

Zeitschrift für  
Datenschutz-,  
Informations- und  
Kommunikationsrecht

# RDV

4/2017

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

BIEKER/HANSEN, Datenschutz „by Design“ und „by Default“ nach  
der neuen europäischen Datenschutz-Grundverordnung

BRINK/SCHWAB, Beschäftigtendatenschutz: Zwischen wirtschaftlicher  
Abhängigkeit und informationeller Selbstbestimmung

## Kurzbeiträge

GOLA, Aus den aktuellen Berichten der Aufsichtsbehörden (31);  
Auswirkungen der DS-GVO auf Auskunftsteien, Inkassounternehmen  
und Kreditwesen

BENEDIKT, Datenportabilität – das neue Recht des Betroffenen

THIEL, Die DSGVO als Herausforderung (auch) für die Aufsichts-  
behörden

## Rechtsprechung Aus dem Inhalt

EUGH, Zur zusätzlichen Identifizierung durch Kopie des Reise-  
passes bei Nicht-EU-Bürger (Ls)

EUGH, Bereitstellung von Teilnehmerdaten an öffentlich zugängliche  
Auskunftsdienste und Teilnehmerverzeichnisse in der EU  
und Einwilligung des Teilnehmers

BGH, Datenerhebungen einer Versicherung zur Feststellung von  
vertraglichen Obliegenheitsverpflichtungen (Ls)

BAG, Kein durchsetzbarer Anspruch auf Inhalt einer bestimmten  
Zeugnisnote

OLG FRANKFURT AM MAIN, Haftung des Landes für Urheberrechts-  
verletzungen eines Lehrers

KG BERLIN, Zugang der Eltern eines verstorbenen Kindes zu  
dessen Daten in einem sozialen Netzwerk (Ls)

33. Jahrgang  
August 2017  
Seiten 163–216



Gesellschaft für Datenschutz  
und Datensicherheit e.V.



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

### Inhaltsverzeichnis

#### Editorial

163

#### Veranstaltungen

164

#### Aufsätze

Felix BIEKER/Marit HANSEN  
Datenschutz „by Design“ und „by Default“ nach der  
neuen europäischen Datenschutz-Grundverordnung 165

Dr. Stefan BRINK/Sabrina SCHWAB  
Beschäftigtendatenschutz: Zwischen wirtschaftlicher  
Abhängigkeit und informationeller Selbstbestimmung 170

#### Kurzbeiträge

Prof. Peter GOLA  
Aus den aktuellen Berichten der Aufsichtsbehörden  
(31): Auswirkungen der DS-GVO auf Auskunfteien,  
Inkassounternehmen und Kreditwesen 187

Kristin BENEDIKT  
Datenportabilität – das neue Recht des Betroffenen 189

Barbara THIEL  
Die DSGVO als Herausforderung (auch) für die  
Aufsichtsbehörden 191

#### Rechtsprechung

Zur zusätzlichen Identifizierung durch Kopie des  
Reisepasses bei Nicht-EU-Bürgern (Ls)  
(EuGH, Urteil vom 06.04.2017) 192

Bereitstellung von Teilnehmerdaten an öffentlich  
zugängliche Auskunftsdienste und Teilnehmerverzeich-  
nisse in der EU und Einwilligung des Teilnehmers  
(EuGH, Urteil vom 15.03.2017) 192

Datenerhebungen einer Versicherung zur Feststellung  
von vertraglichen Obliegenheitsverpflichtungen (Ls)  
(BGH, Urteil vom 22.02.2017) 196

Kein durchsetzbarer Anspruch auf Inhalt einer bestimm-  
ten Zeugnisnote (BAG, Beschluss vom 14.02.2017) 197

Haftung des Landes für Urheberrechtsverletzungen eines  
Lehrers (OLG Frankfurt am Main, Urteil vom 09.05.2017) 198

Zugang der Eltern eines verstorbenen Kindes zu  
dessen Daten in einem sozialen Netzwerk (Ls)  
(KG Berlin, Urteil vom 31.05.2017) 201

Satzungsmäßige Befugnis einer Krankenkasse zur Vorlage  
von Behandlungsunterlagen an Sachverständige (Ls)  
(VerwGH Baden-Württemberg, Urteil vom 10.05.2017) 201

Zur vollständigen Einsicht in Akten des Sozialpsychia-  
trischen Dienstes (Ls)

(OVG Lüneburg, Beschluss vom 08.05.2017) 201

Unerlaubte Datenübermittlung im privaten Umfeld  
(Ls) (LG Düsseldorf, Urteil vom 20.02.2017) 202

Verantwortung der Eltern für datenschutzkonforme  
Smartphone-Nutzung ihrer Kinder (Ls)  
(AG Bad Hersfeld, Beschluss vom 20.03.2017) 202

Zulässigkeit eines Fahrerbewertungsportals  
(VG Köln, Urteil vom 16.02.2017) 202

#### Berichte, Informationen, Sonstiges

Bitkom: Jedes fünfte IT-Unternehmen ignoriert  
bislang die Datenschutz-Grundverordnung 210

Berliner Beauftragte für Datenschutz und Informations-  
freiheit: Beschneidung der Kontrollbefugnisse der  
Datenschutzaufsichtsbehörden nicht hinnehmbar 210

Aufsichtsbehörden: Datenschutz bleibt Chefsache  
– Halbzeit auf dem Weg zur EU-Datenschutz-Grundver-  
ordnung: Zehn Punkte zur Umsetzung 211

Deutscher Bundestag: Wissenschaftliche Dienste zur  
Rechtsgrundlage für den Einsatz sog. intelligenter  
Videoüberwachung durch die Bundespolizei (WD 3 –  
3000 – 202/16) 212

#### Literaturhinweise

##### Buchbesprechungen

*Kranig/Sachs/Gierschmann*, Datenschutz-Compliance  
nach der DS-GVO – Handlungshilfe für Verantwortliche  
inklusive Prüffragen für Aufsichtsbehörden  
(GABRIELA KRADER, LL.M) 213

*Elisa Stettner*, Sicherheit am Bahnhof – Überwachungs-  
maßnahmen zur Abwehr terroristischer Anschläge  
(SCHRIFTFLEITUNG) 213

*Florian Eisenmenger*, Die Grundrechtsrelevanz „virtueller  
Streifenfahrten“ – dargestellt am Beispiel ausgewählter  
Kommunikationsdienste des Internets  
(SCHRIFTFLEITUNG) 214

*Peter Gola (Hrsg.)*, DS-GVO – Datenschutz-Grund-  
verordnung VO (EU) 2016/679, Kommentar  
(DR. GEORG WRONKA) 214

##### Neuerscheinungen

Aufsätze 215

**Nachgefasst** 216

## Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

Prof. Dr. Rolf SCHWARTMANN, Fachhochschule Köln

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

## in Kooperation mit der

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

## Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

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

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

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

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

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

Prof. Dr. Karl LINNENKOHLE, Universität Kassel

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

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

Prof. Dr. Michael RONELLENFITSCH, Hessischer Datenschutzbeauftragter

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

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

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

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

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Iriini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

---

**Beilagenhinweis:** GDD-Mitteilungen 4/2017; Synopse DS-GVO – BDSG; DATAKONTEXT, Frechen; Beck Verlag, München

---

## 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  
33. Jahrgang 2017 Heft 4  
Seiten 163–216

# RDV

## Recht der Datenverarbeitung

33. Jahrgang · August 2017 · Seiten 163–216

## Editorial

### Datenschutz jenseits des Atlantiks

Die DS-GVO hat den Datenschutz endgültig europäisch verankert. Doch wenn ich mit Kollegen aus den USA spreche, dann schütteln auch die, die durchaus Kenntnisse des europäischen und deutschen Rechts haben, beim Datenschutz zuweilen genauso verwundert den Kopf, wie das manch einer von uns im Hinblick auf das ein oder andere Urteil diskriminierungsrechtlichen Strafschadensersatzes eines US-Gerichts tut. Datenschutz, und insbesondere so ernst wie ihn die Deutschen nehmen, ist eine Mischung aus Voodoo und Sozialismus – ganz fern, ganz unverständlich und irgendwo reichlich übertrieben.

Nun sind amerikanische Juristen traditionell zurückhaltend mit der Orientierung an ausländischen Rechtsordnungen. So stellte bereits der jüngst verstorbene Justice Scalia stellvertretend für viele im Hinblick auf rechtsvergleichende Ausführungen des obersten Bundesgerichts fest, diese seien "[d]angerous" denn "this Court... should not impose foreign moods, fads, or fashions on Americans" (Lawrence v. Texas, 539 U.S. 558 [2003]). Am amerikanischen Wesen soll die Welt genesen. Die extraterritoriale Anwendung so mancher US-amerikanischer Rechtsnorm ist deutschem Denken fremd.

Dennoch: Auch deutsches Datenschutzrecht ist vermittelbar. Es ist Per-

sönlichkeitsschutz, und als solcher ist er ernst zu nehmen. So hat gerade auch die Diskussion um die mühsam errungene *Privacy Shield*-Regelungen einen Umdenkprozess auch bei manchen in den USA eingeleitet. Eine kürzlich durchgeführte Befragung des Pew Research Center zeigte eine deutliche Zustimmung für strengeren Datenschutz bei den US-Bürgern. Pew stellte fest, dass „68 percent of internet users believe current laws are not good enough in protecting people’s privacy online.“ Spielt das Thema auch im US-Wahlkampf keine Rolle – dort geht es eher um die Abwehr von Cyber War und welche Daten mehr es dafür braucht –, zumindest die juristische Fachwelt beschäftigt sich nun intensiver mit diesem Thema, der Schrems-Fall und die Datenschutzgrundverordnung wurden hier Katalysator einer Diskussion.

Für das Verständnis des europäischen Datenschutzes muss man werben – jedes internationale Unternehmen kann es aber auch. Zunächst dadurch, dass man Binding Corporate Rules und Standardvertragsklauseln nicht bloß als lästige Pflicht begreift, die es abzarbeiten gilt, sondern als sinnvolles Instrument zum Schutz der Persönlichkeit von Kunden und Arbeitnehmern. Zum anderen aber auch dadurch, dass es sich in Prozessen vor US-Gerichten hierfür stark macht, und auch ange-

sichts von Discovery-Anforderungen auf den Konflikt zum deutschen Recht hinweist, s. etwa jüngst den United States District Court, E.D. Louisiana. In re: Xarelto (Rivaroxaban) Products Liability Litigation 2016 WL 3923873: „[T]here is a clear conflict between the federal discovery rules and the German Data Protection Act.“ Schließlich kann sich auch die Wirtschaft in die Diskussion um die Praktikabilität und Grenzen von Privacy Shield weiterhin einbringen, um hier den Datenschutz gerade im Austausch mit den USA sinnvoll weiter zu entwickeln. Es gibt viel zu tun, packen wir es an.

Prof. Dr. Gregor Thüsing



**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.

Termin	Thema	Ort	Kontakt
04.09.2017	Datenschutz-Schwachstellen und die erheblichen Bußgeldrisiken nach der DS-GVO vermeiden	Köln	GDD e.V. und DATAKONTEXT
05.09.2017	Beschäftigtendatenverarbeitung: Zulässigkeit und Organisation	Köln	GDD e.V. und DATAKONTEXT
05.09.2017	Personalprozesse datenschutzkonform organisieren	Stuttgart	GDD e.V. und DATAKONTEXT
11.-15.09.2017	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Bonn	GDD e.V. und DATAKONTEXT
11.09.2017	Datenschutz-Folgenabschätzung	Stuttgart	GDD e.V. und DATAKONTEXT
12.09.2017	IT-Sicherheit für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
19.09.2017	Datenschutz Aktuell	Stuttgart	GDD e.V. und DATAKONTEXT
19.09.2017	Datenschutz bei Unternehmenstransaktionen	Köln	GDD e.V. und DATAKONTEXT
25.09.2017	ISO 27001 und Datenschutz	Köln	GDD e.V. und DATAKONTEXT
26.09.2017	Einsatz mobiler Endgeräte: Datenschutz und IR-Sicherheit	Köln	GDD e.V. und DATAKONTEXT
27.09.2017	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Köln	GDD e.V. und DATAKONTEXT
28.09.2017	Big Data-Analysen und der Datenschutz	Köln	GDD e.V. und DATAKONTEXT
09.-10.10.2017	Datenschutz Kompakt	Frankfurt/M.	GDD e.V. und DATAKONTEXT
09.-11.10.2017	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Berlin	GDD e.V. und DATAKONTEXT
16.10.2017	Kundendatenschutz nach der DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
16.10.2017	Grenzüberschreitender Datenverkehr unter neuen Spielregeln	Köln	GDD e.V. und DATAKONTEXT
17.10.2017	Datenschutz und Videoüberwachung – was geht und was geht nicht?	Berlin	GDD e.V. und DATAKONTEXT
25.10.2017	Hacker-Tools für Datenschutzbeauftragte	Berlin	GDD e.V. und DATAKONTEXT
02.11.2017	IT-SecurityCircles – was tun, wenn´s brennt oder knallt?	Berlin	GDD e.V. und DATAKONTEXT
06.-07.11.2017	IT-SecurityCircles – sicher durch die Brandung ...	Frankfurt/M.	GDD e.V. und DATAKONTEXT
07.-08.11.2017	Datenschutz-Management – Teil 3	Berlin	GDD e.V. und DATAKONTEXT
08.11.2017	Grundlagen der Auftragsverarbeitung (AV)	Köln	GDD e.V. und DATAKONTEXT
13.11.2017	IT-SecurityCircles – Home-Office – sweet Home-Office?	Leipzig	GDD e.V. und DATAKONTEXT
14.11.2017	Prüfung von SAP-Systemen durch Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
15.11.2017	36. RDV-Forum	Köln	GDD e.V. und DATAKONTEXT

# Aufsätze

Felix Bieker/Marit Hansen

## Datenschutz „by Design“ und „by Default“ nach der neuen europäischen Datenschutz-Grundverordnung

Zu den neuen Anforderungen der Datenschutz-Grundverordnung gehört der Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“. So neu ist die Idee eines eingebauten Datenschutzes zwar nicht: Mitte der 1990er Jahre hatten die Datenschutzbeauftragten der Niederlande und von Ontario, Kanada, mit der Veröffentlichung „The Path to Anonymity“<sup>1</sup> den Begriff der „Privacy-Enhancing Technologies“ (datenschutzfördernde Technik) geprägt. Technik selbst sollte die durch den technischen Fortschritt verursachten Risiken für den Datenschutz eindämmen. In Deutschland griff der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder diese Idee in einer Orientierungshilfe auf.<sup>2</sup> Natürlich reicht es nicht aus, nur bei der Technik anzusetzen. Auch organisatorische Prozesse, die Unternehmenskultur und – ganz wichtig – die Geschäftsmodelle spielen bei der Systemgestaltung eine wesentliche Rolle, wenn es darum geht, Datenschutz einzubauen. 2010 verabschiedete die Internationale Konferenz der Datenschutzbeauftragten die „Privacy by Design Resolution“.<sup>3</sup> Die interdisziplinäre Forschungs-Community, die sich mit Systemgestaltung à la Datenschutz

beschäftigt, wächst. Förderprojekte auf nationaler und europäischer Ebene arbeiten daran, die Tauglichkeit datenschutzfreundlicher Lösungen unter Beweis zu stellen. Allerdings kann man kaum feststellen, dass bisher die Umsetzung der schönen Datenschutz-Ideen Fahrt aufgenommen hätte und die Praxis der Datenverarbeitung prägte.

§ 3a BDSG bezieht sich auf die „Auswahl und Gestaltung von Datenverarbeitungssystemen“, die dem Prinzip der Datenvermeidung und Datensparsamkeit genügen sollen. Allerdings sieht das BDSG keine Sanktionen vor, wenn die verantwortliche Stelle diese Anforderungen nicht ausreichend umsetzt. In der Vergangenheit ist dieser Regelung daher keine große Bedeutung zugekommen. Dies soll mit der Datenschutz-Grundverordnung anders werden. Ein Verstoß gegen Artikel 25 kann gem. Artikel 83 Abs. 4 Buchst. a mit Geldbußen von bis zu 10 Mio. € oder bis zu 2 % des Vorjahresumsatzes geahndet werden.

Dieser Beitrag gibt einen Überblick darüber, wie Artikel 25 DSGVO die Prinzipien von Datenschutz „by Design“ und „by Default“ formuliert und was dies für die Anwender bedeutet.

### I. Datenschutz „by Design“ – Art. 25 Abs. 1 DS-GVO

Nach Artikel 25 Abs. 1 DS-GVO muss der Verantwortliche bereits bei der Festlegung der Mittel einer Datenverarbeitung technische und organisatorische Maßnahmen treffen, um die Anforderungen des Datenschutzes umzusetzen. Dabei entspricht der Wortlaut weitestgehend dem der Artikel 24 Abs. 1 („Verantwortung des für die Verarbeitung Verantwortlichen“) und Artikel 32 Abs. 1 DS-GVO („Sicherheit der Verarbeitung“), die den Verantwortlichen zum Ergreifen und Überprüfen sowie Aktualisieren solcher Maßnahmen verpflichten. Artikel 25 Abs. 1 DS-GVO unterscheidet sich jedoch dadurch, dass er den Zeitpunkt des Ergreifens dieser Maßnahmen festlegt und damit deutlich macht, dass dies von der Gestaltung einer Datenverarbeitung, bis zu deren Ende, also über ihren gesamten Lebenszyklus, zu erfolgen hat. Zudem stellt die Vorschrift klar, dass diese Maßnahmen dem Schutz der von der Datenverarbeitung betroffenen Personen dienen.

Der deutsche Titel des Artikel 25 ist dabei irreführend: Er betitelt die Vorschrift als „Datenschutz durch Technikgestaltung“. In vielen anderen Sprachfassungen, unter anderem Englisch als Verhandlungssprache des Gesetzgebungsprozesses, ist dagegen allgemeiner von „Datenschutz durch Gestaltung“ oder „eingebautem Datenschutz“ die Rede.<sup>4</sup> Die Einschränkung auf Gestaltung von Technik findet sich also

1 Van Rossum/Gardeniers/Borking u.a.: Privacy-Enhancing Technologies: The Path to Anonymity, Volume I und II. Hrsg. von Registratiekamer, The Netherlands & Information and Privacy Commissioner/Ontario, Canada, 1995; abrufbar unter: [http://www.cbppweb.nl/downloads\\_av/av11.pdf](http://www.cbppweb.nl/downloads_av/av11.pdf) (Link zur überarbeiteten Version von 2000).

2 AK Technik der Datenschutzbeauftragten des Bundes und der Länder: Arbeitspapier „Datenschutzfreundliche Technologien“, 1997; abrufbar unter: <http://www.datenschutz-bayern.de/technik/grundsatz/apdsft.htm>.

3 Pbd Resolution 2010] 32nd International Conference of Data Protection and Privacy Commissioners: Privacy by Design Resolution. 27.-29. Oktober 2010, Jerusalem, Israel; abrufbar unter: [http://www.ipc.on.ca/site\\_documents/pbd-resolution.pdf](http://www.ipc.on.ca/site_documents/pbd-resolution.pdf).

4 Vgl. [FR]: Protection des données dès la conception; [ES]: Protección de datos desde el diseño; [NL]: Gegevensbescherming door ontwerp en door standaardinstellingen; [SV]: Inbyggt dataskydd och dataskydd som standard.

in den anderen Versionen der DS-GVO nicht, so dass die Vorschrift wohl weiter zu verstehen ist und sich auch auf organisatorische und rechtliche Gestaltung bezieht.

Im Gegensatz zu Vorgängerregelungen, etwa den §§ 3a oder 9 BDSG, handelt es sich bei Artikel 25 Abs. 1 DS-GVO nicht um eine Zielvorgabe, sondern um eine nach Artikel 83 Abs. 4 Buchst. a DS-GVO sanktionsbewehrte Pflicht des Verantwortlichen.<sup>5</sup> Allerdings enthält diese Pflicht einige einschränkende Bedingungen, auf die sich der Verantwortliche berufen kann, wenn er bestimmte technische und organisatorische Maßnahmen nicht umsetzt: Die Verpflichtung erstreckt sich auf geeignete technische und organisatorische Maßnahmen, die unter Berücksichtigung des Stands der Technik und der Kosten der Implementierung in Abwägung mit den Risiken für die Rechte und Freiheiten natürlicher Personen aufgrund der Verarbeitung bestehen.

Dies eröffnet dem Verantwortlichen einen Spielraum. Der Begriff der „Stand der Technik“ ist zwar nicht neu und wurde bereits in Artikel 17 der DSRL verwendet. Eine genaue Definition fehlt jedoch. Zu den klaren Fällen gehören Maßnahmen, die offensichtlich veraltet und in ihrem Schutzniveau nicht ausreichend sind. Beispielsweise ließe sich leicht argumentieren, dass eine Website ohne SSL/TLS-Verschlüsselung, über die personenbezogene Daten verarbeitet werden, nicht mehr dem Stand der Technik entspricht. Weniger klar ist z. B. die Verwendung von datenschutzfreundlichen attributbasierten Berechtigungsnachweisen, die eine besonders datensparsame Authentifizierung ermöglichen.<sup>6</sup> Zwar ist diese Technik bereits verfügbar und hat in mehreren Anwendungskontexten ihre Funktionsfähigkeit unter Beweis gestellt. Jedoch müsste der Verantwortliche – solange es an Angeboten für entsprechende Infrastrukturen fehlt – seine eigene Infrastruktur für attributbasierte Berechtigungsnachweise aufbauen. Dies wird nicht immer zu verlangen sein.

Mit der Referenz auf den „Stand der Technik“ schafft Artikel 25 Abs. 1 DS-GVO immerhin einen verbindlichen Mindeststandard, der von den Aufsichtsbehörden durchzusetzen ist. In Zukunft wäre es wünschenswert, wenn kompetente Stellen ein Repository zum aktuellen Stand der Technik nicht nur aus Sicht der Sicherheit (Artikel 32 DS-GVO), sondern auch mit Hinblick auf die Datenschutz-Lösungen für die Erfüllung der Anforderungen nach Artikel 25 DS-GVO bereithielten, an dem sich Rechtsanwender orientieren können.<sup>7</sup> Wichtig wäre dabei eine ständige Pflege, damit die Informationen den aktuellen Wissensstand widerspiegeln, und eine Dokumentation von Abhängigkeiten oder etwaigen (unerwünschten) Seiteneffekten.

Ein inhärentes Problem des europäischen Datenschutzrechts, die Fixierung auf den Verantwortlichen, schlägt sich auch in Artikel 25 Abs. 1 DS-GVO nieder. In der Praxis setzen nur wenige Unternehmen oder Behörden für die Datenverarbeitung selbst entwickelte Produkte ein. In den meisten Fällen werden diese von externen Herstellern eingekauft. Diese Hersteller werden jedoch nur in Erwägungsgrund 78 erwähnt. Danach sollen sie „ermutigt“ werden, Datenschutz „by Design“ bei ihren Produkten, Dienstleistungen und An-

wendungen zu berücksichtigen und dadurch sicherzustellen, dass Verantwortliche ihren datenschutzrechtlichen Verpflichtungen nachkommen können. Weiterhin erwähnt Erwägungsgrund 78 öffentliche Ausschreibungen, die zur Umsetzung des Prinzips beitragen können. Die Ermutigung kann in diesem Fall von zwei Seiten kommen: Einerseits sollten Mitgliedstaaten durch finanzielle Anreize, wie Steuererleichterungen oder Förderprogramme für datenschutzfreundliche Systeme, ihre Lenkungs Aufgabe gegenüber der Wirtschaft wahrnehmen. Andererseits sind auch die Verantwortlichen verpflichtet, das Prinzip des Datenschutzes „by Design“ umzusetzen, wenn sie Produkte oder Dienstleistungen einsetzen. Artikel 24 Abs. 1 DS-GVO nennt im Rahmen der Verantwortung des Verantwortlichen im Gegensatz zu den Artikeln 25 Abs. 1 und 32 Abs. 1 DS-GVO auch nicht die Kosten der Implementierung. Diese sind zwar bei der konkreten Umsetzung spezifischer technischer und organisatorischer Maßnahmen zu berücksichtigen, können aber den Verantwortlichen gerade nicht von seiner Verantwortung befreien.

Zudem werden in der Praxis oft Dienstleister im Wege einer Auftragsverarbeitung gem. Artikel 28 DS-GVO eingesetzt. Gerade bei dieser entscheidet aber eben meist der Auftragsverarbeiter über die technischen und organisatorischen Maßnahmen im Rahmen der Entscheidung über die Mittel der Verarbeitung.<sup>8</sup> Der Verantwortliche ist gem. Artikel 28 Abs. 1 DS-GVO aber verpflichtet, nur mit solchen Auftragsverarbeitern zusammenzuarbeiten, die „hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt“. Dies bezieht selbstverständlich auch Artikel 25 DS-GVO mit ein. Indem der Verantwortliche sich für eine bestimmte Art der Verarbeitung für die von ihm festgelegten Zwecke entscheidet und im Rahmen seiner Privatautonomie eine Vereinbarung mit einem Auftragsverarbeiter schließt, verbleibt die Verantwortung für die Verarbeitungstätigkeit bei ihm.<sup>9</sup>

Für die Umsetzung des Prinzips des Datenschutzes „by Design“ in der Praxis ist die Datenschutz-Folgenabschätzung (DSFA) gem. Artikel 35 DS-GVO von großer Bedeutung.<sup>10</sup> Eine solche ist für Verarbeitungstätigkeiten, die voraussichtlich ein hohes Risiko für die Rechte und Freihei-

5 Zur Umsetzung der Vorschriften der DSGVO zum technischen Datenschutz im neuen BDSG, vgl. Bieber/Hansen, Normen des technischen Datenschutzes nach der europäischen Datenschutzreform, DuD 2017, Heft 1, S. 285.

6 Rannenberg/Camenisch/Sabouri (Hrsg.): Attribute-based Credentials for Trust-Identity in the Information Society, Springer, 2015.

7 ENISA: Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, 2015; abrufbar unter: <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets>.

8 Vgl. schon zur DSRL Artikel 29-Datenschutzgruppe, WP 169, S. 30 ff.

9 So auch Artikel-29-Datenschutzgruppe, WP 169, S. 30 f.

10 Dazu ausführlich Friedewald u.a.: White Paper Datenschutz-Folgenabschätzung. Ein Werkzeug für besseren Datenschutz, 2016; abrufbar unter: [https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpaapiere-white-paper/Forum\\_Privatheit\\_White\\_Paper\\_Datenschutz-Folgenabschaetzung\\_2016.pdf](https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpaapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf).

ten natürlicher Person zur Folge haben, verpflichtend; sie empfiehlt sich aber auch für andere Verarbeitungstätigkeiten. Die DSFA ist vor Beginn der Verarbeitungstätigkeit vorzunehmen und hat das Ziel, gem. Artikel 35 Abs. 7 Buchst. d DS-GVO den Nachweis zu erbringen, dass die Verarbeitung die Vorschriften der DS-GVO insgesamt eingehalten wird. Dies geschieht durch eine auf einem Verzeichnis der Verarbeitungstätigkeiten gem. Artikel 30 DS-GVO aufbauende Risikoabschätzung für die Rechte und Freiheiten natürlicher Personen, wobei eben dieses Risiko durch Abhilfemaßnahmen, wie sie auch von Artikel 32 DS-GVO gefordert werden, eingedämmt werden muss. Bei der Auswahl dieser Maßnahmen ist im Rahmen der DSFA die Pflicht zum Datenschutz „by Design“ zu berücksichtigen und im Rahmen der Maßnahmenumsetzung zu dokumentieren.

## II. Datenschutz „by Default“ – Art. 25 Abs. 2 DS-GVO

Datenschutz durch datenschutzfreundliche Voreinstellungen wird von vielen Experten als Konkretisierung von „Datenschutz by Design“ verstanden. In der Tat hat Ann Cavoukian, die sieben Grundprinzipien für „Privacy by Design“ formuliert hat, eines davon „Privacy by Default“ genannt:

*„Privacy as the default setting: If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.“<sup>11</sup>*

„Privacy as the default setting“ trägt also zu „Privacy by Design“ bei. Es klingt sehr schön: Die betroffenen Personen müssen nichts tun, damit ihre Privatheit intakt bleibt. Es ist also kein „opt-out“ notwendig – Datenschutz ist garantiert. Aber so einfach ist es dann doch nicht, wenn die betroffenen Personen Dienste nutzen wollen, bei denen die Weitergabe von Daten für den jeweiligen Zweck erforderlich ist.

Dies hat auch der Europäische Datenschutzbeauftragte in seiner Stellungnahme zum Entwurf der DS-GVO zum Ausdruck gebracht:

*„The principle of data protection by default aims at protecting the data subject in situations in which there might be a lack of understanding or control on the processing of their data, especially in a technological context. The idea behind the principle is that privacy intrusive features of a certain product or service are initially limited to what is necessary for the simple use of it. The data subject should in principle be left the choice to allow use of his or her personal data in a broader way.“<sup>12</sup>*

Der Text von Artikel 25 Abs. 2 DS-GVO geht primär auf die Erforderlichkeit ein und konkretisiert damit die Grundsätze der Zweckbindung und Datenminimierung gem. Artikel 5 Abs. 1 Buchst. b und c. Wieder ist der Verantwortliche derjenige, der aktiv die geeigneten technischen und organisatorischen Maßnahmen treffen muss – allerdings anders als in Artikel 25 Abs. 1 DS-GVO nicht mit den einschränkenden Bedingungen wie „Stand der Technik“ oder „Implementierungskosten“. Es ist eine insoweit unbeschränkte Verpflichtung des Verantwortlichen:

*„Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.“ (Artikel 25 Abs. 2 Satz 1 DS-GVO – deutsche Fassung)*

Zuallererst muss darauf hingewiesen werden, dass sich in der deutschen Sprachfassung fälschlicherweise ein zusätzliches Wort eingeschlichen hat: „grundsätzlich“. Diese Einschränkung findet sich beispielsweise in der englischen Version nicht:

*„The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.“ (Artikel 25 Abs. 2 Satz 1 DS-GVO – englische Fassung)*

Also handelt es sich – anders als die deutsche Sprachfassung suggeriert, in der die Wortwahl „grundsätzlich“ Ausnahmen zulassen würde<sup>13</sup> – um eine absolute Forderung: Es ist durch Voreinstellung zu gewährleisten, dass nur die erforderlichen personenbezogenen Daten verarbeitet werden. Diese initiale Voreinstellung kann von den Nutzenden durch aktives Tun geändert werden, beispielsweise um zusätzliche Daten für weitere Zwecke freizugeben.

Mit dem Anspruch Datenschutz „by Default“ ändert sich das Vorzeichen im Vergleich zum heutigen Status in der Praxis, bei dem die Voreinstellungen nicht maximal datensparsam für den jeweiligen Zweck sind. Heutzutage müssen die Nutzenden, die sich für Datenschutz interessieren, oft mühsam in verschiedenen Menüs der Konfiguration die voreingestellten Datenweitergaben ändern. Wer dies nicht weiß oder wem dies zu kompliziert erscheint, gibt momentan vielfach deutlich mehr an personenbezogenen Daten heraus, als erforderlich ist.<sup>14</sup>

Wie „erforderlich für den jeweiligen bestimmten Verarbeitungszweck“ auszulegen ist, erläutert Artikel 25 Abs. 2 Satz 2 DS-GVO: „Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.“ Es geht also nicht nur darum, wie viele Daten weitergegeben werden, sondern auch, wie sie verarbeitet werden, wie lange sie gespeichert sind und wie die Zugänglichkeit zu den Daten aussieht. Neu – und nicht genauer in der DS-GVO definiert – ist der Begriff der Zugänglichkeit („accessibi-

11 Cavoukian: Privacy by Design. The 7 Foundational Principles, 2011; abrufbar unter: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>.

12 European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the data protection reform package, 7. März 2012; abrufbar unter: [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07\\_EDPS\\_Reform\\_package\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf).

13 So entschied der EuGH schon in der bekannten Rs. 26/69 Stauder v Stadt Ulm, Urteil vom 12. November 1969, ECLI:EU:C:1969:57, Rn. 3: „so verbietet es die Notwendigkeit einheitlicher Anwendung und damit Auslegung, die Vorschrift in einer ihrer Fassungen isoliert zu betrachten, und gebietet es vielmehr, sie nach dem wirklichen Willen des Urhebers und dem von diesem verfolgten Zweck, namentlich im Licht ihrer Fassung in allen vier Sprachen auszulegen“.

14 Leon u.a.: Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising, in: Proc. CHI '12, S. 589-598, 2012.

lity“)<sup>15</sup>: Hierunter ist beispielsweise zu verstehen, dass auch die Zugriffsmöglichkeiten zu den Daten minimiert werden müssen. Daraus ergibt sich ein Rückspiel zu den „Design“-Anforderungen, wenn nämlich über möglichst weitgehend eingeschränkte Zugriffsrechte, über eine Verschlüsselung gegen einen Zugriff auf den Klartext oder auch über Speicherorte entschieden wird. Speicherorte, die zu einer übermäßigen Zugänglichkeit der Daten führen, könnten beispielsweise solche Drittstaaten ohne adäquates Datenschutzniveau sein, in denen gesetzlich behördliche Zugriffe auf die personenbezogenen Daten ausbedungen werden.

Bei dem letzten Satz des Artikel 25 Abs. 3 DS-GVO handelt es sich um ein konkretisierendes Beispiel, dass „personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden“ darf. Dies bedeutet beispielsweise für ein Soziales Netzwerk, dass per Voreinstellung nicht „Friends-of-Friends“ oder globale Suchmaschinen Zugriff auf die hochgeladenen personenbezogenen Daten erhalten dürfen. Es soll nicht passieren, dass Nutzende versehentlich ihre Daten – oder auch personenbezogene Daten ihrer Bekannten – der ganzen Welt zur Verfügung stellen. Stattdessen ist hier als Schutz ein aktives Tun – ein bewusstes Umkonfigurieren der Voreinstellungen – notwendig.

Die Regelungen zu Datenschutz „by Default“ sagen allerdings nichts darüber aus, inwieweit der initiale Schutz mit einem Klick der Umkonfiguration vollständig seine Wirkung verlieren darf. Da ein solcher Klick eine Einwilligung gem. Artikel 7 DS-GVO in eine weitere Datenverarbeitung, zu weiteren Zwecken bedeuten würde, müsste eine derartige Gestaltung der Benutzungsoberfläche auf jeden Fall die Transparenzanforderungen des Artikel 12 DS-GVO und die Informationspflicht nach Artikel 13 DS-GVO erfüllen. Danach soll ein Umkonfigurieren der Voreinstellungen ohne das Bewusstsein des Betroffenen über dessen Auswirkungen ausgeschlossen werden. Zudem gelten auch für diese weiteren Zwecke die Grundsätze der Zweckbindung und Datenminimierung, mit denen eine ausufernde Erweiterung der Zwecke unterbunden wird.

### III. Rolle der Zertifizierung – Art. 25 Abs. 3 DS-GVO

Um nachzuweisen, dass die Anforderungen von Datenschutz „by Design“ und „by Default“ erfüllt werden, kann nach Artikel 25 Abs. 3 DS-GVO ein genehmigtes Zertifizierungsverfahren gem. Artikel 42 als Faktor (im Englischen: „used as an element to demonstrate compliance“) herangezogen werden. Ähnliche Regelungen mit Bezug auf Zertifizierungsverfahren finden sich in den Artikeln 24 Abs. 3, 28 Abs. 5 und 32 Abs. 3 DS-GVO, hier jeweils mit zusätzlichem Verweis auf genehmigte Verhaltensregeln gem. Artikel 40. Dies ist anders beim Artikel 25, der lediglich Zertifizierungsverfahren als einen Faktor zum Nachweis der Einhaltung akzeptiert.

Aus dieser Regelung lässt sich ableiten, dass die genehmigten Zertifizierungsverfahren gem. Artikel 42 die Anforderungen

aus Artikel 25 Abs. 1 und 2 DS-GVO prüfen müssen. Um tatsächlich bewerten zu können, inwieweit eine Zertifizierung Artikel 25 DS-GVO umsetzt, reicht blindes Vertrauen in ein vorhandenes Zertifikat nicht aus. Vielmehr muss der Verantwortliche dies anhand der Dokumentation und der Informationen über das konkret durchgeführte Zertifizierungsverfahren für die datenschutzrechtlichen Anforderungen an seine Verarbeitung überprüfen.

### IV. Hinweise für den Anwender

Für Verantwortliche ist es wichtig, sich mit Artikel 25 DS-GVO und seinen Anforderungen zu beschäftigen. Mit der gewählten abstrakten Formulierung ist diese Regelung zwar offen für zukünftige Entwicklungen, wirft jedoch gleichzeitig Probleme in der praktischen Interpretation für die konkreten Fälle auf. Erwägungsgrund 78 bietet ein wenig Hilfestellung:

- Erwartet wird vom Verantwortlichen die Festlegung interner Strategien (englisch: „adopt internal policies“) zum Datenschutz „by Design“ und „by Default“ und das Umsetzen entsprechender Maßnahmen.
- In den schriftlich niedergelegten „Strategien“ (im Sinne von internen Richtlinien) sollte beschrieben werden, wie Artikel 25 DS-GVO umgesetzt wird. Hierbei bietet sich an, zwischen den Anforderungen aus Artikel 25 Abs. 1 und 2 DS-GVO zu unterscheiden. Es reicht nicht aus, pauschal darauf zu verweisen, dass von einer Umsetzung von Maßnahmen im Sinne von Artikel 25 Abstand genommen wurde, weil keine Maßnahme als „Stand der Technik“ einzustufen war oder die Implementierungskosten als unverhältnismäßig angesehen wurden.
- Zumindest die in Erwägungsgrund 78 beispielhaft aufgeführten Maßnahmen sollten in den internen Strategien aufgenommen werden. Dazu gehören die Minimierung der Verarbeitung personenbezogener Daten und eine schnellstmögliche Pseudonymisierung. Ebenso sind Transparenz der Funktionen und der Verarbeitung personenbezogener Daten und für die betroffenen Personen eine Überwachung einer solchen Verarbeitung (englisch: „monitor the data processing“) umfasst. Zudem sollen Maßnahmen den Verantwortlichen in die Lage versetzen, Sicherheitsfunktionen zu schaffen und zu verbessern (englisch: „create and improve security features“). Dieser letzte Punkt verstärkt die Notwendigkeit, passende Lösungen für unterschiedliche Schutzbedarfe zu ermöglichen und über die Zeit Verbesserungen vornehmen zu können.

Abb. 1 zeigt, welche fundamentalen Entscheidungen die Entwickler bei der Gestaltung der Funktionalität der Datenverarbeitung und zum Systemverhalten in Bezug auf Datenschutz „by Design“ und „by Default“ treffen müssen.

Zunächst ist festzulegen, ob eine bestimmte Funktionalität oder ein bestimmtes Systemverhalten durch die Nutzen-

<sup>15</sup> „Accessibility“ unterscheidet nicht wie die Anlage zu § 9 BDSG nach „Zutrittskontrolle“, „Zugangskontrolle“ oder „Zugriffskontrolle“. Im Endeffekt geht es um die Zugriffsmöglichkeiten, für die jedoch auch Zutritts- oder Zugangsmöglichkeiten zu den Systemen der Datenverarbeitung umfassen können. Zusätzlich kann man darunter auch die Möglichkeiten für eine Auswertung verstehen, wie dies in der Formulierung „strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind“ in Artikel 4 Abs. 1 Nr. 6 zum Ausdruck kommt.

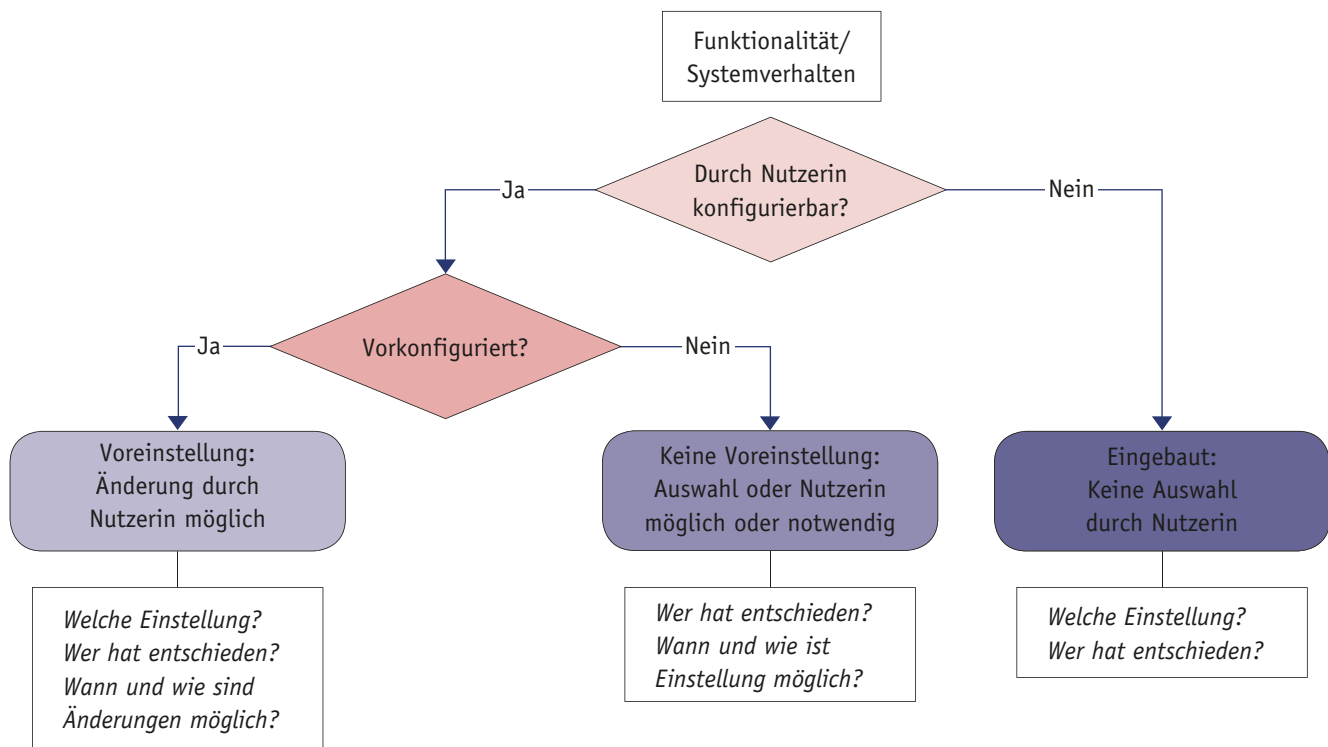


Abb. 1: Entscheidungen in der Systemgestaltung zwischen Datenschutz „by Design“ (rechts) und „by Default“ (links)

den konfigurierbar sein sollen oder nicht. Diese Festlegung ist eine Design-Entscheidung. Was nicht umkonfiguriert werden können soll (rechte Seite in Abb. 1), wird – wieder im Sinne des Datenschutzes „by Design“ – fest eingebaut. Als Beispiel sei eine Verschlüsselung genannt, die von einem Nutzenden nicht deaktiviert werden soll.

Wenn festgelegt wurde, dass eine Konfigurierbarkeit bestehen soll, ist zu prüfen, ob eine Voreinstellung vorgesehen wird (linke Seite in Abb. 1) oder dies nicht der Fall sein soll. Beispielsweise könnte als Voreinstellung bei einer Nutzung eines Internet-Dienstes jede Datenweitergabe im Rahmen eines Trackings ausgestellt sein. Ein Tracking kann dann nur stattfinden, wenn die Nutzenden dies bewusst und gewollt aktivieren, z. B. wenn sie sich davon einen Nutzen – wie eine bessere Beratung – versprechen. Auf keinen Fall darf eine datenschutzfreundliche Voreinstellung dazu führen, dass eine Nutzung des Dienstes faktisch nicht möglich ist und die betroffenen Personen dazu gezwungen werden, mehr als die für den Zweck erforderlichen Daten herauszugeben, um überhaupt eine Dienstnutzung zu erreichen. Allerdings kann es sein, dass für den Fall, dass weniger personenbezogene Daten verarbeitet werden, bestimmte Funktionalität nicht vollständig nutzbar sind. Beispielsweise wäre eine personalisierte Nutzung regelmäßig nicht erforderlich. Jedoch wird es für eine detaillierte Beratung dazu, welche Produkte den personalisierten Anforderungen des Nutzenden genügen, oft nötig sein, dass diese Anforderungen in geeigneter Fassung kommuniziert werden. In der – vom Nutzenden änderbaren – Voreinstellung sollte demnach konfiguriert sein, dass zunächst keine überschüssigen Informationen

für das einfache Nutzungsszenario – ohne personalisierte Beratung – weitergegeben werden.

Es gibt zudem den Fall, dass eine Interaktion mit den Nutzenden notwendig ist und eine Voreinstellung nicht sinnvoll oder nicht rechtskonform wäre. Beispielsweise wäre bei dem Online-Einkauf bei einem neuen Anbieter üblicherweise das Bezahlverfahren aktiv auszuwählen, statt in der Voreinstellung die Entscheidung für ein datenschutzfreundliches Verfahren zu treffen. Zwar wäre gemäß dem Prinzip Datenschutz „by Design“ im Rahmen der Verhältnismäßigkeit normalerweise mindestens ein datenschutzfreundliches Bezahlverfahren zu unterstützen. Jedoch ist für die Aktion „Einkauf“ eine bewusste Willensentscheidung notwendig, und hierzu gehört auch die Bestimmung der Nutzenden über das jeweils zu verwendende Bezahlverfahren, das den eigenen Anforderungen genügt.

## V. Fazit

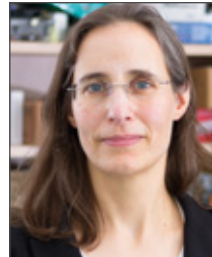
Artikel 25 DS-GVO verlangt von den Anwendern, dass sie auf eingebauten Datenschutz achten. Während im Bereich der Informationssicherheit zunehmend Lösungen zu finden sind, ist der Status Quo für Datenschutzanforderungen zur Zeit unbefriedigend. Da die Verantwortlichen bei der Gestaltung ihrer Datenverarbeitung von Herstellern, Auftragsverarbeitern und (De-facto-)Standards abhängig sind, wird es darauf ankommen, inwieweit dort die Umsetzung des Artikel 25 DS-GVO ernst genommen wird und wie sehr die Verantwortlichen dies nachfragen.

*Der öffentliche Sektor sollte hierbei eine Vorbildfunktion einnehmen. In öffentlichen Ausschreibungen wird es künftig notwendig sein, bei den Anbietern die Erfüllung der Anforderungen aus der DS-GVO einschließlich Artikel 25 DS-GVO abzufragen. Damit Datenschutz „by Design“ und „by Default“ den Weg in die Praxis finden, sollten Impulse von Fördergebern und vom Gesetzgeber dazu beitragen, dass tatsächlich – wie in Erwägungsgrund 78 beschrieben – „die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.“*



**Felix Bieker, LL.M. (Edinburgh)**

ist als juristischer Mitarbeiter im Projektreferat des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) u.a. für das Projekt Forum Privatheit tätig.



**Marit Hansen**

Dipl.-Inform. Marit Hansen ist seit 2015 die Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das ULD.

Dr. Stefan Brink/Sabrina Schwab

## Beschäftigtendatenschutz: Zwischen wirtschaftlicher Abhängigkeit und informationeller Selbstbestimmung

*Die Arbeitswelt und somit auch der Beschäftigtendatenschutz betreffen fast jeden von uns, ob auf Seiten der Wirtschaft als Arbeitgeberin bzw. Arbeitgeber oder auf der anderen Seite als Arbeitnehmerin bzw. Arbeitnehmer.<sup>1</sup> Die jährliche Arbeitszeit beträgt im Durchschnitt 1.552 Stunden.<sup>2</sup> Viel Zeit, um als Arbeitnehmer eine Flut an personenbezogenen Daten zu hinterlassen und als Arbeitgeber diese persönlichen Informationen zu sammeln.*

*Die vorliegende Handreichung gibt einen Überblick über die Problemschwerpunkte des Beschäftigtendatenschutzes*

*im privaten Bereich, wie sie an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) herangetragen werden, und zeigt die zulässige Verwendung personenbezogener Daten von Beschäftigten anhand von Praxisfällen auf. Lehrbücher zu dieser Materie gibt es zur Genüge. Der Fokus liegt hier vielmehr auf der täglichen Arbeit des LfDI BW im Bereich des Beschäftigtendatenschutzes: echte Beratungsanfragen und eingehende Beschwerden – und echte Lösungen.<sup>3</sup>*

### I. Der Weg vom Volkszählungsurteil bis zur verfassungskonformen gesetzlichen Regelung

Wie die vergangenen Jahre gezeigt haben, war der Weg des Gesetzgebers zu einem eigenständigen Beschäftigtendatenschutz nicht gerade kurz – und er ist eigentlich noch immer nicht am Ziel angekommen.

Das allbekannte Volkszählungsurteil des Bundesverfassungsgerichts<sup>4</sup> aus dem Jahr 1983 hat mit dem erstmals als Grundrecht bezeichneten Recht auf informationelle Selbstbestimmung den Grundstein gelegt: Jeder Einzelne hat das Recht grundsätzlich selbst über die Verwendung mit seinen persönlichen Daten zu bestimmen. Die bis dahin erlassenen Datenschutzgesetze hielten diesen verfassungsrechtlichen

Anforderungen nicht stand. Im Jahr 1990 erließ der Bund ein novelliertes Bundesdatenschutzgesetz (BDSG). Bis 2009 hat man sich, trotz seiner großen praktischen Bedeutung, mit einer eigenständigen Regelung für den Arbeitnehmerdatenschutz Zeit gelassen – im Gegensatz zu den Datenschutzgesetzen vieler Länder.<sup>5</sup> Die Praxis musste solange auf die allgemeinen Regelungen des BDSG zurückgreifen. Forderungen

1 Es sind stets Personen männlichen und weiblichen Geschlechts gleichermaßen gemeint; aus Gründen der einfacheren Lesbarkeit wird im Folgenden nur die männliche Form verwendet.

2 Quelle: Institut für Arbeitsmarkt- und Berufsforschung (IAB): Daten zur kurzfristigen Entwicklung von Wirtschaft und Arbeitsmarkt 04/2013, [www.iab.de](http://www.iab.de).

3 Dabei wird die Anonymität der Beschwerdeführer gewahrt.

4 BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83.

5 Vgl. bspw. § 36 Landesdatenschutzgesetz Baden-Württemberg.

gen nach der Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes wurden erst nach dem Bekanntwerden von Datenschutzskandalen bedeutender deutscher Unternehmen erfüllt. Beschäftigte von Lidl, der Deutschen Bahn oder der Deutschen Telekom mussten erst Opfer unzulässiger Überwachungsmethoden werden, bis die Bundesregierung im Februar 2009 die Arbeit an einem Arbeitnehmerdatenschutzgesetz wieder aufnahm. Resultat war der als „Sofortmaßnahme“ am 1. September 2009 in Kraft getretene § 32 BDSG.

Er lautet:

„Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.“<sup>6</sup>

Das in der darauffolgenden Legislaturperiode auf der Agenda stehende ausführliche „Gesetz zur Regelung des Beschäftigtendatenschutzes“ scheiterte an vehementen Protesten von Arbeitgebern und Gewerkschaften.

Derzeit sieht es so aus, als ob der deutsche Gesetzgeber erneut die Möglichkeit eigenständiger und spezifischer Regelungen verstreichen lässt und so den Besonderheiten des Arbeitsverhältnisses als Nähe- und Abhängigkeitsverhältnis nicht gerecht wird. Am 25. Mai 2018 tritt die EU-Datenschutzgrundverordnung<sup>7</sup> mit ihrer unmittelbaren Bindung in Kraft. Für die Datenverarbeitung im Beschäftigungskontext hat der europäische Gesetzgeber durch eine Öffnungsklausel den Weg für eigenständige nationale Regelungen geebnet, die jedoch nicht zu einer absoluten Zersplitterung in diesem Bereich führen darf. Das Gesetz zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung<sup>8</sup> übernimmt zwar den derzeit gültigen § 32 BDSG mit wenigen Zusätzen, stellt aber nach wie vor nur einen Minimalkonsens dar. Die seit Jahrzehnten bestehenden Forderungen nach einem eigenständigen Beschäftigtendatenschutzgesetz bleiben noch immer unerfüllt.

## 1. Die Normenvielfalt im Beschäftigtendatenschutz

Der Beschäftigtendatenschutz ist ein Abbild der bestehenden Regelungen im Arbeitsrecht. Auch dort hat es der Gesetzgeber, trotz nachdrücklicher Postulate verschiedenster Lager, nicht geschafft ein einheitliches Arbeitsrecht zu kodifizieren. Die bestehenden datenschutzrechtlichen Regelungen

finden sich weit verstreut in verschiedenen Gesetzestexten. Beispielhaft ist § 39 Abs. 8 und 9 Einkommensteuergesetz, wonach der Arbeitgeber die auf der Lohnsteuerkarte enthaltenen Merkmale nur für die Einbehaltung der Lohnsteuer verwenden darf. Für die Verwendung der Sozialversicherungsnummer durch den Arbeitgeber findet sich in § 18f im Vierten Sozialgesetzbuch eine Spezialvorschrift. Da verliert man schnell den Überblick ...

Für die Verwendung von Beschäftigtendaten gilt jedoch einheitlich: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.<sup>9</sup> Die Verwendung personenbezogener (Beschäftigten-)Daten ist also grundsätzlich verboten, wenn sie nicht ausdrücklich vom Gesetz erlaubt ist oder eingewilligt wurde.

Beim Fehlen vorrangiger datenschutzrechtlicher Spezialgesetze findet das BDSG als „Auffanggesetz“ Anwendung.<sup>10</sup> Neben dem BDSG kann die Verwendung personenbezogener Daten aber durch Landesnormen, Verordnungen, Satzungen oder kollektiv-arbeitsrechtliche Normen, insbesondere Tarifverträge oder Betriebsvereinbarungen, erlaubt werden.<sup>11</sup>

### Praxistipp:

*Ohne Kenntnis der verstreuten arbeitsrechtlichen Vorschriften ist eine datenschutzrechtliche Bewertung nicht möglich. Arbeitgeber sollten bei der Auswahl betrieblicher Datenschutzbeauftragten auch auf arbeitsrechtliche Fachkenntnisse Wert legen und in spezielle Fortbildungen und Schulungen zum Beschäftigtendatenschutz investieren – fehlt eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten, liegt es am Arbeitgeber, sich dieses wertvolle Wissen selbst anzueignen.*

## 2. Die Regelungen des BDSG

### a) Personenbezogene Daten

Voraussetzung für die Anwendbarkeit datenschutzrechtlicher Bestimmungen ist, dass *personenbezogene Daten* erhoben oder verarbeitet werden. Nach der weiten Legaldefinition in § 3 Abs. 1 BDSG sind dies Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Beispielhaft sind Adressdaten, Geburtsdaten, Bankverbindungsdaten, Familienstand, Steuer-ID, Telefonnummern und E-Mail-Adressen

<sup>6</sup> § 32 Abs. 1 Satz 1 und 2 BDSG.

<sup>7</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

<sup>8</sup> Am 12.05.2017 hat der Bundesrat dem vom Bundestag am 27.04.2017 in der Fassung der Beschlussempfehlung des Innenausschusses (BT-Drucksache 18/12084) verabschiedeten Datenschutz-Anpassungs- und Umsetzungsgesetz – EU (DSAnpUG-EU) und dem darin in Artikel 1 enthaltenen neuem Bundesdatenschutzgesetz (BDSG-neu) zugestimmt.

<sup>9</sup> Vgl. § 4 Abs. 1 BDSG.

<sup>10</sup> Vgl. § 1 Abs. 3 BDSG.

<sup>11</sup> Vgl. § 4 Abs. 1 BDSG.

zu nennen, aber auch Bewerbungen, erbrachte Arbeitszeiten, Krankheits- und Urlaubstage, sind personenbezogene Daten.

Man könnte es sich extrem leicht machen, indem man als Arbeitgeber Datenverarbeitung ohne Personenbezug vornimmt, also mit anonymisierten Daten arbeitet. Sicherlich ist das nicht immer möglich. Aber dort, wo es geht, sollten personenbezogene Daten anonymisiert oder aggregiert werden. Unter aggregierten Daten versteht man die Zusammenfassung von Einzelangaben. Entscheidend ist jedoch, dass die Information nicht auf den Einzelnen rückführbar ist, also nicht auf diesen „durchschlägt“.<sup>12</sup> Sind personenbezogene Daten derart verändert, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können, spricht man von anonymisierten Daten.<sup>13</sup> Und bei diesen Daten ist der Arbeitgeber von der Last des BDSG befreit.

#### Praxistipp:

*Um der Gefahr von Datenschutzverstößen und der Sanktion mit Bußgeldern zu begegnen, sollte immer geprüft werden, ob die verfolgten Zwecke nicht auch mit anonymisierten bzw. aggregierten Daten (zusammengefassten Daten ohne Bezug zu einzelnen Personen) erreicht werden kann.*

*Dies wird spätestens ab Inkrafttreten der DSGVO im Mai 2018 noch wichtiger: Ab dann müssen Arbeitgeber bei bestimmten Rechtsverstößen mit Bußgeldern in Höhe von bis zu 4% des Jahresumsatzes ihres Unternehmens bzw. 20 Millionen Euro Strafe rechnen.*

#### b) Anwendung auf alle Beschäftigten

Um nicht den Rahmen dieser Handreichung durch zahlreiche spezialgesetzliche Regelungen zu sprengen, wird hier nur auf § 32 BDSG und seine Voraussetzungen eingegangen. Diese Norm setzt die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zum Zwecke eines Beschäftigungsverhältnisses voraus. Der Begriff des Beschäftigten wird nach der Legaldefinition des § 3 Abs. 11 BDSG – im Gegensatz zu den engen arbeitsrechtlichen Regelungen – sehr weit gefasst und erstreckt sich zur Gewährleistung eines umfassenden Schutzes auf alle möglichen Arbeitsverhältnisse, auf Bewerber ebenso wie auf Azubis oder Zivis.

#### c) Besonderheiten

Zwei Besonderheiten sind noch zu beachten: Werden Beschäftigtendaten zu anderen Zwecken, also solchen, die nicht mit dem konkreten Beschäftigungsverhältnis verknüpft sind, erhoben, verarbeitet oder genutzt, ist auf die übrigen Regelungen, insbesondere auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG, zurückzugreifen. Das ist etwa der Fall, wenn der Arbeitgeber Pflichten nach dem Geldwäschegesetz oder Anti-Terror-Gesetzen nachkommt – das hat mit dem einzelnen Beschäftigungsverhältnis nichts zu tun.

Für bestimmte Arten besonders sensibler und schutzbedürftiger Daten von Beschäftigten ist § 28 Abs. 6 bis 8 BDSG gegenüber § 32 BDSG vorrangig. Nach § 3 Abs. 9 BDSG sind besondere Arten personenbezogener Daten Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben.

#### Praxistipp:

*Arbeitgeber sollten auf eine geordnete und systematische Sammlung personenbezogener Daten ihrer Bewerber und Beschäftigten achten. Durch datenschutzkonforme Protokollierungs- und Löschkonzepte müssen personenbezogene Daten bei Auskunftsansprüchen und Berichtigungs- und Löschungsbegehren nicht mühselig zusammengesucht werden, sondern können in Kürze extrahiert und den Betroffenen zugänglich gemacht werden.*

#### d) Umfassender Schutz

Durch § 32 Abs. 2 BDSG weitet der Gesetzgeber den Anwendungsbereich des Beschäftigtendatenschutzes erheblich aus – jede Information über Beschäftigte ist in jeder Form geschützt. Der Geltungsbereich des BDSG umfasst ja ansonsten nur den Einsatz von Datenverarbeitungsanlagen bzw. setzt die geordnete Sammlung der Daten in Dateien voraus.<sup>14</sup> Anders beim Beschäftigtendatenschutz: Hier fallen zum Beispiel auch handschriftlich gefertigte Notizen während eines Bewerbungsgesprächs sowie die alltägliche Informationserhebung durch persönliche Befragung oder eine Übermittlung durch Telefonate in den Anwendungsbereich von § 32 BDSG. Durch die Loslösung von einer automatisierten Verarbeitung können auch die im Arbeitsrecht entwickelten zwingenden Schutzprinzipien berücksichtigt werden – etwa beim Fragerecht des Arbeitgebers und dem damit einhergehenden „Recht zur Lüge“ des Beschäftigten, wenn er einem Versuch unzulässiger Informationsbeschaffung ausgesetzt ist. Auch hier hilft ihm das BDSG.

#### e) Das Erforderlichkeitsprinzip

Das informationelle Selbstbestimmungsrecht des Beschäftigten ist mit dem Eigentumsrecht (Art. 14 Abs. 1 und 2 Grundgesetz – GG), mit der unternehmerischen Freiheit (Art. 12 Abs. 1 GG) und der Vertragsfreiheit des Arbeitgebers (Art. 2 Abs. 1 GG) in einen schonenden Ausgleich zu bringen. Hier stehen sich also immer Grundrechte auf beiden Seiten gegenüber.

Daher misst § 32 BDSG die Verwendung personenbezogener Daten am Grundsatz der Erforderlichkeit. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten muss geeignet und zugleich das relativ mildeste Mittel sein, um die unternehmerischen Interessen und Zwecke bei der

<sup>12</sup> BAG, NZA 1995, 185.

<sup>13</sup> Vgl. § 3 Abs. 6 BDSG.

<sup>14</sup> § 1 Abs. 2 Nr. 3 und § 27 Abs. 1 Satz 1 BDSG.

Durchführung des Beschäftigungsverhältnisses zu verwirklichen. Dementsprechend verpflichtet das Erforderlichkeitsprinzip stets zum Vergleich alternativer Handlungsformen und zwingt den Arbeitgeber zur Datenvermeidung und Datensparsamkeit, wo immer dies möglich ist.<sup>15</sup> Der Beschäftigte muss seine Daten nur dann preisgeben, wenn der Arbeitgeber ohne ihre Kenntnis im konkreten Einzelfall eine legitime Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann. Gleichzeitig gibt der Arbeitgeber aber durch seine unternehmerische Entscheidungsfreiheit den Zweck und die konkrete Ausgestaltung des Beschäftigungsverhältnisses vor. Entscheidet sich der Arbeitgeber etwa, besonders qualitätsvolle Produkte anzubieten, so darf er das benötigte gut ausgebildete Personal entsprechend intensiver auswählen und bei der Arbeit überprüfen. Der Maßstab der Erforderlichkeit orientiert sich also in erster Linie an der unternehmerischen Entscheidungsfreiheit, die Zwecke des Beschäftigungsverhältnisses zu bestimmen.

Alles was zur Ausübung von Weisungsrechten eines Arbeitgebers oder einer Kontrolle der Leistung oder des Verhaltens seiner Beschäftigten notwendig ist und nach den Grundsätzen des Arbeitsrechts erlaubt ist, muss aus datenschutzrechtlicher Sicht als erforderlich eingestuft werden.<sup>16</sup> Das heißt aber nicht, dass der Arbeitgeber seine Mitarbeiter einer Totalkontrolle unterziehen darf und sie einem ständigen Überwachungsdruck ausgesetzt sein dürfen – hiervor schützt sie ihr Recht auf informationelle Selbstbestimmung.

#### f) Weitere Datenschutzprinzipien

Der Erforderlichkeitsgrundsatz alleine soll es aber nicht gewesen sein. Der Arbeitgeber ist daneben an weitere Prinzipien des Datenschutzes gebunden. Hierzu zählt der Grundsatz der Direkterhebung (wenn der Arbeitgeber Informationen über einen bestimmten Beschäftigten haben möchte, dann muss er ihn zunächst einmal selbst befragen und darf sich nicht an Dritte wenden)<sup>17</sup>, das Gebot der Datensparsamkeit<sup>18</sup> und das Verbot der Vorratsdatensammlung. Besondere Bedeutung genießt der Zweckbindungsgrundsatz: Nur wenn vor der Datenerhebung, -verarbeitung und -nutzung feststeht, welcher Zweck des Arbeitgebers erreicht werden soll, lässt sich im Nachhinein beurteilen, ob in zulässiger Weise verfahren wurde.

Unsere tägliche Arbeit zeigt, dass vielen Unternehmen diese Grundsätze im schlechtesten Fall völlig fremd sind oder eher als Empfehlung denn als verbindliche Vorgabe verstanden werden – ein leider weit verbreiteter Irrtum.

### 3. Tarifvertrag und Betriebsvereinbarung

Der Abschluss von Tarifverträgen und Betriebsvereinbarungen kann das Fehlen eines eigenständigen Beschäftigtendatenschutzgesetzes in gewissem Umfang wettmachen. Gerade deshalb sollten die Vertragsparteien Tarifverträge und Betriebsvereinbarungen als Regelungsinstrument nicht ungenutzt lassen und die Datenverarbeitungen im Unternehmen entsprechend selbst regeln.

Bedauerlicherweise laufen abgeschlossene Betriebsvereinbarungen nicht selten ins Leere. Unklare oder undurchsichtige Regelungen oder ein das BDSG unterschreitendes Schutzniveau führen mitunter dazu, dass Aufsichtsbehörden eine Betriebsvereinbarung als unwirksam betrachten und auf die allgemeine Regelung des § 32 BDSG zurückgreifen müssen.

Eine Betriebsvereinbarung kann nur dann als „besondere Rechtsvorschrift“ im Sinne von § 4 Abs. 1 BDSG angesehen werden, wenn die Datenerhebung, -verarbeitung und -nutzung hinreichend präzise innerhalb des Erlaubnisumfangs gesetzlicher Bestimmungen geregelt wird und dabei das gesetzliche Schutzniveau nicht unterschritten wird.<sup>19</sup> Auch können Betriebsvereinbarungen vor Begründung des Beschäftigungsverhältnisses keinen datenschutzrechtlichen Erlaubnistatbestand bereitstellen. Der Bewerber gehört dem Betrieb noch nicht an, so dass sich die Wirkung einer Betriebsvereinbarung auch nicht auf ihn erstrecken kann.<sup>20</sup>

Leider führen nicht selten die fehlende Fachkunde im Datenschutz und die Besonderheit eines Arbeitsverhältnisses zu undurchsichtigen Vereinbarungen. Hier sind betriebliche Datenschutzbeauftragte und die Aufsichtsbehörden gleichermaßen gefragt. Sie können der verantwortlichen Stelle, aber auch dem Betriebsrat beratend zur Seite stehen.<sup>21</sup> Nicht auf Anhieb wird die Aufsichtsbehörde als Berater eingeschaltet. Dies kann mit ihrer vermeintlichen Verortung im „feindlichen Lager“ zusammenhängen. Würde jede geplante Betriebsvereinbarung, welche die Verarbeitung personenbezogener Daten zum Gegenstand hat, der zuständigen Aufsichtsbehörde zur Kontrolle vorgelegt werden, würde diese zudem schnell an ihre Beratungsgrenzen stoßen. Durch gezielte Aufklärungsarbeit ist daher ausreichende Sensibilität für den Datenschutz zu schaffen. Werden Prozesse von Anfang an unter dem Gesichtspunkt datenschutzrechtlicher Vorgaben vorangetrieben, werden Entwicklungen auch nicht ausgebremst, sondern von vornherein transparent und nachhaltig gestaltet.

In der Regel wird der LfDI BW durch Beschwerden von Betroffenen auf unzureichenden Regelungen in Betriebsvereinbarungen aufmerksam. Nicht selten sind bestehende Betriebsvereinbarungen den Beschäftigten selbst überhaupt nicht bekannt. Unternehmen müssen ihre Beschäftigten daher wiederkehrend über die geltenden Regelungen im Unternehmen informieren und ihnen diese jederzeit zugänglich machen.

Auch wenn es um den Schutz des Einzelnen geht, zieht ein Beschwerdeverfahren häufig nicht nur ein positives Ergebnis für den betroffenen Beschäftigten nach sich. Abge-

15 NK-GA/Brink, § 32 BDSG Rn. 6.

16 Vgl. BT-Drucks. 16/13657, 21; Thüsing, NZA 2009, 865, 867.

17 Vgl. § 4 Abs. 2 Satz 1 BDSG.

18 Vgl. § 3a BDSG.

19 Dazu Brink, ZD 2015, 295, 299.

20 ErfK/Kania, BetrVG § 77 Rn. 32.

21 Vgl. § 38 Abs. 1 Satz 2 BDSG.

stellte Datenschutzverstöße führen oft zur Verbesserung des Datenschutzes für die gesamte Belegschaft. Die Aufsichtsbehörde wechselt die (angeblichen) Fronten und nimmt die Beraterrolle ein – nicht selten auch für später geplante Datenverarbeitungsprozesse, bei denen personenbezogene Daten betroffen sind.

### Fall 1: Von der unerlaubten Öffnung eines E-Mail-Postfaches zum Abschluss einer Betriebsvereinbarung

Ein ausgeschiedener Mitarbeiter beschwerte sich darüber, dass sein personalisierter E-Mail-Account, *name@unternehmen.de*, nicht unmittelbar nach seinem Ausscheiden gelöscht wurde. Es stellte sich heraus, dass es im Unternehmen keine Regelungen zur Nutzung der Informations- und Kommunikationstechnik (IuK) gab. Die Mitarbeiter gingen davon aus, dass die private Nutzung der betrieblichen IuK gestattet war und wurden auch nicht durch stichprobenartige Kontrollen und daraufhin ausgesprochene Sanktionen vom Gegenteil überzeugt. Als Folge hatte sich die Erlaubnis zur Privatnutzung der IuK durch „betriebliche Übung“ etabliert. Damit war das Unternehmen als Dienstanbieter im Sinne des TKG bzw. TMG anzusehen und dem Fernmeldegeheimnis<sup>22</sup> unterworfen. Der Zugriff auf den E-Mail-Account des ausgeschiedenen Mitarbeiters war somit unzulässig. Und dies betraf nicht nur dessen private Mails, sondern natürlich auch seine dienstlichen, denn in seinem Account waren sie nicht auseinanderzuhalten. Ein massives Problem für das Unternehmen!

Wir haben der verantwortlichen Stelle die verschiedenen Regelungsmöglichkeiten samt ihren Konsequenzen aufgezeigt. Von einer Erlaubnis der Nutzung der betrieblichen IuK zu privaten Zwecken raten wir grundsätzlich ab, zumal hiermit erhebliche Nachteile für den Arbeitgeber verbunden sind: Da er von den Aufsichtsbehörden als Dienstanbieter im Sinne des TKG bzw. TMG angesehen wird und damit an das Fernmeldegeheimnis gebunden ist, verliert er die Zugriffsmöglichkeiten auf für den Betrieb wichtige Kommunikationsergebnisse. Hierdurch erschwert er sich die Einhaltung gesetzlicher Dokumentations- und Kontrollpflichten (nach der Abgabenordnung und dem HGB) und macht sich bei der Ausübung seiner Direktions- und Kontrollrechte von der Einwilligung seiner Beschäftigten abhängig.<sup>23</sup> Das Interesse des Arbeitgebers, seinen Mitarbeitern zumindest während der Pausenzeiten die private Nutzung der betrieblichen IuK zu ermöglichen, kann zum Beispiel durch die Einrichtung eines gesonderten W-LAN-Netzwerks gestillt werden. Wichtig ist es, klare und verständliche Regelungen zu treffen, die den Mitarbeiter ausreichend informieren und es ihm erlauben, seine Einwilligung in die Verarbeitung seiner Daten und ggf. die Kontrolle seines Mail-Accounts wirksam zu erklären.

Mit unserer unterstützenden Beratung hat das Unternehmen mit dem Betriebsrat eine entsprechende Betriebsvereinbarung abgeschlossen, auf deren Grundlage die Beschäftigten jetzt wirksam in die Erhebung, Verarbeitung und

Nutzung ihrer personenbezogenen IuK-Daten einwilligen konnten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat zu dieser Thematik eine „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ veröffentlicht. Sie enthält auch eine Musterbetriebsvereinbarung / Anweisung / Richtlinie und steht unter [https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/02/OH\\_E-Mail\\_Internet\\_Arbeitsplatz.pdf](https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/02/OH_E-Mail_Internet_Arbeitsplatz.pdf) zum Download bereit.

### Praxistipp:

*Durch den Abschluss von Betriebsvereinbarungen können Arbeitgeber und Betriebsrat notwendige Transparenz für die Verwendung von Beschäftigtendaten schaffen. Auch wenn der Gestaltungsspielraum von Betriebsvereinbarung durch die fehlende Rechtsmacht zur Einschränkung der Rechte der Beschäftigten begrenzt ist, können sie ein geeignetes Regelungsinstrument darstellen. Durch verbindliche Regelungen, wie beispielsweise den Ausschluss einer Nutzung der personenbezogenen Daten zu Zwecken der Verhaltens- und Leistungskontrolle oder die Vereinbarung von Beweisverwertungsverböten können die gegenläufigen Interessen in einen angemessenen Ausgleich zueinander gebracht werden.*

## 4. Einwilligung

Lässt sich die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nicht auf eine bereichsspezifische Vorschrift oder das BDSG stützen, bleibt als weitere Datenverarbeitungsgrundlage die Einwilligung, also das vorherige Einverständnis des Betroffenen in die Verwendung seiner Daten. Eine Einwilligung sollte nicht parallel zu einem gesetzlichen Erlaubnistatbestand eingeholt werden. Der Betroffene wird sonst in dem Glauben gelassen, die Verwendung seiner personenbezogenen Daten selbst steuern und diese durch Widerruf der Einwilligung beenden zu können.

Aber kommt eine Einwilligung im Beschäftigungsverhältnis überhaupt in Frage? Googelt man den Begriff Arbeitnehmer, spuckt die Suchmaschine Folgendes aus:

„Person, die abhängig, nämlich bei einem Arbeitgeber, beschäftigt ist.“

Die wirtschaftliche Abhängigkeit einer Person legt den Schluss nahe, sie in einer Zwangslage zu sehen, die ihr eine freie Entscheidung unmöglich macht. Diese Annahme führte bei Datenschützern lange Zeit dazu, eine Einwilligung von Beschäftigten grundsätzlich nicht als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung zu akzeptieren. Zu Recht hat man diesen Extremstandpunkt mittlerweile aufgegeben und den Beschäftigten ihr Recht auf informationelle Selbstbestimmung auch in einem Arbeitsverhältnis zugesprochen. Es liegt nämlich in der Hand jedes Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung

<sup>22</sup> Vgl. § 88 Telekommunikationsgesetz.

<sup>23</sup> Ausf. dazu Brink ZD 2015, 295, 298.

seiner personenbezogenen Daten zu bestimmen – der Arbeitnehmer bestimmt ergo selbst, ob er seinem Arbeitgeber mehr von sich preisgibt, als dieser nach den gesetzlichen Vorgaben befugt wäre zu erfahren. Die Einwilligung kann auch positive Folgen für den einzelnen Arbeitnehmer haben, so dass es mit dem Sinn und Zweck des Datenschutzes nicht vereinbar wäre, die Beschäftigten pauschal der Möglichkeit einer Einwilligung zu berauben.

Das heißt jedoch nicht, dass wir als Aufsichtsbehörde gezwungen sind, Einwilligungen von Beschäftigten ungeprüft als Ermächtigung zur Datenverarbeitung anzuerkennen. Vielmehr sind wir gehalten, die Freiwilligkeit und Wirksamkeit einer jeden Einwilligung einer genauen Einzelfallprüfung zu unterziehen, wie die nächste Falldarstellung veranschaulicht.

## Fall 2: Die „freiwillige“ Urinprobe

Der minderjährige Beschwerdeführer befand sich in einem Berufsausbildungsverhältnis.<sup>24</sup> Weil sein Arbeitgeber ihn verdächtigte, Cannabis zu konsumieren, erklärte sich der Beschwerdeführer bereit, sich einem Drogentest zu unterziehen. Der Arbeitgeber sah die Einwilligung als wirksame Rechtsgrundlage zur Erhebung, Verarbeitung und Nutzung der besonderen Arten personenbezogener Daten (Gesundheitsdaten nach § 3 Abs. 9 BDSG) des Beschäftigten an. Wir mussten ihn jedoch vom Gegenteil überzeugen. Gegen die Wirksamkeit der Einwilligung sprach im vorliegenden Fall neben der mangelnden Freiwilligkeit der Einwilligung und der Minderjährigkeit des Beschwerdeführers auch die Beschäftigung im Berufsausbildungsverhältnis.

Gemäß § 4a Abs. 1 Satz 1 BDSG ist eine Einwilligung nur wirksam, wenn sie auf der freien und informierten Entscheidung des Betroffenen beruht. Daneben ist der Betroffene auf den Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.<sup>25</sup> Es reicht nicht aus, nur auf die Einwilligung zu verweisen. Vielmehr sind auch die Umstände, unter denen die Einwilligung abgegeben wird, einzubeziehen. Eine Einwilligung beruht auf der freien Entscheidung des Betroffenen, wenn sie ohne Zwang abgegeben wird.<sup>26</sup> Sie kann als Verwendungsregulativ nur so lange akzeptiert werden, wie sich der Betroffene nicht in einer Situation befindet, die ihn faktisch dazu zwingt, sich mit dem Zugriff auf seine verlangten Daten einverstanden zu erklären.

Der Arbeitgeber konnte vorliegend nicht ernsthaft von einer zwanglosen Willenserklärung ausgehen. Allein schon die Tatsache, dass sich der Beschwerdeführer in einer Berufsausbildung befand, lässt an der Freiwilligkeit der Entscheidung zweifeln. Beschäftigte in der Berufsausbildung befinden sich gegenüber dem Arbeitgeber in einer noch unterlegeneren Position, als es ausgebildete Beschäftigte tun. Der Auszubildende ist auf die Vermittlungswilligkeit des Ausbilders angewiesen und ist daher besonders zu schützen.<sup>27</sup>

Die in den Blick zu nehmenden begleitenden Umstände stritten demnach eindeutig für eine unter Zwang und Druck abgegebene Erklärung: Nach Angaben des Arbeitgebers hat der Beschwerdeführer bei der Konfrontation mit dem Verdacht des Drogenkonsums stark angefangen zu zittern und diesen mit widersprüchlichen Antworten zu zerstreuen versucht. Zum Schluss soll der Betroffene den Konsum von Cannabis sogar eingeräumt haben. Es musste auch berücksichtigt werden, dass das Gespräch im Beisein weiterer Mitarbeiter stattgefunden hat. Vermutlich wollte der Arbeitgeber sich so eine eventuell noch notwendig werdende Beweisführung sichern. Die durch die Anwesenheit weiterer Personen wachsende Drucksituation und entstehende Prangerwirkung kann aber nur schlecht gezeugnet werden.

Eine freiwillige Entscheidungsfindung scheiterte auch an der Minderjährigkeit des Beschwerdeführers. Ob Minderjährige in die Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten wirksam einwilligen können, beurteilt sich nach dem Grad ihrer Einsichtsfähigkeit. Abstrakte Aussagen, ob ab Erreichen eines bestimmten Alters diese Einsichtsfähigkeit gegeben ist, helfen nicht weiter.<sup>28</sup> Ausschlaggebend ist immer der jeweilige Verwendungszusammenhang. Er entscheidet darüber, ob die Einwilligung des Minderjährigen ausreicht oder ob sein gesetzlicher Vertreter zusätzlich einverstanden sein muss. Im zu entscheidenden Fall sprachen die Umstände des Einzelfalls dafür, neben der Einwilligung des Beschwerdeführers auch die seines gesetzlichen Vertreters als notwendig anzusehen, da die Konsequenzen insbesondere in Bezug auf den weiteren beruflichen Werdegang als gravierend anzusehen waren.

Hinzu kam noch, dass die von § 4a Abs. 3 BDSG gestellten Anforderungen an die Einwilligung zur Erhebung besonderer Arten personenbezogener Daten nicht erfüllt waren. Eine Einwilligung muss sich bei dieser Datenkategorie ausdrücklich hierauf beziehen.

Die Erhebung besonderer Arten personenbezogener Daten war auch nicht nach § 28 Abs. 6 Nr. 3 BDSG erlaubt. Diese Vorschrift knüpft die zulässige Datenverwendung, ebenso wie § 32 BDSG, an das Erforderlichkeitsprinzip. Dass der Arbeitgeber dieses hier grob außer Acht gelassen hat, liegt auf der Hand. Der Beschwerdeführer hatte ja seinen Cannabiskonsum selbst bestätigt; auf Nummer sicher gehen musste der Arbeitgeber daher allemal nicht, ein weiterer Test war überflüssig.

In diesem Zusammenhang ließen wir es uns nicht nehmen, Hinweise zur Durchführung von Drogentests im Allgemeinen zu geben: Sie sind nur zulässig, wenn Beschäftigte hierzu schriftlich wirksam eingewilligt haben. Der Test muss darauf gerichtet sein, eine Alkohol- oder Drogenabhängigkeit nachzuweisen. Es darf nicht lediglich darum gehen, den

24 Zu den Beschäftigten im Sinne des BDSG zählen auch die zu ihrer Berufsausbildung Beschäftigten, vgl. § 3 Abs. 11 Nr. 2 BDSG.

25 Vgl. § 4a Abs. 1 Satz 2 BDSG.

26 Vgl. Simitis, in: Simitis, BDSG, § 4a Rn. 62, 8. Aufl., 2014.

27 Dies belegt schon die Existenz des Berufsbildungsgesetzes.

28 Vgl. Simitis, in: Simitis, BDSG, § 4a Rn. 21, 8. Aufl., 2014.

Alkohol- oder Drogenkonsum zu ermitteln. Nichts anderes macht aber ein THC-Schnelltest. Er trifft keinerlei Aussage über die physische oder psychische Verfassung des Betroffenen, die eine Drogenabhängigkeit belegen könnte. Noch wichtiger: Ein solcher Test muss erforderlich sein, um die Eignung des Arbeitnehmers für die konkret vorgesehene Tätigkeit festzustellen. Arbeitsplatzrelevantes Verhalten liegt allerdings nur vor, wenn der Mitarbeiter durch ein abhängigkeitsbedingtes Fehlverhalten sich selbst, Leben und Gesundheit Dritter oder bedeutende Sachwerte des Arbeitgebers gefährden könnte. Ob der Drogenkonsum strafbar wäre oder nicht, ist nicht die Sache des Arbeitgebers. Dem Arbeitgeber darf zudem nur das Ergebnis der Eignungsuntersuchung vom untersuchenden Arzt mitgeteilt werden, nicht eine nähere Diagnose oder einzelne Gesundheitszustände.

### Praxistipp:

*Die Einwilligung des Beschäftigten kann nur dann als Rechtsgrundlage für die Verwendung seiner Daten dienen, wenn die hohen gesetzlichen Anforderungen – Transparenz, Freiwilligkeit, Schriftform – eingehalten werden. Das Argument der Zwangslage und Unfreiwilligkeit kann der Arbeitgeber minimieren, indem er die Einwilligung an die Gewährung rechtlicher Vorteile knüpft, auf die der Betroffene sonst keinen Anspruch hätte.*

## II. Die Welt des Beschäftigtendatenschutzes aus Sicht des LfDI BW

Praxisfälle aus der täglichen Arbeit der Aufsichtsbehörden bringen die bestehenden Defizite im Bereich des Datenschutzes ans Licht. Gerade der Bereich des Beschäftigtendatenschutzes stellt sich hier als besonders spannende Rechtsmaterie dar. Oft handelt es sich um brisante Fälle, bei deren Meldung der betroffene Arbeitnehmer Konsequenzen für sein Arbeitsverhältnis befürchtet. Vermutlich finden sich in keinem anderen Bereich des Datenschutzes so zahlreiche anonyme Beschwerden oder der Wunsch der Betroffenen, gegenüber dem Arbeitgeber unerkannt zu bleiben. Auf der anderen Seite birgt das Arbeitsverhältnis als höchstpersönliches Näheverhältnis die latente Gefahr, doch als derjenige ausfindig gemacht zu werden, der bei der Aufsichtsbehörde eine Beschwerde eingereicht hat. Bei Unternehmen mit wenigen Beschäftigten erklärt sich dies von selbst; bei Beschwerden, bei denen der Betroffenenkreis von vornherein durch den dargestellten Sachverhalt begrenzt wird, könnten Nachforschungen Rückschlüsse auf die Person des Beschwerdeführers zulassen.

Dem Wunsch der Betroffenen, ihre Beschwerde nicht gegenüber dem Arbeitgeber zu offenbaren, kommen wir als Aufsichtsbehörde selbstverständlich gerne nach. Wir sind rechtlich in der Lage, Nachfragen des Arbeitgebers zur Identität eines Beschwerdeführers zurückzuweisen. Zugleich sprechen wir aber mit dem Beschwerdeführer über die Möglichkeit des Arbeitgebers, Rückschlüsse auf seine Identität auch bei einer anonymen Vorgehensweise zu ziehen.

### 1. Der Weg ins Beschäftigungsverhältnis

Viele kennen das: Mühselig werden alle Bewerbungsunterlagen zusammengesucht, ein freundliches Foto, für das ein überbelegter Fotograf aufgesucht wurde, gut sichtbar auf das Deckblatt der Bewerbungsmappe geklebt. Hat man letzteres weggelassen, sinkt die Wahrscheinlichkeit, zu einem persönlichen Gespräch eingeladen zu werden, gegen Null.

Jeder Arbeitgeber möchte möglichst aussagekräftige Informationen über zukünftige Mitarbeiter, über ihre fachliche Qualifikation, ihren Werdegang, ihre persönlichen Verhältnisse, ihren Gesundheitszustand und ihre Zukunftsplanung erhalten. Welcher Unternehmer möchte schon einen mehrfach straffällig gewordenen, alleinerziehenden Mitarbeiter, der in der Vergangenheit an häufigen Kurzerkrankungen litt, mit der Aufgabe besonders wichtiger Unternehmensinteressen betrauen? Liegt die Verurteilung wegen Beleidigung des Nachbarn als Ursache einer schief geschnittenen Hecke aber mehr als 20 Jahre zurück und ist der Bewerber Vater eines 17 Jahre alten Kindes, sieht die Sache doch wieder ganz anders aus. Wenn die Kurzerkrankungen einmal eine Migräne, einmal ein Infekt, ein anderes Mal eine Erkältung waren und der Bewerber jeweils zwei Tage arbeitsunfähig krankgeschrieben war, haben auch diese Informationen ihre Aussagekraft fast vollständig verloren.

Das Interesse von Arbeitgebern nach aussagekräftigen Informationen potentieller Mitarbeiter wird durch das in der Rechtsprechung entwickelte „Fragerecht des Arbeitgebers“ gestillt.<sup>29</sup> Gleichzeitig werden Inhalte und Grenzen dieses Fragerechts durch das „Recht zur Lüge“<sup>30</sup> bei unzulässigen Fragen konterkariert und können auch mithilfe einer Einwilligung nicht erweitert werden. § 32 BDSG bindet den Arbeitgeber auch in der Phase vor Begründung eines Beschäftigungsverhältnisses an das Erforderlichkeitsprinzip und nimmt somit Einfluss auf die Konzeption und Durchführung des Auswahlverfahrens. Somit dürfen nur solche Informationen erhoben werden, die – je nach Stand des Bewerbungsverfahrens – für die Entscheidungsfindung tatsächlich benötigt werden.

#### a) Fall 3: Zuviel gefragt!

Immer wieder erreichen uns Beschwerden, bei denen Bewerber unzulässige Fragen des Arbeitgebers ausgesetzt sind. Bezüge zur konkreten Tätigkeit fehlen nicht selten vollständig. Oft werden uns Personal- und Bewerberbögen vorgelegt, die der Betroffene im Rahmen seiner Bewerbung ausfüllen soll. Hierbei stoßen wir immer wieder auf die nachfolgend dargestellten Fragen:

##### – Familienverhältnisse

Fragen zu den Familienverhältnissen eines Bewerbers (z.B. Familienstand, alleinerziehend, Zahl und Namen der Kinder) sind grundsätzlich unzulässig. Erkundigungen nach Zahl und Alter der Kinder können ausnahmsweise dann zulässig sein, wenn die Position, für die sich der

<sup>29</sup> Vgl. auch BAG 22.10.1986 – 5 AZR 660/85 – DB 1987, 1048.

<sup>30</sup> BAG AP Nr. 2 zu § 123 BGB, st. Rspr.

Arbeitnehmer bewirbt, regelmäßig mit unvorhersehbaren Einsätzen zu ungewöhnlichen Zeiten verbunden ist, die einem alleinerziehenden Elternteil minderjähriger Kinder nicht oder nur schwer möglich sind. Die Frage ist daher nur in besonderen Ausnahmefällen zulässig.

– Stammdaten

Name, Anschrift, Telefonnummer und E-Mail-Adresse sind für den Arbeitgeber erforderlich, um mit dem Bewerber Kontakt aufnehmen zu können. Es reicht aus, wenn der Bewerber beim Arbeitgeber eine Kontaktmöglichkeit angibt. Entsprechend des Stellenprofils kann die Angabe mehrerer Kontaktmöglichkeiten jedoch erforderlich sein, wenn der Bewerber kurzfristig erreichbar sein muss, etwa als Pressesprecher. Regelmäßig nicht zur Identifizierung des Bewerbers notwendig sind Geburtsort, Geburtsname, Alter und Nationalität. Solche Fragen können Indizien für eine Diskriminierung sein.<sup>31</sup> Allerdings besteht die Möglichkeit für den Arbeitgeber, sich im Rahmen des Vorstellungsgesprächs den Personalausweis des Bewerbers zur Identifizierung vorlegen zu lassen – damit ist aber nicht gesagt, dass eine Kopie hiervon zulässig ist.

– Fahrerlaubnis

Das Vorhandensein einer Fahrerlaubnis ist nur relevant, wenn diese zur Erledigung der geschuldeten Arbeit benötigt wird.

– Fremdsprachen

Nach Sprachkenntnissen darf gefragt werden, wenn diese für die vorgesehene Tätigkeit bedeutsam sind. Das Ziel, eine gute Kommunikation mit Kunden und Kollegen zu gewährleisten, kann die Frage nach ausgezeichneten oder sehr guten Sprachkenntnissen rechtfertigen.

– Vorstrafen und laufende Ermittlungen

Nach Vorstrafen darf ein Arbeitgeber nur unter Beschränkung auf das für den jeweiligen Arbeitsplatz wichtige Strafrechtsgebiet fragen. Als einschlägig anzusehen sind dabei Vorstrafen, die nach der Art ihrer Begehung oder den betroffenen Rechtsgütern objektiv eine besondere Nähe zu der vorgesehenen Beschäftigung aufweisen. Das Bundesarbeitsgericht hat insoweit zwischen Vermögensdelikten (Bankkassierer), Verkehrsdelikten (Berufskraftfahrer), politischen Delikten (Mitarbeiter des Verfassungsschutzes) und Sittlichkeitsdelikten (Jugendpfleger) unterschieden. Der Arbeitgeber muss daher differenziert vorgehen. Ein einzustellender Busfahrer darf nach Verkehrsdelikten gefragt werden, nicht aber nach begangenen Vermögensdelikten. Vorstrafen, die gemäß § 32 Abs. 2 des Bundeszentralregistergesetzes (BZRG) nicht in ein Führungszeugnis aufgenommen werden, der Tilgung unterliegen oder nur in ein Führungszeugnis für Behörden aufgenommen werden, brauchen gemäß § 53 Abs. 1 BZRG nicht offenbart zu werden, worauf der Bewerber hinzuweisen ist. Grob rechtswidrig ist es, den Bewerber eine Selbstauskunft aus dem BZRG vorlegen zu lassen.

Die Frage nach laufenden Straf- und Ermittlungsverfahren ist zulässig, soweit ein solches Verfahren bereits Zweifel

an der persönlichen Eignung und Zuverlässigkeit des Bewerbers für den konkreten Arbeitsplatz begründen kann oder die Verfügbarkeit des Bewerbers durch das Verfahren erheblich eingeschränkt ist, weil mit umfangreichen Ermittlungen, Untersuchungshaft oder der Verurteilung zu einer Freiheitsstrafe zu rechnen ist.

– Pfändungen und Lohnabtretungen

Bei der Besetzung von Vertrauenspositionen, mit denen beträchtliche finanzielle Spielräume verbunden sind, kann sich der Arbeitgeber erkundigen, ob der Bewerber in geordneten wirtschaftlichen Verhältnissen lebt oder überschuldet ist, ob Lohnpfändungen oder -abtretungen erfolgt sind, der Bewerber eine eidesstattliche Versicherung abgegeben hat oder ein privates Insolvenzverfahren eröffnet wurde. Das gilt allerdings nicht für die Kassiererin im Supermarkt. Es gibt keine Belege dafür, dass arme Kassierer unehrlicher sind als reiche.

– Chronische Krankheiten und beantragte Kuren

Fragen nach Vorerkrankungen und dem Gesundheitszustand eines Bewerbers betreffend seine Intimsphäre sind nur eingeschränkt zulässig. Der Arbeitgeber darf sich danach erkundigen, ob eine Krankheit oder eine Beeinträchtigung des Gesundheitszustands vorliegt, durch welche die Eignung für die vorgesehene Tätigkeit auf Dauer oder in periodisch wiederkehrenden Abständen eingeschränkt ist. Nach ansteckenden Krankheiten, die zwar nicht die Leistungsfähigkeit beeinträchtigen, jedoch die zukünftigen Kollegen oder Kunden gefährden könnten, darf gefragt werden. Ebenfalls in Erfahrung gebracht werden darf, ob es zum Zeitpunkt des Dienstantritts bzw. in absehbarer Zeit zu einer Arbeitsunfähigkeit, z.B. durch eine geplante Operation, eine bewilligte Kur oder auch durch eine zur Zeit bestehende akute Erkrankung, kommen kann.

### Praxistipp:

*Arbeitgeber müssen sich vor der Ausschreibung einer vakanten Stelle über die mitzubringenden Qualifikationen und das Anforderungsprofil des Bewerbers im Klaren sein. Bewerberinformationen dürfen nicht nach Belieben erfragt werden, um erst im Nachhinein zu entscheiden, welche dieser Angaben man für die Besetzung der Stelle benötigt.*

*Nur anhand konkreter Stellenprofile ist es einem Bewerber möglich, sich auf ein Bewerbungsgespräch ausreichend vorzubereiten und abzusehen, welche Informationen über ihn für die ausgeschriebene Stelle von Relevanz sind.*

### b) Fall 4: Nachweise in Hülle und Fülle

Wie die Praxis zeigt, sind die beigelegten Nachweise in Form von Zeugnissen und Ausbildungsnachweisen sowie die im Vorstellungsgespräch mitgeteilten Informationen den meisten Arbeitgebern nicht genug. Ganz nach dem Motto: Vertrauen ist gut, Kontrolle ist besser!

31 Thüsing, Arbeitnehmerdatenschutz und Compliance, Rz. 387.

Eine anonym behandelte Beschwerde gegen einen Geld- und Wertdienstleister zeigt, dass manche Arbeitgeber geradezu von einem Kontrollwahn besessen sind. Das Unternehmen ließ sich zu Beginn eines jeden Beschäftigungsverhältnisses und anschließend im jährlichen Turnus eine Schufa-Selbstauskunft und ein einfaches polizeiliches Führungszeugnis aller Mitarbeiter, die mit sicherheitsrelevanten Aufgaben betraut waren, vorlegen. In aller Beharrlichkeit und Ausführlichkeit versuchte man uns davon zu überzeugen, wie dringend notwendig diese Datenerhebung für die Firma sei. Die Argumente waren vielschichtig, gleichzeitig aber auch einseitig, indem sie die Interessen des einzelnen Beschäftigten fast völlig außen vor ließen: Das Unternehmen habe Verpflichtungen gegenüber Verbänden und Versicherern, welche die jährliche Vorlage einer Schufa-Selbstauskunft und eines einfachen polizeilichen Führungszeugnisses fordern würden. Bei deren Nichtbeachtung würde das Unternehmen seinen Versicherungsschutz verlieren und damit die Existenz der Firma im Ganzen riskieren. Dem Wahrheitsgehalt von Angaben der Beschäftigten dürfe man ohnehin keinen Glauben schenken. Dem Unternehmen könne nicht zugemutet werden, Mitarbeitern Geldbestände in Höhe mehrerer Hunderttausend Euro anzuvertrauen, ohne zu wissen, ob sie nicht in ungeordneten wirtschaftlichen Verhältnissen lebten. Gerade weil kein anderes Transportgut einen annähernd hohen Wert habe und dabei so leicht beiseite zu schaffen sei wie Banknoten, bestehe die permanente Gefahr des Missbrauchs und des Treubruchs durch die eigenen Mitarbeiter.

Dass manche dieser Argumente zunächst ganz einleuchtend erscheinen, soll nicht in Abrede gestellt werden. Was aber an dieser Stelle ganz klar gesagt werden muss: Weder die Vorlage einer Schufa-Selbstauskunft noch eines einfachen polizeilichen Führungszeugnisses können das Risiko eines Missbrauchs durch die eigenen Mitarbeiter schmälern. Es gibt keine Erfahrungswerte, die besagen, dass ein Mitarbeiter, der laufende Kredite bedienen muss, der mehrere Handyverträge abgeschlossen hat und gerade ein Auto geleast hat oder der in den letzten fünf Jahren dreimal umgezogen ist, in ungeordneten Vermögensverhältnissen lebt und daher eher zu Straftaten neigt als jemand, der bei der SCHUFA keinen negativen Eintrag hat. Empirische Studien über solche Erfahrungssätze gibt es nicht. Das Unternehmen konnte auch nicht über entsprechende Erfahrungswerte im Unternehmen berichten. Im Gegenteil: Nachforschungen stellten heraus, dass im Unternehmen überhaupt kein Zusammenhang zwischen etwaigen Missbräuchen von Mitarbeitern und deren vorgelegten SCHUFA-Selbstauskünften bestand.

Dem Unternehmen wurde eine klare Absage erteilt, dass Vorgaben von Verbänden und Versicherern keinen Einfluss auf die Zulässigkeit einer Datenerhebung haben können. Ausgearbeitete Verbandsgrundsätze und Versicherungsbedingungen stellen keine „andere Rechtsvorschrift“ im Sinne von § 4 Abs. 1 BDSG dar. Ansonsten ließen sich die gesetzlichen Standards kinderleicht unterlaufen. Auch die im Nachgang vorgelegte Betriebsvereinbarung bekam von uns einen Korb. Wie bereits erläutert, können die Vertragspar-

teien einer Betriebsvereinbarung ihre Autonomie nur innerhalb der Grenzen höherrangigen Rechts ausüben und den Einzelnen nicht seiner Grundrechte berauben.

Im vorliegenden Fall sprachen aber noch viele weitere Punkte gegen die Zulässigkeit der Vorlage einer SCHUFA-Selbstauskunft und eines einfachen polizeilichen Führungszeugnisses.

Eine SCHUFA-Selbstauskunft ist ausgesprochen umfangreich und enthält daher eine Reihe an personenbezogenen Daten, die mit der konkreten Tätigkeit in keinerlei Zusammenhang stehen. Zudem sind Selbstauskünfte nie für Dritte gedacht. Auch das Argument der Firma, dass bei der SCHUFA nur beachtliche Forderungen eingetragen seien, verfängt nicht. Die Höhe einer Forderung spielt für deren Eintragung bei einer Auskunft nämlich keine Rolle. Der tatsächliche Bestand der Forderung wird von der Auskunft selbst nicht geprüft. Ausschlaggebend ist auch die Aussagekraft der Bonitätsauskunft an sich. Sind beispielsweise zehn Forderungen in einer Höhe von 15 Euro eingetragen, so kann daraus nicht zwangsläufig der Schluss gezogen werden, der Beschäftigte befinde sich in einer finanziellen Zwangslage, die ihn dazu nötigt, die Vermögensinteressen seines Arbeitgebers und seine arbeitsvertraglichen Verpflichtungen zu verletzen.

Auch wenn vielleicht der eine oder andere Beschäftigte in ungeordneten Vermögensverhältnissen leben mag, kann nicht die gesamte Belegschaft unter den Generalverdacht gestellt werden, zur Begehung von Straftaten zu neigen. Den Arbeitgeber hat es zudem nicht zu interessieren, welche Verträge seine Arbeitnehmer geschlossen haben.

Unabhängig der vorgehenden Kritik an SCHUFA-Bonitätsauskünften besteht die Gefahr, dass sich Mitarbeiter aufgrund der Pflicht zur jährlichen Enthüllung ihres Privatlebens, in diesem – vielleicht auch nur unbewusst – einschränken lassen. Muss ein Mitarbeiter befürchten, dass ein weiterer Ratenkauf ihn aus Sicht seines Arbeitgebers zum potentiellen Straftäter mutieren lässt, nimmt er eventuell Abstand vom Vertragsabschluss. Auch vor solchen Einschränkungen wollte der Gesetzgeber die Beschäftigten durch die Einführung von § 32 BDSG schützen.

Nichts anderes gilt für die Vorlage von polizeilichen Führungszeugnissen. Für die bearbeitete Beschwerde musste zusätzlich berücksichtigt werden, dass die Mitarbeiter des Unternehmens bereits durch die zuständigen Gewerbeämter einer Zuverlässigkeitsprüfung unterzogen werden, bei der sogar mindestens eine unbeschränkte Auskunft aus dem Bundeszentralregister<sup>32</sup> eingeholt werden kann.<sup>33</sup> Nach den gewerberechtlichen Vorschriften können die Gewerbeämter den Gewerbetreibenden das Ergebnis der Zuverlässigkeitsüberprüfung einschließlich der für die Beurteilung der Zuverlässigkeit erforderlichen Daten übermitteln. Der Gesetzgeber hätte auf die Übermittlungsbefugnis der Gewerbebehörde verzichten können, wenn es dem Gewerbetreibenden selbst erlaubt wäre, die Zuverlässigkeit anhand der Vorlage eines einfachen polizeilichen Führungszeugnisses zu ermitteln.

32 Auskunft nach § 41 Abs. 1 Nr. 9 Bundeszentralregistergesetz.

33 Vgl. § 34a Gewerbeordnung.

Die hiergegen vorgebrachte Begründung, dass die Zuverlässigkeitsüberprüfung durch die Gewerbeämter viel zu selten erfolge, läuft wegen den Vorschriften der Bewachungsverordnung ins Leere. In Strafsachen gegen Bewachungspersonal müssen Staatsanwaltschaften und Gerichte die Gewerbebehörden unter anderem über den Erlass und den Vollzug eines Haftbefehls, oder einer Anklageschrift unterrichten, wenn der Tatvorwurf geeignet ist, Zweifel an der Eignung oder Zuverlässigkeit hervorzurufen.<sup>34</sup> Durch diese Unterrichtungspflicht wird dem zeitlichen Turnus – regelmäßig, mindestens alle fünf Jahre – von Zuverlässigkeitsprüfungen ausreichend Rechnung getragen. Mehr muss der Arbeitgeber nun wirklich nicht wissen!

Wir fragten nach, was einen Mitarbeiter erwartet, wenn im Führungszeugnis eine Verurteilung wegen Diebstahls eingetragen ist. Geantwortet wurde, dass dieser Mitarbeiter sofort anderweitig eingesetzt werden würde. Auch wenn nicht von der Hand gewiesen werden kann, dass ein polizeiliches Führungszeugnis ein allgemeines Bild über die Zuverlässigkeit wiedergeben kann, wird die Aussagekraft von Bundeszentralregistereinträgen über den aktuellen Stand der Zuverlässigkeit allemal überschätzt. Bis eine rechtskräftige Verurteilung ihren Weg ins Bundeszentralregister findet, vergeht nicht selten einige Zeit. Je nach Durchlaufen des Instanzenzuges kann ein strafrechtliches Gerichtsverfahren gut und gerne über ein Jahr und länger in Anspruch nehmen. Die Argumentation, dass man bei relevanten Bundeszentralregistereintragungen sofort arbeitsrechtliche Maßnahmen ergreifen würde, um einen wegen Diebstahls verurteilten Beschäftigten nicht mehr mit Vermögenswerten zu betrauen, verläuft, bei einer zwei Jahre zurückliegenden Tatbegehung, im Sande. Wenn der Mitarbeiter in dieser Zeit die Interessen des Arbeitgebers nicht geschädigt hat – warum sollte er es jetzt nach über zwei Jahren tun? Und dann gibt es noch das Zufallsargument: Beantragt ein Arbeitnehmer im Januar ein einfaches polizeiliches Führungszeugnis und kommt im Februar ein neuer Eintrag hinzu, erfährt der Arbeitgeber erst im nächsten Jahr von einem inzwischen vielleicht drei Jahre zurückliegenden Delikt.

### Praxistipp:

*Arbeitgeber sollten in regelmäßigen Abständen von ihrem zustehenden Fragerecht in zulässiger Weise Gebrauch machen und den Vorgang entsprechend dokumentieren. Antwortet ein Mitarbeiter auf zulässige Fragen wahrheitswidrig, sammelt der Arbeitgeber ausreichend Abmahnungs- und auch Kündigungsgründe. Auch hier versteht es sich von selbst: Es darf nur nach solchen Vorstrafen gefragt werden, die im unmittelbaren Zusammenhang mit der konkreten Tätigkeit stehen.*

### c) Fall 5: Blind-Date? Nicht ohne einen Background-Check!

Die Tage, in denen Arbeitgeber vor Stapeln von Bewerbungsmappen saßen und als erste Informationsquelle nur der Lebenslauf und die beigelegten Nachweise dienten, sind längst gezählt. Ähnlich wie bei einem Blind-Date versuchen

Arbeitgeber vor dem ersten Treffen oder bereits der Einladung dazu über Suchmaschinen und soziale Netzwerke so viel wie möglich über den potentiellen Mitarbeiter herauszufinden. Wenn dabei peinliche Partybilder oder im schlimmsten Fall auch hasserfüllte Posts über den alten Chef auftauchen, hat man sich ein Bild gemacht, das durch ein persönliches Kennenlernen und zahlreiche Qualifikationsnachweise schwer zu verrücken sein wird. Manchmal haben Arbeitgeber Lebensläufe vor sich, die so beeindruckend sind, dass sie sich fragen, warum der Bewerber ausgerechnet bei ihrem Unternehmen anfragt. Die Ungläubigkeit und das Misstrauen verleitet nicht selten zu einer Überprüfung – einem sog. Pre-Employment-Screening oder auch Background-Check genannt. Was soll schon ein Bachelor und Master of Engineering mit den Abschlussnoten 1.3, Studienaufenthalten in USA, Skandinavien und Asien sowie mit den dazugehörigen fließenden Sprachkenntnissen in einem 20 Mann Betrieb ernsthaft wollen? Oder aber Arbeitgeber sind mit fragmentarischen Lebensläufen konfrontiert und versuchen die Lücken mithilfe des Internets selbst zu schließen.

Dass Background-Checks in der Welt von Headhuntern und im Human-Ressource Bereich eines Unternehmens leider als Selbstverständlichkeit betrachtet werden, zeigen die eingehenden Beschwerden.

Ein großes Pharma-Unternehmen beabsichtigte im Rahmen von Einstellungsverfahren eine umfassende Überprüfung der Lebensläufe aller Bewerber durchzuführen. Argumentationsgrundlage war, wie nicht anders zu erwarten, das besonders sicherheitsrelevante Aufgabengebiet und die hohe Verantwortung des Unternehmens gegenüber der Bevölkerung.

Der Regierungsentwurf vom 15.12.2010 für ein eigenständiges Beschäftigtendatenschutzgesetz sah hierzu in § 32 Abs. 6 vor:

„Beschäftigtendaten sind unmittelbar bei dem Beschäftigten zu erheben. Wenn der Arbeitgeber den Beschäftigten vor der Erhebung hierauf hingewiesen hat, darf der Arbeitgeber allgemein zugängliche Daten ohne Mitwirkung des Beschäftigten erheben, es sei denn, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung das berechnete Interesse des Arbeitgebers überwiegt. Bei Daten aus sozialen Netzwerken, die der elektronischen Kommunikation dienen, überwiegt das schutzwürdige Interesse des Beschäftigten; dies gilt nicht für soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind.“ (BT-Drucks. 17/4230)

Auch wenn diese Regelungen eines eigenständigen Beschäftigtendatenschutzes nur Entwurf blieben, findet sich der Aussagegehalt der vorstehenden Regelung im derzeit gültigen § 32 BDSG wieder.<sup>35</sup> Arbeitgeber dürfen Informationen, die vom Fragerecht nicht erfasst sind, auch nicht über allgemein zugängliche Quellen (vgl. dazu § 28 Abs. 1 Nr. 3 BDSG) beschaffen. Anders ist dies nur bei Online-

<sup>34</sup> Vgl. § 15 Bewachungsverordnung.

<sup>35</sup> NK-GA/Brink, § 32 BDSG Rn. 20.

Diensten wie den beruflichen Netzwerken XING oder LinkedIn, die Beschäftigte zur Selbstdarstellung nutzen. Sie lassen ausnahmsweise das schutzwürdige Interesse des Bewerbers hinter dem Interesse des potenziellen Arbeitgebers an einer Datenerhebung ohne Mitwirkung des Beschäftigten zurückstehen. Recherchen in sozialen Netzwerken wie Facebook oder Twitter stellen sich hingegen als datenschutzrechtlich unzulässig dar. Pre-Employment-Screenings sollten auch nicht auf die Einwilligung des Bewerbers als Legitimationsgrundlage gestützt werden. Zumindest aber ist die besondere Situation des Bewerbers in den Blick zu nehmen, die in der Regel dazu führen wird, die von § 4a Abs. 1 BDSG geforderte Freiwilligkeit verneinen zu müssen.

#### Praxistipp:

*Wir empfehlen, auf die Durchführung von Pre-Employment-Screenings zu verzichten. Dem Arbeitgeber stehen genügend Möglichkeiten (bspw. Vorstellungsgespräch, Nachweis von Unterlagen im Original, Assessment-Center) zur Verfügung, um die richtige Personalentscheidung zu treffen.*

#### d) Fall 6: Arbeitgeber unter sich

In einem anderen Fall sah sich ein Arzt und Arbeitgeber infolge eines fehlenden Arbeitszeugnisses in der „Pflicht“, beim vorherigen Arbeitgeber eines Bewerbers nachzufragen. Im Vorstellungsgespräch wurde der Bewerber damit konfrontiert, dass man nun auch wüsste, warum das frühere Arbeitsverhältnis nicht mehr bestehe.

Die Vorgehensweise des Arztes stellt ohne die Einwilligung des Bewerbers einen Verstoß gegen den Grundsatz der Direkterhebung<sup>36</sup> dar. Auch wenn das Gesetz gewisse Ausnahmen hiervon zulässt, sind personenbezogene Daten grundsätzlich beim Betroffenen selbst zu erheben. Auch bei der Besetzung von Positionen mit besonderer Verantwortung rechtfertigt die Sorgfaltspflicht des zukünftigen Arbeitgebers keine Arbeitgeberauskunft ohne die Einwilligung des Betroffenen. Abgesehen davon verletzt der ehemalige Arbeitgeber regelmäßig die aus dem Arbeitsvertrag nachwirkende Treuepflicht, wenn er ohne das Einverständnis des Betroffenen Informationen an Dritte weitergibt. Und ein Verstoß gegen das BDSG ist dies allemal. Das sehen manche Arbeitsgerichte leider anders – aber übersehen dabei den Datenschutz.

#### Praxistipp:

*Personenbezogenen Daten sind grundsätzlich beim Betroffenen zu erheben – Nachfragen beim alten Arbeitgeber damit tabu.*

*Leider konstruieren manche Arbeitsgerichte eine Art arbeitsgeberrechtliche Schicksalsgemeinschaft und halten Nachfragen beim ehemaligen Chef für gerechtfertigt.*

#### e) Fall 7: Mit alten Bewerbungsunterlagen zum neuen Job?

Ist der Kampf im Bewerbungsalltag überstanden, stellen sich viele die Frage: Was passiert eigentlich mit meinen Bewerbungsunterlagen? Die meisten wurden vielleicht schon

bei der Stellenausschreibung darauf hingewiesen, dass eine Rücksendung von postalisch eingegangenen Unterlagen aus Kostengründen nicht erfolgen wird. Werden die Bewerberstapel dann in den hintersten Kellerecken des Unternehmens aufbewahrt oder landen sie am besten ungeschützt in der blauen Tonne, ohne zuvor auch nur einen Aktenvernichter gesehen zu haben? Wie sieht es mit den per E-Mail eingegangenen Bewerbungen aus? Werden sie jemals gelöscht oder können sich auch alle nachfolgenden Personalere oder gar die gesamte Belegschaft problemlos ein Bild der vergangenen letzten Bewerberjahre machen?

Die richtigen Antworten auf diese Fragen hängen erst einmal entscheidend davon ab, ob sich Unternehmen und Bewerber für einander entschieden haben und ein Arbeitsverhältnis eingegangen sind oder nicht. Bei einer Einstellung werden die Bewerbungsunterlagen in der Regel Teil der Personalakte. Pauschale Übernahmen dürfen aber nicht erfolgen, sondern nur in dem zur Durchführung des Beschäftigungsverhältnisses dann erforderlichen Umfang.

Hat sich der Kandidat gegen das Unternehmen als seinen zukünftigen Arbeitgeber entschieden oder dieser die Bewerbung der einzigen Frau bevorzugt behandelt und den männlichen Mitstreitern eine Abfuhr erteilt, sind deren Bewerbungsunterlagen unwiederbringlich zu löschen bzw. zu vernichten. Mit der Entscheidung eines bestimmten Bewerbers für eine vakante Stelle ist der Zweck der übrigen Bewerbungsunterlagen – nämlich das Auswahlverfahren – weggefallen und diese somit zu löschen oder dem Bewerber wieder auszuhändigen. Entsprechend ist zu verfahren, wenn eine Bewerbung von sich aus zurückgezogen wird. Fast jede negative Personalentscheidung birgt jedoch die Gefahr eines Anti-Diskriminierungsprozesses wegen Verstoßes gegen das Allgemeine Gleichbehandlungsgesetz (AGG). Um Schadensersatzforderungen erfolgsversprechend abwehren zu können, benötigen Arbeitgeber häufig die Bewerbungsunterlagen. Ohne sie wird es Arbeitgebern nur schwer möglich sein nachzuweisen, dass ein Bewerber nicht aus Gründen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität benachteiligt wurde.<sup>37</sup> Die Gefahr, einer AGG-Klage ausgesetzt zu werden, besteht aber nicht ewig. Will ein Bewerber eine Benachteiligung wegen eines vom AGG verbotenen Merkmals geltend machen, muss er mit seiner Klage die Zweimonatsfrist des § 15 Abs. 4 AGG einhalten. Der LfDI BW hält eine Speicherung über drei Monate hinaus daher für nicht erforderlich.

#### Praxistipp:

*Um die Löschfrist von drei Monaten für Bewerbungsunterlagen abgelehnter oder nicht mehr interessierter Bewerber auf eine konkrete Stelle, einzuhalten, sollten die Datenverarbeitungsprogramme so konfiguriert werden, dass eine eigenständige Löschung im entsprechenden Turnus erfolgt.*

<sup>36</sup> Vgl. § 4 Abs. 2 Satz 1 BDSG.

<sup>37</sup> Vgl. § 1 Allgemeines Gleichbehandlungsgesetz.

Es gibt aber auch Fälle, bei denen beide Seiten an einer längeren Speicherung bzw. Aufbewahrung der Bewerbungsunterlagen interessiert sind. Solche Konstellationen findet man insbesondere bei weltweit tätigen Konzernen, die laufend neue Stellen ausschreiben, und bei Initiativbewerbungen. Gibt ein Bewerber unmissverständlich zu verstehen, dass er auch an anderen Positionen im Unternehmen interessiert wäre und bei zukünftigen Stellenbesetzungen berücksichtigt werden möchte, dürfen seine Unterlagen auch für längere Zeit gespeichert werden. Oft stellen Unternehmen Bewerbungsportale zur Verfügung, bei denen die Bewerber ihre Unterlagen selbst hochladen und eigenständig bearbeiten und löschen können. Grundsätzlich ist dieses Format zu begrüßen, da es dem Bewerber den weitesten Spielraum über seine Datennutzung gewährt. Voraussetzung ist aber, den Bewerber ausreichend zu informieren, wie seine personenbezogenen Daten verarbeitet werden. Hierzu gehört auch eine Mitteilung, wie die Daten übertragen – hoffentlich auch verschlüsselt! – werden.

Stellt ein Unternehmen zum Einreichen der Bewerbung eine Bewerberplattform zur Verfügung, haben die Bewerber oft auch die Wahl, in einen sogenannten Talentpool aufgenommen zu werden. Hierdurch können die Bewerber auch für zukünftig zu besetzende Stellen berücksichtigt werden.

Bei einer bei uns eingegangenen Beschwerde gegen eine führende Wirtschaftsprüfungsgesellschaft hatte sich ein Bewerber mit der Aufnahme in den Talentpool einverstanden erklärt. Aber auch die Datensammlung in einen Talentpool kann nicht zeitlich unbegrenzt erfolgen. Eine wirksame Einwilligung setzt auch die Kenntnis der Speicherdauer voraus. In den Datenschutzhinweisen der Wirtschaftsprüfungsgesellschaft lasen wir, dass die Speicherdauer drei Jahre beträgt und jede Kontaktaufnahme zu einer Verlängerung um weitere drei Jahre führt. Um was für eine Kontaktaufnahme es sich handeln musste, wurde den Bewerbern nicht mitgeteilt. So könnte bspw. auch ein Löschungsbegehren nach dieser schwammigen Regelung dazu führen, dass weitere drei Jahre gespeichert wird. Solche Fallkonstellationen werden Bewerber bei der Abgabe ihrer Einwilligung mit Sicherheit nicht im Sinn gehabt haben. Durch unsere Beratung konnten wir das Unternehmen davon überzeugen, dass bereits die erstmalige Speicherung von drei Jahren für sich genommen weder im Interesse des Unternehmens noch im Interesse des Bewerbers liegen kann. Auf unsere Frage, welchen Aussagegehalt drei Jahre alte Bewerbungsunterlagen in der heutigen Zeit noch haben können, fand das Unternehmen keine überzeugende Antwort. Schließlich konnte erreicht werden, dass die Unterlagen im Talentpool für einen Zeitraum von einem Jahr gespeichert werden dürfen und nur Kontaktaufnahmen, die mit der Eingehung eines Beschäftigungsverhältnisses im konkreten Zusammenhang stehen, zu einer Verlängerung der Speicherdauer um sechs Monate führen können.

#### **Praxistipp:**

*Entscheidet sich ein Unternehmen Bewerbungsportale zu nutzen und den Bewerbern die Aufnahme in einen Talentpool zu*

*ermöglichen, sollten die Datenschutzhinweise konkret formuliert werden. Hierbei ist insbesondere auf die jederzeitige Widerrufsmöglichkeit der Einwilligung hinzuweisen.*

*Vorratsdatenspeicherungen von Bewerbungsunterlagen dürfen nicht das Ziel sein, sondern Seriosität. Sonst setzen sich Unternehmen dem Vorwurf aus, unwirksame Einwilligungserklärungen zu produzieren.*

#### **f) Fall 8: Der Datenschutz und seine Tücken**

Es kommt nicht selten vor, dass Betroffene unter dem Mantel des Datenschutzes einen Vorteil erzielen wollen – um eine Verletzung in ihrem Recht auf informationelle Selbstbestimmung geht es da manches Mal gar nicht. Als LfDI BW wird man auch mal instrumentalisiert. Erkennen wir, dass der Datenschutz nur als Vorwand dient, um etwa einem früheren Arbeitgeber Ärger zu machen, weisen wir den Betroffenen entsprechend hierauf hin. Dem einen oder anderen Betroffenen kann es dann auch mal die Sprache verschlagen, wie das nächste Praxisbeispiel zeigt:

Der Betroffene bewarb sich aufgrund eines Vermittlungsvorschlags des Jobcenters bei einem Personaldienstleister. Ganz charmant wurde im Bewerbungsschreiben mitgeteilt, dass er die vorgesehene Tätigkeit nicht ausüben könne und auch nicht zur Einarbeitung bereit sei. Für den Fall, dass man ihn zu einem persönlichen Gespräch einladen möchte, behielt er sich vor, von seinem Rechtsbeistand begleitet zu werden. Zur Krönung legte er seiner Bewerbung einen „Übermittlungswiderspruch“ bei, nach dem es dem Personaldienstleister untersagt sein soll, personenbezogene Daten an Dritte weiterzugeben. Hieran hielt sich der Personaldienstleister zum Nachteil des Bewerbers allerdings nicht. Die Folge war die Kürzung von Sozialleistungen durch das Jobcenter.

Entgegen der Auffassung des Beschwerdeführers durften seine personenbezogenen Daten an das Jobcenter übermittelt werden. Nach dem Sozialrecht ist der Arbeitgeber verpflichtet, den Agenturen für Arbeit auf deren Verlangen hin Auskunft über solche Tatsachen zu geben, die für die Entscheidung über einen Anspruch auf Sozialleistungen erheblich sein können.<sup>38</sup> Da das Jobcenter beim Personaldienstleister Nachfragen zur Ernsthaftigkeit der Bewerbung gestellt hat, durfte er diese auch beantworten. Der Beschwerdeführer wollte nicht auf Anhieb verstehen, dass sein als „Übermittlungswiderspruch“ deklariertes Schreiben nicht die gesetzlichen Erlaubnistatbestände außer Kraft setzen kann. Datenschutz ist also auch für Beschäftigte kein Wunschkonzert.

#### **Praxistipp:**

*Nicht selten erfolgen Anfragen der Bundesagentur für Arbeit zu solchen Fällen telefonisch oder per E-Mail. Wir empfehlen den Unternehmen daher, das Auskunftsverlangen der Bundesagentur für Arbeit zu Beweis Zwecken entsprechend zu dokumentieren.*

<sup>38</sup> Vgl. § 57 SGB II.

## 2. Im Beschäftigungsverhältnis angekommen

Ist der Arbeitsvertrag erstmal unterschrieben und sind die neuen Herausforderungen in Angriff genommen, hinterlässt jeder Arbeitnehmer Tag für Tag seine „Datenspuren“ am Arbeitsplatz. Angefangen beim morgendlichen Stechen der Zeitkarte, dem Einloggen am PC, der noch schnell versendeten Erinnerungs-E-Mail an die Ehefrau, die Wäsche in die Reinigung zu bringen, bis hin zur gefertigten Videoaufnahme bei der genommenen Abkürzung durch die Lagerhalle, um eine Raucherpause einzulegen, obwohl eine Dienstanweisung das Aus- und Einstecken hierfür vorschreibt.

### a) Fall 9: Auf Schritt und Tritt

Was ursprünglich zur Positionsbestimmung und Navigation im militärischen Bereich vorgesehen war, hat längst im Arbeitsalltag vieler Beschäftigter Einzug gehalten: Globale Positionsbestimmungssysteme – kurz GPS. Durch GPS kann der Arbeitgeber jederzeit den genauen Standort seiner Beschäftigten ermitteln. Welche Vorteile diese Technik für Arbeitgeber hat und welche Nachteile die Kehrseite der Medaille für die Beschäftigte mit sich bringt, zeigt folgende anonym eingegangene Beschwerde:

Der Beschwerdeführer ist Mitarbeiter eines Unternehmens, das einen Teil der Firmenfahrzeuge mit einem GPS-Ortungssystem ausgestattet hat. Aufgrund verschiedenster Vorfälle in der Vergangenheit, wie etwa unerlaubte Privatnutzung der Fahrzeuge, überflüssige Parallelfahrten und unnötige Mehrfahrten, sah sich das Unternehmen genötigt, über den aktuellen Stand seiner Fahrzeuge und Mitarbeiter stets up to date zu sein. Beim kinderleichten Einbau der Geräte hatte die Geschäftsleitung wohl nicht daran gedacht, dass es den Mitarbeitern durch Herunterladen der zugehörigen kostenlosen App des Herstellers und Eingabe der auf den GPS-Trackern frei zugänglichen Seriennummer selbst möglich war, die verschiedenen Kollegen zu orten. Das Unternehmen versuchte uns davon zu überzeugen, dass das System für die Fahrzeugeinsatzplanung, der Arbeitszeiterfassung und deren stichprobenartigen Kontrolle, der Zuordnung einzelner Kosten zu bestimmten Projekten, dem Diebstahlschutz und einer ordnungsgemäßen Dokumentation der Dienstfahrten gegenüber dem Finanzamt einfach unabdingbar sei. Unabhängig davon habe fast die gesamte Belegschaft „freiwillig“ in die Nutzung der Ortungssysteme eingewilligt.

Aus unserer Sicht kann der Einsatz eines GPS-Ortungssystems durch das Unternehmen nicht auf die Einwilligung der Beschäftigten gestützt werden, da bei einer flächendeckenden Überwachung nicht von der erforderlichen Freiwilligkeit einer Einwilligung der Beschäftigten ausgegangen werden kann.

Die Nutzung von Ortungssystemen, mit denen das Arbeitsverhalten von Beschäftigten dauerhaft kontrolliert wird, ist datenschutzrechtlich unzulässig, da Beschäftigte keineswegs einem permanenten Kontrolldruck ausgesetzt sein dürfen. Dies gilt nicht nur für die Überwachung durch den Arbeitgeber, sondern erst Recht durch die eigenen Kollegen. Die gehen diese Informationen schlicht nichts an.

Nachstehende Punkte sind daher bei der Einführung und dem Betrieb des Ortungssystems von dem betroffenen Unternehmen zu beachten:

- Schon bei der Planung und Ausgestaltung der Systeme ist der Grundsatz der Datensparsamkeit zu verfolgen: Nur die für die betrieblichen Zwecke wirklich erforderlichen Daten, nicht die überflüssigen, sind zu erheben. Eine routinemäßige Ortung eines Fahrzeugs ist unzulässig, wenn sie unabhängig von den notwendigen Planungen erfolgt. Der Einsatz von Ortungssystemen ist nicht erforderlich, wenn der Aufenthaltsort des Beschäftigten auch direkt bei diesem (etwa durch einen Anruf) erhoben werden kann – Grundsatz der Direkterhebung.
- Die Zweckbestimmung muss klar dokumentiert und gegenüber den Beschäftigten in transparenter Weise kommuniziert werden. Sie sind insbesondere über den Erhebungszweck und -umfang sowie über die Auskunftsrechte hinsichtlich der gespeicherten Daten zu informieren. Entsprechend § 33 BDSG sind die Beschäftigten, etwa durch eine Benachrichtigung oder eine Leuchtanzeige am Gerät, darüber in Kenntnis zu setzen, wann eine Ortung erfolgt. Ansonsten liegt eine verbotene heimliche Überwachung der Mitarbeiter vor.
- Die Beschäftigten sind über die Regelungen der Zugangsberechtigung zu den gespeicherten Daten sowie der Protokollierung der Speicherung und der Festlegung der Speicherdauer der Daten zu informieren.

### Praxistipp:

*Wenn betriebliche Abläufe es dem Arbeitgeber grundsätzlich erlauben, Systeme einzusetzen, durch die eine dauernde Verhaltens- und Leistungskontrolle möglich ist, ist der Arbeitgeber gehalten, eine solche Kontrolle durch Betriebsvereinbarungen oder einseitige verbindliche Regelungen auszuschließen. Der Arbeitgeber hat bereits bei der Wahl des Herstellers auf einen möglichen datenschutzkonformen Einsatz der Geräte zu achten – Stichwort: Privacy by design.*

*Es sollte nicht in Geräte und Systeme investiert werden, bei denen bspw. keine Zugriffsbeschränkung möglich ist.*

### b) Wenn personenbezogene Daten auf Wanderschaft gehen

Es ist eigentlich keine Konstellation denkbar, bei der Mitarbeiterdaten das Unternehmen nicht verlassen. Spätestens, wenn es um Fragen wie Sozialabgaben oder Steuern geht, findet immer eine Übermittlung von Beschäftigtendaten an die zuständigen Behörden statt. Die wirklich brisanten Fälle spielen sich aber im täglichen Beschäftigtenalltag ab. Hierzu zählen die Weitergabe an den rechtlich selbstständigen Mutterkonzern, Veröffentlichungen auf der Firmenhomepage oder auch simple Aushänge am schwarzen Brett eines Unternehmens oder im eingerichteten Intranet. Ob die Bekanntgabe an einen Dritten im datenschutzrechtlichen Fachjargon eine Übermittlung<sup>39</sup> darstellt oder intern

39 Vgl. § 3 Abs. 4 Satz 2 Nr. 3 BDSG.

als Nutzung<sup>40</sup> stattfindet oder durch den Abschluss eines Vertrags zur Auftragsdatenverarbeitung privilegiert behandelt wird, muss jeweils im Einzelfall festgestellt werden. Nicht ganz einfach ...

### aa) Das Mutter-Tochter-Verhältnis

Die aus Sicht des Datenschutzes als problematisch einzustufende Weitergabe von Beschäftigtendaten innerhalb einer Unternehmensgruppe oder eines Konzerns zeigt einmal mehr, dass ein eigenständiges Beschäftigtendatenschutzgesetz längst überfällig ist. Die zunehmende Verflechtung von Unternehmensstrukturen wird vom Gesetzgeber nicht übersehen. Vielmehr treibt er sie durch Abschluss internationaler Regelungen zur Förderung freier internationaler Märkte voran. Beim Erarbeiten der datenschutzrechtlichen Bestimmungen hat man aber außer Acht gelassen, dass internationale Entwicklungen auch die Verwendung von Beschäftigtendaten beeinflussen. Die Vorstellung, dass ein Arbeitgeber alleine die Leistungskriterien eines Arbeitsverhältnisses bestimmt, ist überholt. Die meisten Beschäftigten haben nicht mehr nur „einen“ Arbeitgeber. Die gesellschaftlichen Strukturen lassen daher arbeitgeberseitige Weisungs- und Kontrollbefugnisse teilweise auseinanderfallen.

An dieser Stelle kann man es aussprechen: Der Datenschutz hinkt hinterher. Das geltende BDSG kennt kein Konzernprivileg, d.h. jedes eigenständige Unternehmen, das Teil einer Unternehmensgruppe oder eines Konzerns ist, betrachtet das BDSG als jeweils eigene verantwortliche Stelle. Jeder Austausch zwischen Tochterunternehmen und Mutterkonzern bedarf einer Rechtfertigung – gerade so, als seinen Mutter und Tochter nicht miteinander „verwandt“. Klingt nicht nur unpraktikabel, ist es auch. Konzernen kann daher nur empfohlen werden, Konzernbetriebsvereinbarungen abzuschließen, die eine unkomplizierte Weitergabe von Beschäftigtendaten im Rahmen des Notwendigen erlauben. Gleichzeitig kann das Datenschutzniveau durch transparente Information der Beschäftigten über die Datenübermittlung, eine Selbstbindung an Datenschutzregelungen durch Konzernrichtlinien oder auch durch den Abschluss von Datenübermittlungsverträgen<sup>41</sup> erhöht werden.

Die Ungeeignetheit der aktuellen Regelungen wird ab Mai 2018 glücklicherweise durch die DSGVO relativiert. Der europäische Gesetzgeber betrachtet Konzernunternehmen in der Regel als gemeinsame Verantwortliche, die vertraglich unter anderem festzulegen haben, welches Unternehmen für die Erfüllung welcher Betroffenenrechte zuständig ist.<sup>42</sup>

### bb) Fall 10: Know-how hat seinen Preis

Der Bereich Mergers & Acquisitions (M&A) umfasst als Sammelbegriff Transaktionen im Unternehmensbereich wie Fusionen, Unternehmenskäufe, Betriebsübergänge, fremdfinanzierte Übernahmen oder auch Unternehmenskooperationen. Der Wert eines Unternehmens misst sich in erster Linie an seinen Mitarbeitern. Qualifiziertes Personal und das damit verbundene Know-how hat seinen Preis. Da leuchtet es nur ein, dass der potentielle Käufer so viele personenbezogene

Informationen wie möglich verlangt, der Firmeninhaber ihm diese auch nur zu gern geben möchte. Zum Glück hat der Beschäftigtendatenschutz bei den Vertragsverhandlungen auch ein Wörtchen mitzureden.

Ein großer PC-Hersteller veräußerte einen Teil seines Betriebs an ein anderes Unternehmen. Von dem Betriebsübergang waren 20 Mitarbeiter betroffen, wobei sie die Möglichkeit hatten, einer Übernahme durch das neue Unternehmen zu widersprechen und beim alten Arbeitgeber zu gleichbleibenden Bedingungen weiterbeschäftigt zu werden. Um den von der Übernahme betroffenen Mitarbeitern ein Angebot zu machen, erhielt der Erwerber nach Abschluss einer „Vertraulichkeitsvereinbarung“ Kopien der Arbeitsverträge, alle gehaltsrelevanten Daten sowie Daten zur betrieblichen Altersversorgung, Alter, Betriebszugehörigkeit und Arbeitsort der Beschäftigten.

Auch wenn sich die Mitarbeiter durch ein Angebot des Käufers vielleicht wertgeschätzt fühlen, hätten ihre Daten nicht ohne entsprechendes Einverständnis übermittelt werden dürfen. Dies lag im vorliegenden Fall schon wegen des zugesprochenen Widerspruchsrechts jedes Mitarbeiters klar auf der Hand. Ist ein Mitarbeiter unabhängig von verlockenden Angeboten des Erwerbers nicht an einer Übernahme interessiert, ist die Übermittlung seiner Daten erst Recht nicht erforderlich. Umgekehrt bestehen an der Wirksamkeit der Einwilligung in solchen Fällen keine Zweifel, weil die Beschäftigten ja ein Wahlrecht haben, ob sie bleiben oder gehen wollen.

### Praxistipp:

*Bei einer einem Unternehmensverkauf vorausgehenden Vertragsverhandlung kann das Erwerberinteresse häufig durch anonymisierte Beschäftigtendaten gestillt werden. Möchte der Erwerber es ganz genau wissen, dann nur mit Einwilligung des Beschäftigten.*

### cc) Der Mitarbeiter als Aushängeschild

Wirft man einen Blick auf den Internetauftritt eines Unternehmens, wird man meistens mit einem sympathischen Lächeln des Kollegiums begrüßt. Ob es sich hierbei tatsächlich um das Personal des Unternehmens oder um extra hierfür engagierte Schauspieler handelt, erkennt der Besucher nicht. Will das Unternehmen nicht Gefahr laufen, die Homepage wegen einer unwirksamen oder widerrufenen Einwilligung eines Mitarbeiters für teures Geld umgestalten zu lassen, investiert es lieber gleich in „Professionelle“. Was sich anfangs für die meisten als unnötige Investition darstellt, kann am Ende unnötige Gerichtskosten einsparen.

Eine nette Homepage allein nützt vielen Unternehmen aber relativ wenig. Idealerweise soll der meist genutzte Kommunikationsfluss unserer Gesellschaft – das Internet –

<sup>40</sup> Vgl. § 3 Abs. 5 BDSG.

<sup>41</sup> Bei fehlender Weisungsbefugnis des Mutterkonzerns gegenüber der Tochtergesellschaft kommt ein Auftragsdatenverarbeitungsvertrag in der Regel nicht in Betracht. In den meisten Fällen wird es sich um eine Funktionsübertragung handeln.

<sup>42</sup> Vgl. Art. 26 DSGVO.

auch für die Knüpfung neuer Geschäftskontakte sorgen und bestehende pflegen. Ein kundenfreundliches Erscheinungsbild lässt sich nach Ansicht der meisten Arbeitgeber am leichtesten mit der Möglichkeit einer direkten Kontaktaufnahme mit dem zuständigen Mitarbeiter erreichen. Der Kunde möchte wissen, mit wem er es zu tun hat und wer sein Ansprechpartner ist. Hierfür findet er auf der Internetseite des Unternehmens meist den Namen, die Telefonnummer und E-Mail-Adresse, die Funktion und nicht selten auch das passende Foto des Mitarbeiters.

Ein kundenorientiertes Erscheinungsbild ist fast immer als berechtigtes Interesse eines Arbeitgebers anzuerkennen. Im Gegensatz dazu darf nicht vergessen werden, dass eine Veröffentlichung von personenbezogenen Daten im Internet von jedermann global abrufbar ist und die gefundenen Informationen zu einer Person problemlos mit weiteren im Netz vorhandenen Daten zu Persönlichkeitsprofilen zusammengeführt werden können. Der Arbeitgeber hat daher dafür zu sorgen, seinen Internetauftritt so zu konfigurieren, dass Mitarbeiter nicht ohne weiteres von Suchmaschinen wie Google gefunden werden können. Die Veröffentlichung von Arbeitnehmerdaten im Internet ist nur gerechtfertigt, wenn die vertragliche Tätigkeit auch Beziehungen zu Außenkontakten mit sich bringt und der Beschäftigte als direkter Ansprechpartner fungieren soll. So müssen die Kontaktdaten des angestellten Reinigungspersonals selbstverständlich nicht veröffentlicht werden.

Will ein Unternehmen über Namen, Titel, Funktion und dienstliche Erreichbarkeit hinaus der Öffentlichkeit auch ein Foto des Mitarbeiters präsentieren, führt kein Weg an der Einwilligung des Abgebildeten vorbei.<sup>43</sup> Und diese ist freiwillig und kann jederzeit widerrufen werden.

### Praxistipp:

*Die Mitarbeiter sollten vor der Veröffentlichung ihrer Daten im Internet ausreichend informiert werden und die Möglichkeit haben, den Umfang mitzubestimmen, wobei das Motto „Weniger ist mehr!“ gilt. Äußern Mitarbeiter Bedenken, weil die Veröffentlichung etwa ein Sicherheitsrisiko nach sich ziehen könnte, ist der Arbeitgeber verpflichtet, entsprechende Schutzmaßnahmen zu treffen – für den betroffenen Einzelfall ggfs. auch von einer Veröffentlichung abzusehen.*

*Auch hier sind die Mitarbeiter auf die Freiwilligkeit der Einwilligung und ihr Widerrufsrecht hinzuweisen. Machen sie von diesem Gebrauch, ist der Arbeitgeber verpflichtet, die personenbezogenen Daten von der Homepage zu nehmen. Schade, dass das Bundesarbeitsgericht bei seinem Urteil – Az. 8 AZR 1010/13 – nicht die widerrufenen Einwilligung zur Entscheidungsfindung herangezogen hat. Vielmehr hält es die Löschung eines Firmenvideos, zu dem der Kläger früher sein Einverständnis erteilt hatte, lediglich wegen fehlender eindeutiger Erklärung, dass das Video auch über die Beendigung des Arbeitsverhältnisses hinaus genutzt werden dürfe, für geboten.*

### dd) Fall 11: Immer gut informiert

Ein Dauerbrenner in Unternehmen ist die Verwendung von Beschäftigtendaten, die über das „schwarze Brett“ oder das

Intranet veröffentlicht werden. Nicht selten auch über den Kommunikationsdienst WhatsApp.

In einer anonymen Beschwerde informierte uns ein Beschäftigter eines weltweit führenden Technologiekonzerns in der Antriebs- und Fahrwerktechnik darüber, dass die Firma es mit dem Datenschutz nicht besonders genau nimmt: So wurden Krankmeldungen und Arbeitsunfähigkeitsbescheinigungen öffentlich und für jedermann sichtbar am „schwarzen Brett“ ausgehängt. Wem der Weg zum schwarzen Brett zu weit war, warf einen Blick in den für alle einsehbaren Arbeitsplan samt Informationen zu krankheitsbedingten Abwesenheiten von Kollegen.

Selbstverständlich ist es den Arbeitgebern ein nachvollziehbares Anliegen, seine Mitarbeiter über die Abwesenheit von Kollegen zu informieren. Nur wenn die Vertretung weiß, dass sie einspringen muss oder der Gang zum Kollegen im Nachbargebäude nicht lohnt, weil er nicht anzutreffen sein wird, kann ein uneingeschränkter Betriebsablauf sichergestellt werden. Zur Erreichung dieses Ziels muss bei der Veröffentlichung von Arbeitsplänen aber nicht der Grund für die Abwesenheit mitgeteilt werden. Für die Mitarbeiter macht es keinen Unterschied, ob der Kollege im Urlaub oder krank ist – entscheidend ist, dass er nicht da ist und für die Zeit seiner Abwesenheit evtl. Vertretungsregelungen zu beachten sind. Teilt der Arbeitgeber die Abwesenheitsgründe seiner Mitarbeiter der übrigen Belegschaft mit, sorgt er hierdurch möglicherweise nicht nur für Tratsch und Klatsch über den abwesenden Kollegen, sondern auch für eine unzulässige Übermittlung von Daten.

### Praxistipp:

*Bei betriebsöffentlichen Aushängen sollten Fehlzeiten der Beschäftigten ausschließlich in allgemeiner Form, beispielsweise als „abwesend“, aufgeführt werden.*

Obwohl es eigentlich einen Grund zum Feiern gibt, liefern im Unternehmen geführte Geburtstagslisten immer wieder neuen Zündstoff für Konflikte. Den Zweck, zu sehen wie gut oder schlecht sich der ein oder andere Kollege hält oder zur „Pflege des Betriebsklimas“, mag eine Geburtstagsliste vielleicht erfüllen. Zur Durchführung des Beschäftigungsverhältnisses ist sie aber nicht erforderlich.

Das Interesse des Einzelnen, für sich in Würde zu altern und Feierlichkeiten frei sozialer Zwänge nach eigener Entscheidung zu begehen, wiegt schwerer als das Interesse an sozialen Zwecken.

### Praxistipp:

*Möchte ein Unternehmen nicht auf eine Geburtstagsliste verzichten, empfehlen wir, jeden Mitarbeiter nach seiner Einwilligung zu bitten und ihn darüber zu informieren, dass er jederzeit aus der Liste gestrichen werden kann. Als Alternative kann den Mitarbeitern angeboten werden, auf die Angabe ihres Geburtsjahres zu verzichten.*

43 Vgl. die Sondervorschrift des § 22 Kunsturhebergesetzes.

### c) Fall 12: Damit die Stimmung nicht kippt

Den meisten Arbeitgebern ist es ein Anliegen, dass ihre Mitarbeiter gerne zur Arbeit kommen. Motivation, Zufriedenheit und die nötige Wertschätzung steigern die Produktivität der Arbeit und damit auch den Umsatz des Unternehmens. Auf welchem Weg kann der Arbeitgeber das Stimmungsbild in seiner Firma aber am besten ausmachen? Hier wählen die meisten den Weg des vermeintlich geringsten Widerstands: die Mitarbeiterumfrage. Die Idee dahinter klingt verlockend: Der Mitarbeiter macht sich in Ruhe seine Gedanken zum vorgelegten Fragekatalog. Da er sicher ist, nicht als der Urheber des Bogens ausgemacht werden zu können, scheut er sich nicht, vorhandene Defizite anzusprechen. Dass Vorstellung und Realität nicht selten auseinanderfallen, zeigen wiederholt bei uns eingehende Beratungsanfragen zur Gestaltung von Mitarbeiterumfragen.

Im Rahmen eines internen Beurteilungssystems plante ein Betrieb, die Personen mit Führungsverantwortung durch alle Beschäftigten unter Verwendung eines Fragebogens beurteilen zu lassen. Auf die Anonymität der Umfrage wurde jedoch verzichtet, so dass uns ein Mitarbeiter des Unternehmens darum bat ihm mitzuteilen, ob er die Teilnahme an der Umfrage verweigern könne. Die Angst des Beschäftigten, bei einer Weigerung mit arbeitsrechtlichen Konsequenzen rechnen zu müssen, konnten wir ihm leider nicht nehmen. Auch wenn uns unsere Arbeit ohne tiefere arbeitsrechtliche Kenntnisse nicht möglich wäre, obliegt die Beantwortung solcher konkreten Fragen vorrangig den Arbeitsgerichten. Übrigens auch die Frage, ob sich Vorgesetzte solche Umfragen gefallen lassen müssen. Das Abfragen subjektiver Einschätzungen über das Arbeitsumfeld, wie bspw. das Betriebsklima, ist gleichwohl nicht für die Durchführung des Beschäftigungsverhältnisses erforderlich und daher nur auf freiwilliger Basis möglich.

#### Praxistipp:

*Wir empfehlen den verantwortlichen Stellen, die Mitarbeiterumfrage freiwillig und anonym durchzuführen und im Sinne der Transparenz die Beschäftigten über das Vorhaben und die angestrebten Ziele der Befragung rechtzeitig und umfassend zu informieren. Durch die Einschaltung eines Dienstleisters und des Abschlusses eines Vertrags zur Auftragsdatenverarbeitung kann die Anonymität der Umfrage gewährleistet werden. Nur so können Unternehmen ehrliche Antworten erwarten und Ergebnisse sinnvoll zur Verbesserung des Betriebsklimas beitragen.*

### d) Fall 13: „... and action“

Wählt man morgens für den Weg zur Arbeit die U-Bahn statt des Autos oder des Fahrrads, wurde man schon von der einen oder anderen optisch-elektronischen Einrichtung – einer Videokamera – erfasst. Kaum in der Firma angekommen, begegnet einem die nächste Kamera beim Betreten des Grundstücksgeländes. Verfolgt einen das Pech oder doch eher der Arbeitgeber selbst, hat dieser in sämtlichen Betriebsteilen Videokameras installiert. Selbstverständlich nur zu „Zwecken der Gefahrenabwehr und dem Schutz der

eigenen Mitarbeiter“. Der Kreativität von Arbeitgebern, die Installation von Videokameras zu rechtfertigen, ist oft keine Grenze gesetzt.

Was aber ist der entscheidende Unterschied zwischen den Aufnahmen auf dem Weg zur Arbeit in der U-Bahn und der Kamera in den Betriebsräumen? In der U-Bahn geht es um die Überwachung von öffentlich zugänglichen Räumen, bei der Aufnahme in den Betriebsräumen um die Überwachung von Personen, nämlich Beschäftigten, im nicht-öffentlichen Bereich. Ein weiterer entscheidender Aspekt ist, dass der Beschäftigte morgens die Wahl zwischen U-Bahn und Videoaufnahme bzw. Auto und keiner Videoaufnahme hatte. Auch wenn dem Arbeitnehmer für Fälle unzulässiger Videoüberwachung ein Unterlassungsanspruch zusteht und er seine Arbeitsleistung so lange aussetzen kann, bis der ihm zugewiesene Arbeitsplatz nicht mehr im Blickfeld der Kamera liegt<sup>44</sup>, zeigen die täglich eingehenden Beschwerden, dass dieser Weg von den Beschäftigten meist nicht gewählt wird. Die Videoüberwachung stellt daher einen denkbar intensiven Eingriff in das informationelle Selbstbestimmungsrecht der Beschäftigten dar.<sup>45</sup> Die Technik ermöglicht den Arbeitgebern, seine Beschäftigten in ihrer ganzen wahrnehmbaren Persönlichkeit zu beobachten (Monitoring) und reproduzierbar festzuhalten (Aufzeichnung).

Ob die Videoüberwachung zulässig ist, muss für jede Kamera gesondert geprüft werden und hängt von den Umständen des Einzelfalls ab: Welchen Zweck hat die Videoaufnahme? Ist von der Videoüberwachung die gesamte Belegschaft betroffen oder nur bestimmte Personen? Wie lange werden die Aufzeichnungen gespeichert? Sind die Betroffenen über den Einsatz von Videokameras ausreichend informiert oder findet eine heimliche Videoaufzeichnung statt? Hat der Arbeitgeber verbindlich zugesichert, die Aufzeichnungen nicht zum Nachteil der Beschäftigten einzusetzen?

Die Fälle, in denen Beschäftigte Opfer des Überwachungsdrangs ihres Arbeitgebers werden, stellen einen zunehmenden Bereich der täglichen Arbeit des LfDI BW dar.

Wie wir auch von Kollegen aus anderen deutschen Bundesländern erfahren haben, liegt es wohl im Trend vieler Bäckereihinhaber, die Verkaufstheke, also den ausschließlich für Mitarbeiter zugängliche Bereich, mit einer Videokamera zu versehen.

In einem Fall verdächtigte ein Bäcker einen seiner Verkaufsmitarbeiter, sich den einen oder anderen Euro in die eigene Tasche gesteckt zu haben. Da sich der Bäcker nicht mehr zu helfen wusste, installierte er in den Verkaufsräumen eine Videokamera, die ausschließlich den Thekenbereich umfasste. Nachdem sich der Verdacht gegen den einen Mitarbeiter bestätigte und die arbeitsrechtlichen Konsequenzen gezogen wurden, fand der Bäcker die Kamera so nützlich, dass er sie gleich hängen ließ. Da die Videoüberwachung den gesamten Thekenbereich und somit einen

<sup>44</sup> ArbG Dortmund 25.7.1988 – 6 Ca 1026/88 – CR 1989, 715.

<sup>45</sup> Vgl. BAG, Beschluss vom 29. Juni 2004 – 1 ABR 21/03 –, BAGE 111, 173-190.

dauerhaften Arbeitsplatz der Mitarbeiter erfasste, lag ein massiver Eingriff in das informationelle Selbstbestimmungsrecht der Beschäftigten vor. Je weniger Rückzugsmöglichkeiten dem Arbeitnehmer verbleiben, desto stärker wird er in seinem Recht auf informationelle Selbstbestimmung verletzt. Das ist illegal.

Der Gesetzgeber hat für Fälle, in denen bestimmte Mitarbeiter verdächtigt werden, während ihres Beschäftigungsverhältnisses Straftaten zu begehen, mit § 32 Abs. 1 Satz 2 BDSG eine klare Regelung getroffen. Hiernach kann eine Videoüberwachung gegen einen konkreten Beschäftigten zulässig sein, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Diesen Zweck hatte die installierte Videokamera im Fall des Bäckers aber bereits erfüllt. Die zeitlich darüber hinausgehende, rein präventive Videoüberwachung der anderen Mitarbeiter, war nicht mehr von § 32 BDSG gedeckt und somit unzulässig. Die Videokamera wurde schließlich demontiert.

Auch in einem anderen Fall installierte ein Bäcker eine Videokamera, die ausschließlich den Thekenbereich erfasste. Der Zweck dieser Überwachung war aber weitaus origineller als beim vorgehenden Fall. Er bestand darin, den Thekenbestand zu überprüfen und die Bäckerei bei ausgehenden Broten und Kuchen entsprechend und zügig beliefern zu können. Auf unsere Nachfrage, ob nachzuliefernde Ware durch das Verkaufspersonal nicht einfach über das Telefon beim Bäcker angefragt werden kann, erhielten wir die dreiste Antwort, dass man dem Verkaufspersonal diese Fähigkeit nicht zutraue. Durch die Videoüberwachung nehme man diese vertrauensvolle Aufgabe lieber selbst in die Hand. Wie sich herausstellte, wurden die meisten Backwaren vor Ort durch das Verkaufspersonal aufgebacken und nicht, wie behauptet, ständig frisch angeliefert. Dem Bäcker sind die Argumente zur Rechtfertigung der Videokamera endgültig ausgegangen, sie wurde unverzüglich abgebaut. Er backt jetzt kleinere Brötchen ...

### 3. Fall 14: Zum Abschied noch ein Datenschutzverstoß

Nicht immer endet ein Arbeitsverhältnis mit einem festen Handschlag und den besten Wünschen für den weiteren Lebensweg. Nicht selten werden die letzten Worte vor einem Arbeitsgericht gewechselt oder über die Rechtsbeistände ausgetauscht. Hält der ausgeschiedene Mitarbeiter dazu bereits ein anständiges Arbeitszeugnis in den Händen, scheut er sich nicht, der Aufsichtsbehörde alle scheinbaren Datenschutzverstöße der vergangenen Jahre zu präsentieren. Arbeitsvertragliche Konsequenzen muss er bekanntermaßen nicht mehr befürchten und warum nicht den Kollegen zum Abschied was Gutes tun?

Bei allen Konstellationen steht der ehemalige Arbeitgeber vor der Frage: Was passiert mit den personenbezogenen Daten des ausgeschiedenen Mitarbeiters; wie und insbesondere wie lange müssen sie aufbewahrt werden? Dass Unternehmen die Antwort auf die Fragen hin und wieder erst

nach der Trennung von einem Beschäftigten finden, zeigt unsere Beratungspraxis.

Bei einem Unternehmen sind in kürzester Zeit drei Beschäftigte ausgeschieden. Deren personalisierte E-Mail-Accounts wurden auch einige Zeit danach nicht von der Geschäftsführung gelöscht, sondern durchfilzt. Problematisch war, dass die Mitarbeiter ihre E-Mail-Accounts auch zu privaten Zwecken nutzten. Zwar fehlten Regelungen, die eine private Nutzung untersagten, aber eine etablierte betriebliche Übung hatte für Gegenteiliges gesorgt. Also war bereits die Einsichtnahme in die Accounts rechtswidrig. Das Unternehmen sah sich jedoch nicht in der Lage, die E-Mail-Accounts zu löschen, da die Geschäftsführung bedroht gewesen wäre. Sämtliche Kundenanfragen liefen bislang über die ausgeschiedenen Mitarbeiter. Nicht mehr auf die E-Mail-Accounts zugreifen zu können, hätte zum Auftragsverlust und angesichts der schwierigen wirtschaftlichen Lage des Unternehmens zur Insolvenz geführt.

Aufgrund unseres Einschreitens konnten die permanenten Verletzungen des Rechts auf informationelle Selbstbestimmung der ausgeschiedenen Mitarbeiter schnellstmöglich abgestellt werden. Der Zugriff auf die E-Mail-Accounts war ohne die Einwilligung der ehemaligen Beschäftigten nicht erlaubt. Durch unsere weitergehende Beratung hat das Unternehmen klare Regelungen für die Nutzung aller Informations- und Kommunikationstechniken schriftlich und verbindlich getroffen und seine Mitarbeitern entsprechend informiert.

#### Praxistipp:

*Die meiste Geschäftskorrespondenz läuft heutzutage per E-Mail ab. Daher sollten Unternehmen es nicht versäumen, klare Löschkonzepte einzuführen. Nur so können die gesetzlichen Aufbewahrungspflichten, wenn die Korrespondenz als Handelsbrief einzustufen ist, eingehalten werden.*

*Ein durchgängiges Löschkonzept stellt durch organisatorische und technische Maßnahmen sicher, dass zum Ende des Verarbeitungszwecks die Löschung der Daten auch tatsächlich erfolgt.*

Ob personenbezogene Daten nach dem Ausscheiden eines Mitarbeiters noch gespeichert werden dürfen bzw. müssen, hängt in erster Linie davon ab, ob spezielle Aufbewahrungsregelungen hierzu ermächtigen oder verpflichten.<sup>46</sup>

Wie lange Dokumente oder Akten aufzubewahren sind, bevor eine Löschung vorgenommen werden kann, ist abhängig von deren Inhalt. Für Unterlagen, die für die Besteuerung des Unternehmens relevant sind, geben die steuerrechtlichen Vorschriften eine Aufbewahrungszeit von sechs bzw. zehn Jahren vor. Darunter fallen beispielsweise die Buchungsbelege im Zusammenhang mit der Gehaltszahlung. Arbeitszeitnachweise sind zwei bzw. drei Jahre aufzubewahren, damit die Einhaltung von Arbeitszeitregelungen kontrolliert werden kann.<sup>47</sup>

Beide Seiten müssen jedoch für einen gewissen Zeitraum damit rechnen, dass aus dem beendeten Arbeitsverhältnis

<sup>46</sup> Gesetzliche Aufbewahrungsfristen finden sich bspw. in § 147 Abgabenordnung oder auch § 257 Handelsgesetzbuch.

<sup>47</sup> Vgl. § 16 Abs. 2 Arbeitszeitgesetz.

noch Rechte oder Pflichten geltend gemacht werden können, die nur schwer zu belegen sein werden, wenn die entscheidenden Unterlagen einen Monat nach der Beendigung vernichtet wurden, beispielsweise die Ausbezahlung von Urlaub und Überstunden an den Arbeitnehmer oder die Herausgabe eines dienstlichen Laptops an den Arbeitgeber. Nach § 195 des Bürgerlichen Gesetzbuches (BGB) verjähren solche Ansprüche grundsätzlich nach spätestens drei Jahren. Dabei beginnt gemäß § 199 BGB die Frist erst mit dem Ende des Jahres, in dem der Anspruch entstanden ist.

### III. Das Ziel unserer Arbeit

*Wie die kleine Auswahl aus dem Bereich des Beschäftigtendatenschutzes gezeigt hat, ist die Arbeit des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg spannend und vielfältig. Auch wenn der Gesetzgeber uns vorrangig die Rolle einer Aufsichtsbehörde zugesprochen hat, richten wir unser besonderes Augenmerk auf die datenschutzrechtliche Beratung. Durch frühzeitige Einbindung unserer Behörde werden neue wirtschaftliche Entwicklungen im Betrieb nicht durch datenschutzrechtliche Anforderungen gehemmt, sondern langfristig und nachhaltig verbessert.*

*Der LfDI BW ist verpflichtet, neue Entwicklungen kritisch zu beobachten und zu begleiten. Ziel ist es nicht (nur) zu sagen, was alles nicht geht, sondern unter Berücksichtigung aller einzubeziehenden Interessen gemeinsam datenschutzkonforme Lösungen und Alternativen zu erarbeiten.*



#### Dr. Stefan Brink

Der Autor ist Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg. Er wurde vom Landtag Baden-Württemberg für die Dauer von sechs Jahren gewählt.



#### Sabrina Schwab

Die Autorin ist Referentin für Beschäftigtendatenschutz beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

## Kurzbeiträge

### Aus den aktuellen Berichten der Aufsichtsbehörden (31): Auswirkungen der DS-GVO auf Auskunfteien, Inkassounternehmen und Kreditwesen

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

#### I. Vorbemerkung

Der Hessische Datenschutzbeauftragte berichtet in seinem im Mai 2017 vorgelegten 45. Tätigkeitsbericht (2016) über die Abstimmungen zwischen den Aufsichtsbehörden und den Auskunfteien über die im Folgejahr stattfindende Anwendung der DS-GVO. Spezielle Regelungen zur Tätigkeit von Auskunfteien enthält die DS-GVO nicht. Soweit nicht das BDSG n.F. (§ 31) mit einer auf den Bereich abgestellten bereichsspezifischen Vorschrift greift, richtet sich die Tätigkeit der Auskunfteien in Zukunft nach den allgemeinen Vorschriften in Art. 6 DS-GVO.

In dem Abstimmungsverfahren wurde versucht, bestehende Rechtsunsicherheit zu beseitigen und den Auslegungsspielraum des Art. 6 DS-GVO einzuzugrenzen.

Rechtlich geprüft und aufbereitet wurden u.a. folgende Themen.

#### II. Zulässigkeit und Umfang von Bonitätsauskünften (4.2.1.1)

Nach den Aufsichtsbehörden können die in den §§ 28 ff. BDSG kodifizierten Grundsätze im Rahmen der Anwendung von Art. 6 Abs. 1 lit. b und f DS-GVO als Rechtsgrundlage für die Verarbeitung auch weiter zur Anwendung kommen.

Anfragen von verantwortlichen Stellen bei Auskunfteien zur Prüfung der Bonität im vorvertraglichen Bereich, aber

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

auch Bonitätsabfragen etwa zur Prüfung der Erfolgsaussichten von Vollstreckungsmaßnahmen können grundsätzlich im Sinne von Art. 6 Abs. 1 lit. b DS-GVO als erforderlich zur Durchführung vorvertraglicher oder vertraglicher Maßnahmen angesehen werden. Für die Erteilung einer Auskunft durch Auskunftsteil bietet Art. 6 Abs. 1 lit. f DS-GVO eine ausreichende Rechtsgrundlage. Es bleibt also bei der Interessenabwägung, die bisher gemäß §§ 28 Abs. 1 S. 1 Nr. 2 und 29 Abs. 2 BDSG durchgeführt werden musste und immer noch muss. Dies entspricht auch der Wertung von ErWG 47 DS-GVO. Wie bisher kann ein bestehendes oder drohendes kreditorisches Risiko die Rechtmäßigkeit einer Bonitätsabfrage indizieren.

Der vorherige Nachweis der Zulässigkeit einer Bonitätsabfrage gegenüber der Auskunftsteil wird als verzichtbar angesehen. Zwar enthält die DS-GVO nicht mehr die grundsätzliche Privilegierung der Bonitätsabfrage nach § 29 Abs. 2 BDSG. Die Forderung eines Einzelnachweises und dessen Speicherung bzw. Aufbewahrung sei im Massengeschäft jedoch überzogen. Sie würde berechnete und zulässige Datenübermittlungen aus rein formalen Gründen vereiteln. Vielmehr werde es auch weiterhin ausreichen, wenn das berechnete Interesse glaubhaft gemacht wird. Mangels ausdrücklicher gesetzlicher Privilegierung kann jedoch nicht mehr von einer generellen Zulässigkeit der bloßen Glaubhaftmachung ausgegangen werden. Dies gilt vielmehr nur dann, wenn aufgrund bisheriger Erfahrungen oder begründeter Erwartungen die Gewissheit besteht, dass Bonitätsabfragen nur dann durchgeführt werden, wenn diese zulässig sind. Das Maß der Gewissheit muss dabei Zweifel an der Zulässigkeit Schweigen gebieten, ohne sie völlig auszuschließen.

Dies erfordere eine ausreichende Organisationsstruktur, welche unzulässige Bonitätsabfragen verhindert oder zumindest so weit erschwert, dass verbleibenden Zweifeln an dem Unterbleiben unzulässiger Bonitätsabfragen Schweigen geboten wird. Hierfür werde in der Regel die Protokollierung der Bonitätsabfragen inkl. der Person des Abfragenden durch individualisierte und personalisierte Zugangsberechtigungen erforderlich sein. Einzelne Fehlfragen beeinträchtigen die Zulässigkeit nicht. Mehrfache unzulässige Abfragen oder eine vollständig fehlende Vorsorge gegen unzulässige Abfragen vermögen die grundsätzlich bestehende Vermutung, dass Bonitätsabfragen zulässig sind, aber zu entkräften. In solchen Fällen können Bonitätsauskünfte im Massengeschäft nicht mehr zulässig erteilt werden.

### III. Zulässigkeit und Umfang der Datenspeicherung (Ziff. 4.2.1.2)

Informationen über negative Erfahrungen mit dem Zahlungsverhalten einer betroffenen Person dürfen ebenfalls gemäß Art. 6 Abs. 1 lit. f DS-GVO an eine Auskunftsteil übermittelt und dort gespeichert werden. Aber auch hier ist eine Abwägung durchzuführen, die zugunsten der Übermittlung ausfällt, wenn die bisher in § 28a Abs. 1 BDSG kodifizierten Voraussetzungen vorliegen. Nur dann ist sicher gewährleistet, dass ein Sachverhalt vorliegt, der zuverlässig auf eine verminderte oder eingeschränkte Bonität einer betroffenen

Person schließen lässt. Mangels ausdrücklicher Kodifizierung müsse die Prüfung der Voraussetzungen des § 28a Abs. 1 BDSG jedoch nicht zu formell wörtlich, sondern nach Sinn und Zweck betrachtet werden. Sachverhalte, bei denen eindeutig kein bonitätsrelevanter Sachverhalt vorliegt, wie bspw. die Geltendmachung von behaupteten, aber in der Regel zweifelhaften Ansprüchen, rechtfertigen eine Übermittlung daher nicht. Dient die Übermittlung daher nur der Drohung oder Durchsetzung sehr zweifelhafter Ansprüche, wäre sie unzulässig.

Das berechnete Interesse an der Übermittlung der Negativinformationen besteht zum einen in dem Interesse Dritter, über negative Zahlungserfahrungen informiert zu werden, um eigenen negativen Erfahrungen vorzubeugen. Zum anderen besteht es in dem Interesse des übermittelnden Unternehmens, an einem solchen System teilnehmen zu können und ebenfalls über negative Erfahrungen Dritter informiert zu werden; Art. 6 Abs. 1 lit. 192f DS-GVO.

Die Interessen der betroffenen Personen stehen dem nicht entgegen, wenn die Tatsache der negativen Zahlungserfahrung hinreichend sicher ist und dieses Verhalten nach empirischer Erfahrung oder statistischer Auswertung ebenfalls hinreichend sicher auf eine verminderte oder eingeschränkte Bonität einer betroffenen Person und die damit verbundene erhöhte Wahrscheinlichkeit eines Ausfalls schließen lässt. Zusätzlich ist zu berücksichtigen, dass durch die Übermittlung auch betroffene Personen vor dem Eingehen zu hoher Risiken oder einer zu hohen Verschuldung geschützt werden können.

### IV. Speicherfristen (Ziff. 4.2.1.4)

Speicherfristen für Auskunftsteil sind derzeit in § 35 Abs. 2 Satz 2 Nr. 4 BDSG detailliert geregelt. Eine derart detaillierte Regelung enthält die DS-GVO nicht mehr. Art. 17 DS-GVO gibt betroffenen Personen zwar einen Anspruch auf Löschung gespeicherter personenbezogener Daten. Detaillierte Prüf- und Löschfristen sind aber nicht mehr enthalten. Stattdessen normiert die DS-GVO, dass Daten zu löschen sind, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind; Art. 17 Abs. 1 a DS-GVO. Wann dies exakt der Fall ist, lässt die DS-GVO jedoch offen.

Zur Schaffung von Rechtssicherheit haben die Aufsichtsbehörden mit den Auskunftsteil eine Beibehaltung der bisherigen Fristen besprochen. Zur Gleichbehandlung der betroffenen Personen könnten die Fristen allerdings künftig einheitlich ab der Speicherung und nicht – wie bisher – ab dem Ende des Jahres der Speicherung berechnet. Dies wird die Fristen voraussichtlich etwas verkürzen.

Es ist beabsichtigt, dieses Ergebnis im Wege der Selbstverpflichtung umzusetzen.

### V. Umfang von Selbstauskünften (Ziff. 4.2.1.5)

Der Umfang von Selbstauskünften ergibt sich künftig vor allem aus Art. 15 DS-GVO. Auch hier enthält die DS-GVO

nicht mehr die detaillierten Regelungen für Auskunftsteien gemäß § 34 BDSG.

Betroffenen Personen ist jedoch gemäß Art. 15 Abs. 3 DS-GVO eine vollständige Kopie der gespeicherten Daten zur Verfügung zu stellen. Dies umfasst die bisher erteilten Auskünfte jedenfalls dann, wenn diese gespeichert sind.

Durch die umfangreichen Abstimmungsverfahren und die damit verbundene Erzielung von Ergebnissen besteht im Tätigkeitsbereich der Auskunftsteien ab der Geltung des DS-GVO eine deutlich verbesserte Rechtssicherheit für betroffene Personen und die Wirtschaft.

Erforderlich ist nach wie vor die Identifikation der betroffenen Person.

Nur wenn mittels der übermittelten Daten eine eindeutige und zweifelsfreie Identifizierung des Auskunftersuchenden/der betroffenen Person nicht möglich ist (beispielsweise bei abweichenden Adressdaten), kann eine Fotokopie des Ausweisdokuments bzw. der Einwohnermeldeamtsbestätigung angefordert werden. Letzteres ist im Hinblick auf die Wohnanschrift bei einem ausländischen Pass, dem keine Anschriftendaten zu entnehmen ist, der Fall.

Verweigert werden muss auch der Versand der Auskunft an eine innerdeutsche Postfachadresse (Ziff. 4.2.2.1.2), da es nicht möglich ist die seitens des Auskunftersuchenden angegebene Postfachadresse als diejenige der betroffenen Person zweifelsfrei zu verifizieren. Zu unsicher ist auch der Versand an eine Anschrift „wohnhaft bei“ (Ziff. 4. 2.2.1.3). Der Versand einer Selbstauskunft an eine nicht verifizierte Adresse mit dem Zusatz „wohnhaft bei“ sei datenschutz-

rechtlich zu beurteilen wie der Versand an einen Dritten zur Weiterleitung an die betroffene Person. Ein derartiger Versand würde den Missbrauch der Selbstauskunft begünstigen. Gleiches gilt für eine private c/o-Anschrift (Ziff. 2.2.2.1.4).

## VI. Kredit- und Finanzwirtschaft

Ein gleicher Abstimmungsprozess fand zur Vorbereitung auf das Wirksamwerden der Datenschutz-Grundverordnung im Bereich der Kreditwirtschaft statt (Ziff. 4.3.1). Dazu wurden einige als vordringlich bewertete Themen rechtlich geprüft und aufbereitet.

Dabei wurde Konsens erzielt, dass die bisher zulässigen Datenverarbeitungsprozesse der Kreditwirtschaft auch nach der DS-GVO weitgehend zulässig sein werden. Dies gilt insb. für die Verarbeitung von Daten aufgrund von bankaufsichtsrechtlichen oder anderen regulatorischen Vorschriften sowohl auf nationaler als auch auf europäischer Ebene. Der bisher zulässige Datenaustausch mit Auskunftsteien könne zukünftig auf Art. 6 Abs. 1 lit. b und f DS-GVO gestützt werden.

Einwilligungen zur Datenverarbeitung sind jedoch an den Anforderungen der DS-GVO zu messen. Obligatorische Einwilligungen werden daher voraussichtlich nicht mehr zulässig sein. In der Regel kann die Datenverarbeitung und Datenübermittlung aber zukünftig auf die gesetzliche Grundlage des Art. 6 Abs. 1 DS-GVO gestützt werden. Dies gilt auch für den Verarbeitungsschritt des Profilings, der in der Regel aufgrund der Pflicht von Kreditinstituten zur Bonitätsprüfung aufgrund bankaufsichtsrechtlicher Vorschriften zulässig sein wird.

# Datenportabilität – das neue Recht des Betroffenen

Kristin Benedikt, Ansbach\*

Die DS-GVO enthält eine Reihe neuer Instrumente und erweitert den Katalog an Betroffenenrechten. Darunter fällt auch das Recht auf Datenübertragbarkeit. Die Umsetzung dieses Novums stellt die Verantwortlichen vor eine große Herausforderung. Anders als bei dem Recht auf Löschung oder Berichtigung kommt es vor allem auf die technische Ausgestaltung an.

Der Betroffene kann gem. Art. 20 DS-GVO vom Verantwortlichen verlangen, dass ihm seine Daten bereitgestellt (Abs. 1) oder direkt an einen anderen Verantwortlichen übermitteln werden (Abs. 2). Zweck dieser Vorschrift ist es, die Bindung an einen bestimmten Anbieter (sog. „Lock-In-Effekt“) zu verhindern, indem ein Anbieterwechsel erleichtert wird.<sup>1</sup> Es handelt sich daher in erster Linie um eine verbraucher- bzw. wettbewerbsrechtliche Vorschrift.<sup>2</sup> Dennoch entfaltet die Vorschrift auch datenschutzrechtliche Verpflichtungen gegenüber den Verantwortlichen, die insbesondere Fragen

der Datensicherheit und der Datenschutz-Organisation betreffen.

## I. Voraussetzungen

Im Gesetzgebungsverfahren wurde das Recht auf Datenübertragbarkeit zunächst nur im Hinblick auf soziale Netzwerke thematisiert.<sup>3</sup> In der Praxis kommt die Datenportabilität jedoch bei einer Vielzahl von Datenverarbeitungen wie z.B. beim Kontowechsel oder beim Kauf eines Wearables in Betracht. Umso wichtiger ist es, dass sich die Verantwortlichen mit den Voraussetzungen und Folgen für die Praxis vertraut machen.

\* Die Autorin ist Referatsleiterin für den Bereich Telemedien und Geodatendienste beim Bayerischen Landesamt für Datenschutzaufsicht. Der Beitrag gibt die persönliche Auffassung der Autorin wieder.

1 Herbst, in: Kühling/Buchner, DS-GVO, Art. 20 Rn. 1.

2 Kamann/Braun in: Ehmann/Selmayr, DS-GVO, Art. 20 Rn. 3.

3 Europäische Kommission (COM(2012) 11 final).

## 1. Grundlage der Datenverarbeitung

Das Recht auf Datenübertragbarkeit besteht nur, wenn die Daten aufgrund einer Einwilligung oder eines Vertrages verarbeitet werden. Dies schränkt die Menge an übertragbaren Daten erheblich ein. Das Verzeichnis über Verarbeitungstätigkeiten gem. Art. 30 DS-GVO kann dabei helfen, die Datenmenge einzugrenzen.

Die weitere Voraussetzung, dass die Daten mithilfe automatisierter Verfahren verarbeitet werden, hat bei der Vielzahl an Anwendungsfällen im digitalen Zeitalter keine eigenständige Bedeutung.

## 2. Vom Betroffenen bereitgestellt

Gegenstand des Art. 20 DS-GVO sind nur solche Daten, die vom Betroffenen bereitgestellt worden sind. Bereitgestellt sind die Daten, wenn der Betroffene sie bewusst offenlegt, indem er sie dem Verantwortlichen übermittelt oder durch sonstige Weise aktiv und willentlich verbreitet hat.<sup>4</sup> Dies ist z.B. der Fall, wenn der Betroffene sein Profil bei einem Dating-Portal erstellt oder beim Bestellvorgang seine Anschrift eingibt.

Darunter fallen auch solche Daten, die vom Betroffenen durch die Inanspruchnahme und Nutzung eines Dienstes erzeugt werden. Das betrifft Daten, die nach derzeitigen Verständnis unter § 15 Abs. 1 TMG gefasst werden können, wie z.B. Fitness- und Gesundheitsdaten bei Wearables, Playlists bei Streaming-Plattformen oder Bewegungsprofile.

Im Gegensatz dazu sind Daten, die erst durch die Verarbeitung erzeugt werden und auf Rückschlüssen des Verantwortlichen beruhen, nicht von Art. 20 DS-GVO erfasst. Das gilt u.a. für das Scoring oder das Profiling, soweit dem Betroffenen Merkmale und Interessen zugeordnet werden.

## 3. Daten Dritter

Art. 20 DS-GVO setzt weiterhin voraus, dass die zu übertragenden Daten den Antragsteller selbst betreffen. In der Praxis kommt es häufig vor, dass sich die Daten auch auf andere Personen beziehen z.B. Gruppenfotos oder Chat-Verläufe. In diesen Fällen ist der Anspruch auf Datenübertragbarkeit nicht vorschnell abzulehnen, da anderenfalls das Betroffenenrecht ins Leere liefe.<sup>5</sup>

Der Anspruch auf Datenübertragung ist nur dann ausgeschlossen, wenn dadurch die Rechte und Freiheiten anderer Personen beeinträchtigt werden, Art. 20 Abs. 4 DS-GVO. Eine solche Beeinträchtigung kommt sowohl bei den Grundrechten gem. Art. 7 und 8 GRCh, als auch beim Recht am geistigen Eigentum oder bei Geschäftsgeheimnissen in Betracht, vgl. ErwG 63.

## II. Praktische Umsetzung und technische Ausgestaltung

Nach Art. 20 Abs. 1 DS-GVO müssen die Daten in einem „strukturierten, gängigen und maschinenlesbaren Format“ bereitgestellt werden. Zudem werden die Verantwortlichen in

ErwG 68 aufgefordert, „interoperable“ Formate zu entwickeln. Verantwortliche müssen aber nicht erst abwarten, bis es Standards für die Datenübertragung gibt, um ihrer Pflicht gem. Art. 20 DS-GVO nachzukommen. Häufig verwendete Formate wie XML, CSV oder HTML erfüllen diese Voraussetzungen.<sup>6</sup>

Die Verantwortlichen sollten unter dem Gesichtspunkt „Privacy by Design“ die Möglichkeit zur Datenübertragung frühestmöglich im Prozess einbinden. Das bedeutet, dass mit der Umsetzung nicht erst begonnen werden darf, wenn erstmals die Datenübertragung gefordert wird. Eine nachträgliche Umsetzung verursacht nicht nur höhere Kosten, sondern kann auch dazu führen, dass dem Antrag nicht fristgerecht entsprochen werden kann. Dies kann einen Verstoß gegen die bußgeldbewährten Vorschriften Art. 12 und Art. 25 DS-GVO zur Folge haben.

Neben den Voraussetzungen des Art. 20 DS-GVO müssen auch die allgemeinen Vorschriften der Betroffenenrechte beachtet werden. So hat der Verantwortliche die Daten unentgeltlich und unverzüglich, spätestens jedoch innerhalb eines Monats bereitzustellen, vgl. Art. 12 Abs. 3 Satz 1 und Abs. 5 Satz 1 DS-GVO.

Außerdem ist der Verantwortliche angehalten, bei Zweifeln die Identität des Antragstellers zu überprüfen, Art. 12 Abs. 6 DS-GVO. Da Art. 20 DS-GVO überwiegend im Online-Bereich zur Anwendung kommt und der Verantwortliche dadurch schnell über die Identität des Antragstellers getäuscht werden kann, sollte in jedem Fall eine Identitätsfeststellung erfolgen. Erfolgt dies nicht, erhöht sich das Risiko für einen Identitätsdiebstahl. In der Praxis empfiehlt es sich daher, dem Betroffenen die Daten im Online-Konto nach dem Log-In mit Benutzername und Passwort bereitzustellen.

Ein vergleichbares Risiko besteht auch bei direkter Übertragung an einen anderen Verantwortlichen, Art. 20 Abs. 2 DS-GVO. Hier muss sichergestellt werden, dass die Daten nicht nur an den „richtigen“ Empfänger gelangen, sondern zumindest auch über den Transportweg verschlüsselt sind.

## III. Verhältnis zu weiteren Betroffenenrechten

Das Recht auf Datenübertragung ersetzt oder schließt andere Betroffenenrechte nicht aus. Aus Art. 20 Abs. 3 S. 1 DS-GVO geht ausdrücklich hervor, dass das Recht auf Löschung unberührt bleibt. Das Recht auf Datenübertragbarkeit ist auch nicht mit dem Recht auf Auskunft identisch. Das Auskunftsrecht soll den Betroffenen darüber informieren, welche Daten von wem verarbeitet werden. Erst dadurch wird er in die Lage versetzt, weitere Rechte auszuüben. Art. 20 DS-GVO gewährleistet durch kontrollierte Weitergabe des Betroffenen, dass die Verbreitung durch einen weiteren Verantwortlichen fortgesetzt wird.<sup>7</sup>

4 Piltz, K&K 2016, 629, 634.

5 Artikel 29-Arbeitsgruppe WP 242, S. 9.

6 Franck, RDV 2016, 111, 117.

7 Kamann/Braun, in: Ehmann/Selmayr, DS-GVO, Art. 20 Rn. 8.

# Die DSGVO als Herausforderung (auch) für die Aufsichtsbehörden

Barbara Thiel, Hannover\*

In Fragen des Datenschutzes im Bereich der Wirtschaft werden die Aufsichtsbehörden heute vor allem konfrontiert:

- mit einer stetig steigenden Relevanz und Bedeutung der Datenverarbeitung,
- mit rasant fortschreitenden technischen Möglichkeiten der Datenauswertung,
- mit einer um sich greifenden digitalen Vernetzung von Alltagsgegenständen.

Mehr denn je stellt sich deshalb die Frage, wie der Datenschutz auch in Zeiten der Digitalisierung seine Berechtigung wahren und weiter ausbauen kann.

Hier weist uns das neue europäische Recht den Weg. Im digitalen Zeitalter kann Datenschutz nicht mit nationalen Insellösungen durchgesetzt werden. Mit der EU-Datenschutz-Grundverordnung (DSGVO) wird vielmehr ab Mai 2018 ein (weitestgehend) einheitlicher europäischer Rechtsrahmen für den Datenschutz in der digitalen Welt gesetzt. Das schafft gleiche Wettbewerbsbedingungen, mehr Rechtssicherheit und leichtere Rechtsdurchsetzbarkeit.

Die Reform des europäischen Datenschutzrechts wird zugleich einen konsequenten Ausbau effektiver Aufsichtsstrukturen weiter befördern. Nur so kann es gelingen, den europäischen Datenschutz in der digitalen Welt nicht nur auf dem Papier zu modernisieren und zu harmonisieren, sondern im Interesse der betroffenen Bürgerinnen und Bürger schlagkräftig auszugestalten.

## I. Weitreichende Sanktionsbefugnisse

Die Tätigkeit der Aufsichtsbehörden wird entscheidend dafür sein, inwieweit die DSGVO ihr Ziel eines wirksamen Datenschutzes erreichen kann. Eine wichtige Neuerung sind dabei die sehr weit reichenden Sanktionsbefugnisse, die künftig von jeder Aufsichtsbehörde in der EU ausgeübt werden können.

Aus Sicht des Europäischen Parlaments war es ein ganz zentrales Ziel der europäischen Datenschutzreform, Sanktionen einzuführen, die „weh tun sollen“, wie es in einer Stellungnahme des Ausschusses für Bürgerrechte, Justiz und innere Angelegenheiten ausdrücklich heißt. Diese Zielsetzung des Europäischen Parlaments ist Wirklichkeit geworden: Zukünftig können bei rechtswidrigen Datenverarbeitungen Geldbußen in Höhe von bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4% des gesamten weltweit erzielten Jahresumsatzes verhängt werden (Art. 83 Abs. 5) – ein Quantensprung gegenüber der jetzigen Rechtslage. Die Einhaltung der gesetzlichen Bestimmungen ist nun lohnender als ein Verstoß.

Eine besondere Herausforderung für die Aufsichtsbehörden bedeutet es allerdings, dass die Bußgeldtatbestände sehr unbestimmt sind. Es ist davon auszugehen, dass hier erst nach einer längeren Anwendungspraxis eine gewisse Klarheit für die Unternehmen bestehen wird. Abzuwarten bleibt auch, in welcher Weise der Europäische Datenschutzausschuss seinen Auftrag aus Art. 70 Abs. 1 lit. k umsetzen wird. Danach obliegt ihm die Aufgabe, Leitlinien für die Aufsichtsbehörden in Bezug auf die Festsetzung von Geldbußen zu erlassen.

## II. Beratungs- und Unterstützungsaufgaben

Schon heute nehmen die Aufsichtsbehörden neben ihren Kontrollfunktionen auch Beratungs- und Unterstützungsaufgaben wahr. Mit der Geltung der DSGVO wird die Beratungstätigkeit der Aufsichtsbehörden aber nicht nur deutlich zunehmen, sondern auch eine neue Qualität erlangen. So kommen auf die Aufsichtsbehörden insbesondere umfangreiche Sensibilisierungs- und Aufklärungspflichten zu. Diese proaktive Aufgabe der Sensibilisierung und Aufklärung besteht sowohl gegenüber den Betroffenen, die zukünftig auf Anfrage stärker über ihre Rechte informiert werden sollen (Art. 57 Abs. 1 lit. e), als auch gegenüber der Öffentlichkeit, die etwa über Risiken der Datenverarbeitung informiert werden soll (Art. 57 Abs. 1 lit. b).

Auch die datenverarbeitenden Stellen sollen künftig hinsichtlich ihrer Pflichten aufgeklärt und sensibilisiert werden (Art. 57 Abs. 1 lit. d). Neu ist ferner, dass die Aufsichtsbehörden künftig die Unternehmen bei der neu eingeführten Datenschutzfolgenabschätzung zu unterstützen haben. Diese Datenschutzfolgenabschätzungen sollen Technikanbietern, Aufsichtsbehörden und der Öffentlichkeit helfen, die vorwiegend durch datenverarbeitende Technologien entstehenden Risiken für den Datenschutz wirksam einzuschätzen und diese von vornherein so gering wie möglich zu halten. Noch offen ist allerdings, wie und nach welchen Kriterien die Folgenabschätzung erfolgen soll und welchen Inhalt künftige Leitlinien des Europäischen Datenschutzausschusses insoweit haben werden.

Last but not least ist eine Beratung auch bei der Zertifizierung von Datenverarbeitungsvorgängen notwendig. Art. 57 Abs. 1 n DSGVO benennt als Pflichtaufgabe der Aufsichtsbehörden, „die Einführung von Datenschutzzertifizierungsmechanismen und -prüfzeichen anzuregen“. Zertifizierungen für bestimmte Verfahren und Produkte, die gewissenhaft anhand festgelegter Kriterien geprüft worden sind, können mehr

\* Die Autorin ist Landesbeauftragte für den Datenschutz in Niedersachsen und im Jahr 2017 Vorsitzende der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK).

Rechtssicherheit bringen und bei den Nutzern dazu führen, dass Datenschutz in den Unternehmen tatsächlich gelebt wird. Wie die Zertifizierung bzw. die Akkreditierung von Zertifizierungsstellen aussehen wird, ist noch offen. Erklärtes Ziel der deutschen Aufsichtsbehörden ist jedenfalls die Entwicklung länderübergreifender Akkreditierungs- und Zertifizierungsverfahren mit einheitlicher Bewertung.

### III. Kohärenzverfahren

Eine große Herausforderung dürfte für die Aufsichtsbehörden und ihre Arbeitsweise das Kohärenzverfahren darstellen. Bei Datenverarbeitungen, die nicht nur einen Mitgliedstaat betreffen, wird in Zukunft eine enge Zusammenarbeit aller betroffenen Aufsichtsbehörden erforderlich sein. Daraus resultiert ein Abstimmungsverfahren unter den Behörden, das ohne Zweifel ein sehr komplexes Gebilde sein wird. Durchgesetzt hat sich in diesem Zusammenhang, dass die Aufsichtsbehörden sich im Streitfall auch per Mehrheitsentscheid zu einer gemeinsamen Linie verbindlich verpflichten können. Bei streitigen Fragen entscheidet letztlich der neu eingesetzte Europäische Datenschutzausschuss, der die bisherige – nicht verbindliche – Arbeit der Art. 29 Arbeitsgruppe ablösen wird, verbindlich und endgültig. Die Zuständigkeit für Datenverarbeitungen endet damit künftig nicht mehr an der Staatsgrenze.

### IV. Fazit

Der Auftrag der Aufsichtsbehörden ist umfassend. Sie haben die Anwendung der DSGVO zu überwachen und durchzusetzen. Dazu haben sie weitgehende Informationspflichten gegenüber Betroffenen, Verantwortlichen und der Öffentlichkeit. „Vollzug und Beratung“ ergänzen einander, sie sind sozusagen zwei Seiten einer Medaille. Ziel ist es, digitale Wirtschaft und globalen Datenschutz angemessen in Einklang zu bringen. Vielfältige Möglichkeiten und Angebote erfordern differenzierte Lösungen. Die Schwierigkeit in der praktischen Umsetzung wird darin bestehen, auszuloten, wie weit Beratung tatsächlich gehen kann. Keineswegs kann sie die Verantwortlichkeit der Unternehmen ersetzen, die die Voraussetzungen für einen angemessenen Datenschutz im Wettbewerb sicherzustellen und weiter auszubauen haben. Der konstruktive Dialog zwischen Wirtschaft und Aufsichtsbehörden kann hierzu einen wichtigen Beitrag leisten.

Eine besondere Herausforderung der DSGVO besteht künftig darin, dass Entscheidungen innerhalb kurzer Fristen gemeinsam getroffen werden müssen. Dabei ist auch auf nationaler Ebene eine neue Form der Entscheidungsfindung notwendig. Nur durch eine effiziente und agile Zusammenarbeit wird es zukünftig möglich sein, eine starke und zeitgemäße Position innerhalb Europas zu vertreten.

## Rechtsprechung

### Zur zusätzlichen Identifizierung durch Kopie des Reisepasses bei Nicht-EU-Bürgern (Ls)

(Europäischer Gerichtshof, Urteil vom 6. April 2017 – C 668/15 – JyskeFinans)

**Art. 2 Abs. 2 Buchst. a und b der Richtlinie 2000/43/EG des Rates vom 29. Juni 2000 zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft ist dahin auszulegen, dass er einer Praxis eines Kreditinstituts nicht entgegensteht, wonach einem Kunden, in dessen Führerschein ein anderes Geburtsland als ein Mitgliedstaat der Europäischen Union oder der Europäischen Freihandelsassoziation angegeben ist, das Erfordernis einer zusätzlichen Identifizierung durch Vorlage einer Kopie seines Reisepasses oder seiner Aufenthaltserlaubnis auferlegt wird.**

### Bereitstellung von Teilnehmerdaten an öffentlich zugängliche Auskunftsdienste und Teilnehmerverzeichnisse in der EU und Einwilligung des Teilnehmers

(Europäischer Gerichtshof, Urteil vom 15. März 2017 – C-536/15 – Tele 2 /ZiggoBV/Vodafone Libertel BV)

**1. Art. 25 Abs. 2 der Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist dahin auszulegen, dass unter dem darin enthaltenen**

**Begriff „Anträge“ auch der Antrag eines Unternehmens zu verstehen ist, das in einem anderen Mitgliedstaat ansässig ist als die Unternehmen, die Teilnehmern Telefonnummern zuweisen, und das zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen in diesem Mitgliedstaat und/oder in anderen Mitgliedstaaten von diesen Unternehmen die ihnen vorliegenden relevanten Informationen anfordert.**

**2. Art. 25 Abs. 2 der Richtlinie 2002/22 in der durch die Richtlinie 2009/136 geänderten Fassung ist dahin auszulegen, dass er ein Unternehmen, das Teilnehmern Telefonnummern zuweist und nach nationalem Recht verpflichtet ist, die Einwilligung dieser Teilnehmer in die Nutzung der sie betreffenden Daten zum Zweck der Bereitstellung von Auskunftsdiensten und Teilnehmerverzeichnissen einzuholen, daran hindert, dieses Ersuchen so zu formulieren, dass die Teilnehmer bei ihrer Einwilligung in die Nutzung danach differenzieren, in welchem Mitgliedstaat die Unternehmen, die für eine Anforderung der in Art. 25 Abs. 2 genannten Informationen in Betracht kommen, ihre Dienste anbieten.**

#### Sachverhalt:

1. Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 25 Abs. 2 der Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie) (ABL. 2002, L 108, S. 51) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABL. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Universaldienstrichtlinie).

2. Es ergeht in einem Rechtsstreit, den die in den Niederlanden ansässigen Gesellschaften Tele2 (Netherlands) BV, Ziggo BV und Vodafone Libertel BV gegen die Autoriteit Consument en Markt (ACM) (Behörde für Verbraucher- und Marktangelegenheiten) wegen eines Beschlusses führen, den diese Behörde im Rahmen eines Rechtsstreits zwischen den genannten Gesellschaften und der European Directory Assistance NV (im Folgenden: EDA), einer in einem anderen Mitgliedstaat ansässigen Gesellschaft, erlassen hat, der die Frage betrifft, ob diese Gesellschaften die Daten ihrer Teilnehmer EDA zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen im letztgenannten Mitgliedstaat und/oder in anderen Mitgliedstaaten zur Verfügung stellen müssen.

#### Ausgangsverfahren und Vorlagefragen

14. EDA ist eine Gesellschaft belgischen Rechts, die vom belgischen Hoheitsgebiet aus Auskunftsdienste und Teilnehmerverzeichnisse anbietet. Sie beantragte bei den Unternehmen, die Teilnehmern in den Niederlanden Tele-

fonnummern zuweisen (im Folgenden: niederländische Unternehmen), ihr ihre Teilnehmerdaten zur Verfügung zu stellen. Da diese Unternehmen sich weigerten, die angefragten Daten bereitzustellen, stellte EDA am 18. Januar 2012 bei der ACM einen Antrag auf Streitbeilegung.

15. Mit Beschlüssen vom 5. Juni 2013 entschied die ACM als nationale Regulierungsbehörde über den Antrag von EDA und traf folgende Maßnahmen. Erstens könne sich EDA auf Art. 3.1 des Bude berufen, soweit sie die ihr zur Verfügung gestellten Nummern und damit zusammenhängenden Informationen dafür verwende, einen Standard-Teilnehmerauskunftsdienst anzubieten. Zweitens müssten die niederländischen Unternehmen EDA die ihnen vorliegenden Basisdaten ihrer Teilnehmer (Namen, Anschriften, Telefonnummern) zu gerechten, objektiven, kostenorientierten und nicht diskriminierenden Bedingungen zur Verfügung stellen. Drittens müssten die niederländischen Unternehmen innerhalb einer angemessenen Frist sicherstellen, dass die von ihnen bei Vertragsschluss eingeholte Einwilligung ihrer Teilnehmer in die Aufnahme personenbezogener Daten in Standard-Teilnehmerverzeichnisse und in die für einen Standard-Teilnehmerauskunftsdienst verwendeten Teilnehmerdateien mit Art. 3.2 des Bude im Einklang stehe.

16. Gegen diese Beschlüsse der ACM erhoben die niederländischen Unternehmen Klage beim College van Beroep voor het bedrijfsleven (Berufungsgericht für Wirtschaftssachen, Niederlande).

17. Das vorlegende Gericht weist erstens darauf hin, dass durch Art. 3.1 des Bude Art. 25 Abs. 2 der Universalienrichtlinie in niederländisches Recht umgesetzt worden sei, so dass zur Beantwortung der im Ausgangsverfahren strittigen Frage, ob die niederländischen Unternehmen nach Art. 3.1 verpflichtet seien, EDA ihre Teilnehmerdaten zu überlassen, obwohl diese nicht in den Niederlanden ansässig sei, die Tragweite von Art. 25 Abs. 2 der Universalienrichtlinie geklärt werden müsse.

18. Die Auslegung dieser Vorschrift durch den Gerichtshof im Urteil vom 5. Mai 2011, Deutsche Telekom (C-543/09, EU:C:2011:279), betreffe nicht die grenzüberschreitende Überlassung von Teilnehmerdaten und beantworte somit nicht die Frage, ob sie dahin auszulegen sei, dass sie ein Unternehmen dazu verpflichte, seine Teilnehmerdaten einem Anbieter von Auskunftsdiensten und Teilnehmerverzeichnissen aus einem anderen Mitgliedstaat zu überlassen.

19. Zweitens stellt das vorlegende Gericht in Bezug auf die Einholung der Einwilligung der Teilnehmer fest, dass nach Art. 3.2 des Bude der Anbieter verpflichtet sei, die Einwilligung in die Aufnahme der personenbezogenen Daten und der von ihm vergebenen Telefonnummern in Standard-Teilnehmerverzeichnisse und in die für einen Standard-Teilnehmerauskunftsdienst verwendeten Kundendateien einzuholen. Aus der Begründung zu Art. 3.2 des Bude gehe hervor, dass mit ihm „verhindert werden [soll], dass jeder Anbieter allgemein zugänglicher Teilnehmerverzeichnisse und Teilnehmerauskunftsdienste jeden Teilnehmer gesondert um Einwilligung in eine Standardaufnahme ersuchen muss“.

20. Die Parteien des Ausgangsverfahrens stritten zum einen darüber, ob Art. 3.2 des Bude es gestatte, die Einwilligung der Teilnehmer in die Nutzung ihrer personenbezogenen Daten gesondert einzuholen, je nachdem, ob diese Daten für niederländische oder für ausländische Anbieter von Teilnehmerauskunftsdiensten oder Teilnehmerverzeichnissen bestimmt seien, und zum anderen darüber, ob es den Teilnehmern freigestellt werden müsse, ihre Einwilligung davon abhängig zu machen, in welchem Land das Unternehmen, das die Daten anfordere, seine Dienste anbiete. In diesem Zusammenhang stelle sich im Wesentlichen die Frage, wie die Beachtung des Diskriminierungsverbots und der Schutz des Privatlebens im Rahmen des Ersuchens um Einwilligung gegeneinander abzuwägen seien.

21. Unter diesen Umständen hat das College van Beroep voor het bedrijfsleven (Berufungsgericht für Wirtschaftssachen) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Ist Art. 25 Abs. 2 der Universaldienstrichtlinie dahin auszulegen, dass unter Anträgen auch der Antrag eines Unternehmens mit Sitz in einem anderen Mitgliedstaat zu verstehen ist, das zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen, die in diesem Mitgliedstaat und/oder in anderen Mitgliedstaaten angeboten werden, um Informationen er sucht?

2. Falls Frage 1 bejaht wird: Darf ein Anbieter, der Telefonnummern vergibt und aufgrund einer nationalen Regelung verpflichtet ist, den Teilnehmer um Einwilligung in die Nutzung seiner Daten in Standard-Teilnehmerverzeichnissen und Standard-Teilnehmerauskunftsdiensten zu ersuchen, aufgrund des Diskriminierungsverbots bei Ersuchen um Einwilligung danach differenzieren, in welchem Mitgliedstaat das Unternehmen, das um Informationen im Sinne von Art. 25 Abs. 2 der Universaldienstrichtlinie ersucht, das Teilnehmerverzeichnis und den Teilnehmerauskunftsdienst anbietet?

## Zu den Vorlagefragen

### Zur ersten Frage

22. Mit seiner ersten Frage möchte das vorlegende Gericht wissen, ob Art. 25 Abs. 2 der Universaldienstrichtlinie dahin auszulegen ist, dass unter dem darin enthaltenen Begriff „Anträge“ auch der Antrag eines Unternehmens zu verstehen ist, das in einem anderen Mitgliedstaat ansässig ist als die Unternehmen, die Teilnehmern Telefonnummern zuweisen, und das zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen in diesem Mitgliedstaat und/oder in anderen Mitgliedstaaten von diesen Unternehmen die ihnen vorliegenden relevanten Informationen anfordert.

23. Art. 25 der Universaldienstrichtlinie gehört zu ihrem die Interessen und Rechte der Endnutzer betreffenden Kapitel IV. Nach Art. 25 Abs. 1 stellen die Mitgliedstaaten sicher, dass Teilnehmer von öffentlich zugänglichen Telefon-

diensten das Recht auf einen Eintrag in das öffentlich verfügbare Verzeichnis gemäß Art. 5 Abs. 1 Buchst. a der Richtlinie und darauf haben, dass ihre Daten den Anbietern von Teilnehmerauskunftsdiensten und/oder Teilnehmerverzeichnissen gemäß den Bestimmungen von Art. 25 Abs. 2 der Richtlinie zur Verfügung gestellt werden.

24. Hinsichtlich der Zurverfügungstellung von Teilnehmerdaten für die Anbieter von Auskunftsdiensten und/oder Teilnehmerverzeichnissen ergibt sich schon aus dem Wortlaut von Art. 25 Abs. 2 der Universaldienstrichtlinie, dass diese Bestimmung alle zumutbaren Anträge erfasst, die zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen gestellt werden. Außerdem sind die Informationen nach dieser Bestimmung zu nicht diskriminierenden Bedingungen zur Verfügung zu stellen.

25. Im Wortlaut dieser Bestimmung wird also nicht danach unterschieden, ob der Antrag, Teilnehmerdaten zur Verfügung zu stellen, von einem Unternehmen gestellt wird, das im selben Mitgliedstaat ansässig ist wie das Unternehmen, an das sich der Antrag richtet, oder von einem Unternehmen, das in einem anderen Mitgliedstaat ansässig ist als das Unternehmen, an das sich der Antrag richtet.

26. Das Fehlen einer solchen Unterscheidung steht im Einklang mit dem Ziel der Universaldienstrichtlinie, das nach ihrem Art. 1 Abs. 1 u. a. darin besteht, die Verfügbarkeit unionsweiter hochwertiger, öffentlich zugänglicher Dienste durch wirksamen Wettbewerb und Angebotsvielfalt zu gewährleisten und die Fälle zu regeln, in denen die Bedürfnisse der Endnutzer durch den Markt nicht ausreichend befriedigt werden können, sowie mit dem speziellen Ziel von Art. 25 Abs. 2 der Richtlinie, das insbesondere darin besteht, die Einhaltung der in Art. 5 Abs. 1 der Richtlinie vorgesehenen Universaldienstverpflichtung zu gewährleisten (vgl. in diesem Sinne Urteil vom 5. Mai 2011, Deutsche Telekom, C-543/09, EU:C:2011:279, Rn. 35).

27. Hierzu hat der Gerichtshof bereits in Rn. 36 des Urteils vom 5. Mai 2011, Deutsche Telekom (C-543/09, EU:C:2011:279), unter Bezugnahme auf den 35. Erwägungsgrund der Universaldienstrichtlinie festgestellt, dass auf einem wettbewerbsorientierten Markt die Verpflichtung der Unternehmen, die Telefonnummern zuweisen, zur Weitergabe der Daten ihrer eigenen Teilnehmer gemäß Art. 25 Abs. 2 der Richtlinie es grundsätzlich nicht nur dem für die Gewährleistung der Einhaltung der in Art. 5 Abs. 1 der Richtlinie vorgesehenen Universaldienstverpflichtung benannten Unternehmen, sondern auch jedem Telefondienstanbieter ermöglicht, eine umfassende Datenbank zu erstellen und auf dem Markt der Auskunftsdienste und der Teilnehmerverzeichnisse tätig zu werden. Hierfür muss der betreffende Anbieter nur von jedem Unternehmen, das Telefonnummern zuweist, die relevanten Daten seiner Teilnehmer anfordern.

28. Eine Auslegung von Art. 25 Abs. 2 der Universaldienstrichtlinie, wonach er nur zumutbare Anträge von Unternehmen aus demselben Mitgliedstaat wie die Unterneh-

men, die Teilnehmern Telefonnummern zuweisen, erfasst, würde dem Ziel zuwiderlaufen, die Verfügbarkeit unionsweiter hochwertiger Dienste für die Endverbraucher durch wirksamen Wettbewerb zu gewährleisten, und insbesondere dem Ziel, die in Art. 5 Abs. 1 der Universaldienstrichtlinie vorgesehene Universaldienstverpflichtung einzuhalten, die u. a. darin besteht, dass den Endnutzern mindestens ein umfassendes Teilnehmerverzeichnis zur Verfügung steht.

29. Wie bereits in Rn. 24 des vorliegenden Urteils ausgeführt, verlangt Art. 25 Abs. 2 der Universaldienstrichtlinie zudem, dass Unternehmen, die Teilnehmern Telefonnummern zuweisen, allen zumutbaren Anträgen entsprechen, die relevanten Informationen zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen zu nicht diskriminierenden Bedingungen zur Verfügung zu stellen. Es wäre mit diesem Erfordernis unvereinbar, wenn sich Unternehmen, die Teilnehmern in den Niederlanden Telefonnummern zuweisen, nur deshalb weigern würden, die Daten ihrer Teilnehmer den Antragstellern zur Verfügung zu stellen, weil diese in einem anderen Mitgliedstaat ansässig sind.

30. Nach alledem ist auf die erste Frage zu antworten, dass Art. 25 Abs. 2 der Universaldienstrichtlinie dahin auszulegen ist, dass unter dem darin enthaltenen Begriff „Anträge“ auch der Antrag eines Unternehmens zu verstehen ist, das in einem anderen Mitgliedstaat ansässig ist als die Unternehmen, die Teilnehmern Telefonnummern zuweisen, und das zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen in diesem Mitgliedstaat und/oder in anderen Mitgliedstaaten von diesen Unternehmen die ihnen vorliegenden relevanten Informationen anfordert.

### Zur zweiten Frage

31. Mit seiner zweiten Frage möchte das vorlegende Gericht wissen, ob Art. 25 Abs. 2 der Universaldienstrichtlinie dahin auszulegen ist, dass er ein Unternehmen, das Teilnehmern Telefonnummern zuweist und nach nationalem Recht verpflichtet ist, die Einwilligung dieser Teilnehmer in die Nutzung der sie betreffenden Daten zum Zweck der Bereitstellung von Auskunftsdiensten und Teilnehmerverzeichnissen einzuholen, daran hindert, dieses Ersuchen so zu formulieren, dass die Teilnehmer bei ihrer Einwilligung in die Nutzung danach differenzieren, in welchem Mitgliedstaat die Unternehmen, die für eine Anforderung der in Art. 25 Abs. 2 genannten Informationen in Betracht kommen, ihre Dienste anbieten.

32. Nach Art. 25 Abs. 2 der Universaldienstrichtlinie müssen die Mitgliedstaaten sicherstellen, dass alle Unternehmen, die Teilnehmern Telefonnummern zuweisen, allen zumutbaren Anträgen, die relevanten Informationen zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen in einem vereinbarten Format und zu gerechten, objektiven, kostenorientierten und nicht diskriminierenden Bedingungen zur Verfügung zu stellen, entsprechen. Außerdem geht aus

Art. 25 Abs. 5 der Richtlinie hervor, dass Abs. 2 dieses Artikels „vorbehaltlich der Rechtsvorschriften [der Union] über den Schutz personenbezogener Daten und der Privatsphäre [gilt], insbesondere des Artikels 12 der [Datenschutzrichtlinie für elektronische Kommunikation]“.

33. Zur Beantwortung der zweiten Frage ist somit auch zu prüfen, ob Art. 12 Abs. 2 der letztgenannten Richtlinie die Übermittlung personenbezogener Teilnehmerdaten durch ein Unternehmen, das Teilnehmern Telefonnummern zuweist, an ein anderes Unternehmen, das in einem anderen Mitgliedstaat als dem, in dem der Teilnehmer wohnt, öffentlich zugängliche Auskunftsdienste und Teilnehmerverzeichnisse anbietet, von einer gesonderten und speziellen Einwilligung dieses Teilnehmers abhängig macht.

34. Insoweit ist darauf hinzuweisen, dass Art. 12 der genannten Richtlinie, wie der Gerichtshof in Rn. 67 des Urteils vom 5. Mai 2011, Deutsche Telekom (C-543/09, EU:C:2011:279), entschieden hat, dahin auszulegen ist, dass er einer nationalen Regelung nicht entgegensteht, die ein Unternehmen, das öffentliche Teilnehmerverzeichnisse veröffentlicht, verpflichtet, die ihm vorliegenden personenbezogenen Daten von Teilnehmern anderer Telefondienstanbieter an ein drittes Unternehmen weiterzugeben, dessen Tätigkeit darin besteht, ein gedrucktes oder elektronisches öffentliches Teilnehmerverzeichnis zu veröffentlichen oder derartige Verzeichnisse über Auskunftsdienste zugänglich zu machen, ohne dass die Weitergabe von einer erneuten Einwilligung der Teilnehmer abhängig ist. Letztere müssen jedoch zum einen vor der ersten Aufnahme ihrer Daten in ein öffentliches Teilnehmerverzeichnis über dessen Zweck sowie über die Tatsache informiert werden, dass die Daten an einen anderen Telefondienstanbieter übermittelt werden könnten, und zum anderen muss gewährleistet sein, dass die betreffenden Daten nach ihrer Weitergabe nicht für andere Zwecke als diejenigen verwendet werden, für die sie im Hinblick auf ihre erste Veröffentlichung erhoben wurden.

35. Um zu diesem Schluss zu gelangen, hat der Gerichtshof in Anbetracht des 39. Erwägungsgrundes und des Wortlauts von Art. 12 Abs. 2 und 3 der Datenschutzrichtlinie für elektronische Kommunikation ausgeführt, dass ein Teilnehmer, der von dem Unternehmen, das ihm eine Telefonnummer zugewiesen hat, von der Möglichkeit der Weitergabe seiner personenbezogenen Daten an ein drittes Unternehmen zur Veröffentlichung in einem öffentlichen Teilnehmerverzeichnis informiert wurde und der Veröffentlichung der betreffenden Daten in einem solchen Teilnehmerverzeichnis zugestimmt hat, in die Weitergabe derselben Daten an ein anderes Unternehmen, das ein gedrucktes oder elektronisches öffentliches Teilnehmerverzeichnis veröffentlicht oder derartige Verzeichnisse über Auskunftsdienste zugänglich machen möchte, nicht erneut einwilligen muss, sofern gewährleistet ist, dass die betreffenden Daten nicht für andere Zwecke als diejenigen verwendet werden, für die sie im Hinblick auf ihre erste Veröffentlichung erhoben wurden. Die Zustimmung eines ordnungsgemäß unterrichteten Teilnehmers zur Veröffentlichung seiner personenbezogenen

Daten in einem öffentlichen Teilnehmerverzeichnis gemäß Art. 12 Abs. 2 der Richtlinie bezieht sich nämlich auf den Zweck dieser Veröffentlichung und erstreckt sich daher auf jede spätere Verarbeitung der Daten durch dritte Unternehmen, die auf dem Markt öffentlich zugänglicher Auskunftsdienste und Teilnehmerverzeichnisse tätig sind, sofern diese Verarbeitung denselben Zweck verfolgt. Dem Wortlaut von Art. 12 Abs. 2 der Datenschutzrichtlinie für elektronische Kommunikation lässt sich insoweit nicht entnehmen, dass dem Teilnehmer ein Recht auf eine selektive Entscheidung zugunsten bestimmter Anbieter öffentlich zugänglicher Auskunftsdienste und Teilnehmerverzeichnisse zusteht (vgl. in diesem Sinne Urteil vom 5. Mai 2011, Deutsche Telekom, C-543/09, EU:C:2011:279, Rn. 62 bis 65).

36. Der Gerichtshof hat hinzugefügt, dass, sobald ein Teilnehmer der Weitergabe seiner personenbezogenen Daten an ein bestimmtes Unternehmen zur Veröffentlichung in einem öffentlichen Teilnehmerverzeichnis dieses Unternehmens zugestimmt hat, die ohne erneute Zustimmung dieses Teilnehmers vorgenommene Weitergabe derselben Daten an ein anderes Unternehmen, das ein öffentliches Teilnehmerverzeichnis veröffentlichen möchte, das in Art. 8 der Charta der Grundrechte der Europäischen Union verankerte Recht auf Schutz personenbezogener Daten nicht in seinem Wesensgehalt antasten kann (vgl. in diesem Sinne Urteil vom 5. Mai 2011, Deutsche Telekom, C-543/09, EU:C:2011:279, Rn. 66).

37. Aus diesen Gesichtspunkten folgt, dass der Zweck der ersten Veröffentlichung personenbezogener Daten des Teilnehmers, in die er eingewilligt hat, für die Beurteilung der Tragweite dieser Einwilligung entscheidend ist. Insoweit sieht Art. 12 Abs. 3 der Datenschutzrichtlinie für elektronische Kommunikation vor, dass die Mitgliedstaaten die Einholung einer zusätzlichen Einwilligung der Teilnehmer verlangen können, wenn ein öffentliches Verzeichnis anderen Zwecken als der Suche nach Einzelheiten betreffend die Kommunikation mit Personen anhand ihres Namens und gegebenenfalls eines Mindestbestands an anderen Kennzeichen dient.

38. Überdies ist festzustellen, dass ein Unternehmen, das öffentlich zugängliche Auskunftsdienste und Teilnehmerverzeichnisse anbietet, unabhängig davon, wo es in der Union ansässig ist, in einem weitgehend harmonisierten, u. a. aus Art. 25 Abs. 5 der Universaldienstrichtlinie sowie aus Art. 1 Abs. 1 und Art. 12 der Datenschutzrichtlinie für elektronische Kommunikation resultierenden Rechtsrahmen tätig wird, der es ermöglicht, die Einhaltung der Anforderungen im Bereich des Schutzes personenbezogener Teilnehmerdaten unionsweit gleichermaßen sicherzustellen.

39. Unter diesen Umständen besteht, wie der Generalanwalt in den Nrn. 40 und 41 seiner Schlussanträge dargelegt hat, kein Anlass für eine unterschiedliche Behandlung in Abhängigkeit davon, ob das Unternehmen, das die Übermittlung personenbezogener Teilnehmerdaten beantragt, im Hoheitsgebiet des Mitgliedstaats der Teilnehmer ansässig ist oder in einem anderen Mitgliedstaat, sofern es diese

Daten zu Zwecken erhebt, die mit denen identisch sind, für die sie im Hinblick auf ihre erste Veröffentlichung erhoben wurden, so dass ihre Übermittlung durch die von den Teilnehmern erteilte Einwilligung gedeckt ist.

40. Folglich ist es in Anbetracht dieser und der in den Rn. 23 bis 30 des vorliegenden Urteils angestellten Erwägungen für das Unternehmen, das seinen Teilnehmern Telefonnummern zuweist, nicht angezeigt, das an den Teilnehmer gerichtete Ersuchen um Einwilligung so zu formulieren, dass er bei seiner Einwilligung danach differenziert, in welchen Mitgliedstaat die ihn betreffenden Daten übermittelt werden können.

41. Nach alledem ist auf die zweite Frage zu antworten, dass Art. 25 Abs. 2 der Universaldienstrichtlinie dahin auszulegen ist, dass er ein Unternehmen, das Teilnehmern Telefonnummern zuweist und nach nationalem Recht verpflichtet ist, die Einwilligung dieser Teilnehmer in die Nutzung der sie betreffenden Daten zum Zweck der Bereitstellung von Auskunftsdiensten und Teilnehmerverzeichnissen einzuholen, daran hindert, dieses Ersuchen so zu formulieren, dass die Teilnehmer bei ihrer Einwilligung in die Nutzung danach differenzieren, in welchem Mitgliedstaat die Unternehmen, die für eine Anforderung der in Art. 25 Abs. 2 genannten Informationen in Betracht kommen, ihre Dienste anbieten.

## Datenerhebungen einer Versicherung zur Feststellung von vertraglichen Obliegenheitsverpflichtungen (Ls)

(Bundesgerichtshof, Urteil vom 22. Februar 2017 – IV ZR 289/14 –)

1. **Zu den Feststellungen des Versicherungsfalles und des Umfangs der Leistung des Versicherers notwendigen Erhebungen im Sinne des § 14 Abs. 1 VVG zählen auch solche, die klären sollen, ob der Versicherungsnehmer bei Vertragsschluss seine vorvertraglichen Anzeigepflichten im Sinne von § 19 Abs. 1 Satz 1 VVG erfüllt hat.**
2. a) **Zur Feststellung des Versicherungsfalles oder des Umfangs der Leistungspflicht des Versicherers sind auch solche Auskünfte erforderlich im Sinne von § 31 Abs. 1 Satz 1 VVG, die der Prüfung vorvertraglicher Anzeigepflichtverletzungen dienen. Die den Versicherungsnehmer insoweit treffende Mitwirkungsobliegenheit ist nicht auf Fälle beschränkt, in denen bereits eine konkrete Verdachtslage für eine Anzeigepflichtverletzung besteht.**
- b) **Der Versicherungsnehmer hat bei der Erhebung von Daten durch den Versicherer grundsätzlich nur insoweit mitzuwirken, als diese zur Prüfung des Leistungsfalles relevant sind. Kann der Umfang der**

**Datenerhebung nicht von vornherein auf entsprechende Informationen beschränkt werden, weil dem Versicherer noch unbekannt ist, worauf er sein Augenmerk zu richten hat, so erstreckt sich die Obliegenheit des Versicherungsnehmers zunächst auf die Einholung solcher weniger weitreichender und persönlichkeitsrelevanter Vorinformationen, die dem Versicherer eine Konkretisierung ermöglichen, welche Informationen im Weiteren tatsächlich für die Leistungsprüfung relevant sind.**

3. § 213 Abs. 1 VVG steht einer Datenerhebung des Versicherers zum Zwecke der Überprüfung vorvertraglicher Anzeigebliedenverletzungen des Versicherungsnehmers nicht entgegen.

## Kein durchsetzbarer Anspruch auf Inhalt einer bestimmten Zeugnisnote

(Bundesarbeitsgericht, Beschluss vom 14. Februar 2017 – 9 AZB 49/16 –)

**Ein Vollstreckungstitel, der den Arbeitgeber zur Erteilung eines Zeugnisses verpflichtet, dessen Inhalt einer bestimmten Notenstufe entspricht, genügt nicht den zwangsvollstreckungsrechtlichen Bestimmungsanforderungen.**

### Sachverhalt:

Die Schuldnerin, die Beklagte im Ausgangsverfahren, ist eine Gesellschaft mit beschränkter Haftung. Sie beschäftigte den Gläubiger, den Kläger im Ausgangsverfahren, als Mitarbeiter im Innendienst. Mit Schreiben vom 26. November 2015 erklärte die Schuldnerin die Kündigung des Arbeitsverhältnisses zum 31. Januar 2016. Mit seiner am 2. Dezember 2015 beim Arbeitsgericht eingegangenen Klage begehrte der Gläubiger Kündigungsschutz. Am 8. Januar 2016 schlossen die Parteien des Ausgangsverfahrens vor dem Arbeitsgericht einen Vergleich, in dem es unter Ziff. 4 heißt:

„Die Beklagte erteilt dem Kläger ein wohlwollendes qualifiziertes Arbeitszeugnis mit einer sehr guten Führungs- und Leistungsbeurteilung und einer Bedauerns-, Dankes- und gute Wünscheformulierung im Schlusssatz.“

[2] Ende Februar 2016 erteilte die Schuldnerin dem Gläubiger ein auf den 25. Januar 2016 datiertes Arbeitszeugnis, das auszugsweise wie folgt lautet:

„Herr T verfügt über ein umfassendes und fundiertes Fachwissen, das er jederzeit in die Praxis umzusetzen wusste. Er war sehr motiviert und zeigte ein hohes Maß an Initiative und Leistungsbereitschaft. Er arbeitete sehr effizient, zielstrebig und sorgfältig und bewies ein gutes Organisationsgeschick. Dabei war er auch erhöhtem Zeitdruck und Arbeitsaufwand gut gewachsen. Er lieferte stets qualitativ und quantitativ tolle Ergebnisse. Herr T hat unsere Erwartungen stets ausgezeichnet erfüllt. Wir waren mit seinen Leistungen jederzeit sehr zufrieden. Sein Verhalten gegenüber Vorgesetzten, Kollegen und Externen war immer einwandfrei.“

Das Arbeitsverhältnis endet im gegenseitigen Einvernehmen zum 31. 01. 2016 aus betriebsbedingten Gründen. Wir danken Herrn T, bedauern sein Ausscheiden sehr und wünschen ihm für die Zukunft alles Gute.“

[3] Mit Schreiben vom 3. März und vom 6. April 2016 forderte der Gläubiger die Schuldnerin auf, das Zeugnis inhaltlich zu ändern. Dabei rügte der Gläubiger, aus dem Wortlaut des Zeugnisses ergebe sich keine sehr gute Leistungs- und Führungsbeurteilung. Das Zeugnis weise insgesamt strukturell und inhaltlich große Mängel auf.

[4] Der Gläubiger beantragte mit Schriftsatz vom 21. März 2016 eine vollstreckbare Ausfertigung des Vergleichs vom 8. Januar 2016, die ihm das Arbeitsgericht am 21. März 2016 erteilte. Am 25. April 2016 wurde diese der Schuldnerin zugestellt. Zur Durchsetzung der unter Ziff. 4 des Vergleichs vom 8. Januar 2016 geregelten Verpflichtung der Schuldnerin zur Erteilung eines Zeugnisses hat der Gläubiger unter dem 8. Mai 2016 beantragt, gegen die Schuldnerin ein Zwangsgeld festzusetzen und für den Fall, dass dieses nicht beigetrieben werden kann, Zwangshaft gegen ihren Geschäftsführer anzuordnen. Zur Begründung hat er ausgeführt, dass von der Schuldnerin erteilte Zeugnis entspreche nicht den Vorgaben von Ziff. 4 des Vergleichs vom 8. Januar 2016. Mit Beschluss vom 21. Juni 2016 hat das Arbeitsgericht den Antrag des Gläubigers zurückgewiesen.

[5] Hiergegen hat der Gläubiger mit Schriftsatz vom 12. Juli 2016 sofortige Beschwerde eingelegt. Mit Beschluss vom 2. August 2016 hat das Arbeitsgericht der sofortigen Beschwerde nicht abgeholfen und sie dem Landesarbeitsgericht zur Entscheidung vorgelegt. Das Landesarbeitsgericht hat die sofortige Beschwerde mit Beschluss vom 8. September 2016 zurückgewiesen und die Rechtsbeschwerde zugelassen. Zur Begründung hat es ausgeführt, die Regelung unter Ziff. 4 des Vergleichs vom 8. Januar 2016 sei zu unbestimmt und daher nicht vollstreckungsfähig.

[6] Hiergegen wendet sich der Gläubiger mit seiner Rechtsbeschwerde, mit der er geltend macht, hinsichtlich der Durchsetzung eines titulierten Anspruchs auf Erteilung eines Arbeitszeugnisses sei es erforderlich, aber auch ausreichend, dass die Führungs- und Leistungsbeurteilung anhand einer dem Notensystem entsprechenden Stufe aus dem Titel ersichtlich ist. Ihn darauf zu verweisen, den Berichtigungsanspruch in einem weiteren Erkenntnisverfahren geltend zu machen, sei mit dem Gebot eines effektiven Rechtsschutzes nicht zu vereinbaren.

### Aus den Gründen:

[7] II. Die Rechtsbeschwerde des Gläubigers ist zulässig, aber nicht begründet. Das Landesarbeitsgericht hat die sofortige Beschwerde des Gläubigers zu Recht zurückgewiesen.

[8] 1. Das Landesarbeitsgericht ist zutreffend davon ausgegangen, dass Ziff. 4 des Vergleichs vom 8. Januar 2016, wonach die Schuldnerin zur Erteilung eines Zeugnisses mit einer sehr guten Führungs- und Leistungsbeurteilung verpflichtet ist, mangels Bestimmtheit einer Zwangsvollstreckung nicht zugänglich ist.

[9] Nach § 794 Abs. 1 Nr. 1 ZPO findet die Zwangsvollstreckung aus Vergleichen statt, die zwischen den Parteien zur Beilegung eines Rechtsstreits geschlossen worden sind. Ein Prozessvergleich ist jedoch nur dann Vollstreckungstitel, wenn er einen vollstreckungsfähigen Inhalt hat (vgl. Zöller/Stöber ZPO 31. Aufl. § 794 Rn. 14). Fehlt es an einer hinreichenden Konkretisierung der den Schuldner treffenden Leistungspflicht, scheidet eine Vollstreckung aus (vgl. BGH 4. März 1993 – IX ZB 55/92 – zu II 2 der Gründe, BGHZ 122, 16). Die Vollstreckung aus einem Titel kann daher nur in den Fällen erfolgen, in denen hinreichend klar ist, welche konkrete Leistung von dem Schuldner gefordert wird (vgl. BGH 26. November 2004 – V ZR 83/04 – zu II 2 a der Gründe). Ob der zur Vollstreckung anstehende Titel hinreichend bestimmt ist, ist unter Rückgriff auf die für

das Erkenntnisverfahren maßgebliche Regelung des § 253 Abs. 2 Nr. 2 ZPO zu bestimmen (vgl. LAG Rheinland-Pfalz 1. April 2009 – 3 Ta 40/09 – zu II 3 a der Gründe; Baumbach/Lauterbach/Albers/Hartmann ZPO 75. Aufl. Grundz. § 704 Rn. 19 mwN).

[10] a) Verlangt ein Arbeitnehmer nicht nur ein einfaches oder qualifiziertes Zeugnis, sondern außerdem auch einen bestimmten Zeugnisinhalt, so hat er im Klageantrag genau zu bezeichnen, was das Zeugnis in welcher Form enthalten soll (BAG 14. März 2000 – 9 AZR 246/99 – zu II 2 der Gründe). Denn nur wenn der Entscheidungsausspruch bereits eine hinreichend klare Zeugnisformulierung enthält, wird verhindert, dass sich der Streit über den Inhalt des Zeugnisses vom Erkenntnis- in das Vollstreckungsverfahren verlagert (in diesem Sinne BAG 14. März 2000 – 9 AZR 246/99 – aaO). Aufgabe des Vollstreckungsgerichts ist es zu klären, ob der Vollstreckungsschuldner seiner festgelegten Verpflichtung nachgekommen ist, nicht aber, worin diese besteht (vgl. BAG 9. September 2011 – 3 AZB 35/11 – Rn. 13). Diese Erwägungen fußen letztlich auf dem Rechtsstaatsprinzip. Dieses verlangt, dass für den Schuldner erkennbar sein muss, in welchen Fällen er mit einem Zwangsmittel zu rechnen hat (vgl. BAG 9. September 2011 – 3 AZB 35/11 – Rn. 14).

[11] b) In Anwendung dieser Grundsätze geht die herrschende Meinung sowohl in der Rechtsprechung (vgl. LAG Nürnberg 3. Mai 2016 – 2 Ta 50/16 – zu II 2 a der Gründe; Hessisches LAG 19. Februar 2004 – 16 Ta 515/03 – zu II der Gründe) als auch im arbeitsrechtlichen Schrifttum (vgl. HWK/Gäntgen 7. Aufl. § 109 GewO Rn. 54; ErfK/Müller-Glöge 17. Aufl. § 109 GewO Rn. 76a; sh. ferner Weuster/Scheer, Arbeitszeugnisse in Textbausteinen, 13. Aufl. S. 190; in diese Richtung auch Schaub/Linck 16. Aufl. ArbR-HdB § 147 Rn. 34) zu Recht davon aus, dass ein Vollstreckungstitel, der den Arbeitgeber zur Erteilung eines Zeugnisses verpflichtet, dessen Inhalt einer bestimmten Notenstufe entspricht, nicht den zwangsvollstreckungsrechtlichen Bestimmtheitsanforderungen genügt. Es bleibt Sache des Arbeitgebers, das Zeugnis im Einzelnen abzufassen, wobei die Formulierung in seinem pflichtgemäßen Ermessen steht (vgl. BAG 15. November 2011 – 9 AZR 386/10 – Rn. 11, BAGE 140, 15). Anders als bei der Verpflichtung, ein Zeugnis gemäß einem Entwurf des Arbeitnehmers zu erteilen (vgl. hierzu BAG 9. September 2011 – 3 AZB 35/11 – Rn. 15 ff.; LAG Hamm 14. November 2016 – 12 Ta 475/16 – zu II 2 b bb der Gründe), lässt die Vereinbarung einer bestimmten Notenstufe dem Arbeitgeber einen derart weiten Gestaltungsspielraum hinsichtlich der Auswahl und Gewichtung einzelner Gesichtspunkte, des Umfangs des Zeugnistextes sowie der Formulierung der Leistungs- und Führungsbeurteilung, dass von einem konkreten Leistungsbefehl, der die Grundlage einer mit staatlichen Zwangsmitteln zu vollziehenden Vollstreckung bildet, nicht die Rede sein kann. Wollte man anders entscheiden, hätte es der Arbeitnehmer in der Hand, durch die ungenaue Formulierung seines Leistungsbegehrens den Streit in das Vollstreckungsverfahren zu verlagern, in dem sich der Arbeitgeber unter der Androhung von Zwangsmaßnahmen seitens des Vollstreckungsgerichts unklaren Handlungspflichten ausgesetzt sähe.

[12] c) Der Hinweis des Gläubigers auf das Gebot effektiven Rechtsschutzes, dem zufolge es möglich sein muss, materiellrechtliche Ansprüche – auch in der Zwangsvollstreckung – effektiv durchzusetzen (vgl. BAG 15. April 2009 – 3 AZB 93/08 – Rn. 17, BAGE 130, 195), verhilft der Rechtsbeschwerde nicht zum Erfolg. Es obliegt der klagenden Partei eines Rechtsstreits, ihr Leistungsbegehren sprachlich so zu fassen, dass der das Verfahren abschließende Vollstreckungstitel den gesetzlichen Be-

stimmtheitsanforderungen entspricht. Kommt sie dieser Obliegenheit nicht nach, steht es ihr frei, ihre Ansprüche in einem erneuten Erkenntnisverfahren durch die Gerichte für Arbeitssachen vollstreckungsfähig titulieren zu lassen.

[13] 2. Soweit sich der Gläubiger in der Beschwerdeschrift gegen das Ausstellungsdatum des von der Schuldnerin erteilten Zeugnisses gewandt hat, hat das Landesarbeitsgericht zutreffend darauf hingewiesen, dass der zur Vollstreckung anstehende Titel keine Angabe zum Ausstellungsdatum enthält. Der Gläubiger hat hiergegen im Rechtsbeschwerdeverfahren keine Einwände erhoben.

[14] 3. Soweit sich die Schuldnerin im Vergleich verpflichtet hat, das Zeugnis mit einer Schlussformel zu versehen, in der sie dem Gläubiger dankt, sein Ausscheiden bedauert und ihm für die Zukunft alles Gute wünscht, ist der Anspruch des Gläubigers durch Erfüllung erloschen (§ 362 Abs. 1 BGB). Der Gläubiger ist dem weder im Beschwerdeverfahren noch im Rechtsbeschwerdeverfahren entgegengetreten.

## Haftung des Landes für Urheberrechtsverletzungen eines Lehrers

(Oberlandesgericht Frankfurt am Main, Urteil vom 9. Mai 2017 – 11 U 153/16)

**Für Urheberrechtsverletzungen eines im Dienst des Landes stehenden Lehrers, der der Fach- und Dienstaufsicht unterliegt, auf einer Schulhomepage haftet das Land gem. § 99 UrhG. Die inhaltliche Ausgestaltung einer Homepage unterfällt dem Bereich des staatlichen Bildungsauftrags. Der kommunale Schulträger verantwortet demgegenüber die räumliche und sachliche Ausstattung der Schulgebäude. Der in einem schulischen Umfeld erfolgte Urheberrechtsverstoß begründet allein die Vermutung der Wiederholung für gleichgelagerte, ebenfalls in einem schulischen Umfeld erfolgende Verstöße, nicht dagegen Verstöße in allen Behörden des beklagten Landes.**

### Sachverhalt:

Die Klägerin ist Inhaberin der ausschließlichen Verwertungsrechte an dem streitgegenständlichen, nachfolgend abgebildeten Cartoon von X (Anlage Kl):

Er wurde auf der Homepage der A-Schule in 01 am ....2014 und im ... 2015 im Rahmen der dort vorgehaltenen E-card-Versendemöglichkeit öffentlich zugänglich gemacht. Träger dieser Schule ist der Landkreis Y. Ein an der Schule tätiger Lehrer, der im Dienst des beklagten Landes steht, war für die Gestaltung der Homepage verantwortlich. Hinsichtlich des Inhalts der Homepage wird auf Anlage K 17 Bezug genommen.

Die Klägerin hat das beklagte Land wegen dieser öffentlichen Zugänglichmachung auf Unterlassung, Auskunft und Schadensersatz in Höhe von 1.200,00 sowie Erstattung vorgerichtlicher Anwaltskosten in Anspruch genommen.

Im Übrigen werden die tatsächlichen Feststellungen des angefochtenen Urteils gemäß § 540 Abs. 1 ZPO in Bezug genommen.

Das Landgericht hat der Klage – unter Reduzierung der Höhe des Schadensersatzes auf 750,00 und korrespondierend des Erstattungsanspruches für außergerichtliche Rechtsanwaltskosten – im Wesentlichen stattgegeben und zur Begründung wie folgt ausgeführt:

Der Klägerin stünde ein Schadensersatzanspruch gem. § 839 BGB i.V.m. Art. 34 GG zu. Der hier handelnde Lehrer habe bei der Erstellung der Homepage in Ausübung eines öffentlichen Amtes gehandelt. Aus den eigenen Angaben des beklagten Landes folge, dass der Lehrer die Betreuung der Homepage mit dulddender Kenntnis der Schulleitung übernommen habe. Es bestehe auch ein Zusammenhang zu dem ihm als Lehrer anvertrauten öffentlichen Amt. Soweit die hier streitgegenständliche Handlung zwar nicht dem eigentlichen Lehrbetrieb zuzuordnen sei, liege ein erforderlicher enger Zusammenhang zum gesamten Schulbetrieb vor. Die Betreuung der Homepage und deren Inhalte sei eine der eigentlichen Lehrtätigkeit vorgelagerte Handlung und nicht mit Fiskalmaßnahmen, die nicht als Ausübung öffentlicher Gewalt anzusehen wären, vergleichbar. Die Außendarstellung der Schule unterfalle gemäß § 16 Abs. 1 HSchulG dem Bereich der schulischen Aufgaben, für welche nicht der Schulträger, sondern das beklagte Land als Anstellungskörperschaft hafte.

Der Höhe nach sei der Schadensersatzanspruch allerdings unter Bezugnahme auf die von der Klägerin vorgelegte Preisliste auf 750,00 beschränkt.

Das beklagte Land hafte zudem aus urheberrechtlicher Sicht wegen der öffentlichen Zugänglichmachung des streitgegenständlichen Cartoons. Der Anspruch sei nicht auf den räumlichen Bereich des Schulamtes für den Landkreis Y begrenzt, da sich weder aus § 99 UrhG noch unter dem Gesichtspunkt des „typischen“ der Verletzungshandlung ein Anhaltspunkt für eine derartige Beschränkung ergebe. Vergleichbar mit der Struktur eines großen Konzerns habe das beklagte Land vielmehr in allen Teilen seiner Landesbehörden dafür zu sorgen, dass die streitgegenständliche Urheberrechtsverletzung zukünftig unterbliebe.

Hiergegen richtet sich die – beschränkt eingelegte – Berufung des beklagten Landes, mit welcher die Abweisung des Unterlassungsantrags zu 1 sowie – hinsichtlich des Zahlungsantrags zu 4 – die Abweisung eines 169,50 übersteigenden Betrages zur Erstattung vorgerichtlicher Rechtsanwaltskosten verfolgt wird.

### Aus den Gründen:

Die Berufung ist zulässig, insbesondere form- und fristgerecht eingelegt und begründet worden. In der Sache hat sie teilweise Erfolg. Der Klägerin steht ein Unterlassungsanspruch gegen das beklagte Land lediglich in dem tenorierten Umfang zu (unter 1.); ihr Anspruch auf Erstattung vorprozessualer Rechtsanwaltskosten ist im Hinblick auf den beschränkten Inhalt der Abmahnung zu reduzieren (unter 2.).

1. Das beklagte Land ist gemäß §§ 2, 19 a, 97, 99 UrhG verpflichtet, die öffentliche Zugänglichmachung des streitgegenständlichen Cartoons zu unterlassen, wenn dies wie auf der hier streitgegenständlichen schulischen Homepage geschieht. Ein weitergehender Unterlassungsanspruch, der die Unterlassungsverpflichtung – allein unter beispielhafter Bezugnahme auf die hier streitgegenständliche schulische Homepage – anfallende Internetveröffentlichungen der dem beklagten Land zuzurechnenden Behörden erstreckt, besteht dagegen nicht.

a. Das beklagte Land haftet gemäß §§ 2, 19 a, 97, 99 UrhG für die durch den Lehrer der A-Schule als Handlungsstörer auf der streitgegenständlichen Homepage begangene Urheberrechtsverletzung.

§ 99 UrhG enthält eine eigenständige urheberrechtliche Zurechnungsnorm für fremdes Verhalten, welche unabhängig von der Frage einer Amtspflichtverletzung und einer daraus gegebenenfalls folgenden Schadensersatzverpflichtung zu prüfen ist (vgl. auch BGH, Urteil vom 16.01.1992 – 1 ZR 36/90 – Seminar-kopien – Tz. 35 zitiert nach juris, zu § 100 UrhG a. F.). Die in § 99 UrhG normierten Voraussetzungen für eine Zurechnung des Verhaltens des Lehrers sind vorliegend gegeben.

aa. Gemäß § 99 UrhG bestehen die Ansprüche aus § 97 UrhG auch gegenüber dem Inhaber eines Unternehmens, sofern in diesem Unternehmen von einem Arbeitnehmer eine Urheberrechtsverletzung begangen wurde. Sinn der Vorschrift ist es, dem Unternehmer die Möglichkeit der Exkulpation (wie in § 831 Abs. 1 S. 2 BOB) abzuschneiden, wenn Urheberrechtsverletzungen aus seinem Betrieb heraus vorgenommen werden (Bohne, in: Wandtke/Bullinger, Praxiskommentar zum Urheberrecht, 2014, § 99 Rn. 1). Der Unternehmer soll sich nicht hinter seinem Arbeitnehmer „verstecken“ können (Bohne ebenda § 99 Rn. 1).

Der Begriff des Unternehmens i. S. d. § 99 UrhG ist dabei weit zu fassen (Reber, in: Beck'scher Online Kommentar UrhR, Stand 1. 10.2016, § 99 Rn. 2) und findet gemäß höchstrichterlicher Rechtsprechung entsprechend auf juristische Personen des öffentlichen Rechts – wie hier – Anwendung (BGH, Urteil vom 16.01.1992 – 1 ZR 36/90 – Seminar-kopien, Tz. 35 zitiert nach juris zu § 100 UrhG a.F.).

bb. Die streitgegenständliche öffentliche Zugänglichmachung erfolgte auch innerhalb des Unternehmens des beklagten Landes im Sinne des § 99 UrhG.

Dieses Merkmal setzt zum einen voraus, dass das beklagte Land Einfluss auf die Verletzungshandlung nehmen kann; der Bereich, in den das fragliche Verhalten fällt, muss jedenfalls im gewissen Umfang durch das beklagte Land beherrscht werden (vgl. Bohne, in: Wandtke/Bullinger, Kommentar zum Urheberrecht, 4. Aufl., § 99 Rn. 6). Dies ist vorliegend der Fall. Unstreitig steht dem beklagten Land die Dienstaufsicht gemäß § 92 Abs. 3 Nr. 2 HSchG über die Lehrerinnen und Lehrer an öffentlichen Schulen zu.

Zum anderen erfordert die Zurechnung eine enge Verbindung der Rechtsverletzung zum Tätigkeitsbereich des Verletzers, die vorliegend ebenfalls gegeben ist. Die inhaltliche Ausgestaltung einer Schulhomepage unterfällt dem Bereich des gemäß § 92 HSchG vom beklagten Land wahrzunehmenden staatlichen Bildungsauftrags, nicht jedoch der gem. § 158 HSchG dem Schulträger obliegenden räumlich und sachlichen Organisationen und Aufrechterhaltung einer Schule:

Das hessische Schulgesetz enthält keine expliziten Regelungen zur Frage, in wessen Aufgabenbereich die inhaltliche Ausgestaltung eines schulischen Internetauftritts fällt. Maßgeblich sind mithin die allgemeinen Regelungen des hessischen Schulgesetzes, welche für die Zusammenarbeit der Schulträger sowie des beklagten Landes im Sinne von § 137 HSchG bei der Errichtung, Organisation, Aufhebung und Unterhaltung der öffentlichen Schulen gelten. Gemäß § 92 Abs. 1 HSchG steht das gesamte Schulwesen in der Verantwortung des beklagten Landes, welches insbesondere die Schulen berät und unterstützt, die Qualität der Arbeit gewährleistet und die Fach- und Dienstaufsicht sowie die Rechtsaufsicht wahrnimmt. Demgegenüber obliegt den Schulträgem gemäß § 158 Abs. 1 HSchG insbesondere die Errichtung der erforderlichen Schulgebäude und Schulanlagen sowie deren sachliche Ausstattung und ordnungsgemäße Unterhaltung. Die systematische Stellung der genannten Normen verdeutlicht dabei, dass die inhaltliche, pädagogische Ausrichtung einer Schule das beklagte Land zu verantworten hat, während der Schulträger die sachliche Ausstattung der jeweiligen Schulgebäude und Schulanlagen sowie deren Organisation gewährleistet. § 92 HSchG ist Bestandteil des 7. Teils des hessischen Schulgesetzes, welcher den Bereich „Lehrkräfte, Schulleitung und Schulaufsicht“ regelt, während § 158 HSchG dem 12. Teil unterfällt, welcher sich mit Fragen des „Personal- und Sachaufwand“ befasst.

Ausgehend von dieser Aufgabenaufteilung kommt es mithin darauf an, ob ein schulischer Internetauftritt in seiner Gesamtschau dem Bereich der pädagogisch, inhaltlichen Bezüge einer Schule unterfällt oder aber der sachlichen Ausstattung. Die gebotene Gesamtbetrachtung der äußeren, sachlichen und inhaltlichen Eigenschaften eines schulischen Internetauftritts sprechen nach Auffassung des Senats für eine klare Zuordnung des schulischen Internetauftritts zum Aufgabenbereich des beklagten Landes. Insoweit indiziert der Umstand, dass das inhaltliche Konzept des schulischen Internetauftritts von einem der Dienstaufsicht des beklagten Landes unterstehenden Lehrer betreut wurde, bereits einen Bezug dieser Tätigkeit zum beklagten Land (vergleiche auch BGH, Urteil vom 16.01.1992 – 1 ZR 36/90 – Seminarkopien – Tz. 35 zitiert nach juris zu § 100 UrhG a.F.).

Ein schulischer Internetauftritt dient der Realisierung unterschiedlicher Zwecke. Neben reinen Informationen über die Existenz, Ortlichkeit und Erreichbarkeit der Schule unterstützt und erleichtert er ganz wesentlich den Informationsaustausch der am Schulleben Beteiligten. Als eine Art „virtuelle Visitenkarte“ beeinflusst eine Schulhomepage zudem Schulentscheidungen künftiger Schüler. Eine schulische Homepage vermittelt gegenüber Dritten und der jeweiligen Schulgemeinde das „Gesicht“ der Schule. Dieses wird ganz maßgeblich durch die inhaltliche Ausrichtung, vorhandene Schwerpunkte sowie besondere Angebote der Schule geprägt. Entsprechend finden sich auf einer schulischen Internetpräsenz üblicherweise Angaben zum Schulprofil und -konzept, zu besonderen Lern- und/oder Förderangeboten, Schulregeln und Verhaltenskodices. Darüber hinaus bietet eine Homepage Raum, schulische Materialien zur Vor- oder Nachbereitung des Unterrichts bzw. Ergänzung bereitzustellen sowie Austausch in Foren, Chats oder gesonderten Arbeitsbereichen zu pflegen.

Die hier anhand von Anlage K 17 nachvollziehbare inhaltliche Ausrichtung der streitgegenständlichen Schulhomepage entspricht insoweit den dargestellten allgemeinen medialen Zwecken eines schulischen Internetauftritts. Gemäß Anlage K 17 hält die Homepage unter anderem sowohl allgemeine den Schulbetrieb betreffende Informationen bereit (Ferientermine) als auch konkret auf die Schule bezogene Inhalte, wie das Schulkonzept.

Dieses wiederum wird im Einzelnen über das konkrete Schulprogramm, die Schulordnung sowie das Hausaufgabenkonzept im Rahmen der Homepage wiedergegeben (BI. 63 Rs). Darüber hinaus informiert die Homepage etwa über Arbeitsgemeinschaften, die Schulinspektion und deren Auswertung und anstehende Projektwochen und hält einen allein den Lehrern zugänglichen Informationsbereich „teachers only“ bereit. Die Zusammenschau dieser Inhalte verdeutlicht, dass über die Homepage primär das „pädagogische Gesicht“ der Schule nach außen getragen werden soll, d.h. ihre insoweit bestehenden Besonderheiten und Charakteristika. Soweit die Homepage darüber hinaus eine so genannte E-card-Versendemöglichkeit anbietet, kommt es auf den pädagogischen Bezug dieses konkreten Angebots im Hinblick auf die allein ausschlaggebende Gesamtbewertung eines schulischen Internetauftritts nicht an.

Soweit das beklagte Land darauf verweist, die inhaltliche Ausgestaltung einer Homepage gehöre zum ureigenen Bereich eines Schulträgers, da über die Ausgestaltung einer Homepage die in den Verantwortungsbereich des Schulträgers fallende Auslastung einer Schule bestimmt werde, überzeugt dies nicht. Die Auslastung einer Schule hängt maßgeblich von ihrem individuellen Konzept ab. Dieses wird jedenfalls zum ganz überwiegenden Teil durch die jeweiligen pädagogischen Leminhalte/

Schwerpunkte/Angebote geprägt und allenfalls zu einem ganz geringen Teil durch die sachliche Ausstattung. Soweit sich die an inhaltlichen, pädagogischen Aspekten ausgerichtete Schulwahlentscheidung auf den – dem Schulträgers zuzuordnenden – Auslastungsgrad der Schule auswirkt, folgt daraus nicht, dass die pädagogische Konzeption selbst, die über das Medium der Homepage vermittelt wird, dem Aufgabenbereich des Schulträgers zufällt.

Soweit das beklagte Land darüber hinaus auf eine Entscheidung des Oberlandesgerichts Celle verweist, steht diese der dargelegten Auffassung nicht entgegen. Das OLG Celle hat im Rahmen seines Beschlusses vom 09.11.2015 – 13 U 95/15 – offen gelassen, ob der Internetauftritt einer Schule den Bereich des Schulträgers betrifft. Eine Begründung für die dortige Einschätzung, dass dafür „allerdings einiges spricht“, findet sich in dem Beschluss nicht.

b. Das beklagte Land kann allerdings nur insoweit auf Unterlassung in Anspruch genommen werden, als der hier streitgegenständliche Erstverstoß in Form der öffentlichen Zugänglichmachung des konkreten Cartoons gem. Anlage K 1 auf einer schulischen Homepage die Vermutung der Wiederholung begründet. Das gilt unabhängig von der Tatsache, dass sich selbstverständlich auch andere, dem beklagten Land unterstehende Behörden nicht widerrechtlich des streitgegenständlichen Cartoons „bedienen“ dürfen.

Der explizit schulbezogene Inhalt des Cartoons sowie die hier zu beurteilende Verletzungshandlung im Rahmen einer schulischen Homepage indizieren allein eine Wiederholungsgefahr in dem hier aufgetretenen Umfang. Anhaltspunkte für eine Verwendung des Cartoons gemäß Anl. K 1 außerhalb eines schulischen Umfelds lassen sich aus dem Erstverstoß nicht ableiten (vgl. BGH, Urteil vom 09.05.1996 – 1 ZR 107/94 – EDV-Geräte Tz. 34 bei juris). Soweit die Klägerin im Rahmen der mündlichen Verhandlung vor dem Senat erstmals allgemein ausgeführt hat, dass alle Behörden des beklagten Landes ausbilden, mit Pädagogen zusammenarbeiten und Fortbildungen anbieten, ist dies allein nicht geeignet, eine Wiederholungsgefahr für sämtliche dem beklagten Land unterstehenden Behörden zu begründen. Allgemeine Aus- und Fortbildungstätigkeit im Erwachsenenbereich unterscheidet sich ganz maßgeblich von dem hier mit dem Cartoon erfassten schulischen Umfeld.

Der auf die Verletzungshandlung bezogene „insbesondere“-Zusatz im Unterlassungstenor des Landgerichts konnte die notwendige Konkretisierung des Verbots nicht herbeiführen. Ein solcher „insbesondere“-Zusatz ist lediglich eine Auslegungshilfe für den abstrakt formulierten Antrag, führt aber nicht zu dessen Einschränkung (BGH, Urteil vom 02.02.2012 -1 ZR 81/10 – Tribenuronmethyl Tz. 22).

Der Zusatz macht aber deutlich, dass es der Klägerin darauf ankam, jedenfalls ein Verbot des konkret beanstandeten Verhaltens zu erwirken, so dass der Senat den Zusatz als unechten Hilfsantrag bewertet hat, der aus dem oben genannten Gründen Erfolg hat.

2. Die Klägerin hat gemäß § 97 a Abs. 3 S. 1 UrhG Anspruch auf Erstattung vorprozessualer Rechtsanwaltskosten hinsichtlich der berechtigten Abmahnung mit Schreiben vom .... 2015 in Höhe von 865,00 €.

Da sich die Abmahnung – abweichend zum Klageantrag zu 1 – nicht auf sämtliche Behörden des Landes Hessen erstreckte, sondern auf die konkrete Verletzungsform beschränkt worden war, war sie insoweit auch vollumfänglich begründet. Im Hinblick auf den für den Klageantrag zu 1 festgesetzten Gegenstandswert von 30.000,00 € erscheint für diesen beschränkten

Anspruch allerdings allein ein Gegenstandswert von 15.000 € angemessen, aber auch ausreichend. Unter Ansatz einer 1,3-fachen Geschäftsgebühr nebst Auslagenpauschale ergibt sich damit ein Erstattungsbetrag in Höhe von 865,00 €.

III. Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus § 708 Nr. 10 ZPO; die Abwendungsbefugnis findet ihre Grundlage in § 711 ZPO.

Gründe, die Revision zuzulassen im Sinne von § 543 Abs. 2 ZPO, liegen nicht vor. Die Entscheidung beruht auf der Anwendung allgemeiner Rechtsgrundsätze auf den Einzelfall.

## Zugang der Eltern eines verstorbenen Kindes zu dessen Daten in einem sozialen Netzwerk (Ls)

(Kammergericht Berlin, Urteil vom 31. Mai 2017 – 21 U 9/16 –)

1. Die Erben des verstorbenen Nutzers eines sozialen Netzwerks können aufgrund des Fernmeldegeheimnisses (§ 88 TKG) vom Anbieter des Dienstes solange kein Zugang zum Konto des Verstorbenen erhalten, wie dem nicht alle Kommunikationspartner zugestimmt haben, die mit dem Verstorbenen Kommunikationsinhalte ausgetauscht haben, die nur für diese beiden Nutzer oder nur einen eingeschränkten Personenkreis bestimmt waren.
2. Die bloße Kommunikation über das soziale Netzwerk begründet keine ausdrückliche, konkludente oder mutmaßliche Einwilligung in die Weitergabe von Kommunikationsinhalten im Sinne der Nr. 1 an Dritte. Dies gilt auch für die Kommunikation mit einem minderjährigen Nutzer des Netzwerks hinsichtlich der Weitergabe von Inhalten an seine Eltern.
3. Ein Anspruch der Eltern auf Zugang zum Konto ihres minderjährigen Kindes lässt sich auch nicht aus dem Recht der elterlichen Sorge oder dem allgemeinen Persönlichkeitsrecht der Eltern ableiten.

(Nicht rechtskräftig)

## Satzungsmäßige Befugnis einer Krankenkasse zur Vorlage von Behandlungsunterlagen an Sachverständige (Ls)

(Verwaltungsgerichtshof Baden-Württemberg, Urteil vom 10. Mai 2017 – 2 S 1826/16 –)

1. Die satzungsrechtliche Verpflichtung der Mitglieder der Postbeamtenkrankenkasse zur Vorlage der Be-

handlungsunterlagen einschließlich der Verpflichtung, einer Weitergabe dieser Unterlagen an Sachverständige zuzustimmen, sowie die sich bei Verletzung dieser Obliegenheiten ergebenden Rechtsfolgen beruhen auf einer ausreichenden Ermächtigungsgrundlage und sind mit dem Rechtsstaats- und Demokratieprinzip vereinbar (Bestätigung und Fortführung des Senatsurteils vom 24.11.2011 – 2 S 2295/10 –).

2. Bei der Prüfung, ob Leistungen anhand der vom Mitglied vorgelegten Unterlagen „notwendig und angemessen“ sind, darf sich die Postbeamtenkrankenkasse medizinischen Sachverständigen bedienen. Die Auswahl eines geeigneten medizinischen Gutachters darf sie im Grundsatz auch einem auf Vermittlung von Gutachtern spezialisierten Dritten (sog. Gutachtendienst) überlassen.
3. Nach der Satzung der Postbeamtenkrankenkasse besteht solange kein Leistungsanspruch, als das Mitglied seiner satzungsrechtlichen Mitwirkungsverpflichtung nicht nachkommt (hier: Nichtvorlage konkret angeforderter und zur Prüfung benötigter Krankenunterlagen).
4. Bei dem von der Postbeamtenkrankenkasse auf der Grundlage einer satzungsrechtlichen Mitwirkungsverpflichtung eingeholten Sachverständigengutachten handelt es sich um ein Privatgutachten, das die Postbeamtenkrankenkasse in die Lage versetzen soll, eine Entscheidung über einen Leistungsantrag zu treffen. Kommt es aufgrund dieses Privatgutachtens zu einer negativen Entscheidung über den Leistungsantrag, so kann das betroffene Mitglied hiergegen Widerspruch einlegen sowie ggf. Klage erheben. Im Rahmen dieses Klageverfahrens ist das Verwaltungsgericht bei Vorliegen substantiiertester Einwendungen gegen die Verwertbarkeit des als Parteigutachten einzustufenden Gutachtens der Postbeamtenkrankenkasse ggf. verpflichtet, ein gerichtliches Sachverständigengutachten einzuholen (Bestätigung und Fortführung des Senatsurteils vom 24.11.2011 – 2 S 2295/10 –).

## Zur vollständigen Einsicht in Akten des Sozialpsychiatrischen Dienstes (Ls)

(Oberverwaltungsgericht Lüneburg, Beschluss vom 8. Mai 2017 – 14 PS 1/17 –)

1. Personenbezogene Daten Dritter, die gegenüber dem Sozialpsychiatrischen Dienst Auskünfte erteilt oder in anderer Weise an der Erfüllung der Aufgaben nach dem Niedersächsischen Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke mitgewirkt haben, sind wesensmäßig geheimhaltungsbedürftig.
2. So können berechnete Interessen Dritter im Sinne des § 16 Abs. 4 Nr. 3 des Niedersächsischen Datenschutzgesetzes und therapeutische Gründe im Sinne des § 36

Satz 2 des Niedersächsischen Gesetzes über Hilfen und Schutzmaßnahmen für psychisch Kranke einer Offenlegung entgegenstehen.

*(Leitsatz zu 2 nicht amtlich)*

## Unerlaubte Datenübermittlung im privaten Umfeld (Ls)

(Landgericht Düsseldorf, Urteil vom 20. Februar 2017 – 5 O 400/15 –)

1. Gibt ein Gläubiger eines privaten Darlehens die Kontaktdaten und -bestände des Schuldners an einen Dritten „nur so zur Info“ mit der Information weiter, der Schuldner sei pleite, verstößt er einerseits gegen § 28 BDSG und andererseits gegen den Schutz des allgemeinen Persönlichkeitsrechts gemäß § 823 Abs. 1 BGB.
2. Das sog. Haushaltsprivileg (§ 27 Abs. 1 S. 1 Nr. 1 BDSG) kommt nicht zur Anwendung, da die Übermittlung nicht ausschließlich für persönliche und familiäre Zwecke erfolgt.

*(Nicht amtliche Leitsätze)*

## Verantwortung der Eltern für datenschutzkonforme Smartphone-Nutzung ihrer Kinder (Ls)

(Amtsgericht Bad Hersfeld, Beschluss vom 20. März 2017 – F 111/17 EAS –)

1. Überlassen Eltern ihrem minderjährigen Kind ein digitales ‚smartes‘ Gerät (z.B. Smartphone) zur dauernden eigenen Nutzung, so stehen sie in der Pflicht, die Nutzung dieses Geräts durch das Kind bis zu dessen Volljährigkeit ordentlich zu begleiten und zu beaufsichtigen.
2. Verfügen die Eltern selbst bislang nicht über hinreichende Kenntnisse von ‚smarter‘ Technik und über die Welt der digitalen Medien, so haben sie sich die erforderlichen Kenntnisse unmittelbar und kontinuierlich anzueignen, um ihre Pflicht zur Begleitung und Aufsicht durchgehend ordentlich erfüllen zu können.
3. Wer den Messenger-Dienst „WhatsApp“ nutzt, übermittelt nach den technischen Vorgaben des Dienstes fortlaufend Daten in Klardaten-Form von allen in dem eigenen Smartphone-Adressbuch eingetragenen Kontaktpersonen an das hinter dem Dienst stehende Unternehmen.  
Wer durch seine Nutzung von „WhatsApp“ diese andauernde Datenweitergabe zulässt, ohne zuvor von

seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden.

4. Nutzen Kinder oder Jugendliche unter 18 Jahren den Messenger-Dienst „WhatsApp“, trifft die Eltern als Sorgeberechtigte die Pflicht, ihr Kind auch im Hinblick auf diese Gefahr bei der Nutzung des Messenger-Dienstes aufzuklären und die erforderlichen Schutzmaßnahmen im Sinne ihres Kindes zu treffen.

## Zulässigkeit eines Fahrerbewertungsportals

(Verwaltungsgericht Köln, Urteil vom 16. Februar 2017 – 13 K 6093/15 –)

1. KFZ-Kennzeichen zugewiesene Fahrerbewertungsdaten sind infolge der einfachen Registerauskunft nach § 39 Abs. 1 StVG personenbeziehbare Daten des Halters des Fahrzeuges.
2. Fahrerbewertungsportale unterscheiden sich von Berufsbewertungsportalen dadurch, dass sie keinen beruflichen oder gewerblichen Anlass bzw. den Schutzinteressen der Betroffenen vorrangige Gründe für die uneingeschränkte Veröffentlichung der Bewertungsdaten haben.

*(Nicht amtliche Leitsätze)*

### Sachverhalt:

Die Klägerin betreibt das Internetportal [www.fahrerbewertung.de](http://www.fahrerbewertung.de). Zuvor wurde das Portal von der C. GmbH betrieben, deren Gesellschafter mit denjenigen der Klägerin identisch sind. Bei diesem Portal (im Folgenden: Fahrerbewertungsportal) handelt es sich um ein kostenloses Bewertungsportal für Autofahrer, das auch als kostenlose App verfügbar ist. Hiermit bezweckt die Klägerin nach eigenen Angaben, bewerteten Fahrern das eigene Fahrverhalten bewusst zu machen. Durch die so eröffnete Möglichkeit zur Selbstreflexion will die Klägerin zur Sicherheit des Straßenverkehrs beitragen. Nutzer des Portals können das Fahrverhalten anderer Personen unter Angabe eines Kfz-Kennzeichens nach einem Ampelschema (rot = negativ, gelb = neutral, grün = positiv) bewerten. Eine freie Texteingabe ist im Rahmen des Bewertungsvorgangs nicht möglich. Die Bewertung kann ergänzt werden um Angaben zum Fahrzeug, zum Ort sowie um eine Auswahl aus einer Liste vorgegebener Eigenschaften des Fahrverhaltens. Nutzer des Portals können ein Kfz-Kennzeichen eingeben und sich das Ergebnis der bisherigen Bewertungen hierzu in Form einer durchschnittlichen Schulnote anzeigen lassen. Die freiwilligen Zusatzangaben sind auf dieser Übersicht nicht einsehbar; sie fließen lediglich in die Gesamtstatistiken ein. Zudem können sich Nutzer per Email laufend über den aktuellen Stand der Bewertungen zu einem konkreten Kfz-Kennzeichen informieren lassen. Die Klägerin bietet zudem eine auf

Regionen bzw. Städte bezogene Auswertung sowie allgemeine Statistiken zu Hersteller, Fahrstil und Kfz-Typ an. Alle Funktionen des Portals können ohne Registrierung genutzt werden. In § 2 Nr. 6 ihrer allgemeinen Geschäftsbedingungen weist die Klägerin darauf hin, dass Personen, die sich zu Unrecht bewertet sehen, eine Beschwerde an ihre Beschwerdestelle richten können. Auf dem Fahrerbewertungsportal ist Werbung verlinkt.

Erstmals mit Schreiben vom 27. März 2014 teilte der – bis zum 20. September 2015 zuständige – Landesbeauftragte für Datenschutz und Informationsfreiheit für das Land Nordrhein-Westfalen (LDI NRW) der vorigen Betreiberin des Fahrerbewertungsportals seine Bedenken bezüglich der Gestaltung des Portals mit. Mit der Erhebung und Veröffentlichung der Daten auf dem Portal gehe ein Gefährdungspotential einher. Es könnten beispielsweise Bewegungsprofile erstellt werden. Es sei zudem zu verhindern, dass eine allgemein zugängliche „private Verkehrssünderdatei“ erstellt werde. Im Rahmen einer Interessenabwägung sei zu berücksichtigen, dass sich das Fahrerbewertungsportal von anderen Bewertungsportalen unterscheide, weil es nicht in Zusammenhang mit einer beruflichen oder gewerblichen Tätigkeit der Bewerteten stehe und der Nutzerkreis nicht beschränkt sei. Der LDI NRW forderte die ursprüngliche Betreiberin des Fahrerbewertungsportals zur Stellungnahme auf.

Die Klägerin bzw. ihre Vorgängerin nahmen im Wesentlichen wie folgt Stellung:

Auf der Grundlage der auf dem Portal erhobenen Daten seien die Fahrer nicht identifizierbar. Kfz-Kennzeichen seien keine personenbeziehenden Daten. Von diesen könnten weder die Klägerin noch die Nutzer des Portals ohne weiteres auf eine Person schließen. Auskünfte bei entsprechenden Stellen – wie etwa Versicherern, dem Kraftfahrtbundesamt oder Zulassungsstellen – seien nur auf Antrag und unter Darlegung eines berechtigten Interesses erfolgreich. Dies stelle einen hohen Aufwand zur Herstellung eines Personenbezuges dar. Wenn Nutzer diese Möglichkeit in rechtswidriger Weise in Anspruch nähmen, könne dies nicht der Klägerin zugerechnet werden. Im Übrigen sei zu einem Kfz-Kennzeichen nur der Haltername gespeichert. Fahrer und Halter müssten nicht identisch sein. Selbst wenn Nutzer des Portals eine Auskunft zu dem Halter eines Fahrzeugs erhielten, müsse dies nicht der auf dem Portal bewertete Fahrer sein. Auch § 45 StVG sehe lediglich vor, dass es sich bei einem Kfz-Kennzeichen um ein personenbezogenes Datum handeln könne. Damit dies der Fall sei, müssten weitere Umstände bekannt sein, wie zum Beispiel ein Ort oder eine Zeitangabe.

Selbst wenn es sich um personenbeziehende Daten handle, seien deren Erhebung, Speicherung und Nutzung jedenfalls zulässig. Es sei bereits fraglich, ob durch die Erhebung und Speicherung der Daten auf dem Fahrerbewertungsportal überhaupt in das Recht der Betroffenen auf informationelle Selbstbestimmung eingegriffen werde. Jedenfalls sei ein solcher Eingriff gerechtfertigt. Es sei nur die Sozialsphäre der Bewerteten betroffen. Diese werde nur bei einer Stigmatisierung, Prangerwirkung oder sozialer Ausgrenzung verletzt. Solche Wirkungen seien auf dem Fahrerbewertungsportal jedoch ausgeschlossen, weil die Nutzer lediglich aus vorgefertigten sachlichen Bewertungen auswählen könnten. Ein Bewegungsprofil von Fahrern könne nicht erstellt werden. Es sei wegen der bloßen Angabe des Kfz-Kennzeichens immer unklar, wer das Fahrzeug gefahren habe.

Die Meinungs- und Kommunikationsfreiheit der Klägerin und der Nutzer des Portals sowie das Recht auf Information der Allgemeinheit seien höher zu bewerten als die Interessen der Betroffenen. Es gehe der Klägerin nicht um die bloße Befriedigung der Neugier über das Fahrverhalten Dritter. Ziel des Portals sei es unter anderem, Rückschlüsse darauf zuzulassen, wo besonders rücksichtslos gefahren werde. Die von dem LDI NRW angeregten Veränderungen des Portals seien nicht zielführend bzw. rechtswidrig. Bereits jetzt seien für die Nutzer lediglich Durchschnittsdaten einsehbar. Ein von dem LDI NRW vorgeschlagener begrenzter Nutzerkreis kollidiere

mit dem Ziel des Portals, das Fahrverhalten positiv zu steuern. Von dem Konzept der Klägerin sei vorgesehen, dass jeder Halter oder Fahrer mit Bewertungen durch Dritte rechnen müsse. Nur auf diese Weise könne der gewünschte Effekt der Selbstreflexion gewährleistet werden. Zudem könne die Klägerin die Echtheit der Registrierungsdaten nicht überprüfen. Ein Registrierungserfordernis für die Nutzer des Fahrerbewertungsportals laufe dem Grundsatz der Datenvermeidung und Datensparsamkeit zuwider.

Dem stellte der LDI NRW hauptsächlich folgende Argumente gegenüber: Ein Kfz-Kennzeichen sei ein personenbeziehbares Datum. Dies folge aus § 45 Satz 2 StVG. Nutzer des Portals müssten keinen besonderen Aufwand betreiben, um mithilfe des Kfz-Kennzeichens den zugehörigen Halter zu ermitteln. Einfache Registerauskünfte seien unter geringen Voraussetzungen möglich. Die Zuordnung eines Kfz-Kennzeichens sei insbesondere für den weiteren Bekanntheitskreis eines Fahrzeughalters sowie für Kfz-Versicherungen möglich. Das Konzept des Fahrerbewertungsportals setze selbst eine Personenbeziehbarkeit der Bewertungen voraus. Anderenfalls könnten individuelle Fahrstile nicht korrigiert werden. Bei der Abwägung der widerstreitenden Interessen müsse berücksichtigt werden, dass auf dem Fahrerbewertungsportal keine Bewertungen im Zusammenhang mit einer beruflichen Tätigkeit erfolgten und es kein Registrierungserfordernis für die Nutzer gebe. Bei dem Fahrerbewertungsportal sei die Interessenlage anders als etwa bei einem Bewertungsportal für Ärzte. Ein allgemeines Interesse an ordnungsgemäßem Fahrverhalten rechtfertige nicht, Bewertungen zu einem konkreten Kfz-Kennzeichen zu kennen. Es sei auch die Kommunikationsasymmetrie zu beachten, die durch die Anonymität im Internet entstehe. Zudem sei zu befürchten, dass Stellen, die die Daten selbst nicht erheben dürften, Kenntnis von individuellem Fahrverhalten erhalten. So könnten etwa Arbeitgeber ihre Angestellten oder Bewerber überprüfen oder Versicherungen ihre Versicherungsnehmer. Zu bemängeln sei, dass es auf dem Fahrerbewertungsportal keine gut sichtbare Beschwerdemöglichkeit für Bewertete gebe. Außerdem würden Betroffene nicht gem. § 33 Abs. 1 Satz 2 BDSG darüber informiert, dass sie bewertet worden sind.

Mit datenschutzrechtlicher Anordnung vom 22. September 2015, der Klägerin zugestellt am 24. September 2015, gab der LDI NRW der Klägerin auf, an dem Internetportal innerhalb einer Frist von zwei Monaten (Ziffer 5.) folgende Änderungen vorzunehmen:

Die Gesamtbewertung und die Anzahl der Bewertungen zu einem Kfz-Kennzeichen dürfen nur für den entsprechenden registrierten Kfz-Halter als betroffene Person sichtbar sein (Ziffer 1.). Abrufe zu Art, Zahl und Inhalten von zu einem bestimmten Kfz-Kennzeichen vorliegenden Bewertungen dürfen nur registrierten Kfz-Haltern zugänglich gemacht werden. Eine Registrierung als Halter setzt voraus, dass ein Nutzer eine Emailadresse sowie Einzelheiten zu dem Fahrzeug angibt und mittels Anhaken eines vorgegebenen Textes versichert, Halter des Fahrzeugs mit dem genannten Kennzeichen zu sein. Arbeitgeber müssen versichern, dass sie das Portal nicht nutzen, um Mitarbeiter zu überwachen (Ziffer 2.). Einem Kfz-Halter ist das Recht einzuräumen, durch einen an die Klägerin adressierten Widerspruch zu erreichen, dass das Vorliegen von Bewertungen zu seinem Kfz-Kennzeichen auf dem Portal nicht angezeigt wird (Ziffer 3.). Die Möglichkeit laufender Benachrichtigungen über den aktuellen Bewertungsstand zu einem Kfz-Kennzeichen darf nur dem entsprechenden Kfz-Halter offenstehen (Ziffer 4.).

Zur Begründung wiederholte und vertiefte der LDI NRW seine zuvor mitgeteilte rechtliche Bewertung. Ergänzend betonte er, dass das auf dem Portal der Klägerin bewertete Verhalten zwar im öffentlichen Raum stattfinde, aber privat motiviert sei. Der einzelne Fahrer müsse nicht damit rechnen, dass er Objekt einer organisierter Erhebung, Kategorisierung und Bewertung durch private Stellen werde. Die Portalinhalte könnten von einer nicht zu übersehenden

Öffentlichkeit räumlich, zeitlich und inhaltlich unbegrenzt zu beliebigen Zwecken verwendet werden. Es bestehe keine Notwendigkeit für die durch das Portal geschaffene „Nebenjustiz“, weil verkehrswidriges Verhalten bereits ausreichend durch staatliche Behörden überwacht und sanktioniert werde. Das Fahrerbewertungsportal kollidiere zudem mit dem Grundsatz der Gewährleistung der freien und unbeobachteten Bewegung im öffentlichen Raum. Im Gegensatz zu kurzfristigen Videobeobachtungen seien die Bewertungen auf dem Portal dauerhaft und für jedermann sichtbar.

Für den Fall, dass die Klägerin die Änderungen nicht fristgerecht vornehme, drohte der LDI NRW je Ziffer 1. bis 4. ein einheitliches Zwangsgeld in Höhe von 1.000 Euro an.

Die Klägerin hat am 17. Oktober 2015 Klage erhoben.

### Aus den Gründen:

I. Die insgesamt zulässige Klage ist unbegründet, soweit sie sich gegen die datenschutzrechtlichen Anordnungen in Ziffer 1. bis 5. des angefochtenen Bescheides (1.) und den überwiegenden Teil der Zwangsgeldandrohungen in Ziffer 6. des angefochtenen Bescheides (2.) richtet. Der Bescheid vom 22. September 2015 ist insoweit rechtmäßig und verletzt die Klägerin nicht in ihren Rechten, § 113 Abs. 1 Satz 1 der Verwaltungsgerichtsordnung (VwGO).

1. Die datenschutzrechtlichen Anordnungen unter Ziffer 1. bis 5. des angefochtenen Bescheides sind rechtmäßig. Maßgeblicher Zeitpunkt für die Überprüfung der angefochtenen Anordnungen ist derjenige der letzten mündlichen Verhandlung. Die Anordnungen stellen einen Dauerverwaltungsakt dar. Sie enthalten die sich ständig aktualisierende Verpflichtung, die vorgegebenen technischen Eigenschaften des Fahrerbewertungsportals sicherzustellen. Eine einmalige Handlung der Klägerin genügt für die Erfüllung der Anordnung nicht.

Vgl. *Verwaltungsgericht (VG) Berlin, Urteil vom 24. Mai 2011 – 1 K 133.10 –, juris Rn. 16.*

Ermächtigungsgrundlage der Anordnungen ist § 38 Abs. 5 Satz 1 des Bundesdatenschutzgesetzes (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 25. Februar 2015 (BGBl. I S. 162). Nach dieser Vorschrift kann die Aufsichtsbehörde zur Gewährleistung der Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen.

Diese Vorschrift ist auf das Fahrerbewertungsportal der Klägerin anwendbar.

Der sachliche Anwendungsbereich des Bundesdatenschutzgesetzes ist eröffnet. Nach § 1 Abs. 2 BDSG gilt das Gesetz für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Die auf dem Portal der Klägerin zu einzelnen Kfz-Kennzeichen eingegebenen Bewertungsdaten erfüllen diese Voraussetzungen. Anhand der Bewertung zu einem Kfz-Kennzeichen können sowohl die Klägerin als verantwortliche Stelle als auch die Nutzer des Fahrerbewertungsportals als Dritte einen Bezug zu einer bestimmbarer Person herstellen. Die Bestimmbarkeit einer natürlichen Person anhand von Daten ist gesetzlich nicht definiert.

Die Auslegung des Begriffs der Bestimmbarkeit ergibt, dass es nicht allein auf die Möglichkeiten der datenerhebenden,

-verarbeitenden oder -nutzenden Stelle, also der im Sinne des § 3 Abs. 7 BDSG verantwortlichen Stelle selbst (relatives Verständnis) ankommt. Vielmehr ist auch das Wissen Dritter zu berücksichtigen (absolutes Verständnis).

*Allgemein zu den Voraussetzungen der Bestimmbarkeit gem. § 3 Abs. 1 BDSG vgl. Herbst, NVwZ 2016, S. 902 ff.; Bergt, ZD 2015, S. 365 ff.; Brink/Eckhardt, ZD 2015, S. 205 ff.; ausführlich Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 268 ff.*

Der Wortlaut des § 3 Abs. 1 BDSG gibt insoweit keinen Aufschluss. Die offene Formulierung der Vorschrift kann jedoch als Indiz dafür gewertet werden, dass auch das Wissen Dritter bei der Bestimmbarkeit einer Person eine Rolle spielen soll. Denn die Vorschrift schränkt den Begriff „bestimmbar“ nicht durch zusätzliche Kriterien ein. Hätte der Gesetzgeber intendiert, die Bestimmbarkeit allein von dem Wissen der verantwortlichen Stelle abhängig zu machen, wäre eine entsprechende Fassung der Definition zu erwarten gewesen.

Der Sinn und Zweck der Definition in § 3 Abs. 1 BDSG verlangt, nicht allein die Möglichkeiten der verantwortlichen Stelle zur Bestimmung einer konkreten natürlichen Person, sondern auch die Kenntnisse Dritter zu berücksichtigen. Die Definition personenbezogener Daten ist maßgeblich für den in § 1 Abs. 2 BDSG festgelegten Anwendungsbereich des Bundesdatenschutzgesetzes. Ist der Anwendungsbereich nicht eröffnet, weil Daten als nicht personenbezogen zu qualifizieren sind, nehmen diese Daten nicht an dem von § 1 Abs. 1 BDSG bezweckten Schutz teil. Nach dieser Norm ist Ziel des Bundesdatenschutzgesetzes, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Interessen der datenerhebenden bzw. datenverarbeitenden verantwortlichen Stelle unterfallen hingegen nicht dem allgemeinen Schutzzweck des Bundesdatenschutzgesetzes. Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Richtlinie) bezieht Interessen an der Weitergabe von Daten in ihren allgemeinen Schutzzweck ein. In Art. 1 Abs. 2 der Datenschutz-Richtlinie wird der freie Verkehr personenbezogener Daten zum schützenswerten Gut erklärt. Eine vergleichbare Erklärung findet sich im Bundesdatenschutzgesetz nicht. Hierfür besteht auch kein Bedürfnis, weil Interessen der verantwortlichen Stellen im Rahmen der einzelnen Erlaubnistatbestände des Bundesdatenschutzgesetzes zu berücksichtigen sind. Dem durch das Gesetz bezweckten Schutz des Persönlichkeitsrechts entspricht es in besonderem Maße, den Personenbezug von Daten bereits dann anzunehmen, wenn sie von einem Dritten einer Person zugeordnet werden können. Das Schutzniveau wird hingegen dem Gesetzeszweck widersprechend verkürzt, wenn lediglich auf die Möglichkeiten der verantwortlichen Stelle abgestellt wird. Das absolute Verständnis der Personenbeziehbarkeit führt nicht zu einer uferlosen Anwendung des Bundesdatenschutzgesetzes auf jegliche Daten. Insbesondere ist nicht zu befürchten, dass hierdurch Daten einem strengen gesetzlichen Schutz unterzogen werden, bezüglich derer kein Gefahrenpotential für das allgemeine Persönlichkeitsrecht besteht.

Bei Berücksichtigung des Zusatzwissens Dritter für die Bestimmbarkeit einer Person besteht nicht die Gefahr, dass jedes Datum zum personenbezogenen Datum erhoben wird. Die Grenze der Bestimmbarkeit zeigt § 3 Abs. 6 BDSG auf. Diese Vorschrift definiert anonymisierte Daten, die gerade nicht mehr

dem Schutz des Datenschutzgesetzes unterfallen sollen. Danach ist das Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können. Die Bestimmbarkeit einer Person ist demnach erst dann zu verneinen, wenn Dritte einen Personenbezug nur mit unverhältnismäßigem Aufwand herstellen können. Illegale Methoden zur Bestimmung einer Person stellen nicht per se einen unverhältnismäßigen Aufwand dar. Vielmehr ist das Interesse eines Dritten an der Herstellung des Personenbezugs gegen das Risiko einer Ahndung der illegalen Handlung abzuwägen.

*Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 301, 319 f.; Herbst, NVwZ 2016, S. 902 (905); Bergt, ZD 2015, S. 365 (370).*

Wird nur das vernünftigerweise vorhandene bzw. beschaffbare Zusatzwissen Dritter berücksichtigt, besteht auch für die jeweilige verantwortliche Stelle keine unnötige Unklarheit über ihre datenschutzrechtlichen Pflichten.

*Vgl. Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 294.*

Die verantwortliche Stelle kann auch bei dieser Interpretation der Personenbeziehbarkeit abschätzen, welche Mittel Dritte vernünftigerweise zur Herstellung eines Personenbezugs heranziehen werden. Dies bestätigt hier der intensive Austausch zwischen der Klägerin und dem LDI NRW über die tatsächlichen Möglichkeiten für Nutzer des Fahrerbewertungsportals, bewertete Personen konkret zu bestimmen.

Die verfassungskonforme Auslegung des Begriffs in § 3 Abs. 1 BDSG bestätigt dieses weite Verständnis der Personenbestimmbarkeit. Der Schutzbereich des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG beginnt schon auf der Stufe der Persönlichkeitsgefährdung, weil in Bezug auf personenbezogene Daten eine gesteigerte Gefährdungslage besteht. Wegen der Möglichkeiten der elektronischen Datenverarbeitung sind Einzelangaben über persönliche und sachliche Verhältnisse einer Person unbegrenzt in großer Menge speicherbar und jederzeit abrufbar.

*Bundesverfassungsgericht (BVerfG), Urteil vom 11. März 2008 – 1 BvR 2074/05 –, juris Rn. 63 f. zur automatisierten Kennzeichenerfassung.*

Diesem besonderen Schutzniveau entspricht es, die durch das Recht auf informationelle Selbstbestimmung geschützten personenbezogenen Daten bereits dann anzunehmen, wenn der Personenbezug auch von Dritten und nicht lediglich im relativen Verhältnis von der verantwortlichen Stelle mit vernünftigem Aufwand hergestellt werden kann.

Auch die europarechtskonforme Auslegung der Definition personenbezogener Daten steht einem engen Verständnis der Bestimmbarkeit einer Person entgegen. Zwar ist die Definition des Begriffs „bestimmbar“ in Art. 2 Buchstabe a der Datenschutz-Richtlinie ähnlich offen wie in § 3 Abs. 1 BDSG gefasst. Allerdings stellt der Erwägungsgrund 26 der Datenschutz-Richtlinie klar, dass es für den Personenbezug ausreicht, wenn Dritte eine Verbindung zwischen Daten und einer konkreten Person herstellen können. Nach diesem Erwägungsgrund sollen bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu be-

stimmen. Darüber hinaus soll der Datenschutz erst dann nicht mehr greifen, wenn Daten derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. Dementsprechend hat der Europäische Gerichtshof für die Einstufung eines Datums als personenbezogen betont, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Daten in den Händen einer einzigen Person befinden.

*Europäischer Gerichtshof (EuGH), Urteil vom 19. Oktober 2016 – C-582/14 – (Breyer), juris Rn. 43.*

Sowohl für die Nutzer des Portals als auch für die Klägerin besteht die Möglichkeit, ein Kfz-Kennzeichen einer konkreten Person mithilfe einer einfachen Registerauskunft im Sinne des § 39 Abs. 1 des Straßenverkehrsgesetzes (StVG) zuzuordnen. Nach dieser Vorschrift ist für die Auskunftsgewährung lediglich die Darlegung des Empfängers erforderlich, dass er die Halterdaten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Eine solche Anfrage ist mit einem geringfügigen Aufwand für den Anfragenden verbunden. Es ist auch nicht unwahrscheinlich, dass Nutzer des Fahrerbewertungsportals das für die einfache Registerauskunft erforderliche rechtlich relevante Interesse lediglich vorgeben, um den Halter eines Fahrzeugs zu ermitteln. Dass ein Nutzer auch in einem solchen Fall Erfolg hat, ist bei lebensnaher Betrachtung anzunehmen. Denn die einfache Registerauskunft erfordert lediglich die Darlegung des Interesses, keine Glaubhaftmachung. Eine Überprüfung des angegebenen Interesses durch die Zulassungsstelle oder das Kraftfahrt-Bundesamt ist nicht vorgesehen.

*Vgl. BT-Drs. 65/86, S. 74.*

Vor diesem Hintergrund stellt die Ermittlung eines Fahrzeughalters unter Angabe unwahrer Behauptungen keinen unverhältnismäßigen Aufwand bei der Bestimmung einer Person dar. Mangels Überprüfung durch die zuständigen Behörden wird ein solches „falsches“ Interesse in der Regel nicht aufgedeckt oder gar sanktioniert werden.

Bestimmten Personen bzw. Stellen ist die Zuordnung von Kfz-Kennzeichen zu Personen sogar ohne weitere Recherche möglich, weil sie bereits über das erforderliche Zusatzwissen verfügen. Hierzu zählen etwa Kfz-Versicherungen, Arbeitgeber, die einen Fuhrpark betreiben oder Personen aus dem näheren persönlichen Umfeld eines Kfz-Halters wie beispielsweise Familienmitglieder, Freunde, Arbeitskollegen oder Nachbarn.

Der Klägerin ist zuzugeben, dass Fahrer und Halter eines Fahrzeugs nicht ausnahmslos identisch sein müssen. Es kommt vor, dass ein Halter eines Fahrzeugs dieses anderen Personen unentgeltlich oder gegen Entgelt zur Verfügung stellt. Dieser Umstand steht aber nicht der Annahme entgegen, dass zwischen einem auf dem Portal mit einer Bewertung versehenen Kfz-Kennzeichen und einer natürlichen Person – nämlich dem Fahrzeughalter – ein Bezug hergestellt werden kann. Die Nutzer des Portals werden die Bewertungen zu einem Kfz-Kennzeichen, welches sie einer Person zuordnen können, auch dieser Person zuschreiben. Ginge man wie die Klägerin davon aus, dass die Bewertungen auf dem Portal nicht notwendigerweise auf einen Fahrer zurückführbar wären, widerspräche dies dem von der Klägerin verfolgten Ziel, mit ihrem Portal zur Sicherheit im Straßenverkehr beizutragen. Denn wenn mit einer Bewertung nicht der Fahrer eines Fahrzeugs gemeint sein sollte, kann auch kein konkretes Fahrverhalten überdacht werden. Bestände die von

der Klägerin geltend gemachte Unsicherheit im Regelfall, wäre das Konzept des Fahrerbewertungsportals hinfällig.

Auch nach dem Grundsatz der Einheit der Rechtsordnung sind die Bewertungen zu einem konkreten Kfz-Kennzeichen als personenbezogene Daten zu qualifizieren. Gem. § 45 Satz 2 StVG gehört auch das Kennzeichen eines Fahrzeugs zu den Daten, die einen Bezug zu einer bestimmten oder bestimmbarer Person ermöglichen. Dies folgt neben dem klaren Wortlaut auch aus dem systematischen Zusammenhang der Vorschrift, die in den datenschutzrechtlichen Abschnitt des Straßenverkehrsgesetzes eingebettet ist.

Auf die Klägerin ist das Bundesdatenschutzgesetz auch in persönlicher Hinsicht anwendbar. Nach § 1 Abs. 2 Nr. 3 BDSG gilt das Gesetz für 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. Die Klägerin ist als juristische Person des privaten Rechts eine nicht-öffentliche Stelle im Sinne des § 2 Abs. 4 Satz 1 BDSG, da sie keine hoheitlichen Aufgaben der öffentlichen Verwaltung wahrnimmt. Zur Erhebung, Verarbeitung und Nutzung von Daten setzt sie eine Datenverarbeitungsanlage ein, weil das von ihr betriebene Internetportal die dort eingegebenen Bewertungen automatisiert verarbeitet, vgl. § 3 Abs. 2 Satz 1 BDSG, Art. 3 Abs. 1 Alt. 1 der Datenschutz-Richtlinie. Aus diesem Grund findet gem. § 27 Abs. 1 Satz 1 Nr. 1 BDSG auf die Klägerin der dritte Abschnitt des Bundesdatenschutzgesetzes Anwendung, zu dem die Ermächtigungsgrundlage des § 38 Abs. 5 Satz 1 BDSG zählt.

Die datenschutzrechtlichen Anordnungen sind formell rechtmäßig. Insbesondere ist der LDI NRW hierfür gem. § 38 Abs. 6 BDSG, § 22 Abs. 5 Satz 2 des Datenschutzgesetzes für das Land Nordrhein-Westfalen (DSG NRW) hierfür zuständig gewesen.

Die Tatbestandsvoraussetzungen des § 38 Abs. 5 Satz 1 BDSG liegen vor. Die aktuelle Gestaltung des Fahrerbewertungsportals verstößt gegen Vorschriften des Bundesdatenschutzgesetzes. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Vorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Da Einwilligungen der durch das Fahrerbewertungsportal Betroffenen nicht vorliegen, bedarf es für die Erhebung, Speicherung und Übermittlung der Daten durch die Klägerin einer ausdrücklichen Erlaubnis oder Anordnung der Zulässigkeit durch eine Rechtsvorschrift. An einer solchen Erlaubnis fehlt es hier.

Die Erhebung und Speicherung der Daten auf dem Fahrerbewertungsportal ist unzulässig. Die Voraussetzungen der Zulässigkeit richten sich nach § 29 Abs. 1 Satz 1 BDSG. Nach dieser Vorschrift ist das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunftsteilen oder dem Adresshandel dient, nach Maßgabe der Vorgaben in § 29 Abs. 1 Satz 1 Nr. 1-3 BDSG zulässig.

Nicht anwendbar ist hier § 28 BDSG, weil die Datenerhebung und -speicherung durch die Klägerin nicht zur Erfüllung eigener Geschäftszwecke erfolgt. Die Übermittlung der Daten an die Nutzer des Portals ist der Zweck der Datenerhebung und -speicherung. Die Bewertungsdaten werden erhoben und gespeichert, um sie den Nutzern des Fahrerbewertungsportals allge-

mein zugänglich zu machen. Die Klägerin handelt auch geschäftsmäßig. Eine geschäftsmäßige Tätigkeit setzt lediglich eine Wiederholungsabsicht der verantwortlichen Stelle voraus. Einer Gewerbmäßigkeit und der hierfür erforderlichen Gewinnerzielungsabsicht bedarf es hingegen nicht.

*Bundesgerichtshof (BGH), Urteil vom 23. Juni 2009 – VI ZR 196/08 –, juris Rn. 24; Gola/Schomerus, BDSG, 12. Aufl. 2015, § 29 Rn. 7; Ehmann, in: Simitis, BDSG, 8. Aufl. 2014, § 29 Rn. 60.*

Die Datenerhebung und -speicherung auf dem Fahrerbewertungsportal erfolgt planmäßig in einer Vielzahl von Fällen, nämlich bei jeder Eingabe von Bewertungen zu einem Kfz-Kennzeichen.

Als konkreter Erlaubnistatbestand kommt hier § 29 Abs. 1 Satz 1 Nr. 1 BDSG in Betracht. Danach ist die Datenerhebung und -speicherung zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat. Dies ist hier nicht der Fall. Die Betroffenen, also die auf der Plattform der Klägerin bewerteten Personen, haben ein schutzwürdiges Interesse daran, dass die Erhebung und Speicherung ihrer Daten ausgeschlossen werden. Die Schutzwürdigkeit eines Interesses ergibt sich aus einer Abwägung der Interessen der Beteiligten.

*Vgl. zur Erforderlichkeit dieser Abwägung auch im Rahmen des § 29 Abs. Satz 1 Nr. 1 BDSG BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08 –, juris Rn. 26; Plath, in: ders. BDSG/DSGVO, 2. Aufl. 2016, Rn. 35 ff.; Ehmann, in: Simitis, BDSG, a.a.O., § 29 Rn. 155 ff.*

Bei der Interessenabwägung ist der Zweck der Erhebung und Speicherung von Daten – hier die Übermittlung der Daten an Dritte – zu berücksichtigen.

*BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08 –, juris Rn. 26.*

Die vorzunehmende Interessenabwägung fällt zugunsten der Betroffenen und zu Lasten der Klägerin aus.

Das Interesse der Klägerin, auf dem Fahrerbewertungsportal Angaben der Nutzer zu Kfz-Kennzeichen unbeschränkt zu erheben und zu speichern, ist von ihrer durch Art. 12 Abs. 1 GG geschützten unternehmerischen Freiheit erfasst. Die Klägerin strebt eigenen Angaben zufolge zum einen das ideelle Ziel an, zu mehr Sicherheit im Straßenverkehr beizutragen. Zum anderen hat sie ein wirtschaftliches Interesse daran, durch die Besuche ihrer Webseite Werbeeinnahmen zu erzielen. Zudem kann sie sich auf das Recht auf Meinungsfreiheit gem. Art. 5 Abs. 1 Satz 1 GG berufen, auch wenn sie sich die Meinungen der Portalnutzer nicht zu eigen macht. Die Klägerin nimmt an dem Kommunikationsprozess zwischen den Nutzern teil, indem sie Dritten eine Plattform zur Verfügung stellt, auf der ein Austausch zum Fahrverhalten einzelner Personen stattfinden kann. Durch die Übermittlung eines Notendurchschnitts zu einzelnen Kfz-Kennzeichen bündelt die Klägerin die auf ihrem Portal abgegebenen Bewertungen zu einem aus Sicht der Nutzer vollständigen Überblick über die von den Nutzern entäußerten Meinungen.

*Vgl. BGH, Urteil vom 23. September 2014 – VI ZR 358/13 –, juris Rn. 28.*

Die Interessen der Nutzer, Bewertungen zu Kfz-Kennzeichen abzugeben und sich über vorhandene Bewertungen zu informieren, sind ebenfalls durch das Recht auf Meinungs- und Informationsfreiheit aus Art. 5 Abs. 1 Satz 1 GG geschützt.

Diesen verfassungsrechtlich geschützten Interessen der Klägerin und der Portalnutzer steht das Recht der Betroffenen auf informationelle Selbstbestimmung als Ausprägung des allgemei-

nen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG gegenüber. Dieses Recht verleiht dem Einzelnen die Befugnis, grundsätzlich selbst darüber zu entscheiden, ob und wann sowie innerhalb welcher Grenzen seine persönlichen Daten in die Öffentlichkeit gebracht werden.

*Grundlegend: BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, juris Rn. 146.*

Die Abwägung zwischen diesen Interessen fällt zu Lasten der Klägerin bzw. der Portalnutzer aus. Der Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen steht vor dem Hintergrund, dass die Bewertungsdaten an einen unbegrenzten Personenkreis übermittelt werden, außer Verhältnis zu den Interessen der Klägerin und der Portalnutzer.

Die Bewertungen auf dem Portal der Klägerin betreffen zwar grundsätzlich die Sozialsphäre eines Betroffenen, da diese anlässlich der Teilnahme am öffentlichen Straßenverkehr erfolgen. Im Bereich der Sozialsphäre erfolgt die Persönlichkeitsentfaltung von vornherein im Kontakt mit der Umwelt. Äußerungen im Zusammenhang mit der Sozialsphäre einer Person dürfen nur im Fall schwerwiegender Auswirkungen auf das Persönlichkeitsrecht mit negativen Sanktionen verknüpft werden, etwa bei Stigmatisierung oder sozialer Ausgrenzung sowie bei Eintreten einer Prangerwirkung.

*BVerfG, Beschluss vom 17. Dezember 2002 – 1 BvR 755/99 –, juris Rn. 33.*

Das Verhalten von Autofahrern ist allerdings nur bedingt auf den Kontakt nach außen gerichtet. Die Situation, die auf dem Fahrerbewertungsportal bewertet wird, unterscheidet sich grundlegend von den Sachverhalten, die Gegenstand der üblichen Bewertungsportale sind. Anders als etwa Lehrer, Ärzte, Handwerker, Gastronomen oder Reiseveranstalter, deren Verhalten ebenfalls auf verschiedenen Internetportalen bewertet wird, geben Autofahrer keinen beruflichen oder gewerblichen Anlass für eine Bewertung ihres Verhaltens. Letztere begeben sich nicht mit dem Ziel in den öffentlichen Straßenverkehr, mit ihrem Umfeld in Kontakt zu treten. Dieser tatsächliche Unterschied führt zu einer gesteigerten Schutzbedürftigkeit der Betroffenen gegenüber den in den Konstellationen von Berufsbewertungsportalen Betroffenen.

Die Form, die die Klägerin für ihr Fahrerbewertungsportal gewählt hat, birgt die Gefahr, eine Prangerwirkung für die Betroffenen zu entfalten. Die Bewertungen der Nutzer werden von der Klägerin nicht verifiziert. Jedem Nutzer ist es unabhängig von einer tatsächlichen Beobachtung möglich, Bewertungen zu einem beliebigen Kfz-Kennzeichen mit weiteren Erläuterungen abzugeben. Dies kann beliebig oft erfolgen – wenn auch mit einem zeitlichen Abstand von 24 Stunden zwischen zwei Bewertungen. An einem Tag können bei Nutzung verschiedener IP-Adressen fünf Bewertungen abgegeben werden. Dadurch besteht die Gefahr, dass Nutzer aus zweckwidrigen Motiven zu einem Kfz-Kennzeichen unrichtige negative Bewertungen anhäufen und damit das Fahrverhalten einer Person fälschlicherweise als schlecht darstellen. Dies kann für den Betroffenen negative Konsequenzen haben, etwa wenn das Führen von Kraftfahrzeugen zu seiner beruflichen Tätigkeit gehört und die Negativbewertung auf dem Portal der Klägerin dessen Arbeitgeber bekannt wird. Dieser Gefahr kann sich ein Betroffener nur unter erschwerten Bedingungen erwehren. Erst bei positiver Kenntnis von einer (schlechten) Bewertung steht einem Betroffenen die Möglichkeit offen, eine Beschwerde an die Klägerin zu richten. Über eine erste erfolgte Bewertung werden Betrof-

fene durch die Klägerin allerdings nicht unterrichtet – was ihr nach derzeitiger Gestaltung des Portals auch nicht möglich ist. Betroffene können allenfalls durch eigene regelmäßige Kontrolle auf dem Fahrerbewertungsportal in Erfahrung bringen, ob zu ihrem Kfz-Kennzeichen eine Bewertung abgegeben worden ist. Diese Kontrolle setzt allerdings voraus, dass einem Betroffenen das Portal der Klägerin auch bekannt ist. Vor diesem Hintergrund erweist sich die von der Klägerin in ihren allgemeinen Geschäftsbedingungen angebotene Beschwerdemöglichkeit für Betroffene nur als bedingt hilfreich.

Demgegenüber ist nicht ersichtlich, dass es zur Erfüllung des von der Klägerin angestrebten Ziels einer Datenerhebung und -speicherung in dem Umfang bedarf, wie sie die Klägerin aktuell betreibt. Selbst wenn eine Beobachtung und Bewertung des Fahrverhaltens Einzelner den Ergebnissen der von der Klägerin vorgelegten Studie aus dem Jahr 2013 entsprechend zu einer Verminderung von Verkehrsunfällen führte, ist nicht nachvollziehbar, weshalb hierfür die Übermittlung der Bewertungen an jeden Nutzer des Fahrerbewertungsportals essentiell sein sollte. Das von der Klägerin verfolgte Ziel kann auch erreicht werden, wenn Bewertungen lediglich zum Zweck der jeweils ausschließlichen Übermittlung an die Betroffenen erhoben und gespeichert werden. Es ist nicht davon auszugehen, dass ein Fahrer allein durch die Befürchtung, öffentlich einsehbare negative Bewertungen zu erhalten, zu einer Überprüfung des eigenen Fahrverhaltens angehalten werden wird. Zudem stellt die Gestaltung des Fahrerbewertungsportals in Frage, ob das von der Klägerin angestrebte Ziel erreicht werden kann. Die Klägerin stellt nicht sicher, dass auf ihrem Portal lediglich „echte“ Bewertungen abgegeben werden. Es ist wahrscheinlich, dass Nutzer unabhängig von einem tatsächlich festgestellten negativen Fahrverhalten negative Bewertungen abgeben. Ebenso wahrscheinlich ist eine Bewertung des eigenen Fahrverhaltens als positiv. Beide Verhaltensweisen konterkarieren den von der Klägerin vorgegebenen Zweck des Fahrerbewertungsportals.

Die von Art. 12 Abs. 1 GG geschützte unternehmerische Erwerbstätigkeit der Klägerin wird durch die datenschutzrechtlichen Anordnungen ebenfalls nicht verletzt. Hierfür genügt es nicht bereits, wenn eine Regelung Gewinnchancen minimiert. Eine Verletzung des Rechts aus Art. 12 Abs. 1 GG ist erst anzunehmen, wenn sie einer Erwerbstätigkeit die wirtschaftliche Grundlage entzieht.

*BVerfG, Beschluss vom 16. März 1971 – 1 BvR 52/66 –, juris Rn. 58.*

Dies ist hier nicht der Fall. Mit der der Klägerin auferlegten Beschränkung des Zugriffs auf Bewertungsergebnisse wird eine verringerte Besucherzahl auf dem Fahrerbewertungsportal einhergehen. Dies wiederum führt dazu, dass die Klägerin mit der auf dem Portal enthaltenen Werbung voraussichtlich weniger Einnahmen erzielen wird. Es ist aber nicht zu befürchten, dass die Klägerin bei reduzierten Werbeeinnahmen nicht mehr in der Lage sein wird, das Portal zu betreiben – zumal sie eigenen Angaben in der mündlichen Verhandlung zufolge bereits derzeit die Kosten für den Betrieb des Portals nicht durch Werbung refinanzieren kann.

Den Interessen der Nutzer, ihre Meinung über ein Fahrverhalten zu äußern und sich über die Bewertungen zu einem konkreten Kfz-Kennzeichen zu informieren, kommt trotz der grundsätzlichen Bedeutsamkeit des Rechts auf freie Meinungsäußerung ein geringer Stellenwert zu. Die Bewertungen stehen nicht im Zusammenhang mit einer beruflichen Tätigkeit oder einer

Dienstleistung. Das ihnen zugrunde liegende Verhalten ist in der Regel privat motiviert. Beispielsweise haben Nutzer eines Ärztebewertungsportals ein berechtigtes Interesse daran, sich vor einem Arztbesuch über einen Arzt und dessen Praxis anhand von Bewertungen auf einem entsprechenden Portal zu informieren. Diese Information dient dazu, einen für das eigene Anliegen passenden Arzt auszuwählen. Ein vergleichbares Motiv für die Information über Fahrerbewertungen besteht nicht. Aus der Kenntnis der Bewertungsergebnisse zu einem konkreten Kfz-Kennzeichen kann ein Nutzer des Fahrerbewertungsportals keinen individuellen Vorteil ziehen. Ein solcher ist insbesondere auch nicht für Nutzer einer Mitfahrgelegenheit erkennbar. Zunächst dürfte die Anzahl der Personen im Vergleich zu den übrigen Nutzern eher gering sein. Es ist nicht davon auszugehen, dass die bei der Klägerin bislang erfolgten Kennzeichen-Abfragen – dies sind nach ihren Angaben seit Beginn des Projekts insgesamt 1.625.347 gewesen – überwiegend zu dem Zweck erfolgt sind, das Fahrverhalten eines Fahrers vor Inanspruchnahme einer Mitfahrgelegenheit zu überprüfen. Darüber hinaus ist nicht ersichtlich, wie eine Verknüpfung zwischen einem Mitfahrangebot und einem Kfz-Kennzeichen hergestellt werden soll. Bei Angeboten von Mitfahrgelegenheiten werden Kfz-Kennzeichen in aller Regel nicht angegeben. Die Klägerin hat auch nicht näher erläutert, welcher konkrete Vorteil sich daraus ergibt herauszufinden, wo besonders rücksichtslos gefahren wird. Einer Kontrolle des Verhaltens im öffentlichen Straßenverkehr durch private Beobachter, deren Bewertungen zentral auf dem Fahrerbewertungsportal gesammelt und dauerhaft allgemein zugänglich gemacht werden, bedarf es nicht.

Darüber hinaus verstößt die von der Klägerin auf dem Fahrerbewertungsportal vorgenommene Datenübermittlung gegen § 29 Abs. 2 BDSG. Nach dieser Vorschrift ist die Übermittlung im Rahmen der Zwecke nach § 29 Abs. 1 BDSG zulässig, wenn der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Diese Voraussetzungen sind hier nicht erfüllt. Auch eine gem. § 29 Abs. 2 BDSG anzustellende Abwägung der Interessen aller Beteiligten im Einzelfall fällt zu Lasten der Klägerin bzw. der Nutzer ihres Portals aus. Es fehlt – wie bereits dargelegt – an einem glaubhaft dargelegten Interesse der Portalnutzer an der Kenntnis der zu einzelnen Kfz-Kennzeichen auf dem Portal erhobenen und gespeicherten Daten. Aus den vorstehend genannten Gründen besteht auch ein schutzwürdiges Interesse der von Bewertungen auf dem Fahrerbewertungsportal Betroffenen an dem Ausschluss der Übermittlung.

Die in den Ziffern 1. bis 4. des angefochtenen Bescheides getroffenen Anordnungen genügen dem Bestimmtheitsgebot des § 37 Abs. 1 des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen (VwVfG NRW). In allen Anordnungen in Ziffer 1. bis 4. des angefochtenen Bescheides ist jeweils klar und verständlich beschrieben, welche Änderungen die Klägerin im Einzelnen an ihrem Portal vorzunehmen hat.

Die einzelnen Anordnungen zur Umgestaltung des Fahrerbewertungsportals weisen auch keine Ermessensfehler auf, § 114 Satz 1 VwGO. Die Anordnungen sind insbesondere verhältnismäßig. Entgegen der Auffassung der Klägerin verstößt die von ihr geforderte Einrichtung einer Registrierungspflicht für den Abruf der Bewertungsergebnisse zu einem Kfz-Kennzeichen nicht selbst gegen das Bundesdatenschutzgesetz. Der in § 3a BDSG

normierte Grundsatz der Datensparsamkeit ist lediglich eine *Maxime*, die den Adressaten keine konkreten Verpflichtungen auferlegt. Dieser Grundsatz verlangt keine konkreten Verhaltensweisen im Einzelfall.

*Schreiber in: Plath, a.a.O., § 3a Rn. 14.*

Die angeordnete Registrierungspflicht für Fahrzeughalter und die vorgegebene Begrenzung der Datenübermittlung an registrierte Nutzer des Fahrerbewertungsportals (Ziffer 1. und 2. des angefochtenen Bescheides) sind dazu geeignet, die dargestellten datenschutzrechtlichen Verstöße zu beheben. Werden die Bewertungsdaten lediglich den zu einem Kfz-Kennzeichen zugehörigen Fahrern bzw. Haltern übermittelt, erfolgt eine Datenübermittlung ausschließlich an Dritte, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben – nämlich die Bewerteten selbst. Der Geeignetheit der Vorgaben zur Einrichtung einer Registrierungspflicht steht es nicht entgegen, dass Nutzer bei der Registrierung als Halter theoretisch falsche Angaben machen können. Auch wenn die Klägerin nicht überprüfen kann, ob eine Person, die sich als Halter eines Fahrzeugs mit einem konkreten Kennzeichen ausgibt, auch tatsächlich der Halter ist, stellt die angeordnete Registrierungspflicht in ihrer konkreten Gestaltung eine hinreichende Hürde für den Zugriff auf Bewertungsergebnisse zu konkreten Kfz-Kennzeichen dar. Der vorgegebene Registrierungsvorgang, bei dem die Angabe einer Emailadresse sowie Angaben zu Art und Erstzulassung des Fahrzeugs erforderlich sind, wirkt auf missbräuchliche Vorhaben abschreckend. Die beiden vorgegebenen Pflichttexte zur Versicherung, eine Registrierung nicht missbräuchlich vorzunehmen, halten Portalnutzer zusätzlich davon ab, sich zu Unrecht als Halter eines Fahrzeugs zu registrieren. Der zu betreibende Aufwand, um von Bewertungsergebnissen Kenntnis zu erlangen, ist so groß, dass nicht mit einer Vielzahl falscher Registrierungen zu rechnen ist. Wenn sich ein Nutzer etwa für Bewertungen zu mehreren verschiedenen Kfz-Kennzeichen interessiert, müsste er sich jeweils mit unterschiedlichen Emailadressen auf dem Fahrerbewertungsportal anmelden. Hinzu kommt, dass eine Registrierung unter Angabe unrichtiger Daten als Ordnungswidrigkeit gem. § 43 Abs. 2 Nr. 4 BDSG geahndet werden kann.

Die Anordnungen des LDI NRW sind zur Beseitigung der datenschutzrechtlichen Verstöße auch erforderlich. Im Vergleich zu der Beschränkung des Zugriffs auf Bewertungsergebnisse durch eine Registrierungspflicht, der Einrichtung eines förmlichen Widerspruchsrechts für Betroffene und der Unterbindung einer Nachverfolgung der Bewertungen zu einem Kfz-Kennzeichen für Dritte sind keine mildereren Mittel ersichtlich, die mindestens ebenso effektiv zur Beseitigung der unzulässigen Datenerhebung, -speicherung und -übermittlung führen.

Die Anordnungen sind schließlich angemessen. Ihr Zweck steht nicht außer Verhältnis zu den Nachteilen für die Klägerin und die Nutzer des Fahrerbewertungsportals. Die Vorgaben in dem angefochtenen Bescheid schaffen zwischen den widerstrebenden grundrechtlich geschützten Interessen einen angemessenen Ausgleich. Die angeordnete Beschränkung des Nutzerkreises durch Einrichtung einer Registrierungspflicht beschränkt lediglich die Art, in der die Klägerin das Fahrerbewertungsportal betreibt. Das Portal wird weder gezielt noch faktisch untersagt. Auch die Schaffung eines Widerspruchsrechts für Betroffene und die Beseitigung des „Newsfeed“ zu einem Kfz-Kennzeichen für nicht registrierte Nutzer führen nicht zu einer faktischen Untersagung des Fahrerbewertungsportals. Der aus den Anordnungen für das Recht auf informationelle Selbstbestimmung der

Betroffenen folgende Vorteil überwiegt die nur geringfügigen Einbußen für die Klägerin und – soweit dies in der hier gegebenen Anfechtungssituation überhaupt in den Blick zu nehmen ist – die nicht registrierten Portalnutzer.

Die der Klägerin für die Vornahme der vorgegebenen Änderungen gesetzte Frist von zwei Monaten nach Zustellung des Bescheides (Ziffer 5.) ist ebenfalls verhältnismäßig. Die Anordnungen sind technisch innerhalb dieses Zeitraums umzusetzen. Dies gilt insbesondere vor dem Hintergrund, dass es bereits einen umfangreichen Austausch über mögliche Veränderungen an dem Fahrerbewertungsportal gegeben hat.

2. Die Zwangsgeldandrohungen in Ziffer 6. des angefochtenen Bescheides sind – mit Ausnahme der zu Ziffer 2. des Bescheides erfolgten Zwangsgeldandrohung – rechtlich nicht zu beanstanden. Die Voraussetzungen der § 55 Abs. 1, 57 Abs. 1 Nr. 2, § 60, § 63 des Verwaltungsvollstreckungsgesetzes für das Land Nordrhein-Westfalen (VwVG NRW) liegen vor. Die Zwangsgeldandrohungen sind hinreichend bestimmt. Sie lassen eindeutig erkennen, dass den Handlungspflichten in Ziffer 1., 3. und 4. des angefochtenen Bescheides das jeweils angedrohte Zwangsgeld konkret zugeordnet ist. Das angedrohte Zwangsgeld ist auch jeweils der Höhe nach verhältnismäßig. Es orientiert sich an dem wirtschaftlichen Interesse der Klägerin an der Nichtbefolgung der Anordnungen, § 60 Abs. 1 Satz 2 VwVG NRW.

II. Die Klage ist hingegen begründet, soweit sie sich gegen die in Ziffer 6. enthaltene Androhung eines einheitlichen Zwangsgeldes hinsichtlich der Anordnungen in Ziffer 2. des angefochtenen Bescheides richtet. Diese Zwangsgeldandrohung ist rechtswidrig und verletzt die Klägerin in ihren Rechten, § 113 Abs. 1 Satz 1 VwGO. Sie ist nicht hinreichend bestimmt im Sinne des § 63 Abs. 5 VwVG NRW, weil ein Zwangsgeld in Höhe von 1.000 Euro pauschal für den Fall angeordnet wird, dass die Klägerin den Vorgaben in Ziffer 2. des angefochtenen Bescheides nicht fristgerecht nachkommt. In Ziffer 2. des Bescheides werden der Klägerin insgesamt sechs Handlungspflichten aufgegeben. Es ist nicht ersichtlich, ob ein Zwangsgeld in Höhe von 1000 Euro bereits bei Nichterfüllung einer einzelnen Handlungspflicht anfällt oder ob dies erst bei einem Unterlassen der Klägerin hinsichtlich sämtlicher Handlungspflichten nach Ziffer 2 des Bescheides der Fall ist.

Die Kostenentscheidung folgt aus § 155 Abs. 1 Satz 3 VwGO. Das beklagte Land ist lediglich hinsichtlich der auf Ziffer 2. des Bescheides bezogenen Zwangsgeldandrohung und damit nur zu einem geringen Teil unterlegen.

Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 167 Abs. 1 Satz 1, Abs. 2 VwGO i.V.m. § 708 Nr. 11, § 711 ZPO.

Die Berufung war gem. § 124a Abs. 1 Satz 1 VwGO zuzulassen, weil die Rechtssache grundsätzliche Bedeutung hat, § 124 Abs. 2 Nr. 3 VwGO.

# Berichte, Informationen, Sonstiges

## Bitkom: Jedes fünfte IT-Unternehmen ignoriert bislang die Datenschutz-Grundverordnung

Berlin, 16. Juni 2017 – In weniger als einem Jahr drohen IT-Unternehmen in Deutschland Millionen-Bußgelder, wenn sie die europäische Datenschutz-Grundverordnung (DSGVO) nicht umgesetzt haben. Doch immer noch gibt jedes fünfte IT- und Digitalunternehmen (19 Prozent) an, sich noch gar nicht mit dem Thema beschäftigt zu haben. Und nur jedes Dritte (34 Prozent) hat zumindest bereits erste Maßnahmen angefangen oder sogar schon umgesetzt. Vier von zehn Unternehmen (42 Prozent) beschäftigen sich aktuell mit dem Thema, haben aber noch keine Maßnahmen begonnen, und 5 Prozent wollten oder konnten keine Angaben machen. Das ist das Ergebnis einer aktuellen Umfrage unter mehr als 200 IT- und Digitalunternehmen im Auftrag des Bitkom. Im vergangenen Herbst hatten in einer Bitkom-Umfrage 32 Prozent der Unternehmen mit mehr als 20 Mitarbeitern aus allen Branchen angegeben, sich noch nicht mit der DSGVO beschäftigt zu haben, 12 Prozent war das Thema überhaupt nicht bekannt.

Mit der Verordnung werden zahlreiche neue Informations- und Dokumentationspflichten eingeführt, die von den IT-Unternehmen umgesetzt werden müssen. Völlig neu sind gesetzliche Vorgaben wie die Berücksichtigung des Datenschutzes bei der Produktentwicklung (Privacy by Design) oder die Durchführung einer Datenschutz-Folgenabschätzung. Von den IT- und Digitalunternehmen, die aktuell bereits erste Maßnahmen begonnen haben, hat jedes Dritte (31 Prozent) nach eigener Einschätzung gerade einmal höchstens 20 Prozent der notwendigen Arbeiten erledigt. „Allmählich wird die Zeit knapp, um die Vorgaben der Datenschutz-Grundverordnung umzusetzen. Die Übergangsfrist bis Mai 2018 war dafür gedacht, dass die IT-Unternehmen bis dahin die teilweise auf-

wändigen Vorarbeiten leisten können – dies setzt aber eine aktive Beschäftigung mit dem Thema voraus“, sagt Susanne Dehmel, Geschäftsleiterin Vertrauen und Sicherheit beim Digitalverband Bitkom. „IT-Unternehmen, die bis jetzt die Vorgaben der DSGVO ignoriert haben, sollten sich dringend überlegen, wie sie das Thema schnellstmöglich aufarbeiten können.“

Für den Einstieg hat Bitkom „Fragen und Antworten“ (FAQs) zur Datenschutz-Grundverordnung veröffentlicht, die einen ersten Überblick über die Veränderungen zur heutigen Rechtslage geben. Wie verschiedene Verpflichtungen aus der Verordnung praktisch umgesetzt werden können ergibt sich aus den Praxisleitfäden „Verarbeitungsverzeichnis“, „Risk Assessment und Datenschutzfolgenabschätzung“ sowie der „Mustervertragsanlage zur Auftragsverarbeitung“. Alle Leitfäden stehen auf der Bitkom Webseite zum kostenlosen Download bereit: <https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/Inhaltsseite-2.html>

*(Bitkom, Pressemitteilung vom 16.06.2017)*

## Berliner Beauftragte für Datenschutz und Informationsfreiheit: Beschneidung der Kontrollbefugnisse der Datenschutzaufsichtsbehörden nicht hinnehmbar

Am 27. April 2017 hat der Deutsche Bundestag das Datenschutz-Anpassungs- und Umsetzungsgesetz verabschiedet, mit dem das deutsche Datenschutzrecht an die Vorgaben der ab Mai 2018 geltenden EU-Datenschutz-Grundverordnung angepasst werden soll. Zentrale Forderungen der Datenschutzaufsichtsbehörden sind dabei leider weitgehend unberücksichtigt geblieben. So sind etwa die Rechte der Datenschutzaufsichtsbehörden der Länder im Europäischen Datenschutz-

ausschuss weiterhin nicht ausreichend gewahrt. Im Hinblick auf die Einschränkung von Betroffenenrechten sowie die Verarbeitung besonderer Arten personenbezogener Daten, insbesondere Gesundheitsdaten, sind zwar Anpassungen vorgenommen worden, die jedoch hinter den erhobenen Forderungen zurückbleiben.

Auch die Befugnisse der Datenschutzaufsichtsbehörden gegenüber Berufsgeheimnisträgern sollen massiv beschnitten werden. In der Praxis würde die geplante Regelung dazu führen, dass systematische Datenschutzkontrollen bei Rechtsanwälten, Notaren, Steuerberatern und Ärzten, aber auch bei den in den sozialen Berufen und Beratungsstellen tätigen Berufsgruppen wie Sozialarbeitern, Sozialpädagogen, Psychologen, Psychotherapeuten, Ehe-, Erziehungs- und Jugendberatern sowie Beratern für Suchtfragen nicht mehr wirksam erfolgen könnten bzw. sich auf rein technische Aspekte beschränken müssten. Gerade in den Tätigkeitsfeldern von Berufsgeheimnisträgern werden jedoch besonders schützenswerte und sensitive Daten wie etwa Gesundheitsdaten verarbeitet, so dass eine wirksame Kontrolle des datenschutzkonformen Umgangs mit diesen Daten im Interesse und Auftrag der betroffenen Bürgerinnen und Bürger auch und gerade in diesen Bereichen unabdingbar ist.

Der Gesetzgeber geht mit diesen Einschränkungen weit über die Befugnisse hinaus, die ihm von der EU-Datenschutz-Grundverordnung eingeräumt werden. So können hiernach Regelungen getroffen werden, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Dies darf jedoch nicht dazu führen, dass in verfassungsrechtlich bedenklicher Weise die Datenschutzaufsichtsbehörden ihre Kontrollbefugnisse nicht mehr wirksam ausüben können.

*(LfDI Berlin, Pressemitteilung vom 14. Mai 2017)*

## Aufsichtsbehörden: Datenschutz bleibt Chef- sache – Halbzeit auf dem Weg zur EU-Datenschutz- Grundverordnung: Zehn Punkte zur Umsetzung

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die bisher für Unternehmen einschlägigen Regelungen des deutschen Datenschutzrechts weitgehend durch die Verordnung ersetzt werden.

Die Aufsichtsbehörden haben in einem 10-Punkte-Papier Anregungen für Unternehmen zur Vorbereitung auf die DS-GVO zusammengestellt.

### 1. Sensibilisierung durchführen

Geschäftsführungen, Datenschutzbeauftragte und andere für das Thema Datenschutz Zuständige sollten innerhalb des Unternehmens dafür sensibilisieren, dass sich ab dem 25.05.2018 nicht nur der Name einer europäischen Datenschutzregelung ändern wird. Die DS-GVO wird direkte Auswirkungen auf Unternehmen als datenverarbeitende Stellen haben. Anders als eine EU-Richtlinie ist eine EU-Verordnung direkt in den Mitgliedstaaten der Europäischen Union anwendbar, also auch in Deutschland. Neben der DS-GVO wird es weiterhin ein – neues – Bundesdatenschutzgesetz und sektorales Fachrecht mit ausführenden Regelungen zur DS-GVO geben. Bitte beachten Sie: bis zum 24.05.2018 (einschließlich) gilt das JETZIGE Bundesdatenschutzgesetz!

### 2. Bestandsaufnahme machen

Um Änderungsbedarf identifizieren zu können, sollte in einem ersten Schritt eine Bestandsaufnahme der Prozesse durchgeführt werden, in denen personenbezogene Daten verarbeitet werden. Das Verfahrensverzeichnis nach § 4d Bundesdatenschutzgesetz (BDSG) ist ein Ausgangspunkt zur Identifizierung von Verarbeitungsverfahren. Im Folgenden haben wir beispielhaft einige Themen zusammengestellt, bei

denen sich für Unternehmen Änderungsbedarf ergeben kann.

### 3. Rechtsgrundlage prüfen

Auch unter der DS-GVO ist für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich (Artikel 6 bis 11 DS-GVO). Es ist zu prüfen, ob das neue Recht für alle Prozesse Rechtsgrundlagen bereitstellt.

### 4. Personenbezogene Daten von Kindern besonders prüfen

Besondere Anforderungen bestehen für den Umgang mit personenbezogenen Daten von Kindern, wenn es um die Einwilligung in Bezug auf Dienste der Informationsgesellschaft geht (Artikel 8 DS-GVO).

### 5. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy-by-Design“ und „Privacy-by-Default“) umsetzen

Die DS-GVO enthält bestimmte Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei Voreinstellungen umzusetzen sind (Artikel 25 DS-GVO).

### 6. Verträge checken

Unternehmen sollten insbesondere ihre bestehenden Verträge zur Auftrags(daten)verarbeitung überprüfen und überarbeiten. In den Artikeln 26 bis 28 DS-GVO sind Vorgaben für Vereinbarungen mit Auftrags(daten)verarbeitern und zwischen gemeinsam für die Verarbeitung Verantwortlichen geregelt.

### 7. Datenschutzfolgeabschätzung implementieren

Der europäische Gesetzgeber hat die bisherige Vorabkontrolle (§ 4d Abs. 5 BDSG) nicht in die DS-GVO übernommen. Sie wird abgelöst durch die Datenschutz-Folgeabschätzung (Artikel 35 DS-GVO). An eine Datenschutz-Folgeabschätzung kann sich eine verpflichtende Konsultation der zuständigen

Aufsichtsbehörde anschließen (Artikel 36 DS-GVO).

### 8. Melde- und Konsultationspflichten organisieren

Die Melde- und Konsultationspflichten gegenüber den Aufsichtsbehörden (Artikel 33, 36 und 37 DS-GVO) müssen in den internen Abläufen des Unternehmens abgebildet werden.

### 9. Betroffenenrechte und Informationspflichten umsetzen

Die in der DS-GVO geregelten Betroffenenrechte müssen in den unternehmensinternen Abläufen abgebildet und gegenüber den Betroffenen umgesetzt werden, etwa das Recht auf Löschung (Artikel 17) und das Recht auf Datenübertragbarkeit (Artikel 20) einschließlich der übergreifenden Rahmenbedingungen (Artikel 12) sowie die Informationspflichten des Verantwortlichen (Artikel 13, 14).

### 10. Dokumentation organisieren

Die DS-GVO enthält an verschiedenen Stellen Dokumentationspflichten, beispielsweise in Artikel 30 (Verarbeitungsverzeichnis), Artikel 33 Abs. 5 (Dokumentation von Datenschutzvorfällen) oder Artikel 28 Abs. 3 lit. a (Dokumentation von Weisungen im Rahmen von Auftragsverarbeitungsverhältnissen).

*(Pressemitteilung der Datenschutzkonferenz vom 24.05.2017)*

## Deutscher Bundestag: Wissenschaftlicher Dienst zur Rechtsgrundlage für den Einsatz sog. intelligenter Videoüberwachung durch die Bundespolizei (WD 3 – 3000 – 202/16)

### 1. Fragestellung

Es wird um eine kurze Einschätzung der Frage gebeten, inwieweit der Einsatz sog. intelligenter Videoüberwachungs-

systeme, mittels derer unter anderem ein Gesichtsabgleich mit polizeilichen Datenbanken möglich ist, von der Ermächtigungsgrundlage des § 27 Bundespolizeigesetz (BPolG) für den Einsatz „selbsttätiger Bildaufnahme- und Bildaufzeichnungsgeräte“ erfasst wird.

## 2. Selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte i.S.d. § 27 BPolG

### 2.1. Rechtsprechung

Die *Rechtsprechung* hat sich bisher noch nicht mit der Frage befasst, ob der Einsatz intelligenter Videoüberwachungssysteme durch die Bundespolizei auf die Ermächtigungsgrundlage des § 27 BPolG gestützt werden kann.

### 2.2. Auffassungen in der Literatur

In der *Literatur* wird die Frage zur Erreichung des § 27 BPolG auf intelligente Videoüberwachungssysteme uneinheitlich beantwortet<sup>1</sup>:

Nach *einer Ansicht* fallen unter den Anwendungsbereich der Norm auch Überwachungstechniken, die eine „intelligente Selektion“ mittels eines Abgleichs mit zuvor gespeicherten personenbezogenen Daten ermöglichen.<sup>2</sup>

Nach *anderer Ansicht* gestattet die Regelung in § 27 S. 1 BPolG nicht den Einsatz intelligenter Videoüberwachungssysteme.<sup>3</sup> Der Einsatz einer derartigen Technik sei zwar vom Wortlaut des § 27 S. 1 BPolG („Die Bundespolizei kann selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte einsetzen [...]“) gedeckt. Gegen eine Subsumtion dieser Technik unter die Norm würden aber sowohl die *Entstehungsgeschichte* als auch *verfassungsrechtliche Einwände* sprechen.

Zum einen wird auf die entsprechenden *Gesetzesmaterialien* verwiesen. Dort heißt es:

„Nach der Vorschrift darf der BGS für bestimmte Zwecke innerhalb seines Aufgabenbereichs automatische Bildaufnahme- und Bildaufzeichnungsgeräte verwenden. Diese Geräte sind an einem festen Standort installiert, und ihr Bildwinkel ist zumeist – fest oder variabel – vorgegeben, kann aber mitunter auch ferngesteuert verändert werden. Ihre Besonderheit besteht vor

allem darin, daß Bildaufnahmen nicht erst im Falle einer konkreten Gefahr und dann zielgerichtet nur von Störern gefertigt werden. Die Geräte werden vielmehr – zumeist im Dauerbetrieb – an bestimmten, abstrakt gefährdeten Gebäuden oder Anlagen, etwa im Rahmen des Objektschutzes, eingesetzt, um frühzeitig etwaige konkrete Gefahren erkennen zu können. Sie ergänzen oder ersetzen die Polizeistreife und tragen somit zur Erhöhung des Sicherheitsstandards im Rahmen bestimmter polizeilicher Aufgaben wesentlich bei.“<sup>4</sup>

Hieraus wird teilweise abgeleitet, dass der *Gesetzgeber* bei selbsttätigen Geräten zur Bildaufnahme und Bildaufzeichnung *allein an eine automatische Aufzeichnung im Dauerbetrieb gedacht* habe.<sup>5</sup> Ein *differenzierender Ansatz* weist darauf hin, dass es dem Gesetzgeber unmöglich sei, technische Entwicklungen präzise vorherzusagen und Normen dementsprechend offen zu formulieren.<sup>6</sup> Hieraus könne aber nicht geschlossen werden, dass die Normen auf den Stand von Technik und Wissenschaft im Zeitpunkt der Gesetzgebung festgelegt seien. Technische Weiterentwicklungen wie leistungsstärkere Kameras oder vernetzte Überwachungssysteme müssten demnach vom Gesetzeswortlaut gedeckt bleiben. Dies gelte aber nicht für ein *ganz anderes Auswertungsinstrument*. Ein solches aliud stelle jedoch die automatisierte Auswertung gegenüber der visuellen Auswertung dar. Für den Einsatz eines derartigen Instruments bedürfe es zuerst der gesetzgeberischen Entscheidung und der entsprechenden Ergänzung der Rechtsgrundlagen.<sup>7</sup>

Hinsichtlich der Frage der Geltung von bestehenden Ermächtigungsgrundlagen für technische Neuerungen werden teilweise auch – jedoch nicht explizit in Bezug auf das Bundespolizeigesetz – die *Grenzen der Normenklarheit* problematisiert.<sup>8</sup> Nach dem Rechtsstaatsprinzip müssten die Voraussetzungen und Rechtsfolgen so formuliert sein, dass die Betroffenen die Rechtslage erkennen und ihr Verhalten danach einrichten könnten.

Ferner wird auf *verfassungsrechtliche Probleme* verwiesen, die vom Gesetz-

geber nicht bedacht worden seien.<sup>9</sup> Dabei steht jedoch weniger die Verwendung intelligenter Videoüberwachungssysteme zum Zwecke des Abgleichs mit polizeilichen Datenbanken als die Selektion verdächtiger Verhaltensweisen und bestimmter äußerer Erscheinungsmerkmale im Vordergrund. Jedoch wird auch in Hinblick auf den Abgleich mit Fahndungsdatenbanken von einem zusätzlichen und vertieften Grundrechtseingriff gesprochen.<sup>10</sup> Als Vorschlag zur grundrechtsschonenden Gestaltung von intelligenten Videoüberwachungssystemen wurde von Stimmen in der Literatur ein Drei-Stufen-Modell entwickelt, dass zwischen einer allgemeinen beobachtenden Überwachung (1. Stufe), einer gezielten Personenüberwachung (2. Stufe) und einer Personenerkennung (3. Stufe) differenziert.<sup>11</sup>

1 Teilweise wird diese Frage in der Kommentarliteratur auch gar nicht behandelt, siehe etwa Hoppe, in: Heesen/Hönl/Peilert/Martens (Hrsg.), Bundespolizeigesetz, Kommentar, 5. Aufl. 2012, § 27 Rn. 35 ff.

2 Drewes, in: ders./Malmberg/Walter, Bundespolizeigesetz, Kommentar, 5. Aufl. 2015, § 27 Rn. 4; von Zezschwitz, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 9.3 Rn. 41, in Bezug auf die Vorgängerregelung im Bundesgrenzschutzgesetz.

3 Schenke, in: ders./Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 27 BPolG Rn. 18.

4 BR-Drs. 418/94, S. 59.

5 Schenke, in: ders./Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 27 BPolG Rn. 18.

6 Held, Intelligente Videoüberwachung. Verfassungsrechtliche Vorgaben für den polizeilichen Einsatz, 2013, S. 187.

7 Siehe zur Frage, inwieweit neue technische Überwachungsmittel auf bereits vorhandene Ermächtigungsgrundlagen gestützt werden können, auch BVerfGE 112, 304 ff.

8 Hornung/Desoi, „Smart Cameras“ und automatische Verhaltensanalyse, K&R 2011, S. 153 (155 f.).

9 Schenke, in: ders./Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 27 BPolG Rn. 18. Ausführlich zur Verfassungsmäßigkeit der intelligenten Videoüberwachung Held, Intelligente Videoüberwachung. Verfassungsrechtliche Vorgaben für den polizeilichen Einsatz, 2013, S. 63 ff.; siehe auch Schenke, Videoüberwachung 2.0 auf dem Prüfstein des Grundgesetzes, in: Zöller/Hilger/Küper/Roxin (Hrsg.), Gesamte Strafrechtswissenschaft in internationaler Dimension, Festschrift für Jürgen Wolter, 2013, S. 1077 (1080 ff.).

10 Hornung/Desoi, „Smart Cameras“ und automatische Verhaltensanalyse, K&R 2011, S. 153 (155).

11 Roßnagel/Desoi/Hornung, Gestufte Kontrolle bei Videoüberwachungsanlagen, DuD 2011, S. 694 ff.

# Literaturhinweise

*Kranig/Sachs/Gierschmann, **Datenschutz-Compliance nach der DS-GVO – Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden**, Bundesanzeiger Verlag, Köln, 2017, 230 S., broschiert, 44,- €.*

Vor dem Hintergrund ihrer langjährigen Erfahrungen aus Datenschutzaufsicht und Datenschutzberatung werfen die drei Autoren einen pragmatischen und prozessorientierten Blick auf die Umsetzungsmechanik der DSGVO. Die Veröffentlichung gibt Anwendern, Verantwortlichen für die Verarbeitung personenbezogener Daten und insbesondere ihren Datenschutzbeauftragten oder weiteren mit der Wahrnehmung von Datenschutzumsetzungsmaßnahmen betrauten Funktionen eine hilfreiche Orientierung auf dem Weg zur Datenschutz-Compliance. Die Handlungshilfe zeichnet sich dabei insbesondere dadurch aus, dass sie ihren Schwerpunkt bewusst nicht in der zum gegenwärtigen Zeitpunkt noch gar nicht vollumfänglich möglichen Rechtsauslegung der DSGVO setzt. Vielmehr sieht sie sich als Anleitung zur Verfahrensimpementierung und -verbesserung, die letztlich die Reaktionsfähigkeit herstellt, welche zur Umsetzung der Anforderungen der DSGVO aber darüber hinaus auch weiterer gegenwärtiger oder zukünftiger Anforderungen an den Datenschutz unabdingbar ist. Datenschutzmanagement wird dabei als interdisziplinäre Aufgabe unter Einbeziehung verschiedenster Funktionen verstanden.

Nach einer kurzen Einführung zu den wesentlichen Anforderungen der DSGVO und insbesondere der Bedeutung der neu eingeführten Rechenschaftspflicht („Accountability“) gliedert sich die Veröffentlichung in die Bereiche Sicherstellung der Datenschutz-Compliance und Überwachung der Datenschutz-Compliance.

Der Themenblock Sicherstellung der Datenschutz-Compliance bildet dabei den inhaltlichen Schwerpunkt. Neben

einer ausführlichen Betrachtung der Kernprozesse („Datenschutzkonforme Datenverarbeitung“, „Sicherstellung der Betroffenenrechte“ und „Handhabung von Datenschutzverletzungen“), werden die Datenschutzorganisation, das Datenschutz-Risikomanagement, die Datenschutzdokumentation, sowie Datenschutzensensibilisierung und auch die Datenschutzzertifizierung dargestellt. Die anschließenden Ausführungen zu den Inhalten eines Datenschutz-Managementsystems runden das Bild ab.

Im Abschnitt Überwachung der Datenschutz-Compliance werden über umfangreiche Prüflinien wertvolle Anhaltspunkte geliefert, wie eine Aufsichtsbehörde die Einhaltung der Datenschutz-Compliance prüft. Der Leser erhält hierdurch einen guten Einblick in den Erwartungshorizont, welchem Verantwortliche im Rahmen einer Prüfung gegenüberstehen.

Alle Abschnitte und Themenbereiche sind konsequent an der Methodik der kontinuierlichen Prozessverbesserung, d.h. nach dem Plan-Do-Check-Act-Ansatz, ausgerichtet und beschrieben. Den Verfassern gelingt es zudem in herausragender Weise mittels vielfältiger und einprägsamer Grafiken, Übersichten und Schemata die Inhalte einzelner Themenabschnitte schnell und eingängig zusammen zu fassen und auch für ggf. weitere innerbetriebliche Kommunikationsmaßnahmen verwendbar zu machen.

Die Handlungshilfe ist insgesamt als eine empfehlenswerte Darstellung der Grundstrukturen eines DSGVO-gerechten, aber auch insgesamt zeitgemäßen Datenschutzmanagements zu bewerten, die jedem Praktiker wertvolle Unterstützung leistet.

*(Gabriela Krader, LL.M)*

*Elisa Stettner, **Sicherheit am Bahnhof – Überwachungsmaßnahmen zur Abwehr terroristischer Anschläge**. Das*

Recht der inneren und äußeren Sicherheit, Band 7, Duncker & Humblot, Berlin, 2017, 310 S., Print: 89,90 €, E-Book: 79,90 €, Print & E-Book 107,90 €.

Die Abwehr terroristischer Anschläge ist ein hochaktuelles und praxisrelevantes Thema. Vor allem durch den Einsatz neuartiger Technologien soll die Gefahr bereits vor ihrer Entstehung erkannt und der potentielle Schaden verhindert werden. In dieser Arbeit werden ausgewählte Sicherheitsmaßnahmen des Gefahrenvorfelds gegen terroristische Anschläge auf Bahnhöfe auf ihre Vereinbarkeit mit den Grundrechten und den gesetzlichen Vorgaben geprüft. Gegenstand der Untersuchung sind die klassische Videoüberwachung, die Kennzeichenerfassung, die intelligente Videoüberwachung und der Einsatz von Drohnen, Körperscannern und sonstigen abstandsfähigen Detektoren. Obwohl die neuen technischen Möglichkeiten oft zum Datenschutz beitragen, sind die bestehenden Rechtsgrundlagen im Ergebnis in den meisten Fällen für den Einsatz von neuen Technologien nicht hinreichend bestimmt und unverhältnismäßig. Vor diesem Grund hat die Autorin auf der Basis ihrer Untersuchungsergebnisse Rechtsgrundlagen entwickelt, die einen Einsatz in diesen Fällen ermöglichen.

*(RDV-Redaktion)*

*Florian Eisenmenger, **Die Grundrechtsrelevanz „virtueller Streifenfahrten“ – dargestellt am Beispiel ausgewählter Kommunikationsdienste des Internets**, Strafrechtliche Abhandlungen, Neue Folge, Band 276, Duncker & Humblot, Berlin, 2017, 377 S., Print: 89,90 €, E-Book: 79,90 €, Print & E-Book: 107,90 €.*

Die Arbeit befasst sich mit einer seit rund 20 Jahren praktizierten polizeilichen Maßnahme im virtuellen Raum, die dem anlassunabhängigen Auffin-

den strafrechtlich relevanter Inhalte dient. Der Autor konzentriert sich auf die Vereinbarkeit dieser Maßnahme mit den Vorgaben des geltenden Strafprozessrechts und der verfassungsrechtlichen Zulässigkeit verdachtsunabhängiger Ermittlungstätigkeit im Netz. Den Fokus richtet er dabei auf verschiedene Kommunikationsdienste des Internets und untersucht, wie die gewandelte Bedeutung des World Wide Webs als Medium sozialer Interaktion die rechtliche Bewertung der polizeilichen Aufklärungstätigkeit beeinflusst. Er kommt zu dem Ergebnis, dass die »virtuelle Streifenfahrt« im Lichte der Kommunikationskultur der sozialen Medien und des Web 2.0 einen Grundrechtseingriff darstellen kann und insoweit einer klaren, noch zu schaffenden Rechtsgrundlage bedarf, da die derzeit praktizierte Form erhebliche Zweifel an ihrer Rechtmäßigkeit aufwirft.

*(Schriftleitung)*

*Peter Gola (Hrsg.), DS-GVO – Datenschutz-Grundverordnung VO (EU)*

**2016/679**, Kommentar, C.H. Beck, München, 2017, 835 S., 79,- €.

„Die DS-GVO ändert die Konzeption und weitgehend auch die Detailregelungen des geltenden Datenschutzes nicht grundlegend“, schreibt Gola zutreffend am Ende seiner Einleitung (Rdn. 71) des von ihm herausgegebenen und in der bekannten „gelben Reihe“ des Beck-Verlags erschienenen Kommentars. Umso erstaunlicher ist die hohe Zahl kürzlich in rasanter Folge erschienener Erläuterungswerke zu der EU-Verordnung 2016/679 und die Flut von Seminarangeboten zum „neuen Datenschutzrecht“, die das Gegenteil dieser Feststellung nahe zu legen scheinen.

Sicherlich, eine ganze Reihe neuer europäischer Anweisungen nimmt die datenverarbeitenden Stellen künftig zusätzlich in die Pflicht, als in den Grundfesten erschüttert kann das jedenfalls in Deutschland geltende Datenschutzregime aber wahrlich nicht betrachtet werden. So verwundert es auch nicht, dass die Kommentierung der DS-GVO an vielen verschiedenen Stellen an die Erläuterungen im Gola'schen BDSG-Kom-

mentar (12. Aufl.) anknüpft. Die – neben dem Herausgeber weiteren – 11 Mitarbeiter teilen sich Artikel-bezogen die Arbeit und befassen sich überwiegend mit solchen Bestimmungen, für die es bislang keine identische Vorgängerregelung im BDSG gab. Dies geschieht in prägnanter, wenngleich bisweilen etwas sehr knapper Weise, vermittelt wird aber in jedem Fall ein hervorragender Einstieg in die jeweilige Norm. Manche „Konkurrenzwerke“ mögen sich durch vertiefende Ausführungen auszeichnen und damit eine stärkere akademisch-dogmatische Ausrichtung aufweisen, demjenigen jedoch, der im Tagesgeschäft schnellen und fundierten praktischen Rat benötigt, bietet dieser Kommentar zuverlässige Soforthilfe.

Der „neue Gola“ hat sich trotz des erweiterten Autorenteam die Qualitäten des „alten (BDSG-) Gola“ bewahrt: die gute Lesbarkeit, den schnörkellosen Informationstransfer zum Leser, die Handlichkeit des Formats und den bemerkenswert günstigen Preis. Kurzum: Ein überaus empfehlenswerter Kauf.

*(Rechtsanwalt Dr. Georg Wronka, Bonn)*

## Neuerscheinungen

### Aufsätze

Die RDV weist regelmäßig auch auf in anderen Zeitschriften erschienene Beiträge zum Recht der Datenverarbeitung hin, um Recherchen zu relevanten Themen zu erleichtern. Einreichungen von Beiträgen zur Aufnahme eines Hinweises werden gerne entgegengenommen.

*Baumgartner, Ulrich/Gausling, Tina, **Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen**, ZD 2017, S. 308*

Die Autoren zeigen auf, was die Unternehmen insoweit nach der neuen DS-GVO zu beachten haben.

*Eichendorfer, Johannes, **Vom Zweckbindungsgrundsatz zur Interessenabwägung?**, PinG 2017, S. 135*

Ob der Zweckbindungsgrundsatz im Zeitalter von Big Data kontrafaktisch ist, wird von dem Autor beleuchtet, mit dem Ergebnis, dass sich durch das neue BDSG der Zweckbindungsgrundsatz im deutschen Recht auf dem Rückzug befindet, indem er durch weitreichende Zweckänderungsbefugnisse ausgehöhlt wird.

*Gelsdorf, Hubertus, **Hate Speech in sozialen Netzwerken**; MMR 2017, S. 439*

Der Beitrag hat Aktualität angesichts der diesbezüglich laufenden Gesetzgebung, die er bewertet.

*Gola, Peter, **Der neue Beschäftigtendatenschutz nach § 26 BDSG n.F.**, BB 2017, S. 1462*

Der Beitrag liefert eine ausführliche Kommentierung der neuen bereichsspezifischen Vorschriften des Beschäftigtendatenschutzes im BDSG n.F. Insbesondere werden die noch nicht in § 32 BDSG a.F. enthaltenen Zulässigkeitsregelungen bzw. klarstellenden Hinweise behandelt.

*Herber, Torben J./Jentsch, Marc/Zickau, Sebastian, **Datenschutz und Dopingkontrollen**, DuD 2017, S. 427*

Athleten im Spitzensport können nur durch Duldung massiver Eingriffe in ihre Privatsphäre beweisen, dass sie sauberen Sport betreiben. Der Beitrag untersucht, ob Privacy-Enhancing-Technologies (PETs) zu mehr Privatsphäre verhelfen können

*Kort, Michael, **Der Beschäftigtendatenschutz nach § 26 BDSG-neu**, ZD 2017, S. 319*

Der Autor greift einige Aspekte des § 26 BDSG n.F. auf und kommt zu dem Ergebnis, dass § 26 n.F. eine zulässige und cum grano salis sinnvolle Neuregelung des Beschäftigtendatenschutzes ist, die jedoch weiterhin ergänzt wird durch die nicht berührten Vorschriften des DS-GVO, was u.a. für die in § 26 BDSG n.F. nicht angesprochenen Transparenzregelungen gilt.

*Michl, Walther, **Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht**, DuD 2017, S. 349*

Der Autor geht der Frage nach, ob es berechtigt ist, die Grundrechte auf Privatsphäre und Datenschutz bei der Grenzziehung die Digitalisierung nebeneinander zu prüfen, und kommt zu dem Ergebnis, dass das Datenschutzgrundrecht des Art. 8 ein hervorgehobener Teilaspekt des Rechts auf Achtung der Privatsphäre ist, und zeigt, dass die Charta das Thema Digitalisierung ausdrücklich – ggf. in Detailregelungen – adressiert.

*Schwab, Brent, **Betriebsgeheimnisse – Neues aus Brüssel**, CuA 6/2017, S. 32*

Die neue Richtlinie der EU zum Schutz von Geschäftsgeheimnissen enthält auch eine weite Whistleblowerregelung. Sie muss bis Mitte 2018 in nationales Recht umgesetzt werden. Der Beitrag schildert die wesentlichen Regelungen.

*Volkmar, Christian/Kaiser, Ingo, **Das Verzeichnis von Verarbeitungstätigkeiten und die Datenschutzfolgeabschätzung in der Praxis**. PinG 2017, S. 151*

Die Autoren geben eine kurze Zusammenfassung der beiden Datenschutzpflichten des Unternehmens und ihres Zusammenspiels.



Personenoptimierung für das Internet

## Bildgeschichten werden mobil

Wer mit jemandem – Freund oder Fremder – seine Handynummer austauscht, der ist mit ihm häufig über WhatsApp verbunden. Mit der Nummer bekommt man über die Profilbilder Einblicke in das Leben der WhatsApp-Kontakte. Die meisten wählen diese Bilder mit Bedacht aus. Sie sind oft Statements und erzählen manchmal ganze Geschichten. Wie eitel ist man, wie verliebt, wie ausgelassen, oder wie stolz machen einen die Kinder, der Hund oder der Lieblingsverein. Wo macht man gerade Urlaub oder was isst man gerne. Hinzu kommt oft ein Status: vielleicht ein Emoji oder ein Zitat. Manche der Profilbildgeschichten findet man gerade deshalb lustig oder peinlich, weil man die Personen hinter dem Bild kennt. Bilder von Kontakten, die man kaum kennt, wie

Handwerker, Lehrer der Kinder oder Kollegen drängen einem häufig mehr Privatsphäre auf, als ein Handytelefonat des Sitznachbarn im Zugabteil. Weil Profile persönliche Informationen enthalten können, kann man in den Datenschutzeinstellungen auswählen, wer das Bild sehen darf: „Jeder/Meine Kontakte/Niemand“ stehen zur Wahl. Wem man sich in welcher Weise zeigt, entscheidet man besser bewusst. Man wird schließlich von vielen gesehen und jeder Kontakt kann jedes Profilbild speichern und verwenden. Gut ist alles, was einem niemals gegenüber niemandem unangenehm werden kann.

Bilder erzählen Geschichten aber nicht nur bei WhatsApp, sondern auch bei Facebook. Dort beschränken sie sich nicht auf Momentaufnahmen in den Profilen, sondern sie spiegeln lange

Zeitfolgen wider. Vom Essen bis zu Frisuren findet man fast alles. Die Fotos bei Facebook & Co. kann man wandern lassen, wenn die Datenschutz-Grundverordnung erst einmal wirkt. Dafür gibt es dann die Datenportabilität, nach der man bei Unternehmen eingebrachte Inhalte in einem gängigen Format an sich selbst oder an ein anderes Unternehmen herausverlangen kann. Gute Nachrichten also für jeden, der mit seinem Essen und allem was er über die Jahre bei Facebook gepostet hat, zu Instagram umziehen möchte.



# Best Practice. Best Command.



**Neues Muster  
Social Media  
Guidelines**

Redeker (Hrsg.),  
**Handbuch der IT-Verträge**  
Herausgegeben von RA, FA IT-Recht, Dipl.-  
Informatiker Dr. Helmut Redeker.  
Loseblatt, zzt. 5.220 Seiten, 3 Bände.  
Grundwerk mit Fortsetzungsbezug für  
mindestens 2 Jahre, ca. 2 Ergänzungs-  
lieferungen pro Jahr, nur 159,- €,  
ISBN 978-3-504-56008-9.  
Ohne Abonnement 299,- €,  
ISBN 978-3-504-56027-0.

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.

**In der August-Lieferung 2017 u.a. aktualisiert:**

- Kauf einer EDV-Anlage (Standardhardware und -software)
- Arbeitsgemeinschaft und Kooperation für Softwareentwicklung

**Neu:** Social Media Guidelines

Ausführliche Informationen, Bestellung und Leseprobe unter  
[www.otto-schmidt.de/riv](http://www.otto-schmidt.de/riv)



Online im  
juris Partner Modul IT-Recht.  
Jetzt testen!

**otto schmidt**