachverhalte) mit welcher Gewichtung in den Wahrscheinlichkeitswert einfließen und wie sie sich die Wahrscheinlichkeitswerte gegenseitig beeinflussen“ (vgl. Dix, in: Simitis, Bundesdatenschutzgesetz, 8. Auflage, § 34, Rn. 33). Auch hieraus folgt eben kein Anspruch auf Bekanntgabe von etwaigen Verwaltungskosten und erzielten Gewinnen. Der Gesetzgeber wollte mit Einführung der Auskunftsbeurteilung allenfalls im

Zusammenhang mit Scoring die bereits bestehen Auskunftsrechte erweitern. Eine Erstreckung auf andere, nicht personenbezogene Daten kann daraus nicht abgeleitet werden.

c) Soweit der Kläger die „Herausgabe“ von Daten begehrt, ist dies von § 34 BDSG ebensowenig erfasst. Es ist schon nicht ersichtlich, wie die Herausgabe von Daten realisiert werden soll. Daten können gespeichert, verarbeitet, bekanntgegeben und gelöscht werden. Eine Herausgabe unkörperlicher Daten ist tatsächlich unmöglich. Soweit der Kläger damit die Herausgabe von Unterlagen meint, besteht ein entsprechender Anspruch nach § 34 Abs. 1 BDSG nicht. Der Anspruch bezieht sich lediglich auf die Auskunft von (personenbezogenen) Daten, nicht auf körperlicher Herausgabe von oder Einsicht in Akten (vgl. EuGH, Urteil vom 17. Juli 2014 – C-141/12 und C-372/12 –, Rn. 58, juris; indirekt auch Schleswig-Holsteinisches Oberlandesgericht, Beschluss vom 28. Februar 2011 – 5 U 112/10 –, Rn. 18, juris).

II. Der klägerisch verfolgte Anspruch ergibt sich auch nicht aus § 34 Abs. 2 BDSG. Es ist schon nicht ersichtlich, dass für den hier vorliegenden Rentenversicherungsvertrag überhaupt seitens der Beklagten ein Scoring-Verfahren zum Tragen kam. Dies wird klägerseitig weder konkret für den Fall noch abstrakt in dem wohl für eine Vielzahl von gleichartigen Klagen vorformulierten Schriftsatz ohne konkreten Fallbezug behauptet.

III. Ein Auskunftsanspruch besteht zudem nicht aus der auftragsrechtlichen Auskunfts- und Rechenschaftspflicht gemäß § 666 BGB, denn zwischen den Parteien bestand ein Versicherungsvertrag, der keinen Geschäftsbesorgungscharakter im Sinne von § 675 BGB aufweist (vgl. Baumann, in: Bruck/Möller, VVG, 9. Aufl. 2008, § 1 VVG, Rn. 208, m.w.N.; Prölss, in: Martin/Prölss, 27. Aufl. 2004, VVG § 1 Rn. 23, beck-online; vgl. ferner zur fehlenden verfassungsrechtlichen Gebotenheit der Einordnung des Versicherungsvertrags als treuhänderischen Geschäftsbesorgungsvertrag: BVerfG, Nichtannahmebeschluss vom 29. Mai 2006 – 1 BvR 240/98 –, Rn. 31, juris).

IV. Bezüglich der begehrten Auskunft betreffend Abschluss-, Storno- und Verwaltungskosten kann der Kläger gegenüber der Beklagten aus dem Versicherungsvertrag in Verbindung mit § 242 BGB einen entsprechenden Anspruch nicht herleiten.

1. Im Rahmen einer Rechtsbeziehung trifft den Schuldner nach Treu und Glauben ausnahmsweise eine Auskunftspflicht, wenn der Berechtigte in entschuldbarer Weise über Bestehen und Umfang seines Rechts im Ungewissen ist und der Verpflichtete die zur Beseitigung der Ungewissheit erforderliche Auskunft unschwer geben kann (BGH, Urteil vom 26. Juni 2013 – IV ZR 39/10 –, Rn. 24, juris; BGH, Urteil vom 05. November 2002 – XI ZR 381/01 –, BGHZ 152, 307-317, Rn. 28). Weil dieser allgemeine Auskunftsanspruch sich auf die Realisierung eines Rechts beziehen muss, ist dieser lediglich ein Hilfsanspruch, welcher seinerseits erfordert, dass ein Leistungsanspruch dem Grunde nach besteht (BGH, Urteil vom 17. Mai 1994 – X ZR 82/92 –, BGHZ 126, 109-124, Rn. 25; Staudinger/Claudia Bittner (2014) BGB § 260, Rn. 19a), so dass bei einem beendeten Lebensversicherungsvertragsverhältnis Auskunft verlangt werden kann, wenn ausreichende Anhaltspunkte für einen Nachzahlungsanspruch des Versicherungsnehmers, den der dieser mit Hilfe der Auskunft geltend machen will, vorliegen (vgl. BGH, Urteil vom 26. Juni 2013 – IV ZR 39/10 –, Rn. 24, juris). Ein allgemeiner Auskunftsanspruch nur zu dem Zweck, Informationen und Beweismittel für die Durchsetzung eines nicht ausreichend substantiiert darzulegenden Anspruchs zu gewinnen, besteht grundsätzlich nicht (vgl. BGH, Urteil vom 18. Februar 1970 – VIII ZR 39/68 –, Rn. 32, juris).

2. Vorliegend berührt sich der Kläger aber schon keines entsprechenden Zahlungsanspruchs gegenüber der Beklagten aus dem

Versicherungsvertrags, so dass ihm der allgemeine vertragliche Auskunftsanspruch nicht zusteht. Solche Ansprüche wären wahrscheinlich auch verjährt.

V. Ein Anspruch auf Überlassung von Ablichtungen der im Zusammenhang mit dem Versicherungsvertragsverhältnis abgegebenen Erklärungen gemäß § 3 Abs. 1 und 3 VVG in der bis zum 31.12.2007 geltenden Fassung steht dem Kläger nicht mehr zu, denn die entsprechenden Schriftstücke (Versicherungsantrag, Kündigungserklärung und Kündigungsbestätigung nebst Abrechnung des Versicherungsvertrages) sind dem Kläger spätestens als Anlagen zu den Schriftsätzen der Beklagten zugegangen, so dass der Anspruch erfüllt und nach § 362 Abs. 1 BGB untergegangen ist.

VI. Ob die Beklagte gegenüber einem etwaigen Auskunftsanspruch des Klägers letztlich erfolgreich die dauerhafte Einrede der Verjährung gemäß § 214 Abs. 1 BGB erfolgreich entgegenhalten kann, bedarf daher keiner Vertiefung; insbesondere muss nicht entschieden werden, ob der Auskunftsanspruch aus § 34 BDSG ein sog. verhaltener Anspruch ist, dessen Verjährung in entsprechender Anwendung von § 695 S. 2 und § 696 S. 3 BGB erst mit seiner Geltendmachung beginnt (BGH, Urteil vom 3. November 2011 – III ZR 105/11, in: NJW 2012, 58 (61), beck-online; Grothe, in: Münchener Kommentar BGB, 7. Aufl. 2017, § 199 Rn. 7, beck-online).

VII. Das gilt auch für die Frage, ob aufgrund des Zeitablaufs ggf. hier auch eine Verwirkung in Betracht kommt. Neben dem Zeitpunkt könnte hier als Umstandsmoment in Betracht gezogen werden, dass für das erkennende Gericht bisher keinerlei persönliche und eigene Interessen des Klägers ansatzweise am Horizont erkennbar sind, die diese Klage rechtfertigen. Abschließend aufgeklärt hat das Gericht diesen Punkt aber nicht, da die Klage auch schon aus den o.g. Gründen unbegründet ist.

VIII. Mangels einer entsprechenden Hauptforderung steht dem Kläger gegenüber der Beklagten eine Nebenforderung auf Erstattung vorgerichtlicher Rechtsanwaltskosten nebst Prozesszinsen nicht zu. Deshalb bedarf es keiner Entscheidung, ob nicht Zahlung an die Rechtsschutzversicherung hätte verlangt werden müssen.

Kündigung wegen verdeckter Videoaufnahmen von Sportlerinnen (Ls)

(Arbeitsgericht Berlin, Urteil vom 01. November 2017 – 24 Ca 4261/17 –)

1. Einem Trainer, der heimlich Sportlerinnen beim Umziehen mit einer versteckten Kamera filmt, kann fristlos gekündigt werden.
2. Die zweiwöchige Ausschlussfrist des § 626 Abs. 2 Satz 1 BGB beginnt zu dem Zeitpunkt zu laufen, indem der Arbeitgeber von den für die Kündigung maßgebenden Tatsachen eine zuverlässige und möglichst vollständige positive Kenntnis erlangt. Eine ausreichende Kenntnis über die Kündigungsgründe liegt erst vor, nachdem die in diesem Tatbestand ermittelnde Staatsanwaltschaft auf mehrfache Anträge und Nachfragen hin Akteneinsicht gewährt hat.

(Nicht amtliche Leitsätze)

Berichte, Informationen, Sonstiges

Kommentar zu Stephan Pötters, Peter Gola: Wer ist datenschutzrechtlich „Verantwortlicher“ im Unternehmen? Betriebsrat und andere selbstständige Einheiten als Adressaten des Datenschutzrechts, RDV 6/2017

In ihrem Aufsatz gelangen die Autoren bezüglich der Definition von „Verantwortlicher“ in Art. 4 Nr. 7 DS-GVO zu der Feststellung: „Im Ergebnis ist also (nur) jede juristische Person Verantwortlicher, das Datenschutzrecht ist sozusagen gesellschaftsrechtsakzessorisch. [...] Selbstständig agierende Stellen innerhalb einer juristische Person [...] sind hingegen lediglich als Teil des Verantwortlichen Adressat des Datenschutzrechts, auch wenn sie selbst über Zwecke und Mittel der Datenverarbeitung entscheiden“ (RDV 6/2017, S. 281). Dies geht vollkommen an Art. 4 Nr. 7 DS-GVO vorbei. Denn das entscheidende Kriterium für die Bestimmung eines Verantwortlichen ist die selbstständige Entscheidung über Zwecke und Mittel der Datenverarbeitung. Dieses Kriterium allein ist die Bedingung, die erfüllt sein muss, um Verantwortlicher im Sinne der DS-GVO zu sein. Und diese Bedingung kann eine juristische Person, aber eben auch eine natürliche Person oder eine Behörde oder eine Einrichtung oder irgendeine andere Stelle erfüllen. Wenn also eine natürliche Person (etwa Beschäftigte eines Unternehmens) oder auch eine Stelle (z.B. Niederlassung, Abteilung oder Betriebsrat) „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ (Art 4 Nr. 7 DS-GVO), ist sie Verantwortlicher. In Art. 4 Nr. 7 DS-GVO ist keinerlei Ausnahme formuliert für den Fall, dass eine natürliche Person oder eine Stelle als Teil einer wie auch immer verfassten Organisation agiert.

Eine Ausnahme findet sich nur in Art. 29 DS-GVO. Danach darf „jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, [...] diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten“. Natürliche Personen (und auch Stellen, die ja von einer natürlichen Person repräsentiert werden), die als Teile einer juristischen Person personenbezogene Daten verarbeiten, dürfen dies nur weisungsgemäß tun. Wenn sie das tun, entscheiden sie nicht über Zwecke und Mittel der Datenverarbeitung und sind somit auch keine Verantwortlichen im Sinne der DS-GVO; soweit die Ausnahme.

Wenn aber Beschäftigte oder Stellen innerhalb eines Unternehmens ohne oder gegen Weisung der Unternehmensleitung personenbezogene Daten verarbeiten und damit die vorgegebene Zweckbindung übertreten, entscheiden sie eigenständig über Zwecke und auch Mittel (auch das Nutzen von Ressourcen der Organisation ist dann eine eigenständige Entscheidung für ein Mittel) und werden dadurch gemäß Art. 4 Nr. 7 DS-GVO selbst zu Verantwortlichen, mit allen sich daraus ergebenden Konsequenzen.¹ Damit sind Beschäftigte gesetzlich in die Pflicht genommen, sich bei der Datenverarbeitung an die im Unternehmen geltenden Vorgaben zu halten, und es ist klargestellt, dass ein Missachten solcher Vorgaben auch gesetzliche Konsequenzen hat. Für die oberste Leitung einer Organisation ist Art. 29 DS-GVO die Verpflichtung, ihre Rolle als Verantwortlicher so auszufüllen, dass alle Organisationsteile, bis hin zu einzelnen Beschäftigten, klare Vorgaben zur Verarbeitung personenbezogener Daten erhalten. Diese Verpflichtung ist ein wichtiger Aspekt der in Kapitel IV der DS-GVO umrissenen Anforderung, eine sorgfältig geplante Datenschutzorganisation (ein Datenschutzmanagement) wirksam zu implementieren. Die Schadensersatz- und Haftungsvorschriften in Art. 82 und 83 DS-GVO, die auf Un-

ternehmen in ihrer Gänze zielen, setzen den Anreiz, das Datenschutzmanagement von der obersten Leitungsebene einer Organisation her zu organisieren und dies eben nicht einzelnen Organisationsteilen zu überlassen.

Das bedeutet auch, die mit Verweis auf Art. 3 Abs. 1 DS-GVO erfolgte Aussage in dem hier kommentierten Aufsatz: „Wenn also z.B. ein amerikanisches Unternehmen Standorte in London und Frankfurt hat, sind nicht diese Niederlassungen datenschutzrechtlich verantwortlich, sondern nur die amerikanische Gesellschaft“ (RDV6/2017, S. 280), ist nur korrekt, wenn man ergänzt: sofern nicht diese amerikanischen Gesellschaft so organisiert ist, dass ihre Niederlassungen eigenständig über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden (dann sind die Niederlassungen Verantwortliche), freilich mit dem Risiko, dennoch für Datenschutzverstöße einer Niederlassung gesamtgesellschaftlich (mit) in der Haftung zu stehen. Und das wird mutmaßlich regelmäßig der Anlass für Muttergesellschaften sein, Tochtergesellschaften und Niederlassungen gerade nicht die Verantwortung über Verarbeitungen personenbezogener Daten zu überlassen, sondern diese Verantwortung selbst wahrzunehmen und durch eine von oben implementierte und gesteuerte Datenschutzorganisation abzusichern, sodass alle mit der Datenverarbeitung befassten Personen in den einzelnen Organisationsteilen diese Verarbeitung gemäß Art. 29 DS-GVO ausschließlich weisungsgemäß vornehmen, also im Sinne

¹ Entsprechend regelt Art. 28 Abs. 10, dass ein Auftragsverarbeiter Verantwortlicher wird, wenn er, gegen die Regelungen der DS-GVO verstoßend, Zwecke und Mittel der Verarbeitung bestimmt, da der Auftragsverarbeiter dann außerhalb der Weisungen des Verantwortlichen agiert. Schon jetzt können auch einzelne Beschäftigte eines Unternehmens datenschutzrechtlich Verantwortliche sein, wie Beispiele von Bußgeldern gegen Beschäftigte wegen Versendung offener E-Mail-Verteiler durch das Bayerische Landesamt für Datenschutzaufsicht zeigen (6. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2013 und 2014, Nr. 13.1, S. 85).

und unter Kontrolle des letztlich Haftenden und gegebenenfalls Schadenersatzpflichtigen.

Art. 29 DS-GVO gewährleistet also einerseits, dass der Verantwortliche Herr über die unter seiner Verantwortung vorgenommene Verarbeitung personenbezogener Daten bleibt, auch wenn er dazu Erfüllungsgehilfen einsetzt. Andererseits sichert Art. 29 DS-GVO diese Erfüllungsgehilfen ab, da sie, solange sie personenbezogene Daten gemäß den Weisungen eines Verantwortlichen verarbeiten, selber nicht Verantwortliche werden und somit nicht für mögliche durch diese weisungsgebundene Verarbeitung verursachte Datenschutzverstöße in die Haftung genommen werden können. Letzteres ergibt sich auch daraus, dass ein Auftragsverarbeiter nur dann haftet, wenn er gegen die an ihn adressierten Anforderungen der DS-GVO verstößt oder „unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat“ (Art. 82 Abs. 2 Satz 2 DS-GVO).

Wenn nun ein Betriebsrat nicht Verantwortlicher im Sinne der DS-GVO wäre, sondern statt seiner das Unternehmen als die juristische Person, zu der der Betriebsrat gehört, stellte sich die Frage, wie in diesem Verhältnis mit Art. 29 DS-GVO umzugehen ist. Denn wendete man Art. 29 DS-GVO auf solche einem datenschutzrechtlich Verantwortlichen unterstellten Betriebsräte an, die zweifelsfrei Zugang zu personenbezogenen Daten haben und diese auch verarbeiten, dürften diese Betriebsräte dies nur gemäß den Weisungen des Verantwortlichen, also der juristischen Person, also der diese juristische Person repräsentierenden Unternehmensleitung tun. Damit würden § 78 und § 80 Abs. 2 Satz 2 BetrVG teilweise durch die DS-GVO verdrängt, was zu einer nicht unerheblichen Beschränkung der Betriebsratsarbeit führte. Der mögliche Einwand gegen die Anwendbarkeit des Art. 29 DS-GVO auf Betriebsräte, nämlich dass ein Betriebsrat nicht der Unternehmensleitung unterstellt ist, greift nicht. Denn

ein Betriebsrat ist unbestritten Teil des Unternehmens, und wenn man annimmt, die juristische Person Unternehmen ist der datenschutzrechtlich Verantwortliche für alle zu ihr gehörenden Teile, dann ist auch der Betriebsrat datenschutzrechtlich dieser juristischen Person unterstellt. Und der Repräsentant eines Unternehmens ist nun mal die Geschäftsführung, nicht der Betriebsrat. Doch hypothetisch angenommen, der Betriebsrat ist nicht Verantwortlicher und er unterfällt auch nicht der Weisung des Verantwortlichen gemäß Art. 29 DS-GVO: Das schüfe für Unternehmen mit Betriebsrat die Situation, Verantwortliche für Datenverarbeitungen zu sein, über die sie nicht bestimmen können, für die sie aber haftbar und gegebenenfalls schadenersatzpflichtig sind. Und Betriebsräte hätten einen Freibrief, personenbezogene Daten eigenverantwortlich verarbeiten zu dürfen, ohne an irgendwelche Datenschutzstandards gebunden zu sein und ohne für Datenschutzverstöße in die Haftung genommen werden zu können. Denn die Regelungen der DS-GVO, inklusive der Pflichten zum Ergreifen technischer und organisatorischer Maßnahmen zum Schutz der Rechte und Freiheiten Betroffener und zur Datensicherheit sowie der Bestimmungen zu Haftung und Schadenersatz, sind ausschließlich adressiert an Verantwortliche und Auftragsverarbeiter, was Betriebsräte aber beides nicht wären. Beides widerspräche der Ausrichtung der DS-GVO, die, wie oben dargelegt, einerseits darauf abzielt, diejenigen, die über die Verarbeitung personenbezogener Daten bestimmen, voll in die Verantwortung zu nehmen, und andererseits Verantwortlichen die Grundlage liefert, die uneingeschränkte Kontrolle über Datenverarbeitungen ausüben zu können, für die sie gegebenenfalls haften.

Da jedoch Betriebsräte sinnvollerweise allein oder gemeinsam mit der Unternehmensleitung (in Rahmen von Betriebsvereinbarungen) über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden und weisungsfrei Datenverarbeitungen vor-

nehmen, erfüllen sie ohnehin die maßgebliche Bedingung in Art. 4 Nr. 7 DS-GVO für die Bestimmung von Verantwortlichen.

Volker Caumanns

Fitness-App-Anbieter geben kaum Auskunft über Datennutzung

Marktwächter-Experten haben sechs Anbieter abgemahnt

Anbieter müssen auf Anfrage Auskunft darüber erteilen, welche Daten sie von den Nutzern gespeichert haben. Das Marktwächter-Team der Verbraucherzentrale NRW wollte deshalb wissen, inwieweit Verbraucher auf eine solche Anfrage Antwort erhalten. Die Ergebnisse zeigen: „Verbraucher, die bei der Wearable- und Fitness-App-Nutzung ihre eigenen Daten im Blick behalten möchten, haben kaum eine Chance. Selbst dann nicht, wenn sie Informationen direkt beim Anbieter einfordern. Damit wird die Kontrolle der eigenen Daten erschwert oder sogar vollständig blockiert“, so Ricarda Moll, Referentin im Marktwächter-Team Digitale Welt der Verbraucherzentrale NRW.

Auf der anderen Seite räumen sich Anbieter von Smartwatches und Fitness-Apps selbst weitgehende Rechte an den Daten der Nutzer ein – das zeigt aktuell eine Untersuchung der Stiftung Warentest: Diese hat sich 13 Modelle genauer angesehen und bei zwölf Modellen deutliche Mängel im Kleingedruckten der AGBs gefunden. Mit Gut hat deshalb nur ein Modell abgeschnitten, die anderen waren befriedigend bis ausreichend.

Praxistest: Die wenigsten Anbieter beantworten die Fragen

Im Rahmen der Marktwächter-Untersuchung haben zwölf Tester einen Auskunftsantrag gestellt, nachdem sie das Wearable und die dazugehörige Fitness-App zuvor vier Wochen genutzt hatten. Die Verbraucherzentrale selbst tauchte nicht im Antrag auf. Nach zwei Kontaktversuchen hatten zwar acht von zwölf Anbietern reagiert, je-

doch waren nur drei der Antworten zufriedenstellend. Andere Reaktionen bestanden beispielsweise lediglich aus pauschalen Hinweisen zum Umgang mit den erhobenen Daten, ohne jedoch auf die konkreten Fragen der Nutzer einzugehen. Vier der zwölf Anbieter haben innerhalb der genannten Frist überhaupt nicht auf das Auskunftersuchen der Nutzer reagiert.

Recht auf Auskunft: Wer fragt, erlebt Hindernisse

Die Ergebnisse des Praxistests zeigen: Möchten Verbraucher wissen, was mit ihren Daten bei der kombinierten Wearable- und App-Nutzung geschieht, wird es ihnen nicht einfach gemacht. Denn abgesehen davon, dass einige Anbieter bis zuletzt in keiner Weise auf das Auskunftersuchen reagierten, forderten zwei Anbieter zusätzlich weitere Informationen zur Identifikation (z.B. Produktbestellnummer/Personalausweis) vom Verbraucher. Eine Antwort haben die Betroffenen bis heute nicht erhalten, obwohl die aus Sicht der Marktwächterexperten unter Umständen notwendigen Informationen übermittelt wurden.

Konsequenzen: Sechs Anbieter abgemahnt, einer verklagt

Die Marktwächter-Experten der Verbraucherzentrale NRW sehen in den ausbleibenden beziehungsweise unzureichenden Antworten der Anbieter Verstöße gegen geltendes Datenschutzrecht. Daher wurden sechs Anbieter abgemahnt, von denen vier Anbieter die Unterlassungserklärungen abgegeben haben. „Mit diesen Zusagen der Anbieter, das abgemahnte Fehlverhalten zu unterlassen, können wir als Marktwächter-Team weitere Erfolge für den Verbraucher verzeichnen“, so Moll. Einen großen Anbieter haben die Marktwächter-Experten mittlerweile verklagt.

Die Erkenntnisse des Marktwächter-Praxistests ergänzen die Ergebnisse der im April 2017 erschienenen Untersuchung „Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?“. Diese hat gezeigt, dass kaum einer der Anbieter in seinen Datenschutzerklärungen ausreichend über die genaue

Verwendung der zum Teil sensiblen Daten informiert.

(Pressemitteilung vom 22.11.2017)

Bundesnetzagentur geht gegen Kinderuhren mit Abhörfunktion vor

Die Bundesnetzagentur verbietet den Verkauf von Kinderuhren mit Abhörfunktion und ist bereits gegen mehrere Angebote im Internet vorgegangen.

Verbotene Abhörgeräte

Es gibt auf dem deutschen Markt eine große Anzahl von Anbietern, die Smartwatches für Kinder mit einer Abhörfunktion anbieten. Zielgruppe sind Kinder im Alter von 5 bis 12 Jahren.

Diese Uhren verfügen über eine SIM-Karte und eine eingeschränkte Telefoniefunktion, die über eine App eingerichtet und gesteuert werden. Eine solche Abhörfunktion wird häufig als „Babyphone“- oder „Monitorfunktion“ bezeichnet. Der App-Besitzer kann bestimmen, dass die Uhr unbemerkt vom Träger und dessen Umgebung eine beliebige Telefonnummer anruft. So wird er in die Lage versetzt, unbemerkt die Gespräche des Uhrträgers und dessen Umfeld abzuhören. Nach Ermittlungen der Bundesnetzagentur werden die Uhren von Eltern zum Beispiel auch zum Abhören von Lehrern im Unterricht genutzt. Eine derartige Abhörfunktion ist in Deutschland verboten.

Vorgehen gegen Käufer

Die Bundesnetzagentur rät speziell Schulen, verstärkt auf Uhren mit Abhörfunktion bei Schülern zu achten. Sofern Käufer solcher Uhren der Bundesnetzagentur bekannt werden, fordert sie diese auf, die Uhr zu vernichten und einen Nachweis hierüber an die Bundesnetzagentur zu senden. Eltern wird daher geraten, die Uhren eigenständig unschädlich zu machen und Vernichtungsnachweise hierzu aufzubewahren.

Wie ein Vernichtungsnachweis im Falle eines Anschreibens durch die Bundesnetzagentur geführt werden kann, ist zu finden unter: www.bundesnetzagentur.de/spionagekamas.

Dort befindet sich auch eine Übersicht über Produktgruppen, die unerlaubte Sendeanlagen nach deutschem Recht darstellen.

(Pressemitteilung vom 17.11.2017)

Transparenz bei Videoüberwachung nach der DS-GVO

Die Aufsichtsbehörden sind abgestimmt der Auffassung, dass über eine Videoüberwachung vollständig zu informieren ist. Es gilt folgendes:

„Die sich aus Art. 12 ff. DS-GVO ergebenden Anforderungen an transparente und umfassende Informationen sind auch bei Videoüberwachungen angemessen, d.h. adressatengerecht umzusetzen.“

Dabei ist bei Videoüberwachungen davon auszugehen, dass der Informationskatalog des Art. 13 Absatz 1 und 2 DS-GVO zu beachten ist, der folgende Mindestanforderungen umfasst:

- Umstand der Beobachtung – Piktogramm, Kamerasymbol,
- Identität des für die Videoüberwachung Verantwortlichen – Name einschl. Kontaktdaten (Art. 13 Absatz 1 lit. a DS-GVO),
- Kontaktdaten des betrieblichen Datenschutzbeauftragten – soweit bestellt, dann aber zwingend (Art. 13 Absatz 1 lit. b DS-GVO),
- Verarbeitungszwecke und Rechtsgrundlage in Schlagworten (Art. 13 Absatz 1 lit. c DS-GVO),
- Angabe des berechtigten Interesses – soweit die Verarbeitung auf Art. 6 Absatz 1 lit. f DS-GVO beruht (Art. 13 Absatz 1 lit. d DS-GVO),
- Dauer der Speicherung (Art. 13 Absatz 2 lit. a DS-GVO),
- Hinweis auf Zugang zu den weiteren Pflichtinformationen gem. Art. 13 Absatz 1 und 2 DS-GVO (wie Aus-

kunftsrecht, Beschwerderecht, ggf. Empfänger der Daten).

Hinsichtlich der Angabe der Kontaktdaten des betrieblichen Datenschutzbeauftragten genügt die Angabe der Funktion, der Name ist nicht zwingend anzugeben.

Die Zwecke der Datenverarbeitung können stichwortartig angegeben werden, aber nicht zu plakativ (Art. 12 Absatz 7 DS-GVO). Die Stichworte müssen allerdings dem Ziel der Transparenzpflichten aus Art. 5 Absatz 1 lit. a DS-GVO gerecht werden, den Betroffenen

über den Zweck der Videoüberwachung hinreichend konkret zu informieren.

Es wird empfohlen, den in der Anlage beigefügten Entwurf für ein vorgelagertes Hinweisschild und für ein Informationsblatt zu verwenden. (Anlage 1 und 2).“

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung¹



Weitere Informationen erhalten Sie:

- per Aushang (wo genau?)
- an unserer Kundeninformation / Rezeption / Kasse im Erdgeschoss
- (ggf.) zusätzlich im Internet unter ...

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

¹ Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen.

Literaturhinweise

Carlo Piltz, **BDSG – Vorschriften für nichtöffentliche Stellen**, Kommunikation & Recht, Praxiskommentar, Mainz 2017, 372 S., 89,- €

Ab Mai 2018 schafft in ganz Europa die EU-Datenschutz-Grundverordnung (EU-DS-GVO) unmittelbar anwendbare Regeln zum Umgang mit personenbezogenen Daten. Doch bleibt es nicht bei der europäischen Vorgabe. Die EU-DS-GVO gibt den Mitgliedstaaten die Möglichkeit, besondere Bereiche, Verarbeitungssituationen oder den Umgang mit besonderen Kategorien personenbezogener Daten spezifischer auszugestalten.

Von diesen „Öffnungsklauseln“ der DS-GVO will der deutsche Gesetzgeber durch das neue BDSG Gebrauch machen, das zusammen mit der DS-GVO ab Mai 2018 anwendbar sein soll.

Dieser Praxiskommentar richtet sich an nichtöffentliche Stellen, insbesondere Unternehmen und privatwirtschaftlich organisierte Einheiten sowie dort tätige Datenschutzverantwortliche. Er bietet einen Überblick über die für sie relevanten Bestimmungen des neuen BDSG. Hierzu gehören insbesondere: räumlicher und sachlicher Anwendungsbereich, Videoüberwachung, Verarbeitung besonderer Kategorien personenbezogener Daten, Vorgaben zur (Be-)Stellung des Datenschutzbeauftragten, Beschäftigten-Datenschutz und Beschränkungen der Betroffenenrechte. Die Kommentierung orientiert sich an der Praxis und den Anforderungen von Wirtschaft und Industrie.

(Prof. Peter Gola, Königswinter)

Sebastian Bauer, **Soziale Netzwerke und strafprozessuale Ermittlungen**, Strafrechtliche Abhandlungen, Neue Folge (SRA), Band 281, Duncker & Humblot, Berlin 2018, 406 S., 89,90 €

Soziale Netzwerke zählen zu den meistgenutzten Kommunikationsdiensten des

Internets und sind unlängst in den Fokus der Strafverfolgungsbehörden gerückt. Die Arbeit hat es sich zum Ziel gesetzt, *de lege lata* und *de lege ferenda* die rechtlichen Herausforderungen zu bewältigen, welche soziale Netzwerke verfassungs- und strafprozessrechtlich aufwerfen. Der Zugriff auf öffentlich zugängliche Daten, verdeckte Ermittlungen und der Zugriff auf nicht öffentlich zugängliche Daten bilden den Kern dieser Abhandlung. Das Interesse an einer effektiven Strafverfolgung steht der Freiheitsosphäre der Bürger dabei in einem Spannungsverhältnis gegenüber, welches diese Arbeit zu reduzieren versucht. Der Schwerpunkt liegt auf den Anforderungen, welche das Recht auf informationelle Selbstbestimmung, das IT-Grundrecht und das Fernmeldegeheimnis an strafprozessuale Ermächtigungsgrundlagen stellen, sowie auf der Vereinbarkeit von verdeckten Ermittlungen mit der Selbstbelastungsfreiheit. Soweit die StPO keine hinreichenden Ermächtigungsgrundlagen für derartige Ermittlungen enthält, erarbeitet der Autor entsprechende Gesetzentwürfe.

(Prof. Peter Gola, Königswinter)

Schantz/Wolff, **Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis**, C.H. Beck-Verlag, München 2017, 437 S., 59,- €

Mit dem neuen Bundesdatenschutzgesetz (BDSG) vom 30. Juni 2017 wurde nach der europäischen Datenschutz-Grundverordnung (DS-GVO) sowie der europäischen Richtlinie für den Datenschutz bei Polizei und Strafjustiz (JI-RL) vom April 2016 nun auch die größte nationale Datenschutzrechtsreform der letzten Jahrzehnte auf den Weg gebracht. Zwei umfangreiche und komplexe Regelwerke – die DS-GVO mit 99 Artikeln und 173 Erwägungsgründen sowie das novellierte

BDSG mit 85 Paragraphen – geben zukünftig den Rechtsrahmen für private, unternehmerische und öffentliche Datenverarbeitungen vor.

Das rechtliche Zusammenwirken von DS-GVO und BDSG und die Reichweite der jeweiligen neuen Datenschutzpflichten und –rechte sind sehr umstritten. Europäisches und deutsches Datenschutzrecht wird in drei Konstellationen nebeneinander anwendbar sein:

- Im Bereich der DS-GVO wird die Rechtslage aus einer Kombination von europäischem und nationalem Recht gebildet, insb. dem neuen BDSG, das u.a. Regelungen zur Konkretisierung der zahlreichen „Öffnungsklauseln“ der DS-GVO enthält.
- Im Bereich der JI-RL ist vorrangig das nationale Recht heranzuziehen, insb. das neue BDSG, das die Richtlinie umsetzt.
- In Bereichen außerhalb von DS-GVO und JI-RL ist nationales Recht grds. weitgehend isoliert anwendbar.

Der neue Praxisleitfaden stellt die Grundzüge des neuen Rechts eingängig und leicht verständlich dar. Ausgehend von allgemeinen datenschutzrechtlichen Prinzipien werden insbesondere die Neuregelungen durch die Datenschutz-Grundverordnung und das novellierte Bundesdatenschutzgesetz ausführlich behandelt. Dabei werden auch die praktischen Auswirkungen wichtiger Leitentscheidungen des EuGH und des BVerfG erörtert.

Als Fazit ist zu ziehen: Das Buch gibt eine fundierte Experteneinführung in das neue Datenschutzrecht „aus erster Hand“. Es klärt praxisorientiert Anwendungs- und Abrenzungsfragen der DS-GVO und des neuen BDSG anhand anschaulicher Übersichten.

(Schriftleitung)

Ehmann/Selmayr, **Datenschutz-Grundverordnung. Kommentar**, C.H. Beck-Verlag, München 2017, 1243 S., 139,- €

Die Datenschutz-Grundverordnung wird ab dem 25. Mai 2018 anwendbar sein und den Datenschutz in Europa neu ordnen. Es gibt zu ihr gefühlt mehr Kommentare als zum BGB, und das hat seinen guten Grund. Schließlich treibt das Datenschutzrecht Wirtschaft und Datenschutzaufsicht – insbesondere durch die im Vergleich zum noch geltenden Recht deutlich verschärften Pflichten und drastisch erhöhten Bußgeldandrohungen – gleichermaßen um. Der Kommentar zur DS-GVO von Ehmann/Selmayr ist auf dem Stand von Mitte Januar 2018 und muss daher ohne Berücksichtigung des seit Juli 2017 verabschiedeten neuen BDSG auskommen. Der Autorenkreis setzt sich aus teilweise exponierten Praktikern zusammen – unter anderem aus dem EU-Parlament, der Verwaltung, der Aufsicht, der Anwaltschaft sowie aus Hochschulangehörigen.

Die Herausgeber widmen sich einfühlend einem Überblick über die Entstehungsgeschichte der Grundverordnung, dem die besondere Nähe der Autoren zum Entstehungsprozess zu Gute kommt. Wer sich hierzu einen prägnanten und zugleich umfassenden Überblick verschaffen möchte, ist in diesem Werk bestens aufgehoben. Die Kommentierungen selbst erfüllen vom Umfang her, was einem Kurz-Kommentar angemessen ist. Bei einer Kommentierung, die im Vorgriff auf die Anwendbarkeit der kommentierten Rechtsnormen erscheint, liegt die Herausforderung zum einen darin, Sinn und Systematik der Normen zu erklären und zum anderen darin, die Probleme des künftigen Rechts für die Praxis zu antizipieren und der künftigen Anwendung des bevorstehenden Rechts Impulse zu geben. Die erste Anforderung erfüllt der Kommentar solide. Hervorgehoben sei hier etwa die nüchterne und zutreffende Analyse von Heberlein zu Art. 6 Abs. 2 DS-GVO (Rn. 30 ff.).

Diese Öffnungsklausel in der „hinkenden Verordnung“ (Rn. 31 m.w.N.) ist für das Verhältnis zwischen DS-GVO und BDSG neu elementar. Sie dürfte im BDSG neu etwa den Zulässigkeitsrahmen für § 4 BDSG neu mit seinen deutschen Sonderregelungen zur Videoüberwachung aus Gründen des öffentlichen Interesses liefern. Mit Blick auf die Zulässigkeit der Videoüberwachung nach der DS-GVO, die für die unternehmerische Praxis von besonderer Bedeutung ist, stellt die Kommentierung aber keine grundlegenden Erwägungen an, sondern nimmt hierzu punktuell Stellung, etwa im Rahmen der Datenschutz-Folgenabschätzung (Art. 35 Rn. 23).

Allerdings legen die Herausgeber ausweislich des Vorwortes Wert darauf, die Brille des nationalen Rechts mit ihren unterschiedlichen Sichtweisen bewusst abzulegen. Dieser Ansatz hat den Vorteil, eine konsistente Kommentierung liefern zu können, der sich von den namentlich in Deutschland teilweise geltenden Besonderheiten löst. Damit ist aber – wie insbesondere § 4 Abs. 1 und 3 BDSG neu als nationale Präzisierung der Zulässigkeit der Videoüberwachung zeigen – zugleich der Nachteil verbunden, dass dem deutschen Anwender der bewertende Blick auf das Zusammenspiel von DS-GVO und nationalem Recht im Rahmen der Öffnungsklauseln verwehrt wird.

Mit Blick auf die Praxis sind zudem die Informationspflichten nach Art. 12 bis 14 DS-GVO von besonderer Bedeutung. Sie erlegen der unternehmerischen Praxis über die Pflichten im Rahmend der Zulässigkeit hinaus, umfangreiche weitere und neue Pflichten auf. Sie werden von Heckmann/Paschke (Art. 12) und Knyrim (Art. 13 und 14) kommentiert. Die Kommentierung des Art. 12 DS-GVO zu den allgemeinen Grundlagen der Information arbeitet die Voraussetzungen der Norm sicher ab und greift dort, wo es möglich

ist, die Rechtsprechung des EuGH auf. Das ist insbesondere bei der „leichten Zugänglichkeit“ einer Information der Fall (Art. 12 Rn. 14 ff.) und gerade mit Blick auf die Beratung in Streitfällen mit der Aufsicht um die Anforderungen ausgesprochen hilfreich. Art. 13 und 14 betreffen die Datenerhebung bei der betroffenen Person bzw. nicht bei der betroffenen Person. Mit Blick auf die Parallelen ist es gut vertretbar, wenn die Kommentierung in Art. 14 an den entsprechenden Stellen auf Art. 13 verweist. Die Kommentierung ist sowohl präzise, als auch prägnant und beschreibt etwa das eigentümliche, faktisch kumulative Verhältnis der Informationspflichten aus Abs. 1 („immer“) und Abs. 2 („situationsabhängig“) aber mit dem Risiko der Verkennung der Erfordernisse der Situation) auf den Punkt (Art. 13 Rn. 18-20). Zugleich zeigt sich gerade hier, dass es ohne Rechtsprechung schwer ist, der Praxis eine Empfehlung an die Hand zu geben. Umso erfreulicher ist das vergleichsweise klare und plausibel begründete Bekenntnis zur Zulässigkeit des Medienbruches bei der Informationsgewährung (Art. 13 Rn. 13), ohne den die Praxis, denkt man beispielsweise an Automatenkäufe unter Eingabe von Zahlungsdaten oder Telefonbestellungen, nicht rechtskonform handlungsfähig ist.

Im Fazit kann man es kurz machen. Der Ehmann/Selmayr ist ein solider, kompakter, zuverlässiger und deshalb ausgesprochen hilfreicher Ratgeber für die Datenschutzpraxis. Es gelingt den Autorinnen und Autoren die komplexe Materie mit dem für die Anforderungen der Praxis erforderlichen Tiefgang souverän abzubilden, ohne sich in Details zu verlieren. Er hat seinen Platz unter den Kommentierungen zur DS-GVO eingenommen und wird ihn behaupten.

(Prof. Dr. Rolf Schwartmann)

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.

*Brecht, Corinna/Steinbrück, Anne/Wagner, Manuela, **Der Arbeitnehmer 4.0?*** Ping 2018, S. 10

Die Autorinnen zeigen Fragen der Zulässigkeit automatisierter Arbeitgeberentscheidungen durch Sensorik am smarten Arbeitsplatz auf.

*Brüggemann, Dr. Sebastian, **Das Recht auf Datenportabilität,*** K&R 2018, S. 1

Das neue Recht auf Datenportabilität stellt ein Novum, aber auch einen Fremdkörper im datenschutzrechtlichen Kontext dar, zu dessen Einbindung es noch einiger Zeit bedarf. Dazu tragen neben fehlenden etablierten technischen Standards vor allem auch die fehlende Rechtssicherheit im Hinblick auf Art und Umfang der zu übertragenden Daten als auch die ungeklärten Haftungsfragen bei.

*Hartung, Jürgen/Steinweg, Helge, **Vereinbarungen mit Dienstleistern nach dem neuen § 203 StGB und der DSGVO,*** PinG 2018, S. 21

Aufgezeigt wird die datenschutzrechtliche Komponente der nunmehr erlaubten Auslagerungen von Datenverarbeitungen durch Berufsgeheimnisträger, d.h. dass die Vertragsbeziehungen mit dem Dienstleister DS-GVO-konform und auch dem mit dem Patienten/Klienten bestehenden vertraglichen Beziehung vereinbar sein müssen. Beispiele werden in Praxishinweisen dargestellt.

*Hohenstein, Sarah, **Die Vererblichkeit des digitalen Nachlasses,*** K&R 2018, S. 5

Ein Leben ohne Smartphones, Tablets, E-Mail-Accounts, Online-Shops oder soziale Netzwerke ist in der heutigen Gesellschaft so gut wie undenkbar. Doch was passiert nach dem Tod eines Menschen mit dessen "digitalen Spuren"? Erörtert wird, ob Erben auf das E-Mail-Postfach oder den Account eines sozialen Netzwerkes des Verstorbenen zugreifen bzw. Diensteanbieter Zugangsdaten an die Erben herausgeben und einen Zugriff auf die gespeicherten Daten ermöglichen müssen.

*Kraus, Michael, **Neuregelung von § 203 StGB,*** Ping 2018, S. 16

Das „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (BGBl. 2017, Teil I, Nr. 71, S. 3618) eröffnet den Weg für eine straffreie Auslagerung von Dienstleistungen auch für Berufsgeheimnisträger. Der Beitrag stellt die dazu erfolgenden Änderungen des Strafrechts und die neuen berufsrechtlichen Befugnisnormen für Anwälte und Steuerberater vor.

*Schulte, Laura, **Transparenz im Kontext der DSGVO,*** PinG 2017, S. 227

„Transparenz“ zählt zu den zentralen Begriffen des neuen europäischen Rechtsrahmens für den Datenschutz. Der vorliegende Beitrag beleuchtet das der DS-GVO zugrundeliegende Transparenzkonzept und untersucht dessen Konsequenzen.

*Seile, David, **Überblick zur Datenverarbeitung im medizinischen Bereich unter der DSGVO,*** Ping 2018, S. 43

Der Beitrag behandelt ohne Anspruch auf Vollständigkeit datenschutzrechtliche Fragen im medizinischen Bereich mit Blick auf die DS-GVO unter Berücksichtigung der Novellierung des § 203 StGB.

*Veil, Winfried, **Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO?,*** ZD 2018, S. 9

Der Beitrag untersucht, was die in der DS-GVO dem Verantwortlichen auferlegten Nachweispflichten bedeuten und wie weit sie reichen, und zeigt diesbezügliche Unsicherheiten auf.

*Ziehbarth, Wolfgang, **Verbesserte Videoüberwachung? Auswirkungen des Videoüberwachungsverbesserungsgesetz,*** ZD 2017, S. 467

Die durch das Videoüberwachungsverbesserungsgesetz erfolgte Ergänzung des § 6b BDSG a.F. schafft nach Ansicht des Autors zum einen keine neue verbesserte Sicherheitslage und ist zum anderen in der Wiederholung der Norm als § 4 BDSG 2018 mit den Abs. 1 S. 2 und Abs. 3 S. 2 unionsrechtswidrig.



Aus der Frühzeit der Datenlöschkonzepte

Die weiße Wand löscht sicher

Daten, die man nicht mehr braucht, gehören gelöscht. Unternehmen sind rechtlich dazu verpflichtet, wenn der Zweck sie zu nutzen oder zu speichern wegfällt. Die Datenschutz-Grundverordnung befasst sich mit dem komplizierten Zusammenspiel zwischen Löschen und Einschränken der Verarbeitung vor allem in Art. 17 und 18. Komplexe Datenbankstrukturen und Software, die ein punktuell Lösch bisweilen nicht vorsieht, stellen Unternehmen ebenso vor Probleme, wie das Löschen aus Backups. Datenschutzrechtlich müssen sich die Lösungen einerseits an den Vorgaben der Dokumentations- und Nachweisverpflichtungen ausrichten und andererseits dem Grundsatz der Datenminimierung, insbesondere den Löschverpflichtungen Rechnung tragen.

Aber auch im Privaten kommt man am Löschen nicht vorbei. Wie das unwiederbringlich geht, wenn man ein gebrauchtes Smartphone weitergibt, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) erklärt. Zunächst muss man alles, was man behalten will, speichern und dabei darauf achten, dass die Daten auf dem neuen Gerät lesbar sind. Danach geht es ans Löschen. Wer das Gerät dazu nur auf die Werkseinstellungen zurücksetzt, handelt möglicherweise nicht gründlich genug. Oft können Daten danach noch wiederhergestellt werden. Deshalb sollte man vor dem Zurücksetzen, die sog. Speichergrundverschlüsselung auf dem Handy aktivieren, sofern sie nicht schon voreingestellt ist. Gibt es keine Verschlüsselungsfunktion rät das BSI dazu, den Speicher nach dem Lö-

schen mit belanglosen Daten, etwa dem Video einer weißen Wand, zu überschreiben. Erst danach ist das Zurücksetzen auf die Werkseinstellungen sicher. Sim-Karten sind durch PIN und PUK geschützt. Man kann sie endgültig sperren, indem man mehrfach falsche Codes eingibt. Beim neuen Besitzer des Geräts hat die vertragsgebundene SIM-Karte nichts zu suchen. Ist eine Micro-SD-Karte im Gerät, nimmt man sie heraus und behält sie besser. Für den neuen Besitzer legt man dann eine neue passende Karte bei.



PRIVACYSOFT

Die modulare Software-Plattform für alle Aufgaben im Datenschutzmanagement.



DAS DSB-MULTI-TOOL FÜR DEN DATENSCHUTZ NACH EU-DSGVO

Datenschutzdokumentation | Vorlagen und Checklisten | Vorgangsmanagement | Online-Schulungen

Best Practice. Best Command.



**Inklusive CD
mit allen Ver-
tragsmustern**

Redeker (Hrsg.),

Handbuch der IT-Verträge

Herausgegeben von RA, FA IT-Recht,
Dipl.-Informatiker Dr. Helmut Redeker.
Loseblatt, 3 Bände. Grundwerk mit
Fortsetzungsbezug für mindestens
2 Jahre nur 159,- €, ca. 2 Ergänzungs-
lieferungen pro Jahr,
ISBN 978-3-504-56008-9.

Das praxisnahe Werk zur Vertragsgestaltung versorgt Rechtsberater und Entscheider in Unternehmen in verschiedensten IT- und telekommunikationsrechtlichen Bereichen mit **ausführlich kommentierten Vertragsmustern**. Klausel für Klausel nehmen erfahrene Praktiker zu allen praxisrelevanten Fragen u.a. des IT-Vertragsrechts, des Internetrechts und des Telekommunikationsrechts Stellung. Sonderfälle werden mit Alternativklauseln und -mustern berücksichtigt.

Neuerungen und Aktualisierungen u.a. (Stand November 2017):

- Domain-Service-Vertrag
- Datenschutzerklärung
- Festnetz-Provider-Vertrag mit dem Kunden
- Schlichtung

Neu: Geschäftsbesorgungsvertrag mit einem externen Datenschutzbeauftragten

Ausführliche Informationen,
Bestellung und Leseprobe unter
www.otto-schmidt.de/riv



Das Werk online:
juris.de/pmitr

ottoschmidt