ISSN 0178-8930

G 20 141

RDV

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

5/2018

Recht der Datenverarbeitung

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

Aufsätze

KRANIG, DS-GVO – und was die Aufsichtsbehörden daraus machen (sollten)

SCHWARTMANN/JACQUEMAIN, Datenschutzrechtliche Herausforderungen im Auto – neue Risiken durch „Connected Cars"

SCHWARTMANN/HERMANN/MÜHLENBECK, Die Veröffentlichung des Entzuges von Doktorgraden und der Datenschutz

Kurzbeiträge

GOLA, Aus den aktuellen Berichten der Aufsichtsbehörden (37): Der DSB nach DS-GVO und neuem nationalem Datenschutzrecht

LEPPERHOFF/ERMOLA, Kandidatensuche in berufsorientierten sozialen Netzwerken – Rechtsgrundlage und Pflichten

Rechtsprechung

Aus dem Inhalt

EUGH, Gemeinsame Verantwortlichkeit beim Betrieb einer Facebook-Fanpage (Ls)

EUGH (Große Kammer), Dateigebundende Datenverarbeitung bei Datenerhebung im Rahmen des Verkündungsauftrags von Religionsgemeinschaften – Zeugen Jehovas (Ls)

BGH, Facebook-Nutzerkonto ist vererbbar

BGH, E-Mail-Zufriedenheitsbefragung als unzumutbare Belästigung (Ls)

BGH, Keine Funktion als Syndikusanwalt für als externer DSB tätigen angestellten Unternehmensjuristen (Ls)

BGH, Zur Herausgabe der Handakte eines Mandanten durch den Rechtsanwalt

34. Jahrgang
August 2018
Seiten 183–240

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

29

Privacysoft ist eine Marke von Projekt 29 GmbH & Co. KG

PRIVACYSOFT

Die modulare Software-Plattform für alle Aufgaben im Datenschutzmanagement.

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

Datenschutzdokumentation | Vorlagen und Checklisten | Vorgangsmanagement | Online-Schulungen

itsa 2018
Die IT-Security Messe und Kongress
Nürnberg, 09.-11. Oktober 2018
Besuchen Sie uns in Halle 9 am Stand 639

Projekt 29 GmbH & Co. KG | Ostengasse 14 | 93047 Regensburg | www.privacysoft.de

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht

34. Jahrgang 2018
Heft 5
Seiten 241–294

RDV
Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 241

Veranstaltungen 242

Aufsätze

Thomas KRANIG
DS-GVO – und was die Aufsichtsbehörden daraus machen (sollten) 243

Professor Dr. Rolf SCHWARTMANN/Dr. Tobias JACQUEMAIN
Datenschutzrechtliche Herausforderungen im Auto – neue Risiken durch „Connected Cars" 247

Professor Dr. Rolf SCHWARTMANN/Maximilian HERMANN/Robin MÜHLENBECK
Die Veröffentlichung des Entzuges von Doktorgraden und der Datenschutz 252

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten der Aufsichtsbehörden (37): Der DSB nach DS-GVO und neuem nationalem Datenschutzrecht 257

Dr. Niels LEPPERHOFF/Tatjana ERMOLA
Kandidatensuche in berufsorientierten sozialen Netzwerken – Rechtsgrundlage und Pflichten 260

Rechtsprechung

Gemeinsame Verantwortlichkeit beim Betrieb einer Facebook-Fanpage (Ls)
(EUGH, Urteil vom 05.06.2018) 263

Dateigebundende Datenverarbeitung bei Datenerhebung im Rahmen des Verkündungsauftrags von Religionsgemeinschaften – Zeugen Jehovas (Ls)
(EUGH (Große Kammer), Urteil vom 10.07.2018) 263

Facebook-Nutzerkonto ist vererbbar
(BGH, Urteil vom 12.07.2018) 263

E-Mail-Zufriedenheitsbefragung als unzumutbare Belästigung (Ls)
(BGH, Urteil vom 10.07.2018) 274

Keine Funktion als Syndikusanwalt für als externer DSB tätigen angestellten Unternehmensjuristen (Ls)
(BGH, Urteil vom 02.07.2018) 274

Zur Herausgabe der Handakte eines Mandanten durch den Rechtsanwalt
(BGH, Urteil vom 17.05.2018) 274

Zur Prüfungspflicht des Betreibers einer Internet-Suchmaschine bei Persönlichkeitsrechtsverletzungen
(BGH, Urteil vom 27.02.2018) 276

Zum Auskunftsanspruch des Betriebsrats über die von der Konzernmutter gewährten Aktienoptionen und Nachzugsaktien (Ls)
(BAG, Beschluss vom 20.03.2018) 283

Unterlassungsanspruch bei Herstellung eines Fotos
(OLG Dresden, Urteil vom 10.07.2018) 284

DS-GVO und Bildberichterstattung – Das Kunsturhebergesetz (KUG) findet auch unter Geltung der DS-GVO Anwendung
(OLG Köln, Beschluss vom 18.06.2018) 285

Zum Anspruch der Mutter und des Kindes auf Auskunft über Samenspender (Ls)
(OLG Hamm, Urteil vom 19.02.2018) 286

Fristlose Kündigung wegen ausländerfeindlicher Facebook-Veröffentlichung (Ls)
(LAG Sachsen, Urteil vom 27.02.2018) 287

Verarbeitung sensitiver Daten bei Medikamentenvertrieb im Internet (Ls)
(LG Dessau-Roßlau, Urteil vom 28.03.2018) 287

Berichte, Informationen, Sonstiges

Bitkom: Jeder zweite Social-Media-Nutzer kann Werbung von Inhalt nur schwer unterscheiden 288

Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für einen kindgerechten Datenschutz im Umgang mit digitalen Medienangeboten 288

Gesetzesentwurf für das 2. DS-AnPUG liegt vor 289

Beschluss der DSK zu Facebook Fanpages 289

Literaturhinweise

Buchbesprechungen

Silke Jandt/Roland Steidle, Datenschutz im Internet, Rechtshandbuch zu DS-GVO und BDSG
(SCHRIFTLEITUNG) 290

Gernot Sydow, Europäische DS-GVO
(SCHRIFTLEITUNG) 290

Paul Voigt/Axel von dem Busche, EU-DS-GVO
(SCHRIFTLEITUNG) 291

Sebastian Rogge, Die Zukunft der Netzneutralität im Internet
(REDAKTION) 291

Stefan Bucher, Sachqualität und Veräußerung von Dateien – Der Online-Handel mit E-Books, Musik- und Filmdateien
(REDAKTION) 291

Neuerscheinungen

Aufsätze 293

Nachgefasst 294

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

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

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

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

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

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

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

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

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

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

Prof. Dr. Karl LINNENKOHL, Universität Kassel

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. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 5/2018; DATAKONTEXT, Frechen, Tagnungsbericht 41. DAFTA

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

Vertrieb:
Jürgen Weiß
Telefon: (02234) 989 49-71
weiss@datakontext.com

Abo-Service:
Telefon: 089-2183-7110
Telefax: 089-2183-32
aboservice@hjr-verlag.de

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
Wolfgang Scharf
Telefon: (0221) 25 08-60 71
wolfgang.scharf@agentur-8020.de
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Zeitschrift für
Datenschutz–, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
34. Jahrgang 2018 Heft 5
Seiten 241–294

RDV
Recht der Datenverarbeitung

34. Jahrgang · Oktober 2018 · Seiten 241–294

Editorial

Der Datenschutz braucht den betrieblichen Datenschutzbeauftragten

Anfang September 2018 hat die Bundesregierung den Entwurf eines zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 beschlossen. Das 2. DSAnpUG ist ein sog. „Omnibusgesetz", das Detailfragen im Bereich des Datenschutzrechts an die DS-GVO anpasst. So gesehen ist das Gesetz für den betrieblichen Datenschutz wenig spektakulär. Allerdings wird es derzeit im parlamentarischen Raum diskutiert und es kann auch aus politischen Gründen geändert werden. Geht es etwa nach dem Bitkom, dann gibt es auch beim betrieblichen Datenschutzbeauftragten Anpassungsbedarf. In einer Stellungnahme aus dem Juli 2018 fordert der Internetwirtschaftsverband etwa die Anpassung des Schwellenwertes von mindestens zehn ständig mit automatisierter Datenverarbeitung befassten Beschäftigten auf 250. Die Anzahl dieser Unternehmen ist nur gering. Es käme dann, wie in der DS-GVO vorgesehen, darauf an, ob die Kerntätigkeit in der Überwachung von Personen besteht oder ob sensible Daten verarbeitet werden. In Berlin wird auch diskutiert, den Schwellenwert auf 15, 20 oder 50 ständig mit automatisierter Datenverarbeitung beschäftigte Mitarbeiter anzuheben.

Auf diese Weise will man den Unternehmen helfen, „Bürokratie abzubauen". Dieser Schritt wäre fatal. In der unternehmerischen Praxis wird die Abschaffung des Datenschutzbeauftragten faktisch mit der Abschaffung des Datenschutzes gleichgesetzt. Davon kann natürlich keine Rede sein. Vielmehr würde der in der Verantwortung stehende Unternehmer als Verantwortlicher unmittelbar die komplexer gewordenen Interessen des Datenschutzes vertreten müssen. Dazu fehlt der Unternehmensleitung aber die Zeit und im Regelfall die Kompetenz. Mit der Vernachlässigung der datenschutzrechtlichen Pflichten erhöht sich das Bußgeldrisiko beträchtlich. Betrachtet man die Beschäftigtenzahlen, so beschäftigt der weit überwiegende Anteil deutscher Unternehmen ohnehin weniger als zehn Mitarbeiter und kommt ohne Datenschutzbeauftragten aus. Mit einer Anhebung des Wertes auf 20 würde die Zahl der Datenschutzbeauftragten in der Praxis deutlich reduziert und der Datenschutz geschwächt werden.

Weil sich der Datenschutzbeauftragte in vielen Jahren bewährt hat, ist der Gesetzgeber gut beraten, es bei der bewährten Bestellgrenze zu belassen. Um Missverständnissen etwa bei der Frage entgegenzuwirken, ob Friseure und Bäcker oder örtliche Tennisvereine auch unter der Bestellpflicht fallen, könnte der Gesetzgeber erwägen, den Begriff der ständigen Befassung zu überdenken und stattdessen den Begriff der Kerntätigkeit aus der DS-GVO aufzugreifen.

Zeitlich könnte das Gesetz noch in diesem Jahr verabschiedet werden. Will man es nicht in das Jahr 2019 verschieben, dann richtet sich der Terminplan für das Gesetz, dem der Bundesrat zustimmen muss, nach dessen Sitzungsplan. Wenn es schnell geht, dann können die nötigen drei Lesungen im Bundestag noch im November 2018 stattfinden, anderenfalls Mitte Dezember. Der Bundesrat könnte dann in seiner letzten Sitzung 2018 am 14. Dezember entscheiden. Danach tagt er erst wieder Mitte Februar 2019.

Professor Dr. Rolf Schwartmann

Prof. Dr. Rolf Schwartmann
Kölner Forschungsstelle für Medienrecht der Technischen Hochschule Köln, Mitherausgeber von Recht der Datenverarbeitung (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

Termin	Thema	Ort	Kontakt
26.11.2018	Medizinischer Datenschutz – unter den Bedingungen der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
27.11.2018	Compliance Tests und Schwachstellenscannen	Köln	GDD e.V. und DATAKONTEXT
29.11.2018	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Frankfurt/M.	GDD e.V. und DATAKONTEXT
29.11.2018	DS-GVO – Erfolgreich im Unternehmen umsetzen	Köln	GDD e.V. und DATAKONTEXT
26.-30.11.2018	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
03.12.2018	Der neue Kundendatenschutz: Kunden datenschutzkonform gewinnen und binden	Köln	GDD e.V. und DATAKONTEXT
03.-04.12.2018	Update-Workshop zur DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
04.12.2018	DS-GVO-konforme Prüfung personenbezogener Daten mit SAP-Systemen	Köln	GDD e.V. und DATAKONTEXT
05.12.2018	Hacker-Tools für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
10.12.2018	Löschen nach DS-GVO	Köln	GDD e.V. und DATAKONTEXT
10.-11.12.2018	Datenschutz-Management – Teil 3	Köln	GDD e.V. und DATAKONTEXT
09.01.2019	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
22.01.2019	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V. und DATAKONTEXT
28.-29.01.2019	GDD-Winter-Workshop	Garmisch-Partenkirchen	GDD e.V. und DATAKONTEXT
12.-13.02.2019	Update-Workshop zur DS-GVO	Köln	GDD e.V. und DATAKONTEXT
12.-13.02.2019	Update-Workshop zur DS-GVO	Köln	GDD e.V. und DATAKONTEXT
19.02.2019	DS-GVO-konforme Prüfung personenbezogener Daten mit SAP-Systemen	Köln	GDD e.V. und DATAKONTEXT
18.-22.02.2019	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
25.02.2019	Datenschutz-Bußgeldrisiken schnell und effizient identifizieren	Köln	GDD e.V. und DATAKONTEXT
12.03.2019	ISO 27001 und Datenschutz	Stuttgart	GDD e.V. und DATAKONTEXT
19.03.2019	Beschäftigtendatenverarbeitung nach DS-GVO und BDSG 2018	Frankfurt/M.	GDD e.V. und DATAKONTEXT
19.03.2019	Dokumentation, Meldepflichten und IT-Sicherheitsmanagement nach der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
18.-20.03.2019	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Köln	GDD e.V. und DATAKONTEXT
20.03.2019	Datenlöschung und andere SAP-Funktionen für den Datenschutz	Köln	GDD e.V. und DATAKONTEXT
21.03.2019	Big Data-Analysen nach DS-GVO und BDSG neu	Düsseldorf	GDD e.V. und DATAKONTEXT

DATAKONTEXT GmbH, Telefon: 0 22 34/9 89 49 40

Aufsätze

Thomas Kranig

DS-GVO – und was die Aufsichtsbehörden daraus machen (sollten)

Die Datenschutz-Grundverordnung (DS-GVO) ist seit mehr als zwei Jahren in Kraft und seit dem 25. Mai 2018 anwendbar. Eine nicht wirklich neue Erkenntnis. Nicht wirklich neu ist auch die Erkenntnis, dass auch die Aufsichtsbehörden sich sehr schwer damit tun, die Anforderungen wahrzunehmen und – möglichst einheitlich – zu realisieren, die sie selbst betreffen,[1] und auch die Richtung abzustecken und vorzugeben, die in Zukunft Grundlage von Beratungen und insbesondere auch Kontrollen sein wird. Wenn man einen Blick auf den Rechtszustand vor dem 25. Mai 2018 in Europa wirft, ist festzustellen, dass trotz wiederholter Äußerungen des EuGH, dass auch schon die Datenschutzrichtlinie von 1995 eine harmonisierende Bedeutung gehabt habe[2], eine sehr unterschiedliche Datenschutzkultur, Rechtslage und Rechtsverständnis und nicht zuletzt auch ein sehr unterschiedlicher Vollzug in Datenschutzrecht bestanden haben. Davon ausgehend könnte man zu der Auffassung gelangen, dass die Aufsichtsbehörden nun schon eine Menge Arbeit geleistet haben, selbst wenn das nur einen kleinen Bruchteil davon darstellt, was noch zu leisten sein wird.

I. Bemühungen der Europäischen Aufsichtsbehörden um ein einheitliches Verständnis der DS-GVO

Das neue Europäische Datenschutzrecht in Form einer Verordnung zwingt die unabhängigen Aufsichtsbehörden, sich um ein einheitliches Verständnis über das geltende Recht zu bemühen und einen einheitlichen Vollzug sicherzustellen. Dies hat schon früher die Art.-29-Gruppe insbesondere durch die Veröffentlichungen von Working Papers angestrebt. Den Weg hat der nun mit einer eigenen Rechtsnatur ausgestattete Europäische Datenschutzausschuss (EDSA) fortgesetzt und die Fortsetzung dadurch dokumentiert, dass er in den ersten Sitzungen mehrere vor der Anwendbarkeit der DS-GVO entstandene Arbeitspapiere der Artikel-29-Gruppe „bestätigt" hat[3].

Zu den „bestätigten" Papieren gehören unter anderem[4]:

- WP 259 rev.01 (Leitlinien[5] zur Einwilligung)
- WP 260 rev.01 (Leitlinien zur Transparenz
- WP 250 rev.01 (Leitlinien für die Meldung von Datenschutzverletzungen)
- WP 242 rev.01 (Leitlinien zur Datenportabilität)
- WP 243 rev.01 (Leitlinien zum Datenschutzbeauftragten)
- WP 248 rev.01 (Leitlinien zur Datenschutzfolgenabschätzung)
- WP 251 rev.01 (Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling)
- WP 244 rev.01 (Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters)

Seit dem 25. Mai 2018 hat der Europäische Datenschutzausschuss folgende eigene Leitlinien im Sinne von Art. 70 DS-GVO beschlossen[6]:

- Leitlinien Nr. 1/2018 zur Zertifizierung und zu Zertifizierungskriterien
- Leitlinien Nr. 2/2018 zu den Ausnahmebestimmungen gemäß Art. 49 DS-GVO für Datenübermittlungen in Drittstaaten

In der Entwicklung sind derzeit weitere Leitlinien und Stellungnahmen des Europäischen Datenschutzausschusses unter anderem zu folgenden Themen:

1 So hatten die Information einzelner Aufsichtsbehörden nach Art. 13 DS-GVO, die an E-Mails angehängt waren, einmal ausgedruckt einen Umfang von vier DIN A 4 Seiten und ein anderes Mal fünf Zeilen (mit Link auf Webseite). Andere Aufsichtsbehörden machten weiter wie bisher, d.h. ohne spezielle Information – ging auch.

2 So z.B. Urt. v. 24.11.2011, C 468/10 und C 469/10: „Die mit der Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr angestrebte Harmonisierung der nationalen Rechtsvorschriften ist nicht auf eine Mindestharmonisierung beschränkt, sondern führt zu einer grundsätzlich umfassenden Harmonisierung."

3 Der EDSA hat diese Papiere „bestätigt" (endorsement) und mit keinem Wort gesagt, dass sie „Leitlinien im Sinne von Art. 70 DS-GVO" seien. Diesen Begriff hat er nur für Papiere verwendet, die er ab dem 25. Mail 2018 neu beschlossen hat (siehe den Wortlaut der „Bestätigungsentscheidung" unter https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en).

4 Der EDSA hat daneben noch (recht zahlreiche) weitere Papiere der WP29 bestätigt, die von der WP29 nicht als „Leitlinien" bezeichnet wurden (z.B. mehrere Arbeitspapiere zum BCR-Verfahren; vollständige Liste unter https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf)

5 Die Papiere wurden von der WP29 durchaus als „Leitlinien" bezeichnet. Es sind aber eben keine echten, eigenen Leitlinien des EDSA i.S.v. Art. 70 DS-GVO.

6 Diese eigenen Leitlinien des EDSA i.S.v. Art. 70 werden nun anders nummeriert.

- weitere Leitlinien zur Zertifizierung und Akkreditierung
- Leitlinien zum räumlichen Anwendungsbereich der DS-GVO (Art. 3)
- Leitlinien zum Anwendungsbereich von Kapitel V DS-GVO
- Leitlinien zu Art. 46 Abs. 2 a und 3 b DS-GVO betreffend Übermittlungen zwischen öffentlichen Stellen
- Videoüberwachung
- Anwendung von Art. 6 Abs. 1 b DS-GVO im Rahmen kostenfreier Online-Dienste

Es ist sicherlich damit zu rechnen, dass der EDSA auch darüber hinaus sukzessive weitere Leitlinien, Empfehlungen, „bewährte Verfahren" und Stellungnahmen verabschieden bzw. zur Verfügung stellen wird. Wann er darüber hinaus nach Art. 65 DS-GVO in Einzelfällen Entscheidungen treffen und damit Orientierung geben wird, bleibt abzuwarten und hängt ganz maßgeblich davon ab, wann und wie die einzelnen Aufsichtsbehörden ihn zu einer Entscheidung „zwingen".

II. Bemühungen der deutschen Aufsichtsbehörden um ein einheitliches Verständnis der DS-GVO

Selbst wenn der europäische Datenschutzausschuss, wie oben ausgeführt, auf einem guten Weg ist, den Anwendern der DS-GVO Orientierung zu geben, betrifft dies auf längere Zeit nur Einzelthemen, die von einzelnen europäischen Aufsichtsbehörden an den Ausschuss herangetragen und vorbereitet werden müssen. Insofern bleibt den deutschen Aufsichtsbehörden und den Aufsichtsbehörden der anderen Mitgliedstaaten noch jede Menge an Fragestellungen, die „sofort" beantwortet werden müssen. Sicherlich wird es der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) nicht möglich sein, auf die Unmenge an Fragen zum Vollzug der DS-GVO und des BDSG zeitnah einheitliche deutsche Antworten zu haben, so wünschenswert dies aus Sicht der Verantwortlichen und Auftragsverarbeiter vielleicht sein könnte[7]. Wichtig wären derartige einheitliche Antworten aber auch, um auf gefestigte Positionen zurückgreifen zu können, wenn es darum geht, mit einer starken deutschen Position in eine europaweite Abstimmung zu gehen.

Die DSK hat sich entschieden, eine gemeinsame Homepage[8] zu betreiben und auf dieser alle relevanten Entscheidungen der deutschen Aufsichtsbehörden zu veröffentlichen. Dies betrifft insbesondere die so genannten Kurzpapiere, die den Verantwortlichen, Auftragsverarbeitern und betroffenen Personen in Deutschland das Vollzugsverständnis der deutschen Aufsichtsbehörden und konkludent damit die Kriterien für deren zukünftige Prüfungen transparent machen. Zum anderen dienen diese Kurzpapiere auch dazu, wie oben gesagt, eine deutsche Position zu haben, die auf europäischer Ebene bei der Erstellung von Leitlinien, Entscheidungen oder sonstigen Stellungnahmen des EDSA eingebracht werden können. Dabei ist den Aufsichtsbehörden sehr bewusst, dass die ziemlich anstrengende Arbeit der Verständigung auf derzeit 19 Kurzpapiere nur ein Anfang und lange nicht das Ende ihrer Informations- und Sensibilisierungspflicht nach Art. 57 DS-GVO sein kann.

III. Bemühungen einzelner deutscher Aufsichtsbehörden um ein „einheitliches Verständnis" der DS-GVO

Im Verhältnis des EDSA zur DSK zeigt sich, dass die DSK etwas schneller und in größerem Umfang zu Fragen Stellung nehmen kann und muss, als der EDSA dies aufgrund seiner Struktur, d.h. der Einbindung aller europäischen Aufsichtsbehörden, bei der Verabschiedung von Leitlinien u.a. kann. Eine ähnliche Situation gibt es in Deutschland im Verhältnis der DSK zu den einzelnen Aufsichtsbehörden. Letztere werden derzeit mit Anfragen zur Auslegung der DS-GVO und des BDSG, ergänzt mit Anfragen zur Auslegung des jeweiligen Landesdatenschutzgesetzes überhäuft und können auch hier nicht in allen Fällen warten, bis es eine einheitliche deutsche Position gibt. Die Auffassungen der einzelnen Aufsichtsbehörden sind für die Verantwortlichen und Auftragsverarbeiter im jeweiligen Zuständigkeitsbereich notwendig und dem Vernehmen nach auch hilfreich, um zumindest in beschränktem Umfang Rechtssicherheit zu haben.

Insbesondere kleine Unternehmen, Vereine, Verbände oder freiberuflich Tätige, die die zwei Jahre Übergangszeit der DS-GVO nicht wirklich genutzt haben und nun durch irreführende Verlautbarungen von „Datenschutzfachleuten", regelmäßig in Verbindung mit der Aussage, dass die Aufsichtsbehörden Millionenstrafen verhängen, wenn man nicht den (kostenpflichtigen) Empfehlungen dieser Fachleute folgt, verunsichert wurden, sind mit einer Unmenge an Fragen an die Aufsichtsbehörden herangetreten, die, so gut es geht, – und ganz häufig nicht in Abstimmung mit den anderen Aufsichtsbehörden – beantwortet wurden[9]. Viele Aufsichtsbehörden haben deshalb ihr Angebot auf der jeweiligen Homepage aktualisiert, um damit zahlreiche gleich lautende Anfragen zu beantworten. Eine Konsolidierung der Antworten auf viele dieser Fragen, die dadurch geschehen könnte, dass sich die Antworten nicht mehr nur auf den Homepages der einzelnen Aufsichtsbehörden, sondern der Homepage der DSK bzw. des EDSA finden, ist dringend erforderlich und steht in weiten Bereichen noch aus[10].

7 Manche Verantwortliche sehen dies im Hinblick darauf, dass sich in den letzten Jahren bei gemeinsamen Positionen, die nur einstimmig verabschiedet werden konnten, häufig die Version durchgesetzt hat, die die schärfsten (gelegentlich auch nicht durchsetzbaren, wie z.B. bei den Anforderungen an Krankenhausinformationssysteme – KIS) Anforderungen beinhalteten. Mittlerweile beschließen Aufsichtsbehörden ihre Positionen in aller Regel mit Mehrheit.

8 Https://www.datenschutzkonferenz-online.de/

9 Das BayLDA hat, um die zahlreichen Fragen der Vereine abzufangen, für einen Zeitraum von vier Monaten die Dienstleistung einer professionellen Hotline eingekauft, die dortigen Mitarbeiterinnen und Mitarbeiter geschult und in den ersten Wochen mit jeweils einer Person im Hintergrund und parallel dazu konkreten Informationen auf der Homepage unterstützt. Deutlich über 1.000 Anrufe (Stand: August 2018) mit einer Erreichbarkeit von über 90 % zeigen, dass das Projekt erfolgreich war bzw. ist (siehe: https://www.lda.bayern.de/de/hotline.html).

10 So jedenfalls die Auffassung des Verfassers.

Für Verantwortliche scheint diese Situation trotzdem erträglich zu sein, da sie dann, wenn sie sich an das halten, was ihre zuständige Aufsichtsbehörde empfiehlt, in keinem Fall mit Sanktionen rechnen müssen, selbst wenn sie ein Stück weit im Auge haben müssen, dass die Auffassung ihrer Aufsichtsbehörde dann, wenn eine einheitliche Auffassung auf „höherer" Ebene, sei es DSK oder EDSA gefunden wurde, angepasst werden könnte.

IV. Antworten auf häufige Fragestellungen

Aus der Masse der kaum mehr überschaubaren Anfragen zur Auslegung der DS-GVO bzw. des BDSG sollen im Folgenden einzelne Fragen konkret angesprochen werden.

1. Welche Anforderungen gibt es an das Verzeichnis von Verarbeitungstätigkeiten?

In formaler Hinsicht könnte man weitgehend auf ein Verfahrensverzeichnis nach § 4e BDSG-alt aufbauen, wenn es das jemals gegeben haben sollte. Ein einheitliches Muster oder auch eine Empfehlung, ob das Verzeichnis in Word, Excel oder mit einer Spezialsoftware erstellt werden soll, kann es nicht geben, da die Verarbeitungen zu unterschiedlich sind. Grundsätzlich empfiehlt es sich jedoch, über die Mindestangaben gemäß Art. 30 Abs. 1 DS-GVO hinaus Angaben zum Nachweis weiterer Anforderungen der DS-GVO wie z.B. Rechtsgrundlage, Schwellwertanalyse DSFA, Privacy by Design, Betroffenenrechte u.a. zur Verfügung haben.

2. Wie ist die Rechenschafts- und Dokumentationspflicht konkret umzusetzen?

Rechenschaftspflicht kann als Beweislastumkehr gesehen werden. Verantwortliche und Auftragsverarbeiter müssen insbesondere die Rechtmäßigkeit ihrer Verarbeitung und die sonstigen in Art. 5 Abs. 1 DS-GVO genannten Datenschutzgrundsätze nachweisen. Mathematisch könnte man es auf die Formel bringen: Rechenschaftspflicht = Aufbauorganisation + 3 Hauptbereiche (datenschutzkonforme Verarbeitung, Betroffenenrechte, Datenschutzverletzungen) + Dokumentation + (internes) Audit. Bei KMUs könnte dies durch ein (etwas gegenüber den Minimalanforderungen nach Art 30 Abs. 1 DS-GVO erweitertes) Verzeichnis der Verarbeitungstätigkeiten sichergestellt werden. Größere Unternehmen werden um ein Datenschutzmanagementsystem nicht herumkommen.

3. Gibt es die Notwendigkeit für Prozesse, die schon vor Geltung der DS-GVO bestanden haben, eine Datenschutz-Folgenabschätzung durchzuführen?

Eine DSFA muss für bereits laufende Verarbeitungsvorgänge durchgeführt werden, wenn diese wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen und wenn sich deren Risiken im Hinblick auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung geändert haben[11]. Konkret bedeutet dies, dass bestehende Prozesse weiterlaufen können, solange sich risikorelevante Faktoren (z.B. neue Dienstleister, Einsatz neuer oder innovativer Technologien usw.) nicht geändert haben.

Spannend bleibt in diesem Zusammenhang der derzeit laufende Prozess auf europäischer Ebene, eine einheitliche Liste nach Art. 35 Abs. 4 DS-GVO zu konsolidieren. Die von insgesamt ca. 10 (von 28 Mitgliedstaaten) vorgelegten Landeslisten zeigen ein extrem unterschiedliches Verständnis, wann und in welcher Art und Weise eine DSFA durchzuführen ist. Die Arbeit, die auf nationaler Ebene mit großem Aufwand geleistet und in die Kurzpapiere Nrn. 5[12] (Datenschutzfolgeabschätzung) und insbesondere 18[13] (Risiko für die Rechte und Freiheiten natürlicher Personen) eingeflossen ist, ist auf europäischer Ebene (mit ungewissem Ausgang) noch zu leisten.

4. Welche konkreten Anforderungen werden an das Löschen von Daten gestellt?

Grundsätzlich gilt, dass das Sperren von Daten (siehe § 35 Abs. 3 BDSG-alt) wegen eines behaupteten hohen Löschaufwandes nicht mehr möglich ist. Daten sind zu löschen, sobald diese nicht mehr erforderlich und mögliche gesetzliche Aufbewahrungsfristen abgelaufen sind.[14] Sinnvollerweise sollten orientiert an Aufbewahrungsfristen Löschroutinen implementiert werden. Derzeit noch teilweise glaubhafte Aussagen von Verantwortlichen, dass ein Löschen technisch nicht möglich sei, werden mittelfristig nicht davor schützen, mit einer Sanktion belegt zu werden.

5. Welche Empfehlungen gibt es im Zusammenhang mit der Meldepflicht von Datenschutzverletzungen nach Art. 33 DS-GVO?

Dass die Schwelle zur Meldung von Datenschutzverletzungen nach Art. 33 DS-GVO gegenüber der Meldepflicht von Datenpannen nach § 42a BDSG-alt abgesenkt wurde, ist unbestritten. Dass aber die Anzahl der Meldungen von Datenschutzverletzungen nach Art. 33 DSGV in einer Art und Weise explodiert ist[15], haben Aufsichtsbehörden zwar befürchtet, aber nicht wirklich „sich zu erwarten getraut". Natürlich kann es derzeit keine Empfehlung der Aufsichtsbehörden geben, Datenschutzverletzungen, die nach Art. 33 DS-GVO meldepflichtig sind oder vom Verarbeiter als meldepflichtig angesehen werden, nicht zu melden. Wegschauen geht nicht. Nach der DS-GVO müssen Prozesse aufgebaut

11 WP 248 Rev. 01, S. 16

12 Https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.

13 Https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

14 Ob die Rechtsprechung des BAG im Urteil vom 23.08.2018 – 2 AZR 133/18, wonach ein Arbeitgeber Bildmaterial einer Videoüberwachung nicht sofort habe auswerten müssen, sondern damit solange haben warten dürfen, bis er dafür einen berechtigten Anlass sah, Bestand haben kann, erscheint sehr zweifelhaft. Es wäre die Abschaffung des Grundsatzes der Datenminimierung nach Art. 5 Abs. 1 c DS-GVO und der sich daraus ergebenen Löschverpflichtung durch die Hintertür.

15 Im Jahr 2017 wurden dem BayLDA insgesamt 270 Datenpannen, im Jahr 2018 in den Monaten Januar bis April schon 150 und in den Monaten Mai bis August 2018 (d.h. bis zum 24.08.) insgesamt 1.876 Datenschutz-verletzungen gemeldet.

und Mitarbeiter geschult werden, so dass Verletzungen der Sicherheit erkannt werden können. Wegschauen von der Masse der Eingänge geht aber auch nicht für die Aufsichtsbehörden. Notwendig wird es aber sein, die Menge dieser Meldungen, die dem Vernehmen nach in ähnlichem Umfang bei allen deutschen Aufsichtsbehörden eingegangen sind, auszuwerten und gegebenenfalls Verfahren zu implementieren, die eine stärker risikobasierte Art der Bearbeitung der gemeldeten Datenschutzverletzungen wie Hacking-Vorfälle, Softwarefehler, Verlust von Datenträgern, Fehlversand u.a. vorsehen.

6. Wie bewerten die Aufsichtsbehörden die Einschränkungen bei den Betroffenenrechten durch das BDSG?

Die Diskussion darüber, ob und inwieweit Vorschriften des BDSG-neu wegen Anwendungsvorrangs der DS-GVO nicht angewendet werden dürfen, kommt immer wieder in den einzelnen Arbeitskreisen der DSK hoch, wenn einzelne Themenblöcke, wie z.B. Videoüberwachung, bearbeitet werden. Ergebnis der internen Diskussionen unter den Aufsichtsbehörden war bis jetzt jedoch, dass die DSK sich nicht dahingehend zu einzelnen Vorschriften äußert, dass sie nicht anwendbar seien. Der Grund dafür ist, dass diese Entscheidung nicht generell getroffen werden kann, sondern nur im konkreten Einzelfall und dann nur durch die jeweils zuständige Aufsichtsbehörde.

V. Ausblick

Die Aufsichtsbehörden werden noch lange Zeit benötigen, um selbst oder unter Einbindung von Gerichten16 Rechtssicherheit zu schaffen. Dabei sollten Sie aber einem Paradigmenwechsel der DS-GVO Rechnung tragen: Der Verantwortliche ist für seine Datenverarbeitung verantwortlich und bleibt verantwortlich. Dies bedeutet zum Beispiel bei Beratungen17, dass Voraussetzung für eine Äußerung einer Aufsichtsbehörde sein sollte, dass der Verantwortliche der Aufsichtsbehörde nicht nur einen Sachverhalt mit der Bitte, diesen datenschutzrechtlich zu bewerten, mitteilt, sondern seine eigene datenschutzrechtliche Bewertung übermittelt. Davon kann man möglicherweise bei sehr kleinen Verantwortlichen abweichen. Bei allen Verantwortlichen, die verpflichtet sind, einen Datenschutzbeauftragten zu benennen, muss dies Standard sein, und insbesondere auch, wenn ein anwaltlich Bevollmächtigter um Beratung nachsucht.

Zur Herstellung von Synergieeffekten sollten Aufsichtsbehörden für den nichtöffentlichen Bereich die intensivere Zusammenarbeit mit den Verbänden und Kammern suchen, um diese in die Lage zu versetzen, als Multiplikatoren zu wirken und für den jeweiligen fachlichen Bereich einschlägige Muster oder Handreichungen zu erstellen18. Wenn dies in deutlich mehr Fälle als bisher zu genehmigten Verhaltensregeln (CoC) gemäß Art. 40 DS-GVO führen würde, wäre dies für alle Beteiligten hilfreich.

In der Praxis haben sich die ERFA – Kreise, bei denen sich in aller Regel Wirtschaft und Aufsichtsbehörden begegnen, sehr bewährt. Zu überlegen wäre in diesem Zusammenhang, ob die Verbände der Datenschutzbeauftragten, die mittlerweile auch auf europäischer Ebene vernetzt sind, zu einzelnen Themen derartige Kreise auf europäischer Ebene ins Leben rufen, um die Praxis zu vernetzen. Vielleicht könnte dies helfen, ein für die Praxis überzeugendes Verständnis zu entwickeln, wie das Problem mit den Dashcams, die in UK zum Teil verpflichtend betrieben werden müssen, um den Haftpflichtversicherungsschutz nicht zu verlieren, und in Deutschland, sofern sie permanent laufen, um den Hergang eines Unfalls für Versicherungen zu dokumentieren, verboten sind, harmonisierend gelöst werden kann.

Thomas Kranig
ist seit dem Jahr 1997 Richter am Verwaltungsgericht Ansbach. Im Jahr 2011 wurde er schließlich zum Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht in Bayern ernannt.

16 … was bedeutet, dass Aufsichtsbehörden auch vermehrt (zu den wirklich relevanten Fragen) Anordnungen erlassen müssten.

17 Die Aufsichtsbehörden diskutieren zur Zeit intensiv darüber, ob Beratung der Verantwortlichen (anders als nach § 38 Abs. 1 Satz 2 BDSG-alt) nach der DS-GVO noch eine Pflichtaufgabe ist oder nur „fakultativ" in Erfüllung „jeder sonstigen Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten" nach Art. 57 Abs. 1 v DS-GVO geleistet werden kann.

18 Der Bayerisches Landessportverband (BLSV) hat das in vorbildlicher Art und Weise für seine Mitglieder erarbeitet und (teilweise allerdings nur im internen Bereich) veröffentlicht, https://www.blsv.de/blsv/vereinsservice/vereinsberatung/datenschutz.html.

Professor Dr. Rolf Schwartmann/Dr. Tobias Jacquemain, LL.M

Datenschutzrechtliche Herausforderungen im Auto – neue Risiken durch „Connected Cars"

Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen. Vor allem Arbeitgeber stehen in der Kritik, personenbezogene Daten der Fahrzeugnutzer auswerten zu wollen, um damit Rückschlüsse auf das Verhalten ihrer Kunden und Beschäftigten ziehen zu können. Nahezu unbegrenzte Speicherungsmöglichkeiten, Verknüpfungen und Auswertungen der Daten des Fahrers gefährden den Einzelnen in seinen Persönlichkeits- und Freiheitsrechten. Dies geschieht insbesondere dann, wenn der Fahrzeugnutzer nicht weiß, wer welche Daten über ihn hat, was dieser mit den Daten macht und an wen die Daten weitergegeben werden. Datenschutzprobleme drohen vor allem dann, wenn Unternehmen smarte Fahrzeuge einsetzen, sogenannte Connected Cars, die mit Internetzugang und Apps für den Bordcomputer ausgestattet sind.

I. Datenverarbeitung im Auto

1. Welche Daten können erhoben werden? Wer ist betroffen?

a) Allgemeines

Personenbezogene Datenverarbeitung findet auch im Auto statt. Um diese für den Betroffenen transparenter zu gestalten, hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) im April diesen Jahres einen Mustertext für eine Herstellerinformation über die Datenverarbeitung in Auto beschlossen. Elektronische Steuergeräte verarbeiten demnach Daten, die sie zum Beispiel von Fahrzeug-Sensoren empfangen, selbst generieren oder untereinander austauschen. Einige Steuergeräte sind für das sichere Funktionieren eines Fahrzeugs erforderlich, andere unterstützen den Fahrzeugnutzer beim Fahren (Fahrerassistenzsysteme), und optional können sie in Form von Komfort- oder Infotainment-Funktionen auftreten.[1]

In der Praxis werden beim Betrieb des Fahrzeuges Standortdaten, die technischen Eigenheiten von Funknetzen gegenüber kabelbasierten Netzen,[2] Fahrzeugstatus-Informationen (z.B. Geschwindigkeit, Bewegungsverzögerung, Querbeschleunigung, Radumdrehungszahl, Anzeige geschlossener Sicherheitsgurte) oder Umgebungszustände (z.B. Temperatur, Regensensor, Abstandssensor) erhoben und verarbeitet.[3] In der Regel sind all diese Daten flüchtig und werden nicht über die Betriebszeit hinaus gespeichert und nur im Fahrzeug selbst verarbeitet. Steuergeräte im Auto wie auch der Fahrzeugschlüssel enthalten häufig Datenspeicher. Diese werden eingesetzt, um Informationen über Fahrzeugzustand, Bauteilbeanspruchung, Wartungsbedarfe sowie technische Ereignisse und Fehler temporär oder dauerhaft dokumentieren zu können.[4]

Gespeichert werden könnten praktisch darüber hinaus Betriebszustände von Systemkomponenten (z.B. Füllstände, Reifendruck, Batteriestatus), Störungen und Defekte in wichtigen Systemkomponenten (z.B. Licht, Bremsen), Reaktionen der Systeme in speziellen Fahrsituationen (z.B. Auslösen eines Airbags, Einsetzen der Stabilitätsregelungssysteme), Informationen zu fahrzeugschädigenden Ereignissen oder etwa der Ladezustand der Hochvoltbatterie und die geschätzte Reichweite bei Elektroautos.[5]

In besonderen Fällen wie wenn das Fahrzeug eine Fehlfunktion erkannt hat, kann es erforderlich sein, Daten zu speichern, die grundsätzlich flüchtig wären.[6] Fehlerspeicher im Fahrzeug können durch einen Servicebetrieb zurückgesetzt werden. Dies kann entweder im Rahmen von Reparatur- oder Servicearbeiten oder auf den Wunsch des Fahrzeugnutzers geschehen. Dadurch wird dem Grundsatz der Datenminimierung Rechnung getragen.[7] Die lokale Speicherung ist als datenschutzfreundlich zu bezeichnen, da auf eine Übermittlung von Daten hierdurch verzichtet wird.

Existieren Komfort- oder Infotainment-Funktionen im Auto, geht die Datenerhebung unmittelbar auf das individuelle Verhalten des Fahrzeugnutzers zurück. Personalisiert der Fahrzeugnutzer das Fahrzeug, können Komforteinstellungen und Individualisierungen gespeichert, geändert oder zurückgesetzt werden. Dazu gehören bspw. Einstellungen der Sitz- und Lenkradpositionen, Fahrwerks- und Klimatisierungseinstellungen oder Individualisierungen wie Innenraumbeleuchtung. Ebenso können im Rahmen der gewählten Ausstattung Daten in Infotainment-Funktionen des Fahrzeugs eingebracht werden. Dazu gehören Multimediadaten, wie Musik, Filme oder Fotos zur Wiedergabe in einem integrierten Multimediasystem, Adressbuchdaten zur Nutzung in Verbindung mit einer integrierten Freisprecheinrichtung oder einem integrierten Navigationssystem, eingegebene Navigationsziele sowie Daten über die Inanspruchnahme von Internetdiensten. Diese Daten für Komfort- und Infotainment-Funktionen können lokal im Fahrzeug gespeichert werden, oder sie befinden sich auf einem Gerät, das mit

1 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 1.

2 Weichert, SVR 2014, 201 (202).

3 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 2.

4 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 2.

5 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 2 f.

6 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 3.

7 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 3.

dem Fahrzeug verbunden wurde (z.B. Smartphone, USB-Stick oder MP3-Player).[8]

Die mögliche Datenübertragung hängt insbesondere davon ab, ob das Auto befähigt ist, selbstständig zu kommunizieren. Im Fahrzeug möglicherweise verbaute SIM-Karten helfen bei der Bereitstellung diverser Services über den Bordcomputer oder über das Infotainment-System und ermöglichen den Empfang von SMS-Nachrichten und E-Mails (inklusive Vorlesefunktion), den Internet-Zugang oder die Übernahme der wichtigsten Apps auf das Fahrzeugdisplay mittels Integration des Smartphones des Fahrzeugnutzers. Eine Kommunikation der Fahrzeuge untereinander sowie mit Herstellern und anderen Diensteanbietern ist heute schon technisch und praktisch möglich.[9] Genau durch diese Verbindung zwischen Fahrzeug und dem Internet oder einem anderen Netz kennzeichnen sich Connected Cars.[10]

Die zahlreich im Auto erhobenen und verarbeiteten Daten stellen grundsätzlich kein Problem dar. Für den Datenschutz relevant werden sie erst durch den Personenbezug der im Fahrzeug verarbeiteten Daten. Dieser kann schon durch die eindeutige Fahrgestellnummer, die jedes Auto kennzeichnet, eröffnet sein, weil durch diese über eine Auskunft beim Kraftfahrtbundesamt auf den gegenwärtigen und ehemaligen Halter des Fahrzeugs geschlossen werden kann. Es gibt noch weitere Möglichkeiten, wie etwa über das Kfz-Kennzeichen, aus dem Fahrzeug erhobene Daten auf den Halter oder Fahrer zurückzuführen. Die von den Steuergeräten generierten oder verarbeiteten Daten können ebenfalls personenbezogen sein oder zumindest unter bestimmten Voraussetzungen personenbezogen werden. Je nach Datenlage besteht die theoretische Möglichkeit Rückschlüsse bspw. auf das Fahrverhalten, den Standort oder die Fahrtroute bzw. auf das Nutzungsverhalten zu ziehen.[11] Wenn Fahrzeuge ihre Positionsdaten zusätzlich fortlaufend an einen Dritten übertragen und dieser Dritte ermitteln kann, wer das Fahrzeug führt, lassen sich aus den Ortungsdaten Rückschlüsse über das Fahrverhalten und aktuelle Aufenthaltsorte des Fahrers oder der Fahrerin ziehen. Dadurch kann der Personenbezug gegeben sein.

b) eCall schafft zusätzliche Datenverarbeitung im Auto

Für das europaweite automatische Notrufsystem eCall, das seit dem 31.03.2018 für alle neu genehmigten Fahrzeugmodelle gilt, sind Besonderheiten geregelt.[12] Art. 6 der europäischen eCall-VO regelt besondere Rechte zu Privatsphäre und Datenschutz in Ergänzung zur Datenschutz-Grundverordnung (DS-GVO). Genauso wie die DS-GVO statiuiert die eCall-VO in Art. 6 Abs. 9 umfängliche Informationspflichten.

Die Kfz-Hersteller sind nicht nur in der Pflicht, den automatischen Notruf eCall vorzuhalten, sondern dabei gleichzeitig das Datenschutzrecht zu wahren. Durch das auf dem 112-Notruf basierende bordeigene eCall-System darf der Fahrzeugführer nicht verfolgbar werden. Dafür muss der Hersteller technisch gewährleisten, dass die Daten im internen Speicher dieses Systems oder dieser selbstständigen technischen Einheit automatisch und kontinuierlich entfernt werden. Sie dürfen außerhalb des bordeigenen Systems oder der bordeigenen selbstständigen technischen Einheit für keine Einrichtung zugänglich sein, bevor der eCall tatsächlich ausgelöst wird. Zudem ergreift der Hersteller angemessene Sicherungsmaßnahmen, beispielsweise in Form von Verschlüsselungstechniken, zum Schutz der Sicherheit persönlicher Daten im internen Speicher des bordeigenen eCall-Systems oder der bordeigenen selbstständigen technischen eCall-Einheit und zur Verhinderung von Überwachung und Missbrauch.[13]

2. Wer erhält die Daten?

a) Hersteller

Das Auslesen von lokal gespeicherten Fahrzeugdaten erfolgt in der Regel über den gesetzlich vorgeschriebenen Anschluss für OBD („On-Board-Diagnose") im Fahrzeug. Ebendiese ausgelesenen Daten dokumentieren technische Zustände des Autos oder einzelner Komponenten, helfen bei der Fehlerdiagnose, der Einhaltung von Gewährleistungsverpflichtungen und dienen nicht zuletzt der Qualitätsverbesserung. Insbesondere Informationen über Bauteilbeanspruchung, technische Ereignisse, Fehlbedienungen und andere Fehler, können hierfür zusammen mit der Fahrzeugidentifikationsnummer an den Hersteller übermittelt werden. Schließlich unterliegt der Hersteller der Produkthaftung. Die Betriebsdaten aus Fahrzeugen können von den Herstellern deswegen auch für Rückrufaktionen genutzt werden oder um Ansprüche des Kunden auf Gewährleistung und Garantie zu prüfen.[14]

b) Offline-Diensteanbieter

Wenn der Fahrzeugnutzer Serviceleistungen wie eine Reparaturleistungen oder Wartungsarbeiten in Anspruch nimmt, können die gespeicherten Betriebsdaten zusammen mit der Fahrzeugidentifikationsnummer ausgelesen und genutzt werden. Das Auslesen kann durch Mitarbeiter des Servicenetzes in Vertragswerkstätten oder durch den Hersteller selbst erfolgen. Ein solches Vorgehen wird die Regel für Garantiefälle und Qualitätssicherungsmaßnahmen darstellen. Aber auch Dritte, wie der Pannendienst, können die Daten aus dem Fahrzeug auslesen, wenn sie Hilfe leisten.

c) Online-Diensteanbieter

Bis hierher ging es ausschließlich um im Fahrzeug verarbeitete Daten, die nicht nach außen übermittelt werden. Sofern das Automobil über eine Funknetzanbindung verfügt, ist der Austausch von Daten zwischen dem Fahrzeug und weiteren Systemen eröffnet. Das ist der Fall, wenn das Fahrzeug mit dem Mobilfunk verbunden ist. Eine solche Funknetzanbindung wird durch eine fahrzeugeigene Sende- und

8 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 3 f.

9 Fischer, Datenschutz in vernetzten Fahrzeugen, Flottenmanagement 3/2018, 84 (84).

10 Weisser/Färber, MMR 2015, 505 (506).

11 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 1.

12 Vgl. Lüdemann, ZD 2015, 247 (248).

13 Fischer, Datenschutz in vernetzten Fahrzeugen, Flottenmanagement 3/2018, 84 (84 f.).

14 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 3.

Empfangseinheit oder über ein vom Fahrer verwendetes und angeschlossenes Mobiltelefon ermöglicht. Über diese Funknetzanbindung können Online-Funktionen genutzt werden.[15] Bei der Erbringung von Online-Diensten werden in aller Regel personenbezogene Daten verarbeitet. Gerade Online-Dienste Applikationen werden ohne personenbezogene Daten nicht funktionieren. Der Datenaustausch hierzu erfolgt aufgrund des Schutzbedarfs über eine geschützte Verbindung, wie etwa mit den dafür vorgesehenen IT-Systemen des Herstellers.[16]

Der Fahrzeughalter ist aber nicht auf die Online-Angebote des Kfz-Herstellers beschränkt. Vielmehr besitzt er zusätzlich die Möglichkeit, Online-Dienste anderer Anbieter zu nutzen. Bei Inanspruchnahme der Dienste Dritte unterliegen diese der Verantwortung sowie den Datenschutz- und Nutzungsbedingungen des jeweiligen Anbieters. Anders als bei den Online-Diensten des Fahrzeugherstellers können die jeweiligen Funktionen und die damit verbundenen datenschutzrechtlichen Informationen nicht so einfach wie in der Betriebsanleitung oder auf der Internetseite des Fahrzeugherstellers bereitgestellt werden, sondern über die Art, den Umfang und den Zweck der Erhebung und Verwendung personenbezogener Daten im Rahmen von Diensten Dritter muss sich der Halter selbstständig informieren.[17] So sehen es jedenfalls die KFZ-Hersteller. Die Informationspflichten der DS-GVO sind aber an den jeweiligen Verantwortlichen adressiert und verlangen vom Betroffenen keine Holschuld.

d) Arbeitgeber im Falle einer Dienstwagenüberlassung

Bei der Dienstwagenüberlassung können die Daten auch beim Arbeitgeber landen, was aufgrund des Verhältnisses zwischen Arbeitgeber und abhängig Beschäftigtem besondere Probleme birgt. Deswegen sind auch bei der Nutzung und Bereitstellung von Dienstwagen spezifische datenschutzrechtliche Vorgaben zu beachten. Der Arbeitgeber oder eine von ihm beauftragte Stelle könnte nämlich theoretisch auch Bewegungsprofile zur betrieblichen Nutzung der Mitarbeiterinnen und Mitarbeiter erstellen, um so eine Verhaltens- oder Leistungskontrolle zu ermöglichen. Hier sehen aber der Datenschutz und die Mitarbeitervertretung klare Grenzen vor, die dabei überschritten würden. Bewegungs-, Nutzungs- oder Kommunikationsprofile sind durch elektronische Auswertung als Datenauswertung in Echtzeit möglich. Das Bundesverfassungsgericht (BVerfG)[18] hat die persönlichkeitsrechtliche Relevanz von Persönlichkeitsbildern erkannt und ein Verbot von Totalbildern ausgesprochen.[19]

II. Gilt das Datenschutzrecht im Auto?

1. Personenbezug als Voraussetzung

Sowohl die DS-GVO als auch das Bundesdatenschutzgesetz (BDSG) finden immer nur Anwendung auf den Umgang mit personenbezogenen Daten. Gerade bei Smart Services (Geschäftsmodelle, bei denen ein Produkt und eine Dienstleistung digital miteinander verknüpft werden) sind die Daten jedoch reine „Maschinendaten“, ohne Bezug zu einer Person. Allerdings lassen sich viele Maschinendaten zumindest indirekt auf eine identifizierte oder identifizierbare Person beziehen, wie etwa die Person, welche die Bedienung oder Wartung ausführt, sodass der Anwendungsbereich des Datenschutzrechts bei der Nutzung solch technischer Möglichkeiten dennoch eröffnet sein kann.[20] Sofern die betreffenden Automobildaten also Personenbezug aufweisen können, unterfallen sie dem Anwendungsbereich des Datenschutzrechts. Wenn der Hersteller hingegen nicht auf den Personenbezug der Daten angewiesen ist, dann kann er diese gezielt anonymisieren. Das Datenschutzrecht findet dann von vorneherein keine Anwendung auf diese Daten.[21]

2. Anforderungen an Connected Cars

Um den datenschutzrechtlichen Anforderungen Rechnung zu tragen beim Einsatz von Connected Cars, haben die für die Kontrolle des Datenschutzrechts zuständigen Aufsichtsbehörden spezifische Forderungen aufgestellt. Diese richten sich vor allem natürlich an die Automobilindustrie, aber ebenso an Unternehmen, die Connected Cars einsetzen wie z.B. in einem Fuhrpark. Den in der DS-GVO verankerten Prinzipien für einen effektiven Datenschutz und Datensicherheit ist auch bei vernetzten Autos Genüge zu leisten. Der in Art. 5 DS-GVO zu findende Grundsatz der Datenminimierung verlangt, IT-Verfahren entsprechend sparsam zu konfigurieren. Ferner verlangen die Art. 12 ff. DS-GVO, den Fahrer, Halter oder Nutzer von Fahrzeugen zu informieren, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet werden sowie welche Daten an wen, wie und zu welchen Zwecken übermittelt werden. Änderungen sind dem im datenschutzrechtlichen Sinne Betroffenen rechtzeitig anzuzeigen. Darin schließt die Verpflichtung an, Betroffenenrechte wie das Recht auf Löschen oder, der Datenverarbeitung zu widersprechen, durchsetzbar zu gewährleisten.

3. Besondere Anforderungen bei Dienstwagennutzung

a) Rechtmäßigkeit

Ein weiteres Datenschutzproblem ergibt sich, wenn der Eigentümer des Fahrzeugs nicht identisch mit dem Halter oder dem tatsächlichen Nutzer ist. Ein solcher Fall liegt immer dann vor, wenn ein Dienstwagen dem Arbeitgeber gehört oder von diesem geleast, aber dem Arbeitnehmer zur Nutzung überlassen wird. Darf ein Einzelner diesen wie sein eigenes Auto nutzen und hat er die alleinige Kontrolle darüber, obwohl der Arbeitgeber der Halter ist, so ist es wohl kaum zu rechtfertigen, dass der Arbeitgeber Zugriff auf die Daten verlangt. Anders verhält es sich, wenn die Fahrzeuge bestimmungsgemäß von mehreren Arbeitnehmern genutzt werden. Der Arbeitgeber kann in dieser Konstellation ein legitimes Interesse daran besitzen, auf die Daten zuzugrei-

15 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 4.

16 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 5.

17 DSK, Beschluss v. 25./26.04.2018, VDA Mustertext zur Datenverarbeitung im Fahrzeug, 5.

18 BVerfG, NJW 1969, 1707.

19 Weichert, SVR 2014, 241 (241).

20 Heun/Assion, BB 2018, 579 (580).

21 Heun/Assion, BB 2018, 579 (581).

fen, um etwa den Einsatz seiner Fahrzeugflotte besser planen zu können. Für die mit dem Fahren eines Connected Cars verbundene personenbezogene Datenverarbeitung bedarf es in jedem Fall einer Rechtmäßigkeit. Die Zulässigkeit kann sich aus § 26 BDSG ergeben, sofern das Fahren und die damit einhergehende Verarbeitung von personenbezogenen Daten für die Durchführung des Arbeitsverhältnisses erforderlich ist. Problematisch ist die Verarbeitung zusätzlicher Daten, die nicht mehr für die Durchführung des Beschäftigungsverhältnisses erforderlich sind, auf Grundlage einer Einwilligung. Hier drohen Zweifel an der Freiwilligkeit der vom Arbeitnehmer zu erteilenden Einwilligung, da bei einer Weigerung die begründete Sorge vor Benachteiligung oder gar der Auflösung des Beschäftigungsverhältnisses besteht. Insbesondere weil eine Einwilligung jederzeit widerruflich ist, bilden in der Praxis Betriebsvereinbarungen das wesentliche rechtliche Instrument zur Umsetzung von Datenverarbeitungen im Beschäftigtenkontext.[22] Außerdem muss beachtet werden, dass die Einrichtung und Nutzung von Systemen, die eine Überwachung der Beschäftigten zulassen, nach § 87 Abs. 1 Nr. 6 BetrVG ohnehin mitbestimmungspflichtig sind, sofern ein Betriebsrat existiert. Betriebsvereinbarungen werden dieser Mitbestimmungspflicht gerecht, liefern aber gleichzeitig auch eine verlässliche datenschutzrechtliche Rechtfertigungsgrundlage für die Verarbeitung von Beschäftigtendaten.[23] Unabhängig davon, ob eine Einwilligung oder Betriebsvereinbarung als Rechtsgrundlage gewählt wird, gilt es die Nutzung von Connected Cars künftig auch bei der arbeitsvertragsrechtlichen Regelung der Dienstwagenüberlassung zu berücksichtigen.[24]

b) Organisatorische Datenschutzpflichten: privacy by design/default und Datenschutz-Folgenabschätzung

Neben der Kernfrage der Rechtmäßigkeit der Verarbeitung haben datenverarbeitende Unternehmen weitere datenschutzrechtliche Pflichten zu beachten. Nach der DS-GVO muss jeder Anbieter von Smart Services in Bezug auf diesen Smart Service eine Vielzahl von organisatorischen Anforderungen erfüllen. Zu den wichtigsten dieser Pflichten zählen Data protection by design und Data protection by default: D.h. der Smart Service muss bereits auf Ebene der technischen Gestaltung so datenschutzfreundlich aufgebaut sein, und etwaige Voreinstellungen müssen so gewählt sein, dass personenbezogene Daten nur insoweit verarbeitet werden, als dies für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist (Art. 25 Abs. 2 bzw. Abs. 1 DS-GVO).[25] Inwiefern ein Arbeitgeber als derjenige, der seinem Mitarbeiter den Wagen überlässt, überhaupt technisch in der Lage ist die von ihm angeschafften Fahrzeuge entsprechend zu konfigurieren, erscheint in der Praxis höchst zweifelhaft. Gleichwohl trifft ihn diese Rechtspflicht als für die Datenverarbeitung Verantwortlicher unmittelbar.

Wenn sich aus dem Smart Service voraussichtlich ein hohes Risiko für die Interessen der Betroffenen ergibt, muss der Verantwortliche eine vorherige Datenschutz-Folgenabschätzung durchführen (Art. 35 DS-GVO). Diese von der DS-GVO neu geschaffene Dokumentationsanforderung dürfte für einen Fuhrpark relevant werden. Ein Unternehmen muss nämlich dann eine Datenschutz-Folgenabschätzung vornehmen, wenn eine Form der Datenverarbeitung wahrscheinlich ein hohes Risiko verursacht, insbesondere bei neuen Technologien oder aufgrund ihres Wesens, ihres Umfangs, ihres Kontexts oder ihrer Zwecke. Ein Beispiel für solche neuen Technologien sind Systeme, die eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen aufgrund automatisierter Verarbeitung ermöglichen. Hierunter dürften nicht nur neuartige Systeme wie das des (teil-)autonomen Fahrens gehören, sondern ebenso fortgeschrittene Fahrerassistenzsysteme, die im Kontext mit anderen vom Bordcomputer gespeicherten Daten (Navigationssystem, Smartphone-Anbindung, E-Mail-System) Rückschlüsse auf die Leistung und das Verhalten des Dienstwagennutzers zulassen.[26] Gerade bei der Anschaffung von Fahrzeugen mit einer Vielzahl automatischer Systeme wird der Verantwortliche als Fuhrparkinhaber künftig wohl gehalten sein, eine entsprechende Datenschutz-Folgenabschätzung vorzunehmen. So findet sich die „Fahrzeugdatenverarbeitung" auch in den Listen von Verarbeitungsvorgängen der Aufsichtsbehörden, für die eine solche Prüfung vor Inbetriebnahme durchzuführen ist.[27] Für diese Herausforderung wird es erforderlich sein, dass auch die Kfz-Hersteller transparent machen, ob und welche personenbezogene Daten in den einzelnen Fahrzeugsystemen verarbeitet werden. Dieses neue Aufgabengebiet kann auch beinhalten, die Aufsichtsbehörde zu konsultieren, wenn nämlich die Datenschutz-Folgenabschätzung ergibt, dass eine Datenverarbeitung ohne Maßnahmen ein hohes Risiko zur Folge hat.

Neben den vom Verantwortlichen umfänglich zu erfüllenden Transparenzpflichten (Art. 13 u. 14 DS-GVO) und den Dokumentationsanforderungen (Art. 5 Abs. 2 u. 30 DS-GVO) muss der Verantwortliche sicherstellen, sämtliche Betroffenenrechte erfüllen zu können.

III. Betroffenenrechte im Auto

Die betroffene Person soll wissen, für welche Zwecke ihre Daten verarbeitet werden und welche Datenschutzrechte sie hat. Dies gilt selbstredend auch im Auto. So ist der Pkw-Besitzer ebenso wie der Nutzer eines Dienstwagens über die bei der Fahrzeugnutzung anfallende Datenverarbeitung hinreichend zu informieren. Beispielsweise sollte das Fuhrparkmanagement nach Artikel 13 DS-GVO unmittelbar bei der Erhebung der Daten beim Betroffenen auf diesen Umstand hinweisen. Viele Anbieter machen es sich bei der Bereitstellung dieser Informationen einfach, indem sie die gesamten Pflichtangaben in Privacy Policies oder Nutzungsbestimmungen integrieren. Diese Informationsfülle lässt sich sodann vom Verbraucher nicht mehr seriös überblicken.

22 Klösel/Mahnhold, NZA 2017, 1428 (1428).

23 Ebd.

24 Fischer, Auswirkungen der EU-Datenschutz-Grundverordnung, Flottenmanagement 1/2017, 64 (64).

25 Heun/Assion, BB 2018, 579 (582).

26 Fischer, Auswirkungen der EU-Datenschutz-Grundverordnung, Flottenmanagement 1/2017, 64 (68).

27 Vgl. bspw. HBDI, Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO für die gemäß Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung von Verantwortlichen durchzuführen ist, Juni 2018.

Den Fahrzeugnutzern steht klassischerweise ein unentgeltlicher und umfassender Auskunftsanspruch gegenüber dem Fahrzeughersteller sowie gegenüber Dritten wie beispielsweise beauftragte Pannendiensten, Werkstätten oder Anbietern von Online-Diensten im Fahrzeug zu, sofern diese personenbezogene Daten der Fahrzeugnutzer gespeichert haben. Daneben bestehen auch Rechte auf Berichtigung oder Löschung von Daten.[28] Die rechtlichen Anforderungen an Auskunftserteilung und Korrektur sind klar und weitestgehend unstreitig. Probleme bestehen jedoch bei der Realisierung der Betroffenenrechte. Für die praktische Umsetzung des Auskunftsanspruchs genügt es nicht, lediglich das Kundenprofil zum Abruf bereitzustellen. Vielmehr ist so umfänglich zu beauskunften, dass auch die nicht unter dem Klarnamen abgelegten Daten sowie Metadaten, also Verkehrs- und Auswertungsdaten, dem Betroffenen bereitgestellt werden. So besteht jedenfalls theoretisch die Möglichkeit, dass der Fahrzeugführer vom Hersteller die zum Zeitpunkt eines Unfalls im Kfz gespeicherten technischen Daten als Auskunft einholen kann, die zur Unfallaufklärung beitragen können.

Insbesondere bei der Kfz-Mobilkommunikation werden mehr Daten als z.B. bei der stationären Datenverarbeitung beiläufig erfasst, für die es oft nur einen kurzfristigen Speicherbedarf gibt. Dies gilt insbesondere für technische Fahrzeugdaten wie auch für viele Daten, die gerne durch App- und Portalanbieter erfasst werden.

Das Recht auf Löschung gemäß Art. 17 DS-GVO besteht auch im Auto und hinsichtlich der dort erhobenen personenbezogenen Daten. Die tatsächliche Löschung ist nicht nur auf Verlangen des Betroffenen durchzuführen. Unabhängig davon ist die turnusmäßige Löschung von Nutzerdaten vorzusehen, etwa wenn eine App gelöscht bzw. ein Nutzungsvertrag gekündigt wird.[29] Spannend wird es, wenn das Fahrzeug verkauft werden soll und der Halter seine Daten vorher löschen will. Teilweise besteht sogar eine Pflicht, wie etwa bei BMW, sämtliche personenbezogenen Daten vorher selbstständig zu löschen: „Bei Verkauf oder dauerhafter Weitergabe des Fahrzeugs an einen Dritten hat der Kunde dafür Sorge zu tragen, dass alle persönlichen Daten, die im Fahrzeug gespeichert sind, gelöscht werden. Außerdem muss der Kunde die Verknüpfung zwischen dem Fahrzeug und seinem Nutzerkonto über „Mein BMW ConnectedDrive“ beenden. Der Kunde ist verpflichtet, den Dritten, dem er sein Fahrzeug verkauft oder an den er sein Fahrzeug dauerhaft weitergibt, über sämtliche aktiven und deaktivierten Dienste zu informieren.“[30] Dadurch entledigt sich der Hersteller einfach seiner Verpflichtungen und macht den Fahrzeughalter zum Rechtsverpflichteten. Der Gebrauchtwagenhandel ist damit wesentlich komplizierter geworden. Während beim früheren klassischen Autokauf sämtliche Rechte und Pflichten vom Hersteller zum Käufer und später vom Käufer auf den Zweitbesitzer übergingen, sind die Rechtsverhältnisse heute wesentlich komplexer. Die Verantwortlichkeit für die IT bleibt heute des Kfz beim Hersteller, weswegen beim Weiterverkauf Vertragsbeziehungen zum Hersteller übertragen werden müssen, was den Veräußerer dazu zwingt, die AGBs des Herstellers zum Bestandteil seines Kaufvertrages zu machen.[31]

IV. Fazit

Bereits dann, wenn ein Auto keine Daten nach außen übermittelt, ist der Datenbestand eines einzelnen Fahrzeugs beachtlich. Die rechtliche Ausgestaltung des Fahrzeughaltens macht einen Personenbezug in aller Regel unausweichlich. Deswegen findet das Datenschutzrecht selbst in nicht vernetzten Autos Anwendung. Nicht erst in Zukunft, sondern bereits jetzt lassen sich die meisten Autos als Connected Cars qualifizieren. Das verpflichtende eCall-System für Notrufe hat diesen Weg zementiert. Nicht nur der Hersteller, sondern verschiedenste Akteure werden zu Diensteanbietern rund um das Auto und damit zu Verantwortlichen im datenschutzrechtlichen Sinne. Daraus erwächst einerseits die Verpflichtung die Datenverarbeitung rechtmäßig zu gestalten sowie andererseits den Betroffenenrechten und vor allem den umfangreichen Informationspflichten der DS-GVO gerecht zu werden. Für manche Diensteanbieter wird die Transparenz zur Herausforderung, wenn es gar keinen unmittelbaren Kontakt wie im klassischen Kundeverhältnis zwischen Betroffenem und Verantwortlichem gibt. Das stellt innerhalb eines Beschäftigungsverhältnisses nicht die Hürde dar, die es zu meistern gilt. Vielmehr liegt hier das Problem darin, die im Auto vorhandene Technik rechtskonform einzusetzen. Dafür sollte das Dienstwagen überlassende Unternehmen neben der Einbindung des Betriebsrats am besten Kollektivvereinbarungen für die aus datenschutzrechtlicher Sicht damit zulässige Wagenüberlassung treffen, da Einwilligungen als alternativer Rechtmäßigkeitstatbestand widerruflich sind, der Dienstwagen hingegen Teil eines nicht so leicht änderbaren Vergütungsanspruchs sein kann. Hinzu kommt noch aller Voraussicht nach die Aufgabe der Datenschutz-Folgenabschätzung für den Verantwortlichen des Fuhrparks.

Professor Dr. Rolf Schwartmann
Leiter der Kölner Forschungsstelle für Medienrecht an der TH Köln und Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD). Er ist Mitglied der Datenethikkommission der Bundesregierung und berät die Bundesregierung und die Landesregierung NRW in Gremien und ist unabhängiges Mitglied des Stiftungsrats der European Net-ID Foundation.

Dr. Tobias Jacquemain, LL.M
ist promovierter Datenschutzrechtler und als Wissenschaftlicher Referent bei der Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) beschäftigt. Zudem ist er Redakteur bei DataAgenda.de.

28 Fischer, Datenschutz in vernetzten Fahrzeugen, Flottenmanagement 3/2018, 84 (84).

29 Weichert, SVR 2014, 241 (244).

30 BMW, Allgemeine Geschäfts- und Nutzungsbedingungen: BMW ConnectedDrive, Mai 2017, Ziff. 7.2 f.

31 Weichert, SVR 2014, 241 (242).

Professor Dr. Rolf Schwartmann/Maximilian Hermann/Robin Mühlenbeck

Die Veröffentlichung des Entzuges von Doktorgraden und der Datenschutz

Datenverarbeitung der öffentlichen Hand zwischen Datenschutz- und Verwaltungsrecht in der Anwendungspraxis

Die DS-GVO ordnet den Datenschutz in der Europäischen Union durch ein Zusammenspiel von EU-Recht und mitgliedstaatlichem Recht: Während das Datenschutzrecht für die Privatwirtschaft – sieht man von Großteilen des Beschäftigtendatenschutzes ab – voll harmonisiert ist, wird für den Datenschutz öffentlicher Stellen nur ein grober Rahmen über sog. Öffnungsklauseln vorgegeben. Die Mitgliedstaaten müssen hier innerhalb dieses Rahmens tätig werden und eigenes Recht schaffen. Die Verordnung wirkt hier vergleichbar einer Richtlinie. In Deutschland wird die Datenverarbeitung durch öffentliche Stellen im BDSG und den Landesdatenschutzgesetzen geregelt. Die Einpassung des nationalen Rechts in den Rahmen der DS-GVO führt für den öffentlichen Bereich – insbesondere mit Blick auf den engen Gesetzesvorbehalt für Eingriffe in die informationelle Selbstbestimmung nach deutschem Verfassungsrecht – zu Problemen im Zusammenspiel von europäischem und deutschem Datenschutzrecht mit dem Verwaltungsrecht. Konkret soll dies an der Veröffentlichung von Entzugsvermerken von Doktorgraden in (Online-)Bibliotheken illustriert werden.[1]

I. Wissenschaftliches Fehlverhalten als Datenschutzproblem

Wissenschaftliches Fehlverhalten, wie etwa bei Plagiaten, führt die auf Wahrheit angewiesene Wissenschaft in die Irre. Wenn in einem strengen und klaren Regeln folgenden Verfahren von einer Hochschule wissenschaftliches Fehlverhalten (z.B. in Form des Plagiats) rechtskräftig festgestellt wird, so ist die Entziehung des Doktorgrades die Konsequenz. Allerdings wissen nur die Beteiligten des Entzugsverfahrens, also die Hochschule und der Betroffene davon, dass die Arbeit einen wissenschaftlichen Mangel aufweist und der Doktorgrad infolge dessen entzogen wurde. Die durch wissenschaftliches Fehlverhalten entstandene Arbeit ist dagegen bislang ohne erkennbaren Makel in (Online-) Bibliotheken verfügbar und erzeugt den Anschein, korrekt entstanden zu sein. Das ist für die Wissenschaft und für die Allgemeinheit gleichermaßen unzumutbar. Deshalb wollen Hochschulen im Sinne der Glaubwürdigkeit der Wissenschaft in Zukunft in (Online-)Bibliotheken auf den Entzug des Doktorgrades hinweisen. Auch wenn das zwar wissenschaftlich geboten ist, stecken in diesem Hinweis zahlreiche Rechtsprobleme. Denn der Entzugsvermerk stellt schließlich eine Verarbeitung personenbezogener Daten dar und ist daher am Recht auf informationelle Selbstbestimmung des Plagiierenden zu messen (dazu III. 1.), das die DS-GVO und das Datenschutzrecht der Mitgliedstaaten in einem Zusammenspiel schützen (dazu II.). Unabhängig vom Datenschutz bedarf aber auch die in der Veröffentlichung liegende Information der Allgemeinheit über den Entzug des Doktorgrades einer Ermächtigung (dazu III.), die mit der datenschutzrechtlichen zwar verknüpft, aber dennoch von ihr zu trennen ist (dazu III. 2. und 5.).

II. Datenverarbeitung durch öffentliche Stellen nach DS-GVO im Zusammenwirken mit BDSG oder LDSG

Die Information über den Entzug eines Doktorgrades durch Aufnahme eines entsprechenden Vermerks in eine (Online-) Bibliothek ist eine Verarbeitung personenbezogener Daten durch eine öffentliche Hochschule und damit durch eine öffentliche Stelle. Deren Zulässigkeit regelt die DS-GVO in Art. 6 Abs. 1 S. 1 lit. e) i.V.m. Art. 6 Abs. 3 S. 1, 2 DS-GVO.[2]

Dabei ist im Rahmen von Art. 6 Abs. 3 DS-GVO wie folgt zu differenzieren: Art. 6 Abs. 3 S. 1 DS-GVO erteilt für öffentliche Stellen vergleichbar einer Richtlinie einen Regelungsauftrag zur Schaffung mitgliedstaatlichen Rechts.[3] Art. 6 Abs. 3 S. 2 DS-GVO gibt dabei den pflichtigen Mindeststandard für die Umsetzung vor. Der Bund und alle Länder bis auf Sachsen-Anhalt, das zum jetzigen Zeitpunkt keine

1 Die Verfasser haben im Auftrag des Gremiums „Ombudsman für die Wissenschaft" im September 2018 ein Rechtsgutachten mit dem Titel „Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen" vorgelegt, abrufbar unter: http://www.ombudsman-fuer-die-wissenschaft.de; vgl. dazu auch Schwartmann, Plagiate müssen erkennbar sein, F.A.Z. vom 19. September 2018, Seite N4, online abrufbar unter: http://www.faz.net/aktuell/feuilleton/hoch-schule/wissenschaftsliches-fehlverhalten-plagiate-muessen-erkennbar-sein-15793168.html (zuletzt abgerufen: 09.10.2018).

2 Eine Rechtfertigung der Verarbeitung personenbezogener Daten aufgrund von Art. 6 Abs. 1 S. 1 lit. a–d oder f DS-GVO scheidet aus. Eine Einwilligung scheitert an der (fehlenden) Freiwilligkeit. Denn wird die Durchführung der Promotion von der Erteilung der Einwilligung abhängig gemacht, verbleibt dem Antragsteller bei realistischer Betrachtung kein Entscheidungsspielraum, die Einwilligung zu verweigern und dennoch promoviert zu werden. Zusätzlich besteht jederzeit die Möglichkeit des Widerrufs durch die betroffene Person, vgl. dazu ausführlich Schwartmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 18.

3 HK-DS-GVO/BDSG, Schwartmann/Jacquemain, Art. 6 Rn. 167.

Generalklausel in Umsetzung des Art. 6 Abs. 3 S. 2 DS-GVO erlassen hat, haben diese Pflicht zur Umsetzung des Mindeststandards (Art. 6 Abs. 3 S. 2 DS-GVO) erfüllt und jeweils eine Generalklausel[4] erlassen, die als Grundlage für eine Datenverarbeitung durch öffentliche Stellen dienen kann. Als Rechtsgrundlage im Rahmen des nationalen Rechts muss sie (entsprechend der Vorgaben des Art. 6 Abs. 3 S. 2 DS-GVO) den Zweck der Verarbeitung festlegen oder für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Art. 6 Abs. 3 S. 3 DS-GVO eröffnet den Mitgliedstaaten demgegenüber die weitergehende Möglichkeit, über die Erfüllung der Pflichtinhalte des S. 2 hinaus spezifischere datenschutzrechtliche Bestimmungen zu erlassen. Die Bundesländer Bayern, Bremen, Nordrhein-Westfalen und Rheinland-Pfalz haben es gleichwohl bei der von Art. 6 Abs. 3 S. 2 DS-GVO verlangten Pflichterfüllung belassen und darüber hinaus kein eigenes spezifischeres mitgliedstaatliches Datenschutzrecht im Rahmen des Art. 6 Abs. 3 S. 3 DS-GVO erlassen. Die übrigen Länder[5] haben sich ebenso wie der Bund dazu entschieden, zusätzlich zur pflichtigen Umsetzung noch eine spezifische Regelung zur Zulässigkeit der Datenverarbeitung öffentlicher Stellen in die Gesetze aufzunehmen, indem sie die rechtmäßige Aufgabenerfüllung als Zweck der Datenverarbeitung zusätzlich von der Zuständigkeit der Behörde zur Aufgabenerfüllung abhängig machen. Sie haben damit die Öffnungsklausel des Art. 6 Abs. 3 S. 3 DS-GVO genutzt.[6] Die Nutzung der Öffnungsklausel des Art. 6 Abs. 3 S. 3 DS-GVO ist dabei für den Prüfungsmaßstab entscheidend: Während im Rahmen einer pflichten Umsetzung nach Art. 6 Abs. 3 S. 2 DS-GVO die mitgliedstaatlichen Regelungen durch die europäischen Vorgaben der DS-GVO determiniert werden und damit der Kontrolle des EuGH unterliegen, entlässt Art. 6 Abs. 3 S. 3 DS-GVO die Mitgliedstaaten im Falle der weitergehenden Nutzung der Öffnungsklausel aus ihrer europarechtlichen Verantwortlichkeit zugunsten eines nationalen Prüfungsmaßstabs entsprechend der Rechtsprechung des Bundesverfassungsgerichts und den Vorgaben des Grundgesetzes. Folglich unterliegen die datenschutzrechtlichen Umsetzungen des Bundes und der Länder bis auf Bayern, Bremen, Nordrhein-Westfalen, Rheinland-Pfalz und Sachsen-Anhalt nationalen Vorgaben.[7]

III. Prüfung der Voraussetzungen der datenschutzrechtlichen Generalermächtigung

1. Verfassungsrechtliche Anforderungen

Im Rahmen der Beurteilung der datenschutzrechtlichen Zulässigkeit der Anbringung des Entzugsvermerks ist also zunächst entscheidend, ob die Regelungen des Bundes und der o.g. Länder (materiell) verfassungsgemäß sind und daher als taugliche Grundlage für einen Eingriff in das Recht auf informationelle Selbstbestimmung herangezogen werden können. Das Bundesverfassungsgericht verlangt bei einem Eingriff in das Recht auf informationelle Selbstbestimmung, dass sich aus dem Gesetz ergeben muss, welche staatliche Stelle zur Erfüllung welcher Aufgaben für die geregelte Datenverarbeitung zuständig sein soll.[8] Diese Anforderungen erfüllen die Normen des Bundes und der betroffenen Länder. Gleichwohl erfüllen die Generalklauseln, die die Öffnungsklausel des Art. 6 Abs. 3 S. 3 DS-GVO spezifizierend mittels des zusätzlichen Kriteriums der „Zuständigkeit für die Aufgabenerfüllung" ausfüllen, mit Blick auf ihre Normenklarheit und Zweckfestlegung lediglich die in der Volkszählungsrechtsprechung festgelegten Mindestvoraussetzungen des Bundesverfassungsgerichts zur materiellen Verfassungsmäßigkeit eines Eingriffs in die informationelle Selbstbestimmung.[9] Sie können deshalb nur geringfügige Eingriffe in die informationelle Selbstbestimmung rechtfertigen.[10] Die Intensität des Eingriffs richtet sich unter anderem danach, ob der Betroffene den Anlass für die Datenverarbeitung gesetzt hat.[11] Das ist im Falle wissenschaftlichen Fehlverhaltens des Betroffenen gegeben und der Eingriff in die

4 Vgl. § 4 DSG BW, Art. 4 I BayDSG, § 5 BdgDSG, § 3 BlnDSG, § 3 I BremDSG, § 4 HmbDSG, § 3 HDSG, § 4 I DSG M-V, § 3 I, II DSG NRW, § 3 NDSG, § 3 LDSG RP, § 4 I, II SaarlDSG, § 4 I SächsDSG, § 3 I DSG SH, § 16 I ThürDSG.

5 Eine Ausnahme ist Sachsen-Anhalt. Dort hat der Gesetzgeber bislang (Stand: Oktober 2018) keine Generalklausel in Umsetzung des Art. 6 Abs. 3 DS-GVO erlassen.

6 Das ist vor dem Hintergrund der Volkszählungsrechtsprechung des Bundesverfassungsgerichts bedeutsam, weil das spezifizierende Zusatzkriterium der „Zuständigkeit" nicht nur den Kreis der Berechtigten der Datenverarbeitung festlegt, sondern als innerstaatliches Recht zugleich die Zuständigkeit des Bundesverfassungsgerichts begründet. Die Auslegung des Datenschutzrechts dieser Länder unterliegt nicht der Rechtsprechung des Bundesverfassungsgerichts, weil die kein eigenständiges, spezifisches mitgliedstaatliches Recht im Rahmen der Öffnungsklausel des Art. 6 Abs. 3 S. 3 DS-GVO geschaffen haben. Weil die DS-GVO in den Mitgliedstaaten selbst unmittelbar keine Rechtsgrundlage für die Datenverarbeitung der öffentlichen Hand darstellt, kann man das aus der DS-GVO im Rahmen von Art. 6 Abs. 3 S. 1 und S. 2 DS-GVO übernommene „umsetzungspflichtige" Recht der DS-GVO in den betroffenen Bundesländern nur unmittelbar an den Grundsätzen des EU-Datenschutzgrundrechts messen. Dafür ist der Europäische Gerichtshof zuständig. Für die Überprüfung der Zulässigkeit von Entzugsvermerken von Doktorgraden ergibt sich so eine gespaltene Zuständigkeit innerhalb des Bundes und elf Bundesländern auf der einen sowie fünf Bundesländern auf der anderen Seite. Die datenschutzrechtliche Zulässigkeit der Entzugsvermerke nach den Generalklauseln in Bund und Ländern werden also teils durch das Bundesverfassungsgericht und teils durch den EuGH (Bayern, Bremen, Nordrhein-Westfalen, Rheinland-Pfalz und Sachsen-Anhalt) jeweils an verschiedenen Grundrechten (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG – Grundrecht auf informationelle Selbstbestimmung bzw. Art. 8 GrCh) überprüft.

7 Vgl. dazu Schwartmann/Hermann/Mühlenbeck Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 25 unter Hinweis auf BVerfG Beschl. v. 13.03.2007, Az.1 BvF 1/05.

8 Vgl. BVerfG, Beschl. v. 23.02.2007, Az. 1 BvR 2368/06, NVwZ 2007, 688 (690 f.) sowie BVerfG, Urt. v. 19.09.2018, Az. 2 BvF 1/15, 2 BvF 2/15 Rn. 218 ff.

9 Schwartmann/Hermann/Mühlenbeck Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 32 unter Hinweis auf BVerfG, Beschl. v. 23.02.2007, Az. 1 BvR 2368/06, NVwZ 2007, 688 (690 f.) sowie BVerfG, Urt. v. 19.09.2018, Az. 2 BvF 1/15, 2 BvF 2/15 Rn. 218 ff.

10 So im Ergebnis auch Kühling/Buchner-Petri, DS-GVO BDSG, § 3 BDSG Rn. 9, Wolff/Brink-Wolff, BeckOK Datenschutzrecht, § 3 BDSG Rn. 1.

11 Schwartmann/Hermann/Mühlenbeck Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 7 und 34 unter Hinweis auf BVerfG, Beschl. v. 14.07.1999, Az. 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, BVerfGE 100, 313 (376); BVerfG, Beschl. v. 12.03.2003, Az. 1 BvR 330/96 und 1 BvR 348/99, BVerfGE 107, 299 (318 ff.); BVerfG, Beschl. v. 03.03.2004, Az. 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279 (353); BVerfG, Beschl. v. 04.04.2006, Az. 1 BvR 518/02, NJW 2006, 1939 (1942).

informationelle Selbstbestimmung deshalb nicht intensiv, so dass die spezifizierenden Generalklauseln die Veröffentlichung eines Entzugsvermerks in datenschutzrechtlicher Hinsicht bei Vorliegen der tatbestandlichen Voraussetzungen grundsätzlich rechtfertigen können.[12]

2. Systematik der datenschutzrechtlichen Generalklauseln

Systematisch knüpfen alle Generalklauseln in Bund und Ländern die Rechtmäßigkeit der Datenverarbeitung tatbestandlich an die Voraussetzung, dass diese „zur Erfüllung einer öffentlichen Aufgabe" erforderlich ist. Deshalb muss zunächst die Information über den Entzug in Erfüllung der Aufgaben des Verantwortlichen erfolgen. Sie muss dabei als solche im Sinne des Verwaltungsrechts rechtmäßig sein. Erst daran anschließend kann die Erforderlichkeit der Datenverarbeitung zum Zwecke der Aufgabenerfüllung überprüft werden. Das rechtliche Schicksal der Zulässigkeit der Datenverarbeitung hängt somit von der Rechtmäßigkeit des Informationshandelns ab. Dies führt zu einer Verzahnung von Datenschutz- und Verwaltungsrecht. Die Information über den Entzug einerseits und der Datenverarbeitungsvorgang, der im Anbringen des Entzugsvermerks andererseits liegt, fallen zwar tatsächlich in einem Akt zusammen, sind aber wegen der unterschiedlichen Rechtfertigungsanforderungen rechtlich voneinander zu trennen. Die rechtliche Trennung ist erforderlich, weil die verfassungsrechtlichen Anforderungen aus dem Datenschutzrecht hinsichtlich der Datenverarbeitung höher sind als diejenigen, die an die Verfassungsmäßigkeit der Information als solche nach Verwaltungsrecht zu stellen sind. Die datenschutzrechtlichen Generalermächtigungen, die die Datenverarbeitung als Eingriff in das Recht auf informationelle Selbstbestimmung legitimieren, können daher nur auf einem rechtmäßigen Informationshandeln der Hochschule aufbauen. Ist das Informationshandeln als nicht rechtmäßig zu qualifizieren, kann die Datenverarbeitung auch nicht durch eine Generalklausel legitimiert werden. Insofern ist ein rechtmäßiges Informationshandeln seinerseits Tatbestandsvoraussetzung für die Rechtmäßigkeit der Datenverarbeitung.

3. Datenschutzrechtliche Tatbestandsvoraussetzungen

Für die Zulässigkeit der Datenverarbeitung ist erforderlich, dass die Voraussetzungen der (jeweiligen) datenschutzrechtlichen Generalklausel erfüllt sind, so wie der Bund und die Länder[13] sie vorsehen. Die Verarbeitung personenbezogener Daten muss zur Erfüllung einer in der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich sein. Die Veröffentlichung des Entzugsvermerkes muss also der Aufgabenerfüllung der öffentlichen Stelle dienen. Voraussetzung ist dabei zunächst, dass mit dem Entzugsvermerk auf das wissenschaftliche Fehlverhalten als Entzugsgrund hingewiesen wird. Ohne diese Angabe würde der Vermerk nicht den Zweck der Wahrung der Glaubwürdigkeit der Wissenschaft erfüllen, denn es würde nicht deutlich, ob der Entzug des akademischen Grades auf inhaltlich wissenschaftlichen Gründen oder auf anderen Gründen, etwa Täuschung über die Voraussetzungen zur Zulassung zur Promotion, beruht. Für die sich aus den hochschulrechtlichen Normen ergebende Aufgabe ist aber letztlich nur entscheidend, ob die Arbeit an wissenschaftlichen Mängeln leidet, die den Entzug des Grades rechtfertigen. Anderenfalls würde es an einem hochschulrechtlichen Grund für die Datenverarbeitung fehlen.

4. Verwaltungsrechtliche Implikationen: Rechtmäßiges Informationshandeln

Die Zulässigkeit des Informationshandelns über den Entzug setzt im Rahmen des Gesetzesvorbehalts zunächst grundsätzlich eine Ermächtigung voraus. Eine solche enthalten die Hochschulgesetze der Länder für die Information über den Entzug eines Doktorgrades jedenfalls nicht ausdrücklich. Es ist mit Blick auf das Informationshandeln der öffentlichen Hand in der Rechtsprechung des Bundesverfassungsgerichts aber anerkannt, dass dieses in besonderen Fällen von der Reichweite einer bestehenden Aufgabennorm mitumfasst sein kann.[14]

a) Verwaltungsrechtliche Ermächtigung zur Information

So kann also die Aufgabe zur Wahrung der Glaubwürdigkeit der Wissenschaft die Befugnis zur Information im Wege eines Entzugsvermerks bei wissenschaftlichem Fehlverhalten umfassen.[15] Dies gilt jedenfalls, soweit das Informationshandeln als solches keinen selbstständigen Eingriff in Grundrechtspositionen darstellt. Für die Information über den Entzug bedarf es damit dann keiner expliziten gesetzlichen Ermächtigung, wenn das Informationshandeln die Schwelle zu einem Grundrechtseingriff nicht überschreitet. Denn in diesem Fall wird der Gesetzesvorbehalt mangels Eingriff nicht ausgelöst.[16] Es kommt also maßgeblich darauf an, ob der Vermerk über den rechtskräftigen Entzug eines Doktorgrades einen selbständigen Eingriff darstellt. Auf Basis des „modernen Eingriffsbegriffs"[17] fehlt es beim Informationshandeln der Hochschule im Wege der Veröffentlichung eines Entzugsvermerks am Eingriffscharakter. Betrachtet man den rechtskräftigen Entzug des Doktorgrades

12 Schwartmann/Hermann/Mühlenbeck Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 54.

13 Mit Ausnahme von Sachsen-Anhalt.

14 Zur Zulässigkeit staatlichen Informationshandelns ohne ausdrückliche Ermächtigung BVerfG, Beschl. v. 26.06.2002, Az. 1 BvR 558/91, 1428/91, BVerfGE 105, 252 = NJW 2002, 2621 (Glykol) und BVerfG, Beschl. v. 26.06.2002, Az. 1 BvR 670/91, BVerfGE 105, 279 = NJW 2002, 2626 (Osho).

15 Schwartmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 44 unter Hinweis auf BVerfG Beschl. v. 21.03.2018, Az. 1 BvF 1/13, NJW 2018, 2109 (2110).

16 Schwartmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 45 ff.

17 Vgl. Kingreen/Poscher, Grundrechte – Staatsrecht II, 33. Aufl. 2017, Rn. 294; Sachs, Verfassungsrecht II – Grundrechte, 3. Aufl. 2017, Kap. 8 Rn. 15 ff., 20 ff. (S. 132 ff.); ders., in: Sachs (Hrsg.), GG-Kommentar, 8. Aufl. 2018, vor Art. 1 Rn. 78 ff., 83 ff.; s. ferner Peine, Der Grundrechtseingriff (§ 57), in: Merten/Papier (Hrsg.), Handbuch der Grundrechte, Bd. III, 2009, S. 87 ff.; Bethge, Mittelbare Grundrechtsbeeinträchtigungen (§ 58), in: Merten/Papier (Hrsg.), Handbuch der Grundrechte, Bd. III, 2009, S. 113 ff.

und die Veröffentlichung der Information darüber, so liegt der Eingriff in die Rechtssphäre des Betroffenen im Entzug selbst. Das Informationshandeln ist dabei nur die unselbstständige Fortsetzung eines bereits erfolgten Eingriffs im Sinne eines rein formalen Akts. Also stellt sich die Informationshandlung letztlich als bloßer unselbstständiger Annex im Rahmen einer rechtskräftigen Entscheidung über den Entzug des Doktorgrades dar.[18] Der informierende Vermerk erweist sich, bezogen auf den rechtskräftigen Entzug des Doktorgrades, als notwendige Folgemaßnahme ohne Eingriffsgehalt. Das Informationshandeln ist vielmehr nur eine Art „Folgenbeseitigung" des zu Unrecht verliehenen Doktorgrades. Der bereits öffentlich gewordene falsche Schein, es liege ein wissenschaftliches Werk vor, wird wiederum auch öffentlich korrigiert. Hierdurch werden keine über die bereits im Rahmen des Entzugs selbst betroffenen Grundrechtspositionen hinaus tangiert. Unterhalb der Eingriffsschwelle ist ein staatliches Informationshandeln zulässig, wenn durch die Informationshandlung eine staatliche Aufgabe wahrgenommen wird, die Kompetenzordnung gewahrt bleibt sowie der Sachverhalt im Rahmen des Möglichen sorgsam und verlässlich aufgeklärt wird. Die Informationen müssen dem Gebot der Sachlichkeit, Richtigkeit sowie der Verhältnismäßigkeit entsprechen.[19]

b) Information über den Entzug als Aufgabe der Hochschule

Die Aufgabe der Hochschule über den Entzug nach wissenschaftlichem Fehlverhalten zu informieren, lässt sich damit aus den Hochschulgesetzen der Länder ableiten. Hochschulen dienen nach ihren gesetzlich normierten Aufgaben der Gewinnung wissenschaftlicher Erkenntnisse sowie der Pflege und Entwicklung der Wissenschaft durch Forschung, Lehre, Studium und Förderung des wissenschaftlichen Nachwuchses.[20] Die Universitäten gewährleisten eine gute wissenschaftliche Praxis.[21]

Das Informationshandeln in Wahrnehmung der landesrechtlich normierten Aufgabe der Hochschulen ist rechtlich nicht zu beanstanden, weil es unterhalb der Eingriffsschwelle bleibt. Da es nicht als Eingriff in die Rechtssphäre des Betroffenen zu qualifizieren ist, wird der Gesetzesvorbehalt nicht ausgelöst, so dass es für das Informationshandeln als solches keiner expliziten Ermächtigung bedarf.[22]

Teilt man diese Auffassung nicht und kommt zu dem abweichenden Ergebnis, dass das Informationshandeln der Hochschule als solches die Schwelle zum Eingriff überschreitet, muss dem dadurch ausgelösten Gesetzesvorbehalt durch den Erlass einer expliziten Rechtsgrundlage in den Hochschulgesetzen der Länder für das Informationshandeln der Hochschule Rechnung getragen werden. Der Eingriff wäre gleichwohl verfassungsrechtlich gerechtfertigt, da dem Schutzgut der Wissenschaft so Rechnung getragen würde. Für die „Reinheit" der Wissenschaft ist es nämlich unverzichtbar, öffentliche Kenntnis darüber zu erlangen, ob ein als wissenschaftlich geltendes Werk auch tatsächlich wissenschaftlich korrekt erarbeitete Aussagen enthält. Die Wissenschaft baut auf dem öffentlich sichtbaren Austausch wissenschaftlicher Ansichten auf. Die Information über den Entzug des Doktorgrades bezieht sich final nur auf die in dieser Weise publizierte, d.h. in die Öffentlichkeit des wissenschaftlichen Diskurses eingespeiste Dissertation, die dort in der Erwartung aufgenommen wird, dass das, was der wissenschaftlichen Öffentlichkeit als wissenschaftliche Leistung präsentiert wird, auch tatsächlich eine wissenschaftliche Leistung ist. Aufgabe der Hochschulen ist es, die Glaubwürdigkeit der Wissenschaft zu erhalten. Dazu müssen Arbeiten, die einen inhaltlich-wissenschaftlichen Mangel aufweisen, gekennzeichnet werden. Während bspw. der Entzug einer Fahrerlaubnis nicht öffentlich gemacht werden muss, um den Straßenverkehr zu schützen, kann der wissenschaftliche Diskurs eben nur durch die Veröffentlichung des Entzuges geschützt werden.[23]

Es ist Forschern und der Integrität der Wissenschaft nicht zuzumuten, unwissentlich auf Ergebnisse aufzubauen, die den Makel des rechtskräftigen Entzugs des akademischen Grades tragen.

5. Verzahnung von Verwaltungsrecht und Datenschutzrecht

Die in der Information liegende und mit dieser verzahnte Datenverarbeitung knüpft also an das rechtmäßige Informationshandeln im hochschulrechtlichen Sinne an. Da jede Verarbeitung personenbezogener Daten einen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Person darstellt, bedarf es für die Rechtmäßigkeit der Datenverarbeitung einer Rechtsgrundlage, die in den Generalklauseln des Bundes und der Länder[24] auf Basis von Art. 6 Abs. 3 S. 2 DS-GVO (Bayern, Bremen, Nordrhein-Westfalen und Rheinland-Pfalz) oder Art. 6 Abs. 3 S. 3 DS-GVO (Bund und übrige Länder) liegt. Diese Generalklauseln können aber nur geringfügige Eingriffe in die informationelle Selbstbestimmung rechtfertigen. Dass der Eingriff beim Informationshandeln über den Entzug nach rechtskräftig festgestelltem, wissenschaftlichen Fehlverhalten der zuständigen Hochschule ganz fehlt oder nur gering ist und dann durch eine zu erlassende Norm gerechtfertigt werden muss, rechtfertigt datenschutzrechtlich den auch hier nur schwachen Eingriff in die informationelle Selbstbestimmung auf Grund-

18 Schwartmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 48 ff.

19 Schwartmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 49 f.

20 So etwa § 3 Abs. 5 S. 1 Landeshochschulgesetz (LHG) Baden-Württemberg, Art. 6 Abs. 1 S. 3 Hs. 1 Bayerisches Hochschulgesetz, § 4 Abs. 5 S. 2 Brandenburgisches Hochschulgesetz (BbgHG), § 4 Abs. 4 S. 1 Hochschulgesetz NRW oder § 8 Abs. 2 S. 3 Thüringer Hochschulgesetz.

21 § 3 Abs. 5 S. 3 Landeshochschulgesetz (LHG) Baden-Württemberg, § 4 Abs. 5 S. 2 Brandenburgisches Hochschulgesetz (BbgHG).

22 Schwartmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 48 ff.

23 Schwartmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 12.

24 Mit Ausnahme von Sachsen-Anhalt.

lage der jeweiligen datenschutzrechtlichen Generalklausel. Deren Tatbestandsvoraussetzungen liegen vor, weil die im Anbringen des Entzugsvermerks liegende Datenverarbeitung zur Aufgabenerfüllung der Hochschule (Wahrung der Glaubwürdigkeit und „Reinheit" der Wissenschaft) erforderlich ist. In einem online zugänglichen Bibliothekskatalog darf also nach derzeitigem Recht auf den Grund für den Entzug des akademischen Grades hingewiesen werden, wenn auch auf das inhaltlich-wissenschaftliche Fehlverhalten hingewiesen wird.[25]

IV. Kein Löschanspruch nach Zeitablauf

Aber gilt das zeitlich unbefristet oder wäre eine befristete Speicherung eines solchen Vermerks für beispielsweise zehn Jahre zulässig? Das hängt davon ab, ob der Zweck der Datenverarbeitung erfüllt ist. Der Betroffene hat etwa nach Ablauf von zehn Jahren kein „Recht auf Vergessenwerden", präziser gesagt keinen Anspruch auf Löschung des Vermerks auf der Katalogseite, weil der Zweck für die in der Information liegende Datenverarbeitung bestehen bleibt. Jedenfalls solange die betroffene Arbeit verfügbar ist, kann die Integrität der Wissenschaft nur durch den öffentlichen Fortbestand des Entzugsvermerks gewahrt werden. So wie das Plagiat nicht verjährt, verjährt auch die Pflicht, es öffentlich zu machen, nicht.[26]

V. Fazit

Der öffentliche Hinweis auf den rechtskräftigen Entzug eines Doktorgrades ist bei näherer Betrachtung zwar ein typischer, aber zugleich komplexer Fall einer Datenverarbeitung der öffentlichen Hand, dessen Zulässigkeit zunächst im Verhältnis zwischen DS-GVO und mitgliedstaatlichem Recht ausgelotet werden muss. Hier zeigt sich, dass der Bund und ein Teil der Länder für den öffentlichen Bereich unterschiedliche Wege bei der Anpassung des nationalen Rechts an die DS-GVO beschritten haben. Innerstaatlich spielt bei Datenverarbeitungen nicht nur deren Zulässigkeit nach Datenschutzrecht eine Rolle, sondern auch die Rechtmäßigkeit des in der Datenverarbeitung liegenden Verwaltungshandelns. Nur dann, wenn das Verwaltungshandeln rechtmäßig ist, kann die Datenverarbeitung überhaupt zulässig sein. Sie ist gesondert an den engen Anforderungen des Datenschutzrechts zu messen. Nur bei nicht intensiven Eingriffen in die informationelle Selbstbestimmung, kann auf die Generalklauseln in Bund und Ländern zurückgegriffen werden. Intensive Eingriffe setzen eine spezielle und normenklare Ermächtigung voraus, die den Anforderungen der Volkszählungsrechtsprechung gerecht werden muss.

Professor Dr. Rolf Schwartmann
Leiter der Kölner Forschungsstelle für Medienrecht an der TH Köln und Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD). Er ist Mitglied der Datenethikkommission der Bundesregierung und berät die Bundesregierung und die Landesregierung NRW in Gremien und ist unabhängiges Mitglied des Stiftungsrats der European Net-ID Foundation.

Maximilian Hermann
Wissenschaftlicher Mitarbeiter an der Kölner Forschungsstelle für Medienrecht an der TH Köln. Er beschäftigt sich im Rahmen seiner wissenschaftlichen Arbeit unter anderem mit datenschutzrechtlichen Fragestellungen.

Foto: Thilo Schmülgen/TH Köln

Robin Mühlenbeck
Wissenschaftlicher Mitarbeiter an der Kölner Forschungsstelle für Medienrecht an der TH Köln. Er beschäftigt sich im Rahmen seiner wissenschaftlichen Arbeit unter anderem mit datenschutzrechtlichen Fragestellungen.

Foto: Thilo Schmülgen/TH Köln

25 Schwartmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 41 und 54 f.

26 Schwartmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-) Bibliothekskatalogen, S. 56.

Kurzbeiträge

Aus den aktuellen Berichten der Aufsichtsbehörden (37): Der DSB nach DS-GVO und neuem nationalem Datenschutzrecht

Ausgewählt und kommentiert von Prof. Peter Gola*

Die Landesdatenschutzbeauftragten der Länder Hessen (6. TB, 2017 v. 07.08.2018, Abschnitt 2.3) und Bremen 40. TB, 2017 v. 25.05.2018, Abschnitt 3 ff.)) widmen sich in ihren Tätigkeitsberichten ausführlich der Rolle und den Aufgaben, die betriebliche und behördliche Datenschutzbeauftrage nach dem 24.05.2018 wahrzunehmen haben. Bestimmt wird die Rechtslage durch die zentralen Regelungen zur Benennung, Stellung und zu den Aufgaben der Datenschutzbeauftragten in den Art. 37 bis 39 DS-GVO und den §§ 5 bis 7 und 38 BDSG nF und für behördliche DSB im Länderbereich durch die Regelungen der zwischenzeitlich auch novellierten Landesdatenschutzgesetze.

Ausführlich sind die Hinweise des Hessischen Landesdatenschutzbeauftragten, der, obwohl die in den Art. 37 bis 39 DS-GVO enthaltenen Regelungen sowie die ergänzenden Regelungen des BDSG nF die Rechtsfigur der oder des Datenschutzbeauftragten nicht neu kreieren, sondern an bereits bekannte und bewährte Regelungen anknüpfen, eine Handreichung erarbeitet hat, die in 12 – hier zusammengefasst wiedergegebenen – Kernpunkten die Voraussetzungen der Benennung, die persönlichen Anforderungen an Datenschutzbeauftragte, ihre Aufgaben, Pflichten und Stellung vor dem Hintergrund der neuen Regelungen beleuchtet (im Volltext abrufbar: https://www.datenschutz.hessen.de/download.php?download_ID=373&download_now=1).

I. Keine erleichterte Abberufung oder Kündigung bereits bestellter Datenschutzbeauftragter durch die Neu-Regelung

Grundsätzlich können bereits vor Inkrafttreten der DS-GVO bestellte Datenschutzbeauftragte nicht mit Verweis auf die neuen gesetzlichen Bestimmungen abberufen oder gekündigt werden. Um die Datenschutzbeauftragten mit der zukünftigen Rechtslage vertraut zu machen, müssen Arbeitgeber bzw. Dienstherren bereits bestellten Datenschutzbeauftragten ausreichend Ressourcen (d.h. Fortbildungsmaßnahmen, Lehrmaterial, Zeitschriften etc.) zur Verfügung stellen.

II. Benennungspflicht

Gemäß Art. 37 Abs. 1 lit. a DS-GVO und § 5 Abs. 1 BDSG nF müssen öffentliche Stellen grundsätzlich eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten benennen.

Neben den Tatbestandsvoraussetzungen der Benennung nach Art. 37 Abs. 1 lit. b und c DS-GVO für betriebliche Datenschutzbeauftragte gilt aufgrund der Öffnungsklausel des Art. 37 Abs. 4 Satz 1 DS-GVO auch weiterhin die quantitative Benennungspflicht bei ab zehn beschäftigten Personen, die ständig mit automatisierter Verarbeitung personenbezogener Daten befasst sind. Von der Möglichkeit der Öffnungsklausel des Art. 37 Abs. 4 Satz 1 DS-GVO hat der deutsche Gesetzgeber zudem für Stellen, die einer Datenschutz-Folgenabschätzung unterliegen oder die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung nutzen, Gebrauch gemacht und in § 38 Abs. 1 BDSG nF in Ergänzung zu Art. 37 Abs. 1 DS-GVO die Pflicht zur Benennung einer oder eines Datenschutzbeauftragten näher normiert.

Am Beispiel einer konzernangehörigen Firma macht die Landesbeauftragte von Bremen deutlich, dass die Auslagerung der Personalverwaltung und des Rechnungswesens an die Konzernzentrale zumeist keineswegs zur Befreiung von der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragen führt, da gleichwohl im Vorfeld umfangreich automatisiert personenbezogene Daten zum Beispiel zu Urlaubsanträgen, zur Auszahlung der Gehälter, zur Arbeitszeiterfassung und zu Erkrankungen der Mitarbeiterinnen und Mitarbeiter erhoben, gespeichert und an die Muttergesellschaft zur weiteren Bearbeitung übermittelt werden. Im Bereich des Einkaufs des Unternehmens werden personenbezogene Lieferantendaten und Kundendaten erhoben, gespeichert und zur Erfüllung der Aufgaben des Rechnungswesens an die Muttergesellschaft übermittelt. Darüber hinaus wurden im Technikbereich des Unternehmens personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter zum Beispiel für arbeitsorganisatorische Zwecke verarbeitet. Die Ermittlung der Anzahl der bei den festgestellten unterschiedlichen Verarbeitungsaktivitäten mit der Verarbeitung personenbezogener Daten beschäftigten Personen führte zu dem Ergebnis, dass diese deutlich mehr als neun beträgt und somit eine betriebliche Datenschutzbeauftragte oder ein betrieblicher Datenschutzbeauftragter zu bestellen war.

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

III. Benennungspflicht für Verantwortliche und Auftragsverarbeiter

Sowohl Verantwortliche als auch Auftragsverarbeiter müssen nach Art. 37 Abs. 1 DS-GVO und § 38 Abs. 1 BDSG nF eine oder einen Datenschutzbeauftragten benennen. Aus deutscher Sicht handelt es sich mithin um eine Erweiterung der bisher bestehenden Bestellpflicht, da bisheriger Normadressat des BDSG nur die verantwortliche Stelle war.

IV. Veröffentlichungs- und Mitteilungspflicht

Nach Art. 37 Abs. 7 DS-GVO sind die Kontaktdaten der bzw. des Datenschutzbeauftragten durch die Verantwortlichen und die Auftragsverarbeiter zu veröffentlichen und der Aufsichtsbehörde mitzuteilen (vgl. zum Verfahren Ziff. 2.4. des Berichts).

V. „Konzernprivileg" für Benennung

Die DS-GVO schafft in Art. 37 Abs. 2, Abs. 3 DS-GVO und § 5 Abs. 2 BDSG nF für Verantwortliche und Auftragsverarbeiter die Möglichkeit der Benennung einer oder eines Datenschutzbeauftragten für eine Unternehmensgruppe, vorausgesetzt diese bzw. dieser kann von jeder Niederlassung leicht erreicht werden. Zukünftig ist daher eine separate Benennung für jedes einzelne Konzernunternehmen nicht mehr zwingend erforderlich. Im Verhältnis zur bisherigen Regelung des BDSG handelt es sich somit um eine Erleichterung der formalen Anforderungen.

Unter dem Begriff der leichten Erreichbarkeit ist zum einen die Sicherstellung der persönlichen Kommunikation durch ausreichend verfügbare Kontaktmöglichkeiten, z.B. die Einrichtung eines Kontaktformulars auf der Webseite, Bereitstellung einer Telefonnummer und/oder E-Mail-Adresse, regelmäßige Sprechstunden für Beschäftigte zu verstehen, zum anderen müssen Datenschutzbeauftragte in der Lage sein, mit Aufsichtsbehörden und Betroffenen sprachlich zu kommunizieren.

VI. Interne oder externe Benennung möglich

Datenschutzbeauftragte können sowohl Beschäftigte benennpflichtiger Unternehmen sein als auch auf der Grundlage von Dienstleistungsverträgen tätig werden. Diese Wahlfreiheit wird für öffentliche Stellen durch die Vorschriften Art. 37 Abs. 6 DS-GVO und § 5 Abs. 4 BDSG nF eingeführt, für Unternehmen war dies aktuell bereits gegeben (vergleiche § 4f Abs. 2 Satz 3 und 4 BDSG).

VII. Datenschutzteam und Benennung juristischer Personen

Neben der Benennung einer einzelnen Person als Datenschutzbeauftragte bzw. Datenschutzbeauftragter ist es auch möglich, dass mehrere Personen gemeinsam die Aufgaben der bzw. des Datenschutzbeauftragten wahrnehmen. Auch die Benennung einer juristischen Person zum Datenschutzbeauftragten ist nach Ansicht der WP 29 zulässig. Diese hat hierzu im Dezember 2016 das Working Paper 243 „Guidelines on Data Protection Officers ('DPOs')" veröffentlicht. Aktuell vertreten die deutschen Aufsichtsbehörden hierzu noch unterschiedliche Auffassungen. Nach dem HessLDSB ist eine solche Gestaltung der Position der bzw. des Datenschutzbeauftragten denkbar, sofern eine solche Konstruktion allen Anforderungen genügt.

VIII. Freiwillige Benennung

Im Falle der freiwilligen Benennung betrieblicher Datenschutzbeauftragter gelten sämtliche Vorschriften des vierten Abschnitts der DS-GVO. Zu beachten ist aber, dass der zur DS-GVO hinzutretende Abberufungs- und Kündigungsschutz nach dem Wortlaut des § 38 Abs. 2 BDSG-neu nur bei der verpflichtenden Benennung zur Anwendung gelangt. Sofern der Abberufungs- und Kündigungsschutz dennoch zur Anwendung gelangen sollen, bedarf es einer entsprechenden Regelung zwischen den Parteien.

IX. Persönliche Anforderungen an den Datenschutzbeauftragten

Sowohl die DS-GVO als auch das BDSG nF verlangen, dass die Auswahl und Benennung von Datenschutzbeauftragten auf der Grundlage folgender drei Voraussetzungen erfolgt:

- berufliche Qualifikation,
- Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis,
- Fähigkeit zur Erfüllung der in der DS-GVO bzw. BDSG nF genannten Aufgaben.

Zu fordern sind hiernach jedenfalls Kenntnisse des nationalen und europäischen Datenschutzrechts und ein vertieftes Verständnis der DS-GVO, wobei sich das konkret zu fordernde Fachwissen an der Sensitivität, Komplexität und dem Umfang der Verarbeitungsvorgänge orientieren sollte. Auch das Betätigungsfeld verantwortlicher Stellen oder Auftragsverarbeiter und die hiermit verbundenen Datenverarbeitungsvorgänge (z.B. Gesundheitsdatenschutz, Beschäftigtendatenschutz oder Kundendatenschutz) können bei der Frage des erforderlichen Fachwissens der Datenschutzbeauftragten eine besondere Rolle spielen.

Über die berufliche und fachliche Qualifikation hinaus verlangt die WP 29 im Zusammenhang mit der Fähigkeit zur Erfüllung der in der DS-GVO genannten Aufgaben, dass Datenschutzbeauftragte ein hohes Maß an persönlicher Integrität und Berufsethik aufweisen (Working Paper 243, Seite 12).

X. Aufgaben und Pflichten

Bei einer Gesamtschau der Regelungen der DS-GVO sowie des BDSG nF sieht der Hessische LDSB folgenden Kernaufgaben für Datenschutzbeauftragte:

- Unterrichtung und Beratung,
- Überwachung der Einhaltung der DS-GVO und anderer Datenschutzvorschriften der Union bzw. der Mitgliedsstaa-

ten (oder des BDSG und sonstiger Vorschriften über den Datenschutz)/Zuweisung von Zuständigkeiten,
- Sensibilisierung und Schulung,
- Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung,
- Zusammenarbeit mit der Aufsichtsbehörde,
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde.

Die DS-GVO bzw. das BDSG nF seien zudem nicht nur ein beschreibender Aufgabenkatalog, sondern gäben Datenschutzbeauftragten auch gleich die Maxime mit, bei der Erfüllung ihrer Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung zu tragen, wobei sie dabei die Art und den Umfang, die Umstände und Zwecke der Verarbeitung zu berücksichtigen haben.

Überdies stehe es Behörden und Unternehmen frei, die Rolle der Datenschutzbeauftragten strategischer und proaktiver auszugestalten, als dies in der DS-GVO und dem BDSG-neu vorgesehen ist, da die Vorschriften keine abschließende Aufgabenzuweisung enthalten.

XI. Stellung des Datenschutzbeauftragten

Von ausschlaggebender Bedeutung für eine wirkungsvolle Tätigkeit ist die unabhängige und organisatorisch herausgehobene Stellung der Datenschutzbeauftragten, da sie andernfalls den zuvor beschriebenen Aufgaben und Pflichten nur schwerlich gerecht werden können.

Der HessLDSB stellt zusammengefasst folgende Themenkreise heraus.
- ordnungsgemäße und frühzeitige Einbindung der Datenschutzbeauftragten,
- Bereitstellung erforderlicher Ressourcen,
- Weisungsfreiheit und Unabhängigkeit,
- keine Benachteiligung: Abberufungs- und Kündigungsschutz,
- unmittelbarer Berichtsweg zur höchsten Führungsebene,
- Anrufungsrecht der Betroffenen,
- kein Interessenkonflikt,
- Zusammenarbeit mit der Aufsichtsbehörde.

Kernstück der Unabhängigkeit der Datenschutzbeauftragten ist die Weisungsfreiheit. Sie ist nach der DS-GVO und dem BDSG nF auf solche Handlungen beschränkt, die sich auf die Ausübung der Aufgaben der Datenschutzbeauftragten beziehen. Unternehmen und Behörden dürfen Datenschutzbeauftragten gegenüber somit keine Weisungen in ihrer Funktion als Datenschutzbeauftragte erteilen. Aus diesem Grund sind z.B. Vorgaben zur Erreichung eines bestimmten Ziels, zur Art und Weise der Bearbeitung von Beschwerden oder zum Austausch mit Aufsichtsbehörden unzulässig.

Der deutsche Gesetzgeber hat sich für eine Stärkung der Unabhängigkeit der Datenschutzbeauftragten entschieden. Das BDSG nF enthält daher die Regelung, dass eine Abberufung nur in entsprechender Anwendung des § 626 BGB möglich und Kündigungen nur aus wichtigem Grund zulässig sind. Darüber hinaus ist nach dem BDSG nF eine Kündigung des Arbeitsverhältnisses nach dem Ende der Tätigkeit als Datenschutzbeauftragte oder als Datenschutzbeauftragter innerhalb eines Jahres nach der Abberufung unzulässig, es sei denn, die kündigende Stelle ist zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt. Die bereits aus dem BDSG aF bekannten Privilegierungen bleiben somit bestehen.

XII. Sanktionen und Haftung

Verstöße gegen die gesetzlichen Regelungen zu Datenschutzbeauftragten können zukünftig mit Geldbußen von bis zu 10.000.000 EUR oder im Falle eines Unternehmens bis zu 2% seines gesamten, weltweit erzielten Jahresumsatzes geahndet werden, je nachdem, welcher Betrag höher ist. Verglichen mit den aktuell anzuwendenden Bußgeldtatbeständen des BDSG zeigt sich, dass sich mit der Neuregelung des Art. 83 DS-GVO eine erhebliche Sanktionsverschärfung für Verantwortliche und Auftragsverarbeiter ergibt.

Aufgrund des zukünftigen Aufgabenkatalogs, d.h. der deutlich erweiterten Kontroll-, Hinweis- und Beratungspflichten der Datenschutzbeauftragten, wurde in den vergangenen Monaten vermehrt diskutiert, ob hiermit auch eine weitergehende Haftung und Verantwortlichkeit der Datenschutzbeauftragen einhergeht. Die WP 29 hat sich hierzu bereits im Working Paper 243 positioniert und führt aus, dass Überwachung der Einhaltung der gesetzlichen Bestimmungen nicht bedeute, dass Datenschutzbeauftragte automatisch auch persönlich verantwortlich seien, wenn ein Verstoß gegen datenschutzrechtliche Bestimmungen festgestellt werde. Die Einhaltung des Datenschutzes sei vielmehr die unternehmerische Pflicht der Verantwortlichen / Auftragsverarbeiter und nicht der Datenschutzbeauftragten. Verantwortlich bleiben daher in erster Linie die Verantwortlichen oder Auftragsverarbeiter.

Soweit Datenschutzbeauftragte jedoch die ihnen von der DS-GVO und dem BDSG nF unmittelbar übertragenen Aufgaben nicht erfüllen, kann, ganz unabhängig von der Umsetzungsverantwortung, unter Umständen auch eine persönliche Haftung der Datenschutzbeauftragten in Betracht kommen. Es wird daher den Datenschutzbeauftragten dringend empfohlen, eigenständig die Beratungs- und Überwachungsmaßnahmen zu dokumentieren, um nachweisen zu können, dass sie die ihnen obliegenden Aufgaben ordnungsgemäß erfüllen.

Kandidatensuche in berufsorientierten sozialen Netzwerken – Rechtsgrundlage und Pflichten

Dr. Niels Lepperhoff*[1]/Tatjana Ermola*[2], Düsseldorf

I. Gezielte Recherche als Mittel gegen Personalknappheit

Offene Stellen und wenige oder keine geeigneten Bewerber führen verstärkt dazu, dass Unternehmen geeignete Personen in sozialen Netzwerken recherchieren, um sie anzuwerben. Ob eine solche Suche gesetzeskonform ist, bedarf einer näheren Betrachtung.

Wenn der Betreiber eines sozialen Netzwerkes die erlaubte Nutzung auf private oder nicht-kommerzielle Zwecke beschränkt oder eine Ansprache zur Abwerbung oder Personalsuche ausdrücklich untersagt, würde eine Suche und Ansprache von Personen zur Anwerbung gegen die Nutzungsbedingungen verstoßen. Besteht kein Verbot seitens der Nutzungsbedingungen, sind trotzdem die Datenschutzvorschriften, insbesondere der Datenschutz-Grundverordnung (DS-GVO) sowie des Bundesdatenschutzgesetzes (BDSG) zu beachten, weil bei einer Suche personenbezogene Daten elektronisch verarbeitet werden.

II. Zulässigkeit der Recherche

Bewirbt sich ein Kandidat von sich aus auf eine ausgeschriebene Stelle, erfolgt im Falle einer späteren Einstellung die Einstellungsentscheidung auf Grundlage von § 26 Abs. 1 S. 1 BDSG zur Begründung eines Beschäftigungsverhältnisses. Dieser Rechtsgrundlage ist immanent, dass die Initiative vom Kandidaten ausgegangen ist. Durch eine Bewerbung wird ein vertragsähnliches Verhältnis begründet.[1]

Sucht ein Unternehmen selbst nach den geeigneten Kandidaten, so entsteht kein vertragsähnliches Verhältnis und der § 26 Abs. 1 S. 1 BDSG ist als Rechtsgrundlage nicht anwendbar. Die Zulässigkeit der Recherche sollte sich daher aus einer anderen Rechtsgrundlage ergeben. Art. 6 Abs. 1 DS-GVO nennt drei weitere theoretisch anwendbare Rechtsgrundlagen:

- Einwilligung der betroffenen Person,
- Gesetzliche Erlaubnis und
- Interessensabwägung.

Eine Einwilligung müsste vor der Suche erteilt werden. Damit sie hinreichend bestimmt ist, bedarf sie regelmäßig der Nennung des Unternehmens, dem die Datenverarbeitung erlaubt wird. Praktisch bedeutet dieses, dass ein Kontakt zwischen der betroffenen Person und dem Unternehmen besteht. Das ist gerade nicht die vorliegende Situation, in der unbekannte Personen ermittelt werden sollen.

Eine gesetzliche Erlaubnis jenseits des hier nicht einschlägigen § 26 Abs. 1 BDSG ist nicht ersichtlich.

So bleibt die Interessensabwägung übrig. Um zu entscheiden, ob die berechtigten Interessen des Unternehmens die Interessen der betroffen Person überwiegen, bedarf es einer näheren Analyse.

Das Interesse geeignete Mitarbeiter zu suchen, ist offensichtlich berechtigt. Es fußt in der unternehmerischen Freiheit aus Art. 16 GRCh.

Ob eine Suche zulässig ist, hängt von verschiedenen Faktoren ab:

- für welchen Personenkreis das Profil sichtbar ist und
- ob die Person erkennbar eine Stelle sucht.

Eine Rechtsgrundlage für eine Suche in freizeitorientierten sozialen Netzwerken, wie z.B. Facebook, ist nicht erkennbar, weil hier die Interessen der Benutzer an Unterlassung der Suche überwiegen.

1. Profilsichtbarkeit

Ein Individuum steuert eine Datenauswertung durch ein Unternehmen bereits dann, wenn es seine Profildaten für diverse Leserkreise freischaltet.

Die DS-GVO enthält keine Norm, die eine generelle Nutzung öffentlich zugänglicher Daten erlaubt. Die Tatsache der öffentlichen Zugänglichkeit kann im Rahmen der Interessensabwägung zu Gunsten des Unternehmens berücksichtigt werden. Dies gilt jedenfalls dann, wenn kein Grund zur Annahme besteht, dass die Daten zweckgebunden oder gegen den Willen der betroffenen Person veröffentlicht wurden.

Daten, die für alle Internetnutzer auch außerhalb des sozialen Netzwerkes sichtbar sind, gelten als veröffentlicht. Der Begriff „veröffentlicht" bedeutet, dass die Daten einem für die betroffene Person nicht mehr überschaubaren Personenkreis zugänglich sind.[2] Gleiches gilt auch für Daten, die allen angemeldeten Benutzern eines sozialen Netzwerkes zugänglich sind.

Daten, die nur für Kontakte sichtbar sind, dürfen grundsätzlich nicht ausgewertet werden. Ein Unternehmen sollte daher bei einer Kontaktanfrage explizit angeben, dass es die Daten zur Anwerbung verwenden möchte,[3] und die betroffene Person muss die Kontaktanfrage angenommen haben.

Von einem Überwiegen des berechtigten Interesses eines Unternehmens spricht man jedenfalls dann, wenn eine Mehrzahl der folgend aufgelisteten Kriterien erfüllt ist:

- Die Veröffentlichung des Profils ist durch die betroffene Person steuerbar – das jeweilige soziale Netzwerk er-

*[1] Der Autor ist Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (einem Gemeinschaftsunternehmen des BvD e.V. und der GDD e.V.).

*[2] Die Autorin ist Datenschutzberaterin der Xamit Bewertungsgesellschaft mbH.

1 Göpfert/Koops, E-Recruiting über soziale Netzwerke – Herausforderungen für die arbeitsrechtliche Praxis, in: ArbRAktuell 2017, 186.

2 Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 9, Rn. 148.

3 Göpfert/Koops, E-Recruiting über soziale Netzwerke – Herausforderungen für die arbeitsrechtliche Praxis, in: ArbRAktuell 2017, 186.

laubt, die Sichtbarkeit auf Kontakte oder noch restriktiver einzuschränken.
- Die Daten sind für alle Netzwerk-Mitglieder, oder auch außerhalb des Netzwerkes sichtbar.
- In einem beruflichen Netzwerk zählt die Ansprache zur Anwerbung zu den erwarteten Nutzungsformen öffentlich sichtbarer Daten.

2. Erkennbarer Wille

Neben der Sichtbarkeit lässt auch die Formgestaltung des Profils Rückschlüsse auf die Interessen der betroffenen Person zu. Sind die Daten des Profils aktuell gehalten, spricht Vieles dafür, dass die betroffene Person die Ansprache interessierter Unternehmen erwartet. Als argumentum e contrario weisen veraltete oder nicht vervollständigte Angaben eines Profils darauf hin, dass der Nutzer nicht an einer Anwerbung interessiert ist.

Der Wunsch der betroffene Person ist zu berücksichtigten, sowohl wenn diese sich zustimmend, beispielsweise „ich suche eine neue Stelle", als auch wenn sie sich ablehnend, „bitte keine Jobangebote unterbreiten", äußert. Während eine Pflicht zum Jobangebot nicht besteht, sollte der Wunsch, keine Jobangebote zu erhalten, unbedingt respektiert werden. Durch diesen Wunsch überwiegt das Interesse der betroffenen Personen bei einer Interessensabwägung zu ihren Gunsten, was eine weitere Datennutzung zu diesem Zweck unzulässig macht.

III. Rechtsgrundlage für die Ansprache

Beim Vorliegen der oben genannten Bedingungen dürfen die Profildaten dahingehend ausgewertet werden, ob die jeweilige Person ein geeigneter Kandidat wäre. Eine Ansprache ist damit noch nicht erlaubt. Diese ergibt sich zusätzlich aus der Gegebenheit der Sichtbarkeit der Kontaktdaten, oder nämlich nicht.

Ist die Sichtbarkeit eines Profils durch die betroffene Person auf ihre direkten Kontakte, oder noch restriktiver eingestellt, so ist eine Kontaktaufnahme nur zulässig, wenn bei der Anfrage als neuer Kontakt der Zweck deutlich genannt und die Kontaktanfrage auch bestätigt wurde. Ein sich Verschaffen der Kontaktdaten oder Erfragung dieser Daten bei Dritten ist im Rahmen der hier diskutierten Interessensabwägung regelmäßig unzulässig. Dazu zählt auch die Suche nach der geschäftlichen Email-Adresse oder Telefonnummer, beispielsweise auf der Webseite des aktuellen Arbeitgebers.

IV. Beachtung der Informationspflicht

Die Informationspflicht lebt auf, sobald personenbezogene Daten erhoben werden. „Erheben" wird in der DS-GVO im Unterschied zu § 3 Abs. 3 BDSG-alt nicht (mehr) definiert. Folgt man der alten Definition, bedeutet Erheben „das Beschaffen von Daten über den Betroffenen". Für diese Interpretation spricht, dass sie dem Sinnzusammenhang entspricht, in der „Erheben" in der DS-GVO verwendet wird.

Eine visuelle Betrachtung eines Profils stellt folglich eine Erhebung von Daten über den Betroffen dar. Darüber hinaus spricht man von einer Erhebung auch bei einer Übertragung der Kontaktdaten und Eckdaten eines Profils in Listen zur späteren Entscheidung oder Kontaktaufnahme. Nach der visuellen Betrachtung eines Profils bzw. der Übertragung dessen in Listen, sind die Personen, deren Profile angesehen wurden, darüber in Kenntnis zu setzen. Die Informationspflicht besteht auch dann, wenn eine spätere Ansprache ausbleibt.

Es ist von einer direkten Erhebung im Sinne des Art. 13 DS-GVO auszugehen, da die betroffene Person die Daten selber bereitgestellt hat. Daraus folgt, dass die Information nach Art. 13 DS-GVO umzusetzen ist. Das gilt unabhängig von einer späteren Ansprache.

Die Information des Betreibers eines sozialen Netzwerks macht eine Informationspflicht desjenigen, der die Daten erhoben hat, nicht obsolet, da diese einen anderen Inhalt hat. Auf die Information kann daher lediglich dann verzichtet werden, wenn die betroffene Person eine explizit identische Information bereits erhalten hat.

V. Umsetzung des Widerspruchsrechts

Die betroffene Person kann durch den Umstand der Informierung über ihre Widerspruchsmöglichkeit eine künftige Nutzung ihrer Daten verbieten. Wird durch eine Person ein Widerspruch erhoben, so wirkt dieser ex nunc für eine künftige Verwendung der Profildaten. Zur operativen Umsetzung wäre es ratsam, eine Widerspruchsliste zu führen und jedes Profil mit dieser Liste abzugleichen.

VI. Fazit

Die Zulässigkeit der Ansprache von geeigneten Personen in berufsorientierten sozialen Netzwerken ergibt sich aus einer Interessensabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO. Die Zulässigkeit des Vorgehens bemisst sich an dem Vorliegen der Erfüllung der folgenden Kriterien:
- Die Veröffentlichung des Profils ist durch die betroffene Person steuerbar, d.h. das soziale Netzwerk bietet die Möglichkeit, die Sichtbarkeit auf Kontakte oder noch restriktiver einzuschränken.
- Die Daten sind für alle Mitglieder des Netzwerkes oder auch außerhalb des Netzwerkes sichtbar.
- In einem beruflichen Netzwerk zählt die Ansprache zur Anwerbung zu den erwarteten Nutzungsformen öffentlich sichtbarer Daten.
- Positive Willensäußerung im Profil wie z.B. „Bin offen für neue Positionen".
- Die Kontaktdaten sind sichtbar und bedürfen keiner Ermittlung oder eines „Erschleichens".

Äußert sich die betroffene Person ablehnend, „bitte keine Jobangebote unterbreiten", ist eine weitere Datenverarbeitung zur Abwerbung unzulässig.

Unabhängig von einer tatsächlichen Ansprache sind die betroffenen Personen über die Verarbeitung zu informieren. Das Widerspruchsrecht der betroffenen Person ist zu beachten.

Europäischer Blick aus erster Hand.

BUßGELDER
VON BIS ZU 4% DES GLOBALEN KONZERNUMSATZES

Ehmann/Selmayr
Datenschutz-Grundverordnung

2. Auflage. 2018. XXXVIII, 1132 Seiten.
In Leinen € 149,–
ISBN 978-3-406-72006-2
Neu im August 2018

beck-shop.de/bxaicn

Der aktuelle Kommentar

erläutert die DS-GVO aus europäischer Sicht und besonders praxisorientiert. Das Werk zeichnet sich durch eine klare Systematik aus und bietet eine wissenschaftliche Vertiefung an den entscheidenden Stellen.

Die Neuauflage

berücksichtigt die aktuelle **Rechtsprechung des EuGH,** die ersten Leitlinien der **Artikel-29-Datenschutzgruppe** zur DS-GVO, die **Evaluierung des EU-US Privacy Shields** sowie die Auswirkungen des **Brexit auf Datentransfer**s zwischen der EU und Großbritannien. Außerdem werden die nationalen Ergänzungsregelungen Deutschlands (BDSG 2018) und Österreichs (Datenschutzgesetz 2018) zur DS-GVO nachgewiesen, bei der Kommentierung der einschlägigen Bestimmungen der DS-GVO berücksichtigt und aus europarechtlicher Sicht kritisch gewürdigt.

Von echten Kennern der Materie

Die Herausgeber Dr. Eugen **Ehmann** (er kommentierte bereits die EU-Datenschutzrichtlinie aus dem Jahr 1995) und Prof. Dr. Martin **Selmayr** (der zuletzt als Kabinettschef von EU-Kommissionspräsident Juncker die Entstehung der DS-GVO maßgeblich beeinflusst hat) warten auf mit einem europäisch ausgerichteten Team von Mitarbeitern der EU-Kommission und Experten aus Aufsichtsbehörden, Wissenschaft und Anwaltschaft.

„

… ist dem »Ehmann/Selmayr« eine profunde und praxisorientierte Kommentierung der ‚DS-GVO' gelungen, die sicherlich dankenswerte Aufnahme in Wissenschaft und Praxis als Standardwerk zur ‚DS-GVO' erfahren wird.
ObRegR Dr. Holger Greve, in: NVwZ 19/2017, zur Vorauflage

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 168499
facebook.com/verlagCHBECK LinkedIn.com/company/Verlag-C-H-Beck twitter.com/CHBECKRecht

C.H.BECK

Rechtsprechung

Gemeinsame Verantwortlichkeit beim Betrieb einer Facebook-Fanpage (Ls)

(**Europäischer Gerichtshof**, Urteil vom 5. Juni 2018 – C-210/16 –)

1. **Art. 2 Buchst. d der 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 ist dahin auszulegen, dass der Begriff des „für die Verarbeitung Verantwortlichen" im Sinne dieser Bestimmung den Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage umfasst.**

3. **Art. 4 Abs. 1 Buchst. a und Art. 28 Abs. 3 und 6 der Richtlinie 95/46 sind dahin auszulegen, dass die Kontrollstelle eines Mitgliedstaats, wenn sie beabsichtigt, gegenüber einer im Hoheitsgebiet dieses Mitgliedstaats ansässigen Stelle wegen Verstößen gegen die Vorschriften über den Schutz personenbezogener Daten, die von einem Dritten begangen wurde, der für die Verarbeitung dieser Daten verantwortlich ist und seinen Sitz in einem anderen Mitgliedstaat hat, die Einwirkungsbefugnisse nach Art. 28 Abs. 3 dieser Richtlinie auszuüben, zuständig ist, die Rechtmäßigkeit einer solchen Datenverarbeitung unabhängig von der Kontrollstelle des letztgenannten Mitgliedstaatens zu beurteilen und ihre Einwirkungsbefugnisse gegenüber der in einem Hoheitsgebiet ansässigen Stelle asuüben, ohne zuvor die Kontrollstelle des anderen Mitgliedstaats um ein Eingreifen zu ersuchen.**

Dateigebundende Datenverarbeitung bei Datenerhebung im Rahmen des Verkündungsauftrags von Religionsgemeinschaften – Zeugen Jehovas (Ls)

(**Europäischer Gerichtshof** (Große Kammer), Urteil vom 10. Juli 2018 – C-25/17 –)

1. **Art. 3 II der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist im Licht von Art. 10 I der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass die Erhebung personenbezogener Daten, die durch Mitglieder einer Religionsgemeinschaft im Ramen einer Verkündigungstätigkeit von Tür zu Tür erfolgt, und die anschließenden Verarbeitungen dieser Daten weder Verarbeitungen personenbezogener Daten darstellen, die für die Ausübung von Tätigkeiten im Sinne von Art. 3 II erster Gedankenstrich dieser Richtlinie erfolgen, noch Verarbeitungen personenbezogener Daten, die von natürlichen Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen werden, wie in Art. 3 II zweiter Gedankenstrich dieser Richtlinie vorgesehen.**

2. **Art. 2 Buchst. c der Richtlinie 95/46 ist dahin auszulegen, dass der in dieser Bestimmung genannte Begriff „Datei" eine Sammlung personenbezogener Daten, die im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erhoben wurden und zu denen Namen und Adressen sowie weitere Informationen über die aufgesuchten Personen gehören, umfasst, sofern diese Daten nach bestimmten Kriterien so strukturiert sind, dass sie in der Praxis zur späteren Verwendung leicht wiederauffindbar sind. Um unter diesen Begriff zu fallen, muss eine solche Sammlung nicht aus spezifischen Kartotheken oder Verzeichnissen oder anderen der Recherche dienenden Ordnungssystemen bestehen.**

3. **Art. 2 Buchst. d der Richtlinie 95/46 ist im Licht von von Art. 10 I der Charta der Grundrechte dahin auszulegen, dass eine Religionsgemeinschaft gemeinsam mit ihren als Verkündiger tätigen Mitgliedern als Verantwortliche für die Verarbeitung personenbezogener Daten angesehen werden kann, die durch diese Mitglieder im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erfolgt, die von dieser Gemeinschaft organisiert und koordiniert wird und zu der sie ermuntert, ohne dass es hierfür erforderlich wäre, dass die Gemeinschaft Zugriff auf diese Daten hat oder ihren Mitgliedern nachweislich schriftliche Anleitungen oder Anweisungen zu diesen Datenverarbeitungen gegeben hat.**

Facebook-Nutzerkonto ist vererbbar

(**Bundesgerichtshof**, Urteil vom 12. Juli 2018 – III ZR 183/12 –)

Beim Tod des Kontoinhabers eines sozialen Netzwerks geht der Nutzungsvertrag grundsätzlich nach § 1922 BGB auf dessen Erben über. Dem Zugang zu dem Benutzerkonto und den darin vorgehaltenen Kommunikationsinhalten stehen weder das postmortale Persönlichkeitsrecht des Erblassers noch das Fernmeldegeheimnis oder das Datenschutzrecht entgegen.

Sachverhalt:

Die Parteien streiten über den Zugang zum Benutzerkonto eines sogenannten sozialen Netzwerks, das die Beklagte betreibt. Die Klägerin beansprucht, den Zugang zu dem bei der Beklagten unterhaltenen Konto ihrer verstorbenen, minderjährigen Tochter und „den darin vorgehaltenen Kommunikationsinhalten" zu gewähren. Sie ist neben deren Vater Mitglied der Erbengemeinschaft. Beide Elternteile waren zu Lebzeiten die gesetzlichen Vertreter der Erblasserin.

Über das Netzwerk können die Nutzer miteinander internetbasiert über die Server der Beklagten kommunizieren und Inhalte austauschen. Dies umfasst etwa das Hochladen, Speichern und Teilen von Bildern, Videos oder Links zu anderen Webseiten, das Veröffentlichen („Posten") von Kommentaren und Statusmeldungen sowie den Austausch und das Speichern von Nachrichten. Für die Nutzung des Netzwerks ist nach einer Registrierung die Eingabe von Kontozugangsdaten in Form von Benutzername und Passwort erforderlich. Die Dienste des sozialen Netzwerks werden durch die F. mit Sitz in den USA und die Beklagte mit Sitz in Irland erbracht. Nach den Allgemeinen Geschäftsbedingungen von F. ist die Beklagte Vertragspartnerin der Nutzer mit Wohnsitz außerhalb der USA.

Am 4. Januar 2011 registrierte sich die Erblasserin im Alter von 14 Jahren mit Einverständnis ihrer Eltern beim sozialen Netzwerk der Beklagten und unterhielt dort ein Benutzerkonto („Account"). Am Abend des 3. Dezember 2012 verunglückte sie unter bisher ungeklärten Umständen tödlich, als sie in einem U-Bahnhof von einem einfahrenden Zug erfasst wurde.

Die Klägerin versuchte hiernach, sich unter Verwendung der Zugangsdaten ihrer Tochter in das Benutzerkonto der Erblasserin einzuloggen. Dies gelang jedoch nicht, weil die Beklagte das Konto nach Mitteilung des Todes der bisherigen Nutzerin durch einen Dritten am 9. Dezember 2012 in den sogenannten Gedenkzustand versetzt hatte. In diesem ist ein Zugang zu dem Benutzerkonto auch mit den zutreffenden Zugangsdaten nicht mehr möglich. Das Konto an sich einschließlich der auf den Servern der Beklagten gespeicherten Inhalte bleibt aber bestehen, und die vom Verstorbenen geteilten Inhalte sind für die Zielgruppe, mit der sie geteilt wurden, weiterhin sichtbar. Die Kommunikationspartner („Freunde") des Verstorbenen können – abhängig von den Privatsphäreeinstellungen des Kontos – in der in den Gedenkzustand versetzten Chronik Erinnerungen teilen. Im Übrigen hat jedoch außer der Beklagten niemand mehr Zugriff auf den Kontoinhalt, z.B. die gespeicherten Fotos und Nachrichten. Die Regelungen zum Gedenkzustand sind im Hilfebereich der Internetseite der Beklagten abrufbar. In den allgemeinen Nutzungsbedingungen wird hierauf nicht verwiesen.

Die Klägerin trägt vor, die Erbengemeinschaft benötige den Zugang zu dem Benutzerkonto, um Aufschluss darüber zu erhalten, ob die Erblasserin kurz vor ihrem Tod Suizidabsichten gehegt habe. Ferner benötige sie den Zugang, um Schadensersatzansprüche des U-Bahn Fahrers abzuwehren. Die persönlichen Kommunikationsinhalte im Benutzerkonto ihrer Tochter seien an die Erbengemeinschaft vererbt worden. Dem stehe auch nicht der Schutz des Fernmeldegeheimnisses aus § 88 TKG entgegen, weil diese Regelung auf die Beklagte weder in persönlicher noch in sachlicher Hinsicht anwendbar sei. Jedenfalls sei die Beseitigung der durch den Gedenkzustand bewirkten Zugangssperre gerechtfertigt. Der Datenschutz zugunsten der Kommunikationspartner der Erblasserin trete im Rahmen der praktischen Konkordanz der betroffenen Grundrechtspositionen hinter den Zugangsanspruch der Erben zurück. Schließlich seien die Nutzungsbestimmungen zum Gedenkzustand, soweit überhaupt wirksam einbezogen, gemäß § 307 Abs. 1 Satz 1 BGB unwirksam.

Das Landgericht hat die Beklagte verurteilt, der Erbengemeinschaft Zugang zu dem vollständigen Benutzerkonto der Erblasserin und den darin vorgehaltenen Kommunikationsinhalten zu gewähren (FamRZ 2016, 738). Auf die Berufung der Beklagten hat das Kammergericht die Klage abgewiesen.

Mit der vom Berufungsgericht zugelassenen Revision verfolgt die Klägerin ihr Klagebegehren weiter.

Aus den Gründen:

Die zulässige Revision der Klägerin hat Erfolg. Sie führt zur Aufhebung des angefochtenen Urteils und zur Zurückweisung der Berufung der Beklagten und damit zur Wiederherstellung des klagezusprechenden Ersturteils.

I. Das Berufungsgericht (FamRZ 2017, 1348) hat offen gelassen, ob die Erbengemeinschaft aus erbrechtlicher Sicht nach § 1922 BGB einen Anspruch auf Zugang zu dem Benutzerkonto der Erblasserin habe. Jedenfalls verbiete § 88 Abs. 3 Satz 3 TKG der Beklagten, den Eltern der Erblasserin den Inhalt und die Umstände der über das Benutzerkonto abgewickelten und auf den Servern der Beklagten noch gespeicherten Kommunikation mitzuteilen.

Als Betreiberin des sozialen Netzwerks sei die Beklagte Diensteanbieterin nach § 3 Nr. 6 TKG, wenn hierüber Nachrichten und Inhalte ausgetauscht oder geteilt würden. Sie übertrage zwar nicht selbst Signale, müsse sich aber die fremde Signalübertragungsleistung der Telekommunikationsunternehmen zurechnen lassen. Außerdem sei die Beklagte Diensteanbieterin gemäß § 2 Satz 1 Nr. 1 TMG, so dass – über § 3 Abs. 3 Nr. 1, 2 und 4 TMG – nach § 7 Abs. 3 Satz 2 TMG die Regelungen in § 88 Abs. 3 TKG Anwendung fänden.

Der Schutzbereich des § 88 TKG umfasse den Inhalt und die Umstände der über den Dienst der Beklagten ausgetauschten privaten Nachrichten und der mit einem begrenzten Nutzerkreis geteilten Inhalte. Dies gelte unabhängig von der Kenntnisnahme durch den Empfänger, solange der Kommunikationsinhalt auf den Servern der Beklagten gespeichert sei.

Insbesondere fehle es an einer gesetzlichen Erlaubnis zur Weitergabe von Telekommunikationsinhalten an die Erben nach § 88 Abs. 3 Satz 3 TKG, die sich ausdrücklich auf Telekommunikationsvorgänge beziehe. Diese Voraussetzungen würden weder § 1922 BGB noch §§ 91 ff. TKG erfüllen. Die Erben seien auch nicht am Kommunikationsvorgang beteiligt und daher „andere" im Sinne von § 88 Abs. 3 Satz 3 TKG. Das Fernmeldegeheimnis müsse zudem nicht im Wege der praktischen Konkordanz hinter die Interessen der Erben zurücktreten, weil dieses keine Rechtfertigung für einen Eingriff ohne entsprechendes Gesetz biete.

Die Zugangsgewährung sei auch nicht aufgrund einer Einwilligung der Kommunikationsteilnehmer möglich. Ungeachtet dessen, ob die Erblasserin eine solche Einwilligung erteilt habe, fehle jedenfalls eine konkludente oder mutmaßliche Einwilligung ihrer Kommunikationspartner in die Weitergabe von Kommunikationsinhalten an die Erben.

Schließlich bestehe auch kein Schadensersatzanspruch nach §§ 280, 1922 BGB auf Rückgängigmachung des Gedenkzustands, weil die Beklagte zu dessen Einrichtung berechtigt gewesen sei. Das elterliche Sorgerecht habe mit dem Tod der Erblasserin geendet, und aus dem Totenfürsorgerecht lasse sich ein Zugangsanspruch ebenfalls nicht herleiten. Dies gelte auch für das allgemeine Persönlichkeitsrecht der Eltern und ihren Wunsch, Gewissheit über die Umstände und Hintergründe des Todes ihres Kindes zu erlangen. Da sich der Schutz- und Wirkungsbereich des Bundesdatenschutzgesetzes auf lebende Personen beschränke, bestehe auch kein Auskunftsanspruch analog § 34 BDSG.

II. Das Berufungsurteil hält den Angriffen der Revision nicht stand.

1. Zutreffend haben die Vorinstanzen im Ergebnis die Zulässigkeit der Klage bejaht (zur internationalen Zuständigkeit siehe jedoch Art. 17 Abs. 1 Buchst. c), Abs. 2 i.V.m. Art. 18 Abs. 1 Var. 2 der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen – Brüssel Ia-VO; ABl. L 351 vom 20. Dezember 2012, S. 1). Die Beklagte erhebt insoweit auch keine Rügen mehr.

2. Entgegen der Auffassung des Berufungsgerichts ist die Klage begründet. Die Klägerin ist berechtigt, von der Beklagten zu verlangen, der Erbengemeinschaft Zugang zum Benutzerkonto der Erblasserin sowie den darin enthaltenen Inhalten zu gewähren. Ein solcher Anspruch ist vererblich, und es stehen ihm weder das postmortale Persönlichkeitsrecht noch das Fernmeldegeheimnis, datenschutzrechtliche Regelungen oder das allgemeine Persönlichkeitsrecht der Kommunikationspartner der Erblasserin entgegen (ebenso z.B.: BeckOK BGB/Müller-Christmann, Stand 1. Mai 2018, § 1922 Rn. 101; BeckOGK BGB/Preuß, Stand 1. Juni 2018, § 1922 Rn. 387 ff.; MüKoBGB/Leipold, 7. Aufl., § 1922 Rn. 25 ff.; Biermann, ZErb 2017, 210 ff.; Bock, AcP 217, 370 ff.; Herzog, ZErb 2017, 205 ff.; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, §§ 4 und 5; Klas/Möhrke-Sobolewski, NJW 2015, 3473 ff.; Lange/Holtwiesche, ZErb 2016, 125 ff. und 157 ff.; Lieder/Berneith, FamRZ 2016, 743 f.; Litzenburger, FD-ErbR 2017, 392155; Ludyga, JM 2016, 442 ff.; und ZEV 2018, 1 ff.; Salomon, NotBZ 2016, 324 ff.; Seidler, Digitaler Nachlass, S. 114 ff.; Solmecke/Köbrich/Schmitt, MMR 2015, 291 ff.; Willems, ZfPW 2016, 494, 502 ff.; a.A. Staudinger/Kunz (2017), BGB § 1922 Rn. 596.6 ff.; Brinkert/Stolze/Heidrich, ZD 2013, 153 ff.; Leeb, K&R 2014, 693 ff.; Martini, JZ 2012, 1145 ff.).

a) Der Anspruch auf Zugang zu dem Benutzerkonto und den dort gespeicherten Inhalten ergibt sich aus dem auf die Erben übergegangenen schuldrechtlichen Vertrag zwischen der Erblasserin und der Beklagten.

aa) Das Berufungsgericht ist zutreffend davon ausgegangen, dass die Beklagte und die Erblasserin mit Einwilligung ihrer gesetzlichen Vertreter (§ 107 BGB) einen schuldrechtlichen Vertrag über die Einrichtung und Nutzung eines „Accounts" geschlossen haben (vgl. Redeker, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Stand Februar 2018, Teil 12 Rn. 424; Redeker, IT-Recht, 6. Aufl., D. Rn. 1174; Kosmides, in: Schneider, Handbuch EDV-Recht, 5. Aufl., W. Rn. 525 ff.; Staudinger/Klumpp (2017), BGB § 107 Rn. 30; Kutscher, Der digitale Nachlass, S. 45 f.). Die Rechtsnatur dieses Vertrags (vgl. hierzu Redeker, in: Hoeren/Sieber/Holznagel, aaO; Kutscher, aaO; Seidler, Digitaler Nachlass, S. 129 ff.; Bräutigam, MMR 2012, 635) kann dahingestellt bleiben, da diese für die hier relevanten Rechtsfragen nicht erheblich ist.

bb) Zu Recht und ohne dass dies von den Parteien angegriffen wird, haben die Vorinstanzen auf das Vertragsverhältnis deutsches Recht angewandt. Der Vertrag unterliegt nach Art. 3 Abs. 1, Art. 6 Abs. 2 der Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I-VO; ABl. L 177 vom 4. Juli 2008, S. 6) dem von den Parteien gewählten deutschen Recht. Dessen Anwendbarkeit ergäbe sich zudem nach Art. 6 Abs. 1 Rom I-VO, weil ein Verbrauchervertrag vorliegt.

cc) Das Vertragsverhältnis mit seinen Rechten und Pflichten ist mit dem Tod der Erblasserin nach § 1922 Abs. 1 BGB auf die Erben übergegangen, die hierdurch in dieses eingetreten sind und deshalb als Vertragspartner einen Anspruch auf Zugang zu dem Benutzerkonto der Erblasserin sowie den darin enthaltenen vermögensrechtlichen und höchstpersönlichen (digitalen) Inhalten haben.

Nach § 1922 Abs. 1 BGB geht das Vermögen als Ganzes auf die Erben über. Hierzu gehören grundsätzlich auch Ansprüche und Verbindlichkeiten aus schuldrechtlichen Verträgen wie dem hier vorliegenden Nutzungsvertrag, wobei der Erbe in die vertragliche Rechtsstellung mit sämtlichen Rechten und Pflichten eintritt (vgl. MüKoBGB/Leipold, 7. Aufl., § 1922 Rn. 20 und 25; BeckOGK BGB/Preuß, Stand 1. Juni 2018, § 1922 Rn. 173 ff.).

Die Vererbbarkeit des aus dem Nutzungsvertrag folgenden Anspruchs auf Zugang zu dem Benutzerkonto ist weder durch die vertraglichen Bestimmungen ausgeschlossen (hierzu unter (1)), noch lässt sich ein Ausschluss der Vererbbarkeit aus dem Wesen des Vertrags ableiten (hierzu unter (2)). Auch eine Differenzierung nach der Art des Inhalts der auf dem Konto gespeicherten Daten ist abzulehnen (hierzu unter (3)).

(1) Die Vererbbarkeit von Ansprüchen kann vertraglich ausgeschlossen werden (vgl. MüKoBGB/Leipold, 7. Aufl., § 1922 Rn. 21; BeckOGK BGB/Preuß, Stand 1. Juni 2018, § 1922 Rn. 173). Dies ist hier indes nicht der Fall.

(1.1) Die Nutzungsbedingungen der Beklagten enthalten keine Regelung zur Vererbbarkeit des Benutzungsvertrags und der Inhalte des Benutzerkontos. Zwar ist dieses hiernach unter einem realen Namen einzurichten (Nummer 4) und die Weitergabe von Zugangsdaten oder des Benutzerkontos an Dritte nicht zulässig (Nummern 3.5, 4.1, 4.8 und 4.9). Zutreffend hat das Berufungsgericht hierzu jedoch ausgeführt, dass sich diese Regelungen lediglich auf das Verhalten des Nutzers zu Lebzeiten beziehen und keine Aussage für den Todesfall enthalten. Offen bleiben kann dementsprechend, ob die Vererbbarkeit des vertraglichen Nutzungsverhältnisses und des daraus folgenden Kontozugangsrechts in Allgemeinen Geschäftsbedingungen grundsätzlich wirksam ausgeschlossen werden kann (befürwortend im Rahmen einer Einzelfallbetrachtung: MüKoBGB/Leipold, 7. Aufl., § 1922 Rn. 29; Biermann, in: Scherer, Münchener Anwaltshandbuch Erbrecht, 5. Aufl., § 50 Rn. 58 ff.; Staudinger/Kunz (2017), BGB § 1922 Rn. 596.22 ff.; Bock, AcP 2017, 370, 411 ff.; Lange/Holtwiesche, ZErb 2016, 125, 127 ff.; Raude, ZEV 2017, 433, 437; ablehnend unter Hinweis auf § 1922 BGB: Gloser, MittBayNot 2016, 12, 19; Herzog, NJW 2013, 3745, 3751; Kutscher, Der digitale Nachlass, S. 126 f.; NK-NachfolgeR/Herzog, Kap. 9 Rn. 92; Pruns, AnwZert ErbR 16/2016 Anm. 2 mwN).

(1.2) Eine Unvererblichkeit ergibt sich auch nicht aus den Regelungen der Beklagten zum Gedenkzustand.

(1.2.1) Diese finden hier schon deshalb keine Anwendung, weil die Bestimmungen nicht Bestandteil des Nutzungsvertrags geworden sind, § 305 Abs. 2 BGB (vgl. Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 5 Rn. 18 ff.; Ludyga, ZEV 2018, 1, 3; Pruns, AnwZert ErbR 16/2016 Anm. 2; Willems, ZfPW 2016, 494, 509). Die dem Vertrag zwischen der Erblasserin und der Beklagten zu Grunde liegenden Nutzungsbedingungen enthalten keine Regelungen zum Gedenkzustand. Vielmehr befanden sich diese lediglich im Hilfebereich des sozialen Netzwerks, ohne dass hierauf in den Nutzungsbedingungen oder auf andere Weise bei Vertragsschluss verwiesen oder Bezug genommen wurde, wie es gemäß § 305 Abs. 2 Nr. 1 und 2 BGB erforderlich gewesen wäre, um die Regelungen Vertragsbestandteil werden zu lassen.

(1.2.2) Die Regelungen zum Gedenkzustand schließen ungeachtet dessen auch nach Maßgabe von § 307 Abs. 1, Abs. 2 Nr. 1 BGB die Vererbbarkeit des aus dem Nutzungsverhältnis fol-

genden Kontozugangsrechts nicht wirksam aus (für eine Unwirksamkeit der Regelungen zum Gedenkzustand auch MüKoBGB/Leipold, 7. Aufl., § 1922 Rn. 29; NK-NachfolgeR/Herzog, Kap. 9 Rn. 95; Deusch, ZEV 2016, 189, 195; Gloser, DNotZ 2016, 537, 548 f.; Kutscher, Der digitale Nachlass, S. 126 ff.; Litzenburger, FD-ErbR 2017, 392155; Ludyga, JM 2016, 442, 446; ders., ZEV 2018, 1, 3; Pruns, AnwZert ErbR 16/2016 Anm. 2; Raude, RNotZ 2017, 17, 23; offen: Lange/Holtwiesche, ZErb 2016, 125, 129; aA im Hinblick auf § 88 TKG: Staudinger/Kunz (2017), BGB § 1922 Rn. 596.26 f.). Sie verändern nachträglich die Leistungspflichten der Beklagten. Diese müsste nach Mitteilung des Todes zwar weiterhin die Kommunikationsplattform für das Benutzerkonto der Erblasserin zur Verfügung stellen, allerdings den Erben als neuen Vertragspartnern keinen Zugang zu dem Konto und den dort gespeicherten nicht öffentlichen Inhalten mehr gewähren.

(1.2.2.1) Entgegen der Auffassung des Berufungsgerichts unterliegen diese Regelungen der Inhaltskontrolle nach § 307 Abs. 1 und 2 BGB. Es handelt sich nicht um nach § 307 Abs. 3 Satz 1 BGB der Inhaltskontrolle entzogene Leistungsbestimmungen. Die Freistellung von der Inhaltskontrolle gilt nur für Abreden über den unmittelbaren Leistungsgegenstand, während Regelungen, die die Leistungspflicht des Verwenders einschränken, verändern, ausgestalten oder modifizieren, inhaltlich zu kontrollieren sind (ausführlich und mwN: Senat, Urteil vom 5. Oktober 2017 – III ZR 56/17, NJW 2018, 534 Rn. 15 f.). Für die der Überprüfung entzogene Leistungsbeschreibung verbleibt nur der enge Bereich von Regelungen, ohne deren Vorliegen mangels Bestimmtheit oder Bestimmbarkeit des wesentlichen Vertragsinhalts ein wirksamer Vertrag nicht mehr angenommen werden kann (Senat aaO). Dies ist bei den Regelungen zum Gedenkzustand nicht der Fall. Sie stellen nicht eine zum Kernbereich der Vereinbarung gehörende Abrede über den unmittelbaren Leistungsgegenstand dar, sondern eine nachträgliche Änderung des bestehenden Leistungsumfangs. Die grundsätzlich unbeschränkt bestehende vertragliche Hauptleistungspflicht der Beklagten, dem Nutzer den Zugang zu seinem Konto und den dort gespeicherten Inhalten sowie die Verfügungsmöglichkeit hierüber zu gewähren, wird hierdurch gegenüber den Erben für die Zeit nach Mitteilung des Todes eingeschränkt und damit ein wesentlicher Inhalt der Ansprüche aus dem Nutzungsvertrag modifiziert.

(1.2.2.2.) Im Hinblick auf die erhebliche Einschränkung der vertraglichen Rechte der in den Nutzungsvertrag eingetretenen Erben liegt eine unangemessene Benachteiligung im Sinne von § 307 Abs. 1, Abs. 2 BGB vor. Die Klauseln verhindern zwar die Vererbung des Nutzungsverhältnisses als solches nicht, sie höhlen dieses aber aus, indem den Erben als Vertragspartnern nach der Mitteilung des Todes durch einen beliebigen Dritten das Recht des Zugangs zu dem Konto verwehrt wird und sie damit einen Hauptleistungsanspruch verlieren. Dies widerspricht im Sinne von § 307 Abs. 2 Nr. 1 BGB den wesentlichen Grundgedanken des § 1922 BGB, der den Übergang eines Schuldverhältnisses mit allen Rechten und Pflichten auf den Erben vorsieht. Weiterhin ist zu berücksichtigen, dass der Grundsatz der Universalsukzession auch der eindeutigen Zuordnung des Vermögens und damit der Rechtssicherheit der Beteiligten dient (Pruns, AnwZert ErbR 16/2016 Anm. 2). Dies wäre nicht gewährleistet, wenn durch den Gedenkzustand ein „Datenfriedhof" geschaffen würde, auf den bis auf die Beklagte niemand einen Zugriff erhält. Entgegen einer im Schrifttum vertretenen Auffassung besteht auch kein berechtigtes Interesse der Beklagten an dieser Regelung im Hinblick auf das Fernmeldegeheimnis, weil sie bei Zugangsgewährung gerade nicht gegen die in § 88 TKG statuierten Verhaltenspflichten verstößt (hierzu unten 2c; a.A. Staudinger/Kunz (2017), BGB § 1922 Rn. 596.27).

Zugleich liegt ein Verstoß gegen § 307 Abs. 2 Nr. 2 BGB vor, da das Versetzen in den Gedenkzustand dazu führt, dass die wesentlichen Rechte aus dem Vertragsverhältnis, nämlich der Zugang zu dem Benutzerkonto, der Zugriff auf die dort gespeicherten Inhalte und die Verfügungsbefugnis hierüber, entfallen, so dass die Erreichung des Vertragszwecks nicht mehr möglich ist (vgl. Gloser, DNotZ 2016, 537, 548 f.; Kutscher, Der digitale Nachlass, S. 126 ff.; Raude, RNotZ 2017, 17, 23).

Auf sich beruhen kann, ob die Regelungen zum Gedenkzustand auch nach § 308 Nr. 4 BGB unwirksam sind, weil die Beklagte sich darin vorbehält, Inhalte „möglicherweise" und „in seltenen Fällen" trotz der Versetzung eines Kontos in diesen Zustand herauszugeben.

(2) Auch aus dem Wesen des Vertrags ergibt sich eine Unvererbbarkeit nicht.

Eine solche kann ohne vertragliche Regelung anzunehmen sein, wenn unter Berücksichtigung des sich aus § 399 BGB sowie § 38 BGB ergebenden Rechtsgedankens der Inhalt des Rechts in einem solchen Maß auf die Person des Berechtigten oder des Verpflichteten zugeschnitten ist, dass bei einem Subjektwechsel die Leistung in ihrem Wesen verändert würde (MüKoBGB/Leipold, 7. Aufl., § 1922 Rn. 21; Staudinger/Kunz (2017), BGB § 1922 Rn. 596.10 f.). Das ist hier nicht der Fall.

(2.1) Die Pflichten der Vertragsparteien – der Beklagten und des jeweiligen Nutzers – sind nicht höchstpersönlicher Natur. Nicht die Leistungen der Beklagten, die bei jedem Nutzer gleich sind, sondern nur die – von der Vertragsgestaltung unabhängigen – Inhalte, die von den Nutzern geschaffen und kommuniziert werden, sind persönlichkeitsrelevant (z.B. das Gestalten der Profilseite oder das Versenden von Nachrichten; vgl. Kutscher, Der digitale Nachlass, S. 157). Die Beklagte verpflichtet sich gegenüber ihrem Vertragspartner, die Kommunikationsplattform zur Verfügung zu stellen und entsprechend dem Auftrag des Nutzers Inhalte zu veröffentlichen oder Nachrichten an ein anderes Benutzerkonto zu übermitteln sowie die übermittelten Nachrichten beziehungsweise die mit diesem Konto geteilten Inhalte zugänglich zu machen. Insoweit handelt es sich um rein technische Leistungen der Beklagten, die nicht personenbezogen sind. Diese können – anders als etwa bei einem Behandlungsvertrag mit einem Arzt – unverändert auch gegenüber den Erben erbracht werden (Staudinger/Kunz (2017), BGB § 1922 Rn. 596.11; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 4 Rn. 42; Lange/Holtwiesche, ZErb 2016, 125, 129 f.; Raude, ZEV 2017, 433, 436; i.E. auch Willems, ZfPW 2016, 494, 506; a.A. Klas/Möhrke-Sobolewski, NJW 2015, 3473, 3474).

Zutreffend ist zwar, dass das Vertragsverhältnis insoweit auf den Kontoberechtigten zugeschnitten und damit personenbezogen ist, als nur dieser unter seinem Konto Inhalte veröffentlichen („posten") und Nachrichten schreiben darf. Dies führt aber nicht zu dessen Unvererbbarkeit, sondern könnte allenfalls dazu führen, dass – wie beim Girovertrag (hierzu BGH, Urteile vom 18. Januar 2000 – XI ZR 160/99, NJW 2000, 1258 und vom 10. Oktober 1995 – XI ZR 263/94, BGHZ 131, 60, 64) – die aktive Weiternutzung des Kontos des Erblassers durch den Erben, die in der Praxis ohnehin regelmäßig nicht beabsichtigt sein

wird, nicht von seinem Erbrecht umfasst ist (vgl. hierzu Herzog, NJW 2013, 3745, 3749; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 4 Rn. 37 f.; Raude, RNotZ 2017, 17, 20). Vorliegend kann dies auf sich beruhen, denn Gegenstand des Rechtsstreits ist lediglich die Bereitstellung der vorhandenen Kontoinhalte zum Abruf durch die Erben. Der Inhalt dieser Leistung der Beklagten hängt aber nicht von der Person ab, der gegenüber sie erbracht wird, so dass in dieser Hinsicht gerade kein schutzwürdiges Interesse der Beklagten daran besteht, sie nicht gegenüber den Erben erbringen zu müssen.

Im Hinblick darauf, dass vorliegend als erbrechtliche Position nicht die – von der Klägerin wie regelmäßig von den Erben auch nicht beabsichtigte – Fortführung des Kontos durch aktive Nutzung in Rede steht, ist auch nicht erheblich, ob die Beklagte – wie von ihr in der Berufungsinstanz vorgetragen – über interne Verfahren verfügt, um die Identität ihrer Nutzer regelmäßig zu prüfen, und ob sie eine derartige Prüfung vornimmt. Auch dies würde keine die Vererbbarkeit in diesem Sinne ausschließende Höchstpersönlichkeit begründen. Denn die gegenüber dem Erben geschuldete Leistungserbringung in Form der Zugangsgewährung zu dem bestehenden Kontoinhalt hat als solche keinen höchstpersönlichen Bezug.

(2.2) Die höchstpersönliche, eine Vererbbarkeit ausschließende Natur des Vertrags ergibt sich auch nicht daraus, dass die Nutzer der Beklagten die „nicht-exklusive, übertragbare, unterlizensierbare, gebührenfreie, weltweite Lizenz für die Nutzung jeglicher IP-Inhalte" (Nummer 2.1. der AGB) gewähren. Zwar erhält die Beklagte hierdurch – die Wirksamkeit der Klausel vorausgesetzt – Rechte auf individuelle, personenbezogene Daten. Diese bleiben aber ungeachtet des erbrechtlichen Übergangs bestehen. Denn durch den Erbfall wird die Datenbasis, über die die Beklagte vertragsgemäß verfügen darf, nicht verändert. Die im Zeitpunkt des Erbfalls vorhandenen Daten bleiben nutzbar, weitere persönliche Daten kommen nicht hinzu, da der Anspruch der Klägerin nicht auf die aktive Fortführung des Kontos und das Erstellen von Inhalten, sondern auf den Zugang zu dem bestehenden Konto und dessen Inhalten zielt. Insofern ist für die Beklagte ein Wechsel der Person des Kontoberechtigten nicht unzumutbar.

(2.3) Der höchstpersönliche Charakter und damit der vertragliche Ausschluss der Vererbbarkeit des Zugangsrechts zu dem Benutzerkonto folgt auch nicht aus im Nutzungsvertrag stillschweigend vorausgesetzten und damit immanenten Gründen des Schutzes der Persönlichkeitsrechte der Kommunikationspartner der Erblasserin. Zwar mag der Abschluss eines Nutzungsvertrags mit dem Betreiber eines sozialen Netzwerks in der Erwartung erfolgen, dass Nachrichten zwischen den Teilnehmern des Netzwerkes und sonstige nicht öffentlich geteilte Inhalte jedenfalls grundsätzlich vertraulich bleiben und durch die Beklagte dritten Personen gegenüber nicht offengelegt werden. Es besteht jedoch nach den vertraglichen Regeln und den zugrunde liegenden technischen Bedingungen kein schutzwürdiges Vertrauen, dass diese Diskretion des Austausches zwischen dem verstorbenen Nutzer und den übrigen Teilnehmern des Netzwerks – auch über den Tod hinaus – gegenüber den Erben gewährleistet ist.

(2.3.1) Die vertragliche Verpflichtung der Beklagten zur Übermittlung und Bereitstellung von Nachrichten und sonstigen Inhalten ist von vornherein kontobezogen.

Die Pflicht der Beklagten bezieht sich nicht darauf, die Nachrichten und sonstigen Inhalte an eine bestimmte Person zu übermitteln beziehungsweise für diese zugänglich zu machen, sondern auf die Übermittlung beziehungsweise Bereitstellung für das angegebene Benutzerkonto. Angesichts der systemimmanenten, dem verständigen Nutzer bewussten und von der Beklagten nicht kontrollierbaren Anonymität des sich jeweils bei dem Benutzerkonto anmeldenden Nutzers kann nicht von einer Verpflichtung der Beklagten zur Übermittlung an eine bestimmte Person, sondern nur zur Übermittlung an beziehungsweise Bereitstellung für das ausgewählte Benutzerkonto ausgegangen werden (vgl. Herzog, ZErb 2017, 205, 208; NK-NachfolgeR/Herzog, Kap. 9 Rn. 68; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 4 Rn. 61). So ist weder für die Beklagte noch für den Versender einer Nachricht oder Teilenden eines Inhalts prüfbar, ob die sich mit den Benutzerdaten anmeldende Person mit der als Empfänger benannten Person identisch ist. Ebenso wenig ist für den Übermittler der Nachricht erkennbar, ob die als Empfänger genannte Person tatsächlich Inhaber des Benutzerkontos ist. Vielmehr ist Identifikationsmerkmal des Adressaten ein von dem Versender ausgewähltes Benutzerkonto. An dieses sollen die Nachrichten übermittelt werden beziehungsweise für dieses sollen die geteilten Inhalte freigegeben werden. Zugang erhält damit bestimmungsgemäß derjenige, der sich mit den zutreffenden Kontozugangsdaten bei dem jeweiligen Benutzerkonto anmeldet. Das Risiko, dass das Benutzerkonto unter falschem Namen geführt wird, trägt der Kommunikationspartner (vgl. hierzu Graulich in Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl. 2015, § 88 Fernmeldegeheimnis Rn. 65). Gleiches gilt hinsichtlich der Gefahr, dass ein Dritter die Nachrichten und sonstigen Inhalte lesen kann, weil er durch Weitergabe der Zugangsdaten seitens des Kontoinhabers Zugriff auf den Inhalt des Benutzerkontos hat oder weil der Kontoberechtigte die Inhalte an Dritte weiterleitet oder diesen zeigt. Insoweit gilt nichts anderes als bei analogen Kommunikationswegen – das Briefe zustellende Unternehmen ist nur für den Einwurf in den richtigen Briefkasten verantwortlich, nicht aber dafür, ob auch die als Empfänger benannte Person den Brief öffnet oder ob sie diesen Dritten zeigt. Dem verständigen und durchschnittlichen Nutzer eines sozialen Netzwerks ist ebenso wie dem Absender eines Briefs bewusst, dass er nach dem Versenden einer Nachricht nicht mehr kontrollieren kann, wer letztlich von deren Inhalt Kenntnis nimmt, und dass er grundsätzlich keine Möglichkeit hat, die übermittelte Nachricht beziehungsweise den Inhalt zurückzufordern. Er begibt sich insoweit der Verfügungsbefugnis über die Nachrichten (vgl. NK-NachfolgeR/Herzog, Kap. 9 Rn. 68; Bock, AcP 217, 370, 408; Herzog/Pruns, aaO, § 4 Rn. 84; Kutscher, Der digitale Nachlass, S. 145; Pruns, NWB 2014, 2175, 2182 f.).

Die Beklagte erfüllt ihre vertragliche Verpflichtung somit, indem sie eine Nachricht an das benannte Benutzerkonto übermittelt, deren jederzeitigen Abruf durch den mit den zutreffenden Kontozugangsdaten bei dem Benutzerkonto angemeldeten Nutzer ermöglicht und sonstige Inhalte für die ausgewählten Benutzerkonten zur Verfügung stellt. Die geschützte Kommunikation umfasst demnach die Speicherung, Bereitstellung und Übermittlung von Inhalten für denjenigen, der sich mit den zutreffenden Daten bei dem Benutzerkonto anmeldet. Greift nicht der Kontoberechtigte, sondern ein anderer mit den Zugangsdaten hierauf zu, ist eine derartige Kenntnisnahme allein der durch die Kommunikationsteilnehmer beherrschten und bei verständiger Würdigung bekannten Risikosphäre zuzuordnen. Trägt der Kommunikationspartner des Kontoinhabers bereits das Ri-

siko, dass zu dessen Lebzeiten Dritte Kenntnis von den dort gespeicherten Inhalten erlangen, gilt dies erst recht für den Zugriff der Erben des Nutzers auf diese.

Der Auftrag zur Übermittlung einer Nachricht an das vom Absender benannte Benutzerkonto wirkt dabei – vorbehaltlich einer dem Versender in Grenzen möglichen vorherigen Festlegung des Zeitpunkts, an dem die Nachricht ausgeblendet werden soll – zeitlich unbegrenzt auch über den Todesfall hinaus und umfasst die Möglichkeit, die auf dem Server der Beklagten gespeicherte Nachricht durch den Nutzer des Empfängerkontos abzurufen, solange dieses besteht. Bestimmungsgemäß befinden sich an ein konkretes Benutzerkonto gesendete Nachrichten nicht mehr im Zugriffsbereich des Absenders, sondern in dem des Berechtigten des Empfängerkontos, der einen Anspruch gegen das soziale Netzwerk hat, ihm jederzeit und dauerhaft den Zugriff hierauf zu ermöglichen. Deshalb kann der Absender nach der Übermittlung grundsätzlich auch nicht mehr verlangen, dass die Nachricht vom Empfängerkonto gelöscht wird, worauf die Beklagte in ihrem Hilfebereich hinweist. Insoweit ist die Situation ebenfalls vergleichbar mit analogen Übermittlungswegen – auch dort besteht keine Möglichkeit mehr, das übermittelte Dokument zurückzufordern, sobald es in den Zugriffsbereich des Adressaten gelangt ist, also zum Beispiel in seinen Briefkasten eingeworfen wurde.

Der Absender einer Nachricht kann mithin zwar darauf vertrauen, dass seine Nachricht von der Beklagten nur für das von ihm ausgewählte Empfängerkonto bereitgestellt wird. Er muss aber damit rechnen, dass Dritte dennoch Kenntnis vom Inhalt seiner Nachricht erhalten können. Dies gilt sowohl zu Lebzeiten des Kontoberechtigten im Hinblick auf die von diesem jederzeit veranlassbare Zugangsgewährung an Dritte als auch im Todesfall im Hinblick auf die Vererbung des Vertragsverhältnisses. Denn er muss damit rechnen, dass sein Kommunikationspartner versterben könnte und Dritte das Benutzerkonto erben, in das Vertragsverhältnis eintreten und damit als neue Kontoberechtigte Zugang auf die Kontoinhalte haben.

Für mit dem Benutzerkonto des Erblassers geteilte Inhalte anderer Nutzer gilt Entsprechendes, solange der Teilende die Berechtigung für dieses nicht ändert oder den geteilten Inhalt löscht. Insoweit muss der Teilende in gleicher Weise damit rechnen, dass weitere Personen sowohl zu Lebzeiten als auch nach dem Tod des Berechtigten des Empfängerkontos Kenntnis von dem geteilten Inhalt erlangen. Er hat es allerdings in der Hand, die Berechtigung zur Einsicht in den geteilten Inhalt zu ändern und damit den Erben für die Zukunft vom Zugang hierauf auszuschließen.

(2.3.2.) Überdies kann der Kommunikationspartner des Kontoinhabers eines sozialen Netzwerks keine berechtigte Erwartung haben, dass der Empfänger einer Nachricht diese auf dem Server des Netzwerkbetreibers belässt und nicht auf dem eigenen Computer oder einem anderen Medium (z.B. USB-Stick) lokal abspeichert oder auf Papier ausdruckt. In diesem Fall würde der Erbe ohne weiteres Zugang zum Inhalt der Nachrichten erhalten, was auch dem Versender bewusst sein muss.

(3) Die im Schrifttum teilweise befürwortete Differenzierung der Vererbbarkeit des Kontozugangs nach dem Inhalt des Benutzerkontos ist abzulehnen. Nach dieser Auffassung sollen zwar E-Mails beziehungsweise Nachrichten in einem sozialen Netzwerk mit vermögensrechtlichem Bezug vererbbar sein, nicht hingegen solche mit nichtvermögensrechtlichem, insbesondere höchstpersönlichem Inhalt (Hoeren, NJW 2005, 2113, 2114; Martini, JZ 2012, 1145, 1152; Brinkert/Stolze/Heidrich, ZD 2013, 153, 155; hierzu auch: Bräutigam, Stellungnahme des DAV zum Digitalen Nachlass, S. 16, 24 f.). Die für das Andenken an den Verstorbenen und sein postmortales Persönlichkeitsrecht erheblichen Informationen seien nicht dem Erben, sondern den nächsten Angehörigen des Erblassers zuzuleiten (Hoeren, aaO, S. 2114). Diskutiert wird hierbei zur Wahrung des postmortalen Persönlichkeitsrechts eine „Infektion" des gesamten Benutzerkontos aufgrund der Existenz von höchstpersönlichen Inhalten (zu diesem Ansatz z.B. Bräutigam, aaO, S. 24 f.; Rott/Rott, NWB-EV 2013, 160, 164; Kutscher, Der digitale Nachlass, S. 105 f) und die von einem Dritten durchzuführende Trennung zwischen vermögensrechtlichen und höchstpersönlichen Inhalten (Martini, aaO).

Selbst nach dieser Auffassung wäre hier der Zugang zu gewähren, weil die Klägerin und der Vater der Kontoinhaberin nicht nur deren Erben, sondern auch deren nächste Angehörige sind. Unabhängig davon lehnt das überwiegende Schrifttum eine solche Differenzierung zu Recht ab (BeckOK BGB/Müller-Christmann, Stand 1. Mai 2017, § 1922 Rn. 100; BeckOGK BGB/Preuß, Stand 1. Juni 2018, § 1922 Rn. 387 f.; MüKoBGB/Leipold, BGB, 7. Aufl., § 1922 Rn. 26; NK-NachfolgeR/Herzog, Kap. 9 Rn. 38 ff.; Staudinger/Kunz (2017), BGB § 1922 Rn. 596.6 ff.; Biermann, ZErb 2017, 210, 213 f.; Bock, AcP 217, 370, 383 ff.; Bräutigam, in: Burandt/Rojahn, Erbrecht, 2. Aufl., § 1922 BGB Anhang Digitaler Nachlass Rn. 10 f.; Herzog, NJW 2013, 3745, 3748 f.; Herzog, ZErb 2017, 205 ff.; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 4 Rn. 11; Klas/Möhrke-Sobolewski, NJW 2015, 3473, 3474; Kutscher, Der digitale Nachlass, S. 102 ff.; Lange/Holtwiesche, ZErb 2016, 125 ff.; Lieder/Berneith, FamRZ 2016, 743; Litzenburger, FD-ErbR 2017, 392155; Ludyga, jM 2016, 442, 444 ff. und ZEV 2018, 1, 4; Salomon, NotBZ 2016, 324, 326 f.; Solmecke/Köbrich/Schmitt, MMR 2015, 291; Steiner/Holzer, ZEV 2015, 262 f.).

Nach der gesetzgeberischen Wertung gehen auch Rechtspositionen mit höchstpersönlichen Inhalten unabhängig von einem Vermögenswert auf die Erben über, wie sich aus § 2047 Abs. 2 BGB und § 2373 Satz 2 BGB ergibt. Zwar enthalten diese Bestimmungen keine unmittelbare Regelung über die Vererbbarkeit höchstpersönlicher Rechtspositionen. Allerdings setzen sie diese voraus und gebieten damit den Rückschluss auf deren Vererbbarkeit sowie darauf, dass das Gesetz insoweit nicht zwischen höchstpersönlichem und vermögenswertem Nachlass differenziert. So hat der Gesetzgeber in § 2047 Abs. 2 BGB geregelt, dass Schriftstücke, die sich auf die persönlichen Verhältnisse des Erblassers beziehen, nicht verteilt werden, sondern gemeinschaftlich bleiben (vgl. hierzu Mugdan, Die gesammten Materialien zum Bürgerlichen Gesetzbuch für das Deutsche Reich, V. Band S. 371, 507). § 2373 Satz 2 BGB regelt, dass Familienschriften und Familienbilder beim Erbschaftskauf nicht als mitverkauft anzusehen sind (vgl. Mugdan, aaO, II. Band S. 197). Beide Vorschriften setzen voraus, dass diese höchstpersönlichen Dokumente zur Erbmasse gehören. Unstreitig werden dementsprechend höchstpersönliche analoge Dokumente, z.B. Tagebücher und Briefe, vererbt.

Es besteht aus erbrechtlicher Sicht kein Grund dafür, digitale Inhalte anders zu behandeln, da das entscheidende Kriterium der Höchstpersönlichkeit bei analogen und digitalen Inhalten gleichermaßen betroffen ist (s. NK-NachfolgeR/Herzog, Kap. 9 Rn. 40; Herzog, ZErb 2017, 205, 206 f.; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 2 Rn. 43 ff.; Litzenburger, FD-ErbR 2017, 392155; Steiner/Holzer, ZEV 2015, 262, 263). Auf das Speicher- beziehungsweise Trägermedium

kommt es dabei nicht an. Eine Differenzierung danach, ob der digitale Inhalt auf einem lokalen Speichermedium wie einer Festplatte oder einem USB-Stick gespeichert ist oder sich auf Servern eines Diensteanbieters befindet, wäre inkohärent und durch das Gesetz nicht veranlasst (vgl. Herzog/Pruns, aaO, § 4 Rn. 9 f.; Kutscher, Der digitale Nachlass, S. 115 f., i.E. auch Staudinger/Kunz (2017) BGB, § 1922 Rn. 596.8 f.; jeweils mwN zur aA). Denn die Höchstpersönlichkeit ergibt sich nicht aus der Art der Verkörperung und Speicherung, sondern aus dem Inhalt. Ein Unterschied besteht lediglich in der Art und Weise der Vererbbarkeit: Während bei Schriftstücken oder Speichermedien im Eigentum beziehungsweise Besitz des Erblassers diese Rechtspositionen auf die Erben übergehen, treten bei – wie hier – auf Servern befindlichen Inhalten die Erben in das Vertragsverhältnis ein. Eine unterschiedliche Behandlung im Hinblick auf die Vererbbarkeit an sich rechtfertigt dies nicht.

Letztlich würde eine Differenzierung zwischen höchstpersönlichen und sonstigen Inhalten zu erheblichen kaum zu bewältigenden praktischen Problemen führen. Da E-Mail- und Benutzerkonten – oder sogar einzelne E-Mails oder Nachrichten – regelmäßig nicht ausschließlich höchstpersönlichen oder vermögensrechtlichen Zwecken dienen, wäre eine Durchsicht und Zuordnung sämtlicher digitaler Inhalte erforderlich. Es ist nicht ersichtlich, wer diese vornehmen sollte und rechtlich dürfte (s. auch Bräutigam, in: Burandt/Rojahn, Erbrecht, 2. Aufl., § 1922 BGB Anhang Digitaler Nachlass Rn. 10; Biermann, ZErb 2017, 210, 213; Bock, AcP 217, 370, 392 f.; Kutscher, Der digitale Nachlass, S. 105 f., 113 f.; Lange/Holtwiesche, ZErb 2016, 157, 161). Darüber hinaus sind die Grenzen zwischen höchstpersönlichen und vermögenswerten Inhalten unscharf und klare und eindeutige Abgrenzungskriterien kaum zu definieren, zumal auch höchstpersönliche Inhalte beim Erbgang vermögensrechtliche Relevanz erlangen können (Bräutigam, in: Burandt/Rojahn, Erbrecht, 2. Aufl., § 1922 BGB Anhang Digitaler Nachlass Rn. 10; Lange/Holtwiesche, ZErb 2016, 157, 161).

b) Entgegen einer im Schrifttum vertretenen Auffassung (MüKoBGB/Rixecker, 7. Aufl., § 12 Anh. Rn. 160; Martini, JZ 2012, 1145, 1150 ff.; Hoeren, NJW 2005, 2113, 2114; Brinkert/Stolze/Heidrich, ZD 2013, 153, 155) steht das postmortale Persönlichkeitsrecht der Erblasserin der Vererbbarkeit digitaler höchstpersönlicher Inhalte nicht entgegen.

Dieses wird aus dem Grundrecht der Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG hergeleitet und dient dem Schutz des allgemeinen Achtungsanspruchs, der dem Menschen kraft seines Personseins zusteht, und des sittlichen, personalen und sozialen Geltungswerts, den die Person durch ihre eigene Lebensleistung erworben hat (st. Rspr., s. nur BVerfG, NVwZ 2008, 549 Rn. 7 f.; BGH, Versäumnisurteil vom 16. September 2008 – VI ZR 244/07, NJW 2009, 751 Rn. 16). Bei einem Eingriff in dessen immaterielle Bestandteile können die nächsten Angehörigen des Verstorbenen Abwehrrechte in Form von Unterlassungs- und Widerrufsansprüchen geltend machen (vgl. BGH, Urteile vom 5. Oktober 2006 – I ZR 277/03, BGHZ 169, 193 Rn. 11 und vom 6. Dezember 2005 – VI ZR 265/04, BGHZ 165, 203, 206, jeweils mwN; MüKoBGB/Rixecker, 7. Aufl., § 12 Anh. Rn. 49, 55; MüKoBGB/Leipold, 7. Aufl., § 1922 Rn. 123; Staudinger/Kunz (2017), BGB § 1922 Rn. 596.8; Bock, AcP 217, 370, 389). Ein dem Erbrecht vorgehendes Recht der nächsten Angehörigen an den höchstpersönlichen digitalen Inhalten begründet dies nicht (vgl. Bräutigam, in: Burandt/Rojahn, Erbrecht, 2. Aufl., § 1922 BGB Anhang Digitaler Nachlass Rn. 10; BeckOGK BGB/Preuß, Stand 1. Juni 2018, § 1922 Rn. 387 f.; MüKoBGB/Leipold, 7. Aufl., § 1922 Rn. 26; Staudinger/Kunz (2017), BGB § 1922 Rn. 596.7 ff.; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 2 Rn. 56 ff. und § 4 Rn. 43; Ludyga, ZEV 2018, 1, 5; Bock, AcP 217, 370, 391 ff.; Solmecke/Köbrich/Schmitt, MMR 2015, 291, 292; a.A. MüKoBGB/Rixecker, 7. Aufl., § 12 Anh. Rn. 160; Martini, JZ 2012, 1145, 1150 ff.; Hoeren, NJW 2005, 2113, 2114; Brinkert/Stolze/Heidrich, ZD 2013, 153, 155), weshalb es im vorliegenden Zusammenhang nicht entscheidungserheblich ist, dass hier die Erben ohnedies zugleich die nächsten Angehörigen der Verstorbenen sind.

c) Entgegen der Auffassung des Berufungsgerichts scheitert ein Anspruch der Erbengemeinschaft auf Zugang zu dem vollständigen Benutzerkonto der Erblasserin und den darin vorgehaltenen Inhalten auch nicht an § 88 Abs. 3 TKG. Das Fernmeldegeheimnis schützt weder den Erblasser noch den jeweiligen Kommunikationspartner vor einer Kenntnisnahme des Erben vom Inhalt des Benutzerkontos. Dies gilt sowohl für die zum Zeitpunkt des Todes durch den Erblasser noch nicht abgerufenen als auch hinsichtlich der bereits zur Kenntnis genommenen, auf den Servern der Beklagten zwischen- beziehungsweise endgespeicherten Inhalte.

Nach § 88 Abs. 3 Satz 1 TKG ist es Diensteanbietern untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen.

Es kann dahingestellt bleiben, ob und bezüglich welcher Leistungen die Beklagte Anbieterin von Telekommunikationsdiensten oder Telemediendiensten ist (s. dazu ausführlich Grünwald/Nüßing, MMR 2016, 91 ff.; Karg/Fahl, K&R 2011, 453, 456 ff.; Kühling/Schall, CR 2016, 185; Schneider, ZD 2014, 231, 235). Ein Verstoß gegen § 88 Abs. 3 TKG liegt jedenfalls deshalb nicht vor, weil der Erbe eines Kommunikationspartners entgegen der Auffassung des Berufungsgerichts nicht „anderer" im Sinne dieser Vorschrift ist (MüKoBGB/Leipold, 7. Aufl., § 1922 Rn. 27; Biermann, ZErb 2017, 210, 215; Herzog, ZErb 2017, 205, 208; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 4 Rn. 60; Litzenburger, FD-ErbR 2017, 392155; Salomon, NotBZ 2016, 324, 327; Seidler, Digitaler Nachlass, 2016, S. 114 f.; Steiner/Holzer, ZEV 2015, 262, 264; Wüsthof, ErbR 2017, 496, 510; Wissenschaftliche Dienste des Deutschen Bundestages, Digitaler Nachlass – Zum Umgang mit digitaler Hinterlassenschaft, S. 9; Bericht der Arbeitsgruppe „Digitaler Neustart" vom 15. Mai 2017, http://www.jm.nrw.de/JM/schwerpunkte/digitaler_neustart/index.php, S. 343 ff.; a.A. Staudinger/Kunz (2017), BGB § 1922 Rn. 596.35 ff.; Bock, AcP 217, 370, 406).

aa) Andere im Sinne von § 88 Abs. 3 TKG sind Personen oder Institutionen, die nicht an dem geschützten Kommunikationsvorgang beteiligt sind. Die Beteiligten eines Telekommunikationsvorgangs sollen davor bewahrt werden, dass der Inhalt und die näheren Umstände der Telekommunikation Dritten, die an dem Vorgang nicht beteiligt sind, zugänglich werden (Beck TKG/Bock, 4. Aufl., § 88 Rn. 19; Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl., TKG § 88 Rn. 23). Dies entspricht dem verfassungsrechtlichen Schutz nach Art. 10 Abs. 1 GG, dessen Träger die – auch minderjährigen – tatsächlichen Kommunikationsteilnehmer sind (BVerfGE 120, 274, 340; 85, 386, 398 f.; Maunz/Dürig/Durner, GG, Stand Januar 2018, Art. 10 Rn. 100 f. jeweils mwN).

bb) Der Erbe ist nicht anderer in diesem Sinne, sondern vielmehr mit dem Erbfall Beteiligter der im Zeitpunkt des Erbfalls nicht beendeten und deshalb dem Schutz des Fernmeldegeheimnisses unterstehenden Kommunikationsvorgänge geworden.

Es kann im vorliegenden Fall unterstellt werden, dass, wovon das Berufungsgericht ausgegangen ist, die auf den Servern der Beklagten unter den Benutzerkonten der Teilnehmer ihres Netzwerks abgespeicherten Inhalte noch dem Schutzbereich des Fernmeldegeheimnisses unterliegen, auch wenn der technische Übermittlungsvorgang abgeschlossen ist (so z.B. auch: Biermann, ZErb 2017, 210, 214; Bock, AcP 217, 370, 405 f.; Deusch, ZEV 2017, 386, 399; Leeb, K&R 2014, 693, 696 f.; Uhrenbacher, Digitales Testament und digitaler Nachlass, S. 176; kritisch hierzu: Brisch/Müllerter Jung, CR 2013, 446, 450 f.; Klas/Möhrke-Sobolewski, NJW 2015, 3473, 3477 f.; Kutscher, Der digitale Nachlass, 2015, S. 144 f.).

Die Bereitstellung der Inhalte des Benutzerkontos für den Erben verstößt ebenso wenig gegen das Fernmeldegeheimnis wie die fortlaufende Bereitstellung für den ursprünglich Kontoberechtigten. Die Beklagte macht weiterhin entsprechend ihrer vertraglichen Verpflichtung einerseits gegenüber dem Absender beziehungsweise Teilenden und andererseits gegenüber dem Berechtigten des Empfängerkontos – nunmehr dem Erben – die Inhalte für das betreffende Benutzerkonto zugänglich. Die Zugangsgewährung für den Erben erfolgt im Rahmen des – unterstellt – durch das Fernmeldegeheimnis geschützten Kommunikationsvorgangs. Denn der Erbe wird mit dem Tod des ursprünglichen Kontoberechtigten als neuer Vertragspartner und Kontoberechtigter zum Teilnehmer der auf Grund der Speicherung und Bereitstellung der Inhalte für das Benutzerkonto fortlaufenden Kommunikationsvorgänge. Der Erblasser dagegen scheidet mit seinem Tod als geschützter Kommunikationspartner aus. Teilnehmer einer Kommunikation und damit vom Fernmeldegeheimnis geschützt kann begriffsnotwendig nur eine lebende Person sein (ebenso Bericht der Arbeitsgruppe „Digitaler Neustart" vom 15. Mai 2017, http://www.jm.nrw.de/JM/schwerpunkte/digitaler_neustart/index.php, S. 346).

Aus den in den obigen Ausführungen zur Vererbbarkeit des vertraglichen Zugangsrechts der Verstorbenen genannten Gründen erfordert auch der Zweck des § 88 Abs. 3 TKG nicht, den Erben den Zugang zu dem Benutzerkonto im Hinblick auf schutzwürdige Interessen der Kommunikationspartner (2 a cc 2.3) oder das postmortale Persönlichkeitsrecht des Verstorbenen (2 b) zu versagen.

cc) Ein Vergleich mit der erbrechtlichen Rechtslage bei analoger Briefpost sowie ausgedruckten oder auf Medien des Erblassers gespeicherten digitalen Inhalten, bei denen ein erbrechtlicher Übergang stattfindet, bestätigt dieses Ergebnis. Bei digitalen Inhalten würde – sollte das Fernmeldegeheimnis auf den Erben angewendet werden – die Zugangsmöglichkeit für diesen davon abhängen, einerseits ob Inhalte etwa durch Ausdrucken verkörpert oder auf einem Medium des Erblassers gespeichert sind und andererseits ob diese lediglich digital auf Servern des Anbieters abrufbar sind. So erhielte der Erbe Zugang zu einer über den „Messenger" der Beklagten an das Benutzerkonto des Erblassers gesandten Nachricht, wenn dieser sie auf einem eigenen Medium abgespeichert hätte, während dem Erben der Zugang zu derselben Nachricht verwehrt würde, wenn der Erblasser die Nachricht auf dem Server der Beklagten belassen hätte. Diese unterschiedliche Behandlung desselben Inhalts abhängig von dem Speichermedium oder der Verkörperung und damit letztlich von Zufällen ist nicht gerechtfertigt. In allen Fällen ist der Grad des Vertraulichkeitsinteresses sowohl des Absenders als auch des Empfängers gleich.

Ein Vertraulichkeitsinteresse hat nach den Grundsätzen der Gesamtrechtsnachfolge gegenüber dem Erben zurückzustehen. Die Rechtsordnung sieht, wie sich aus § 2047 Abs. 2 und § 2373 Satz 2 BGB ergibt, einen Übergang auch höchstpersönlicher Inhalte auf den Erben vor, ordnet das Geheimhaltungsinteresse des Erblassers und der Kommunikationspartner folglich grundsätzlich dem durch Art. 14 Abs. 1 Satz 1 GG geschützten Erbrecht unter. Der Übergang auch nichtvermögensrechtlicher Inhalte an den Erben ist demnach von der Rechtsordnung gebilligt und gewollt. Dies ist auch im Rahmen der Auslegung des Begriffs „anderen" im Sinne des § 88 Abs. 3 TKG zu berücksichtigen. Dem wird nur eine Interpretation, wonach ein Erbe nicht anderer im Sinne dieser Vorschrift ist, gerecht. Dies abweichend zu beurteilen, würde ohne nachvollziehbaren Grund zu einer Durchbrechung des erbrechtlichen Grundsatzes der Universalsukzession führen, ohne dass dies im Telekommunikationsgesetz eine Anknüpfung findet (vgl. Biermann, ZErb 2017, 210, 215; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 4 Rn. 60). Die – im Unterschied zur analogen Post oder zu auf einem Medium des Erblassers gespeicherten digitalen Inhalten – bei serverbasierten Speicherungen fortbestehende Zugriffsmöglichkeit des Betreibers kann zwar dazu führen, dass der Diensteanbieter weiter zur Wahrung des Fernmeldegeheimnisses verpflichtet ist und damit eine Weitergabe an außerhalb des Kommunikationsverhältnisses stehende Dritte unzulässig bleibt. Die fortlaufende Zulässigkeit der Bereitstellung für das auf den Erben übergegangene Benutzerkonto wird hierdurch aber nicht berührt.

d) Schließlich steht dem Anspruch der Klägerin auch Datenschutzrecht nicht entgegen.

aa) Der Senat hat zur Beurteilung dieser Frage die seit dem 25. Mai 2018 unmittelbar geltende 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, ABl. L 119 vom 4. Mai 2016, S. 1) heranzuziehen. Maßstab für die Überprüfung eines Berufungsurteils ist die Rechtslage im Zeitpunkt der Revisionsentscheidung. Zu berücksichtigen ist dabei auch ein erst nach Erlass der Berufungsentscheidung geltendes Gesetz, sofern es nach seinem zeitlichen Geltungswillen das streitige Rechtsverhältnis erfasst (st. Rspr., vgl. Senat, Urteil vom 26. Februar 1953 – III ZR 214/50, BGHZ 9, 101, 102; BGH, Urteile vom 19. Februar 1993 – V ZR 269/91, NJW 1993, 1706, 1707, insoweit nicht in BGHZ 121, 347 abgedruckt; vom 21. Februar 1962 – V ZR 144/60, BGHZ 36, 348, 350; Beschluss vom 20. Januar 2005 – IX ZB 134/04, NJW 2005, 1508, 1509).

Dies ist hier der Fall. Das Klagebegehren der Klägerin zielt auf eine künftige Handlung der Beklagten, die zeitlich nach dem Anwendungsbeginn der Verordnung vorzunehmen sein wird und deshalb an deren Vorgaben zu messen ist. Denn sie gilt gemäß Art. 99 Abs. 2 DS-GVO ab dem 25. Mai 2018 unmittelbar in allen Mitgliedstaaten. Aus Art. 99 in Verbindung mit Erwägungsgrund 171 Satz 3 der DS-GVO ergibt sich, dass sie ab diesem Zeitpunkt uneingeschränkt für Datenverarbeitungsvorgänge Anwendung findet. Selbst Verarbeitungen, die zu diesem Zeitpunkt bereits begonnen haben, sollen binnen zwei Jahren nach dem Inkrafttreten (24. Mai 2016, vgl. Art. 99 Abs. 1 DS-GVO), mithin bis zum Anwendungsbeginn, mit der Verordnung in Einklang gebracht werden. Ab diesem Zeitpunkt verdrängt die Verordnung in ihrem Anwendungsbereich die nationalen Gesetze

(vgl. zum Vorrang ausdrücklich § 1 Abs. 5 BDSG in der Fassung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30. Juni 2017, BGBl. I, S. 2097). Die in den Instanzen umstrittene Frage, ob irisches oder deutsches Datenschutzrecht anwendbar ist, stellt sich damit nicht mehr.

bb) Datenschutzrechtliche Belange der Erblasserin sind nicht betroffen und werden von der Beklagten auch nicht geltend gemacht. Die Datenschutz-Grundverordnung bezieht sich – wie schon die zuvor geltenden nationalen Vorschriften – nur auf lebende natürliche Personen. Dies ergibt sich aus dem Erwägungsgrund 27 der Verordnung, worin festgehalten ist, dass die Verordnung nicht auf personenbezogene Daten Verstorbener anzuwenden ist.

cc) Auch datenschutzrechtliche Belange der Kommunikationspartner der Erblasserin stehen dem Anspruch der Klägerin nicht entgegen.

(1) Mit dem Zugang zum Benutzerkonto des Erblassers erhält der Erbe die Möglichkeit, auf die Kommunikation oder die mit dem Erblasser geteilten Bilder und sonstigen Inhalte zuzugreifen. Sowohl die Nachrichten als auch die veröffentlichten („geposteten") Inhalte können personenbezogene Daten darstellen oder solche beinhalten. Die Beklagte als Betreiberin des sozialen Netzwerks ist in den Kommunikationsprozess insoweit eingebunden, als sie die Nachrichten zum Abruf für das Empfängerkonto bereitstellt sowie den Zugriff auf die geteilten Inhalte ermöglicht und die entsprechende Plattform zur Verfügung stellt. Dabei verarbeitet sie notwendigerweise die in den Inhalten enthaltenen sowie für die Bereitstellung erforderlichen Daten des jeweils kommunizierenden oder veröffentlichenden Nutzers.

(2) Es kann dahinstehen, ob der Anwendungsbereich der Datenschutz-Grundverordnung im Hinblick auf die der Zugangsgewährung für die Erben immanente Verarbeitung von inhaltlichen Daten der Kommunikationspartner überhaupt eröffnet ist (für einen umfassenden Anwendungsausschluss: Bericht der Arbeitsgruppe „Digitaler Neustart" vom 15. Mai 2017, http://www.jm.nrw.de/JM/schwerpunkte/digitaler_neustart/index.php, S. 348 f.). Die Verarbeitung der personenbezogenen Daten der Kommunikationspartner der Erblasserin durch die Übermittlung und dauerhafte Bereitstellung der jeweiligen Inhalte für die Erben ist jedenfalls sowohl nach Art. 6 Abs. 1 Buchst. b Var. 1 DS-GVO als auch nach Art. 6 Abs. 1 Buchst. f DS-GVO zulässig.

(2.1) Nach Art. 6 Abs. 1 Buchst. b Var. 1 DS-GVO ist eine Verarbeitung rechtmäßig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Partei ist, erforderlich ist. Umfasst ist sowohl die Erfüllung der vertraglichen Leistungs- und Nebenpflichten, als auch der diesbezüglichen gesetzlichen Verpflichtungen (Buchner/Petri, in: Kühling/Buchner, DS-GVO, BDSG, 2. Aufl., Art. 6 DS-GVO Rn. 33; Assion/Notel/Veil, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, Art. 6 Rn. 88 ff.). Ob die Verarbeitung „erforderlich" – und nicht nur zweckdienlich – ist, hängt von dem Vertragsinhalt und der vertragscharakteristischen Leistung des jeweiligen Schuldverhältnisses ab (Buchner/Petri, in: Kühling/Buchner, DS-GVO, BDSG, 2. Aufl., Art. 6 DS-GVO Rn. 39).

Die Voraussetzungen der genannten Vorschrift sind erfüllt. Die Übermittlung und Bereitstellung von Nachrichten und geteilten Inhalten der Kommunikationspartner an das Benutzerkonto der Erblasserin erfolgt auch in Erfüllung einer gegenüber diesen bestehenden vertraglichen Hauptleistungspflicht. Denn nach dem Inhalt des Nutzungsvertrags zwischen der Beklagten und ihren Nutzern ist die Bereitstellung und Übermittlung von Nachrichten und sonstigen Inhalten an das vom jeweiligen Absender benannte Empfängerkonto wesentliche Vertragspflicht der Beklagten sowohl gegenüber dem Absender – hier also den Kommunikationspartnern der Erblasserin – als auch gegenüber dem Berechtigten des Empfängerkontos. Die notwendigerweise damit einhergehende Verarbeitung der in den Inhalten enthaltenen oder für die Bereitstellung benötigten Daten der Kommunikationspartner ist für die Erfüllung dieser Hauptleistungspflicht erforderlich im Sinne von Art. 6 Abs. 1 Buchst. b Var. 1 DS-GVO. Die Beklagte macht datenschutzrechtliche Bedenken für die zu Lebzeiten der Erblasserin erfolgten Übermittlungen und Bereitstellungen von Inhalten auch nicht geltend.

An der Berechtigung der Datenverarbeitung nach der genannten Vorschrift ändert sich durch den Eintritt des Erbfalls nichts. Die Beklagte macht weiterhin entsprechend ihrer Verpflichtung einerseits gegenüber dem Absender beziehungsweise Teilenden und andererseits gegenüber dem Berechtigten des Empfängerkontos die Inhalte für das betreffende Benutzerkonto zugänglich. Denn der Auftrag der Kommunikationspartner der Erblasserin zur Übermittlung einer Nachricht oder eines geteilten Inhalts wirkt zeitlich unbegrenzt – auch über den Tod des Berechtigten des Empfängerkontos hinaus – und umfasst die dauerhafte Ermöglichung des Abrufs der auf dem Server der Beklagten gespeicherten Nachricht durch den Nutzer des Empfängerkontos, solange dieses besteht, beziehungsweise bei geteilten Inhalten, solange der Absender die Berechtigung nicht ändert, siehe hierzu oben 2 a cc 2.3.1. Wie dort ausgeführt, bezieht sich die vertragliche Verpflichtung der Beklagten nicht darauf, die Nachricht oder den geteilten Inhalt an eine bestimmte Person zu übermitteln beziehungsweise für diese zugänglich zu machen. Vielmehr ist diese kontobezogen, so dass die Beklagte sie erfüllt, indem sie Nachrichten an das benannte Benutzerkonto übermittelt, deren jederzeitigen Abruf durch den mit den zutreffenden Daten bei dem Benutzerkonto angemeldeten Nutzer ermöglicht sowie Inhalte für die ausgewählten Benutzerkonten zur Verfügung stellt. Der Tod des ursprünglich Berechtigten ändert hieran nichts, da das Konto nach dem Erbfall fortbesteht und der Erbe damit Berechtigter wird.

(2.2) Abgesehen davon ist die Datenverarbeitung auch zur Wahrung der berechtigten Interessen der Klägerin und des Vaters der Erblasserin erforderlich (Art. 6 Abs. 1 Buchst. f DS-GVO).

Die Frage der Zulässigkeit einer Datenverarbeitung aufgrund von berechtigten Interessen eines Dritten ist grundsätzlich von den konkreten Umständen des betroffenen Einzelfalls abhängig und dementsprechend auch einzelfallbezogen zu ermitteln und zu beurteilen (EuGH, NJW 2016, 3579 Rn. 62 [zu dem Art. 6 Abs. 1 Buchst. f DS-GVO entsprechenden Art. 7 Buchst. f der Richtlinie 95/46/EG]). Hier liegen berechtigte Interessen der beiden Erben vor, die eine Datenverarbeitung in Form der Zugangsgewährung erforderlich machen. Die Interessen, Grundrechte und Grundfreiheiten der betroffenen Kommunikationspartner der Erblasserin überwiegen diese berechtigten Interessen nicht.

(2.2.1) Zu den berechtigten Interessen zählen neben rechtlichen auch tatsächliche, wirtschaftliche oder ideelle Interessen, nicht jedoch bloße Allgemeininteressen (Buchner/Petri, in: Kühling/Buchner, DS-GVO, BDSG, 2. Aufl., Art. 6 DS-GVO Rn. 146 f.; Auernhammer/Kramer, DS-GVO, BDSG, 5. Aufl., Art. 6 DS-GVO Rn. 30). Die in den Erwägungsgründen 47 bis 50 genannten Beispiele berechtigter Interessen wie die Verarbeitung zur Verhinderung von Betrug (EG 47 Satz 6), zum Zweck der Direktwerbung (EG 47 Satz 7), im Rahmen einer konzerninternen Übermittlung (EG 48 Satz 1) oder zur Verbesserung der Netz- und Informationssicherheit (EG 49) zeigen, dass vielfältige und

unterschiedlich bedeutsame berechtigte Interessen berücksichtigungsfähig sind.

Hier bestehen berechtigte Interessen der Klägerin und des Vaters der Erblasserin:

(2.2.1.1) Die Erbengemeinschaft kann sich auf das durch Art. 14 Abs. 1 Satz 1 GG geschützte Erbrecht berufen und ein berechtigtes Interesse geltend machen, weil – wie dargelegt – das mit der Beklagten bestehende Vertragsverhältnis nach dem anzuwendenden deutschen Recht auf die Erben übergegangen ist und diese deshalb als Vertragspartner einen Primärleistungsanspruch auf Zugang zu dem Benutzerkonto der Erblasserin sowie den darin enthaltenen vermögensrechtlichen und höchstpersönlichen (digitalen) Inhalten haben. Es stellt bereits für sich genommen ein gewichtiges berechtigtes Interesse eines Vertragspartners dar, die Hauptleistungsansprüche aus diesem Vertragsverhältnis auch geltend machen zu können. Würde den Erben der Zugang verweigert, würden ihnen die durch den erbrechtlichen Übergang von Rechten und Pflichten aus dem Vertragsverhältnis entstandenen Rechtspositionen faktisch entzogen und der Grundsatz der Universalsukzession ausgehöhlt.

(2.2.1.2) Als Erben sind die Klägerin und der Vater der Erblasserin nicht nur Vertragspartner des Nutzungsvertrags geworden, sie haben auch etwaige vermögensrechtliche Ansprüche der Erblasserin geerbt und haften für deren Verbindlichkeiten. Informationen über derartige Ansprüche und Verbindlichkeiten können sich auch aus den Inhalten des Benutzerkontos ergeben, die nicht nur höchstpersönliche, sondern auch vermögensrechtliche Bedeutung haben können. Der Zugang zu dem Benutzerkonto dient deshalb regelmäßig auch dazu, um zu prüfen, ob sich aus dem Inhalt Ansprüche der Erblasserin gegen Dritte oder Ansprüche Dritter gegen die Erblasserin ergeben, die die Erben weiterverfolgen können oder müssen, oder ob sonstige Handlungen rechtsgeschäftlicher Art erforderlich sind. Die Anforderungen an ein diesbezügliches berechtigtes Interesse können nicht hoch angesetzt werden, weil die Erben – wie hier – regelmäßig keine Kenntnis von den Inhalten des Benutzerkontos haben und ihnen deshalb in der Regel eine nähere Darlegung der möglicherweise enthaltenen Inhalte mit vermögensrechtlichem Bezug nicht möglich ist.

Im vorliegenden Fall besteht über das allgemeine berechtigte Interesse der Erben an der Prüfung der Inhalte auf vermögenswerte Relevanz hinaus ein näher konkretisiertes derartiges Interesse deshalb, weil die Erben mit der Zugangsgewährung auch vermögensrechtliche Abwehrinteressen gegenüber dem U-Bahn-Fahrer verfolgen, der sie auf Schadensersatz in Anspruch nimmt. Die Geltendmachung, Ausübung und Verteidigung eigener Rechte ist ein berechtigtes Interesse für die Datenverarbeitung (Assion/Notel/Veil, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, Art. 6 Rn. 136; Sydow/Reimer, Europäische Datenschutzgrundverordnung, Art. 6 Rn. 55; vgl. für das berechtigte Interesse im Sinne des Art. 7 Buchst. f der Richtlinie 95/46/EG eines Dritten, eine persönliche Information über einen Schädiger zu erlangen, um eine Schadensersatzklage zu erheben EuGH, CR 2017, 504 Rn. 29).

(2.2.1.3) Als berechtigtes Interesse der Klägerin und des Vaters der Erblasserin als Erben sowie Eltern der minderjährigen Verstorbenen ist auch anzuerkennen, dass diese durch den Zugang zu dem Benutzerkonto Aufschluss darüber erhalten möchten, ob die Erblasserin kurz vor ihrem Tod Suizidabsichten gehegt hat. Entgegen der Auffassung der Beklagten sind nicht nur zwingende rechtliche Interessen, sondern ist auch ein derartiges ideelles Interesse im Rahmen der Abwägung berücksichtigungsfähig.

(2.2.2) Die Datenverarbeitung ist vorliegend erforderlich, weil keine geeigneteren und milderen Mittel möglich sind, um die berechtigten Interessen der Erben zu erfüllen (vgl. Auernhammer/Kramer, DS-GVO, BDSG, 5. Aufl., Art. 6 DS-GVO Rn. 34; Plath/Plath, BDSG/DS-GVO, 2. Aufl., Art. 6 DS-GVO Rn. 23).

(2.2.3) Die Interessen, Grundrechte oder Grundfreiheiten der betroffenen Kommunikationspartner, die den Schutz personenbezogener Daten erfordern, überwiegen die berechtigten Interessen der Erben nicht.

(2.2.3.1) Auf Seiten der Kommunikationspartner der Erblasserin ist das Grundrecht aus Art. 8 Abs. 1 EUGRCh auf Schutz ihrer personenbezogenen Daten zu berücksichtigen. Dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sieht sich die Datenschutz-Grundverordnung verpflichtet (EG 1 und 2), und auch der Gerichtshof der Europäischen Union hebt die Bedeutung des durch Art. 8 EUGRCh gewährleisteten Grundrechts hervor (vgl. EuGH, NJW 2015, 3151 Rn. 38 f. und 78 mwN). Darüber hinaus ist das damit im Zusammenhang stehende Grundrecht auf Achtung des Privat- und Familienlebens und der Kommunikation gemäß Art. 7 EUGRCh zugunsten der Kommunikationspartner mit in die Abwägung einzustellen (Heberlein in: Ehmann/Selmayr, EU-DS-GVO, Art. 6 Rn. 24; s. auch EuGH, NJW 2015, 3151 Rn. 39). Schutzwürdig sind insoweit das Persönlichkeitsrecht im Allgemeinen und die informationelle Selbstbestimmung im Speziellen. Die Schutzbedürftigkeit ist dabei umso höher, je persönlicher die betroffenen Daten sind. Insoweit ist zu berücksichtigen, dass die von den Kommunikationspartnern verfassten Inhalte der übermittelten Nachrichten und Veröffentlichungen („Postings") – wie die Revisionserwiderung geltend macht – auch höchstpersönliche oder sensible Daten, die besonders schutzwürdig sind, enthalten oder hierauf hinweisen könnten.

Als gewichtig sind nach Art. 6 Abs. 1 Buchst. f DS-GVO zudem die Belange betroffener Kinder zu berücksichtigen. Dies spiegelt sich auch in deren Erwägungsgrund 38 wieder. Da die Erblasserin im Todeszeitpunkt selbst 15 Jahre alt war, liegt es nahe, dass ihre Kommunikationspartner zumindest teilweise auch noch Kinder gewesen sind. Dies bedeutet allerdings nicht, dass gegenüber Kindern eine Datenverarbeitung grundsätzlich nicht gerechtfertigt ist, sondern lediglich, dass ihre Interessen, entsprechend einer vom Alter abhängigen Schutzbedürftigkeit, im Vergleich zu Erwachsenen ein höheres Gewicht haben (Assion/Notel/Veil, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, Art. 6 Rn. 144; Buchner/Petri, in: Kühling/Buchner, DS-GVO, BDSG, 2. Aufl., Art. 6 DS-GVO Rn. 155; Sydow/Reimer, Europäische Datenschutzgrundverordnung, Art. 6 Rn. 64).

(2.2.3.2) Der Maßstab für die Abwägung folgt aus den in Art. 1 und Art. 5 genannten Grundsätzen und Leitprinzipien der Datenschutz-Grundverordnung unter Berücksichtigung der Wertmaßstäbe der Grundrechtecharta und des übrigen Primärrechts. Dabei sind unter anderem die relevanten Grundrechtsbezüge, die Eingriffsintensität, die Art der verarbeiteten Daten, die Art der Betroffenen, mögliche Aufgaben oder Pflichten und die Zwecke der Datenverarbeitung zu berücksichtigen (Gola DS-GVO/Schulz, Art. 6 Rn. 53). Dabei geht es im Kern um einen Ausgleich zwischen den Privatheitsinteressen des Betroffenen einerseits und den Verwendungsinteressen der Verantwortlichen beziehungsweise Dritten andererseits im konkreten Einzelfall (Buchner/Petri, in: Kühling/Buchner, DS-GVO, BDSG, Art. 6 DS-GVO Rn. 149; Assion/Notel/Veil, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, Art. 6 Rn. 140 ff.; Schaffland/Holthaus, in: Schaffland/Wiltfang, DS-GVO/BDSG, Art. 6 DS-GVO Rn. 126 ff. [Stand Oktober 2017]). Es sind Art, Inhalt und Aussagekraft der

betroffenen Daten an dem mit der Datenverarbeitung verfolgten Zweck zu messen und gegenüberzustellen (Buchner/Petri, in: Kühling/Buchner, DS-GVO, BDSG, 2. Aufl., Art. 6 DS-GVO Rn. 149; zu § 32 BDSG a.F.: Senatsurteil vom 15. Dezember 1983 – III ZR 207/82, NJW 1984, 1889, 1890). Teilweise wird hierbei auch mit demselben Ergebnis auf die zum Grundrecht auf informationelle Selbstbestimmung entwickelten Kriterien wie Anlasslosigkeit, Streubreite und Einschüchterungswirkung zurückgegriffen (Sydow/Reimer, Europäische Datenschutzgrundverordnung, Art. 6 Rn. 61; s. auch BVerfG, NVwZ 2007, 688, 691).

Die Erwägungsgründe zur Güterabwägung nach der Datenschutz-Grundverordnung präzisieren insoweit die Abwägung (Auernhammer/Kramer, DS-GVO, BDSG, 5. Aufl., Art. 6 DS-GVO Rn. 37). Bedeutung hat hierbei insbesondere Erwägungsgrund 47 Satz 1 der Datenschutz-Grundverordnung, der als wichtigen Gesichtspunkt der Interessenabwägung „die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen" nennt. Insoweit ist auch zu berücksichtigen, ob die „betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird" (EG 47 Satz 3). Maßgebend ist ein objektivierter Maßstab, das heißt, welche Erwartungen ein vernünftiger Dritter in der Person des Betroffenen hätte (Auernhammer/Kramer, DS-GVO, BDSG, 5. Aufl., Art. 6 DS-GVO Rn. 37; Plath/Plath, BDSG/DS-GVO, 2. Aufl., Art. 6 DS-GVO Rn. 23).

(2.2.3.3.) Eine nach diesen Grundsätzen durchgeführte Interessenabwägung führt dazu, dass die Interessen der Kommunikationspartner die berechtigten Interessen der Klägerin und des Vaters der Erblasserin nicht überwiegen.

Zu berücksichtigen ist dabei zunächst, dass die relevanten Daten von den Kommunikationspartnern freiwillig und bewusst an die Beklagte übermittelt wurden, um sie für ein bestimmtes Benutzerkonto zur Verfügung zu stellen. Inhalt und Umfang der preisgegebenen persönlichkeitsrelevanten Daten sowie den zur Kenntnisnahme befugten Personenkreis kann der Nutzer selbst bestimmen. Es handelt sich also nicht um von der Beklagten erhobene, sondern um von den Kommunikationspartnern im Rahmen des bestehenden Vertrags (EG 47 Satz 2) freiwillig und selbstbestimmt sowie inhaltlich kontrollierbar übersandte Daten (vgl. Gola DS-GVO/Schulz, Art. 6 Rn. 53). Der Nutzer forciert bei der Kontaktaufnahme durch persönliche Nachrichten oder das Teilen von Inhalten den Außenkontakt und lehnt ihn nicht grundsätzlich zur Wahrung der Vertraulichkeit ab (vgl. Buchner/Petri, in: Kühling/Buchner, DS-GVO, BDSG, 2. Aufl., Art. 6 DS-GVO Rn. 150).

Der Absender weiß und will, dass die Beklagte die Inhalte vertragsgemäß an das Empfängerkonto übermittelt und für dieses bereitstellt. Dabei ist dem Nutzer zugleich ebenso – oder noch viel mehr – wie dem Absender eines Briefs bewusst, dass er nach dem Versenden einer Nachricht nicht mehr kontrollieren kann, wer nach der Übermittlung und Bereitstellung durch die Beklagte letztlich von deren Inhalt Kenntnis nimmt, und dass er grundsätzlich keine Möglichkeit hat, die übermittelte Nachricht beziehungsweise den Inhalt zurückzufordern. Er begibt sich insoweit der Verfügungsbefugnis über die Nachrichten (vgl. hierzu oben 2 a cc 2.3; NK-NachfolgeR/Herzog, Kap. 9 Rn. 68; Bock, AcP 217, 370, 408; Herzog/Pruns, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, § 4 Rn. 84; Kutscher, Der digitale Nachlass, S. 145; Pruns, NWB 2014, 2175, 2182 f.). Dies gilt für erwachsene Nutzer gleichermaßen wie für minderjährige. Denn auch und gerade Minderjährige, die bereits selbständig F. nutzen und ein eigenes Benutzerkonto besitzen, kennen bei der gebotenen typisierenden Betrachtungsweise die vielfältigen Möglichkeiten, eine an ein bestimmtes Benutzerkonto gesandte Nachricht auch Dritten zugänglich zu machen.

Die Kommunikationspartner der Erblasserin konnten darüber hinaus vernünftigerweise absehen, dass die Datenverarbeitung durch Bereitstellung der Nachrichten und Inhalte für das Empfängerkonto auch nach dem Tod der ursprünglichen Kontoberechtigten fortgesetzt würde und die Erben Kenntnis von diesen Daten erlangen könnten (EG 47 Satz 3). Denn der Absender einer Nachricht oder eines sonstigen Inhalts muss damit rechnen, dass der Kontoberechtigte versterben könnte, Dritte das Benutzerkonto erben und in das Vertragsverhältnis eintreten und damit als neue Kontoberechtigte Zugang auf die Kontoinhalte haben.

In die Interessenabwägung einzustellen ist weiter der eng begrenzte Zweck der vorliegenden Datenverarbeitung. Es geht hier ausschließlich um die Übermittlung und Bereitstellung von personenbezogenen Daten und Inhalten für ein konkretes, vom Absender selbst ausgewähltes Benutzerkonto im Rahmen des zwischen den Kommunikationspartnern und der Beklagten bestehenden Vertragsverhältnisses (s. EG 47 Satz 2; vgl. auch Auernhammer/Kramer, DS-GVO, BDSG, 5. Aufl., Art. 6 DS-GVO Rn. 38) allein zum Zweck der Kenntnisnahme der bereits vorhandenen Inhalte durch die Mitglieder der Erbengemeinschaft. Demgegenüber erfolgt die Verarbeitung nicht zu weitergehenden Zwecken, etwa für Werbezwecke oder zur Erstellung eines Persönlichkeitsprofils durch die Beklagte (Buchner/Petri, in: Kühling/Buchner, DS-GVO, BDSG, 2. Aufl., Art. 6 DS-GVO Rn. 152 f.). Damit sind zugleich die durch die konkrete Art der Datenverarbeitung entstehenden Risiken begrenzt (vgl. zum risikobasierten Ansatz der DS-GVO: Gola DS-GVO/Schulz, Art. 6 Rn. 53). Denn die Daten werden durch die Bereitstellung für das Benutzerkonto nicht einem größeren, unbeherrschbaren Personenkreis oder völlig unbeteiligten Dritten bekannt, sondern nur dem von vornherein eng begrenzten Personenkreis, nämlich der aus zwei Personen bestehenden Erbengemeinschaft, die zudem nächste Angehörige der verstorbenen Nutzerin sind.

Vor diesem Hintergrund kommt den Interessen der Kommunikationspartner im Verhältnis zu denen der Erben keine überwiegende Bedeutung zu, unabhängig davon, ob diese minderjährig sind oder nicht und ob teilweise auch sensible Inhalte enthalten sind. Die oben dargelegten berechtigten Interessen der Klägerin und des Vaters der Erblasserin als Erben und nahe Angehörige sind von deutlich höherem Gewicht. Die Interessen der Kommunikationspartner rechtfertigen es nicht, das gesetzliche Erbrecht der Erben teilweise auszuhöhlen. Gestützt wird dieses Ergebnis hier durch die besondere persönliche Interessenlage der Erben, die zugleich nächste Angehörige sind und ein sowohl ideelles als auch vermögenswertes Interesse an der Aufklärung der Umstände des Todes ihrer Tochter haben.

(3) Die Erlaubnistatbestände des Art. 6 Abs. 1 Buchst. b und f DS-GVO begründen jeweils eigenständig die datenschutzrechtliche Zulässigkeit der Zugangsgewährung für die Klägerin. Eine Vorlage an den Gerichtshof der Europäischen Union gemäß Art. 267 AEUV ist entbehrlich. Die richtige Anwendung des Europarechts ist jedenfalls im Hinblick auf Art. 6 Abs. 1 Buchst. f DS-GVO derart offenkundig, dass für vernünftige Zweifel kein Raum mehr bleibt (vgl. Senat, Urteil vom 17. April 2014 – III ZR 87/13, BGHZ 201, 11 Rn. 29; Beschluss vom 14. Dezember 2017 – III ZR 117/17, BeckRS 2017, 136439 Rn. 7). Fragen der Auslegung dieser Vorschrift, die eine Vorlage erforderlich machen könnten, stellen sich nicht mehr. Denn nach der Rechtspre-

chung des Gerichtshofs der Europäischen Union zur inhaltsgleichen Vorgängerregelung des Art. 7 Buchst. f der Richtlinie 95/46/EG steht fest, dass eine von den Umständen der konkreten Konstellation abhängige Einzelfallabwägung zu erfolgen hat (EuGH, NJW 2016, 3579 Rn. 62, acte éclairé), die auf Grundlage der vorliegenden Umstände zugunsten der Erben ausfällt.

e) Ohne Erfolg beruft sich die Beklagte in der Revisionserwiderung auch auf einen Ausschluss des Zugangs wegen des allgemeinen Persönlichkeitsrechts der Kommunikationspartner der Erblasserin. Dieses steht dem Anspruch der Klägerin ebenso wenig entgegen wie das Fernmeldegeheimnis oder Datenschutzrecht. Die Gründe, die zur Verneinung einer Verletzung des Fernmeldegeheimnisses oder datenschutzrechtlicher Vorschriften führen, gelten auch insoweit.

3. Das angefochtene Urteil ist demnach aufzuheben (§ 562 Abs. 1 ZPO).

Da die Sache zur Endentscheidung reif ist, kann der Senat die Berufung der Beklagten selbst zurückweisen (§ 563 Abs. 3 ZPO).

E-Mail-Zufriedenheitsbefragung als unzumutbare Belästigung (Ls)

(**Bundesgerichtshof**, Urteil vom 10. Juli 2018 – VI ZR 225/17 –)

1. **Die Verwendung von elektronischer Post für die Zwecke der Werbung ohne Einwilligung des Empfängers stellt grundsätzlich einen Eingriff in seine geschützte Privatsphäre und damit in sein allgemeines Persönlichkeitsrecht dar.**
2. **Eine Kundenzufriedenheitsbefragung in einer E-Mail fällt auch dann unter den Begriff der (Direkt-)Werbung, wenn mit der E-Mail die Übersendung einer Rechnung für ein zuvor gekauftes Produkt erfolgt.**
3. **Dem Verwender einer E-Mail-Adresse zu Werbezwecken nach Abschluss einer Verkaufstransaktion ist es zumutbar, bevor er auf diese Art mit Werbung in die Privatsphäre des Empfängers eindringt, diesem – wie es die Vorschrift des § 7 Abs. 3 UWG verlangt – die Möglichkeit zu geben, der Verwendung seiner E-Mail-Adresse zum Zwecke der Werbung zu widersprechen. Ansonsten ist der Eingriff grundsätzlich rechtswidrig.**

Keine Funktion als Syndikusanwalt für als externer DSB tätigen angestellten Unternehmensjuristen (Ls)

(**Bundesgerichtshof**, Urteil vom 2. Juli 2018 – AnwZ (Brfg) 49/17 –)

1. **Bei dem Merkmal der anwaltlichen Tätigkeit in „Rechtsangelegenheiten des Arbeitgebers" (§ 46 Abs. 2 Satz 1, Abs. 5 BRAO) handelt es sich nicht lediglich um eine Beschränkung der Rechtsdienstleistungsbefugnis des Syndikusrechtsanwalts, sondern – ebenso wie bei den Bestimmungen in § 46 Abs. 2 bis 4 BRAO – um eine tatbestandliche Voraussetzung für die Zulassung als Syndikusrechtsanwalt.**
2. **In Rechtsangelegenheiten des Arbeitgebers nach § 46 Abs. 2 Satz 1, Abs. 5 Satz1, 2 BRAO ist nicht tätig, wer von diesem bei dessen Kunden als externer Datenschutzbeauftragter eingesetzt wird.**
3. **§ 46 Abs. 5 BRAO verstößt, soweit danach ein als externer Datenschutzbeauftragter bei Kunden seines Arbeitgebers eingesetzter angestellter Unternehmensjurist nicht in Rechtsangelegenheiten des Arbeitgebers tätig wird, nicht gegen Art. 12 Abs. 1 Satz 1 GG oder Art. 3 Abs. 1 GG.**

Zur Herausgabe der Handakte eines Mandanten durch den Rechtsanwalt

(**Bundesgerichtshof**, Urteil vom 17. Mai 2018 – IX ZR 243/17 –)

Ein Rechtsanwalt ist grundsätzlich verpflichtet, seinem Mandanten auf Verlangen die gesamte Handakte herauszugeben. Soweit der Anwalt die Herausgabe mit Rücksicht auf Geheimhaltungsinteressen sonstiger Mandanten verweigert, hat er dies unter Angabe näherer Tatsachen nachvollziehbar darzulegen.

Aus den Gründen:

1. Auf den Anwaltsdienstvertrag finden nach § 675 BGB auch die Vorschriften der §§ 666, 667 BGB Anwendung. Der Anspruch des Klägers auf Herausgabe der die anwaltliche Tätigkeit des Beklagten betreffenden Akten folgt aus § 667 BGB in Verbindung mit § 50 BRAO.

a) Zu den nach § 667 BGB herauszugebenden Unterlagen gehören die Handakten des Rechtsanwalts (BGH, Urteil vom 30. November 1989 – III ZR 112/88, BGHZ 109, 260, 264; vom 3. November 2014 – AnwZ 72/13, NJW-RR 2015, 186 Rn. 11; RGRK/Steffen, BGB, 12. Aufl., § 667 Rn. 12; Soergel/Beuthien, BGB, 13. Aufl., § 667 Rn.11; Dauner-Lieb/Langen/Schwab, BGB, 3. Aufl., § 667 Rn. 7; Erman/Berger, BGB, 16. Aufl., § 667 Rn. 8). Diese Herausgabepflicht wird auch in § 50 BRAO vorausgesetzt (vgl. Henssler/Prütting/Offermann-Burckart, BRAO, 4. Aufl., § 50 Rn. 27, 35 ff.; Feuerich/Weyland/Träger, BRAO, 9. Aufl., §50 Rn. 17; Tauchert/Dahns, in: Gaier/Wolf/Göcken, Anwaltliches Berufsrecht, 2. Aufl., § 50 BRAO Rn. 11; Kleine-Cosack, BRAO, 7. Aufl., §50 Rn. 4). Dokumente, die der Rechtsanwalt aus Anlass seiner beruflichen Tätigkeit von dem Auftraggeber oder für ihn erhalten hat, hat er gemäß § 50 Abs. 1 BRAO seinem Auftraggeber auf Verlangen herauszugeben. Dabei fallen die Unterlagen, die dem Anwalt von seinem Auftraggeber ausgehändigt worden sind, unter die erste Alternative und der Schriftverkehr, den der Anwalt für seinen Auftraggeber geführt hat, unter die zweite Alternative des §667 BGB.

Aus der Geschäftsbesorgung erlangt ist daher insbesondere der gesamte drittgerichtete Schriftverkehr, den der Rechtsan-

walt für den Auftraggeber erhalten und geführt hat, also sowohl die dem Rechtsanwalt zugegangenen Schriftstücke als auch Kopien eigener Schreiben des Rechtsanwalts. Die herauszugebenden Unterlagen umfassen auch Notizen über Besprechungen, die der Anwalt im Rahmen der Besorgung des Geschäfts geführt hat (BGH, Urteil vom 30. November 1989, aaO S. 265).

Nach Eröffnung des Insolvenzverfahrens über das Vermögen der Schuldnerin steht der Herausgabeanspruch aus § 667 BGB dem Kläger zu. Der Geschäftsbesorgungsvertrag zwischen der Schuldnerin und der Beklagten ist mit Insolvenzeröffnung erloschen (§§ 115, 116 InsO). Für ein Fortbestehen des Mandats nach der Ausnahmeregelung des § 115 Abs. 2 InsO fehlt es an tatsächlichen Anhaltspunkten. Daraus folgt, dass die aus dem beendeten Mandatsverhältnis entstandenen Ansprüche der Schuldnerin in die Insolvenzmasse fallen und der Verwaltungs- und Verfügungsbefugnis des Klägers unterliegen (§ 80 InsO). Dies bedeutet, dass der Kläger unter den gleichen Voraussetzungen und in demselben Umfang Herausgabe oder Einsichtsgewährung der Handakte verlangen kann, wie es ohne die Insolvenz die Schuldnerin bei einer anderweitigen Mandatsbeendigung selbst gekonnt hätte (BGH, aaO S. 264).

b) Der Anwalt ist jedoch nicht stets zur umfassenden Herausgabe der Handakte verpflichtet. Ausnahmsweise können Eigeninteressen des Anwalts oder Geheimhaltungsinteressen Dritter Vorrang genießen.

aa) Eine Ausnahme hinsichtlich der Herausgabepflicht gilt für solche Unterlagen, die nicht lediglich über das Tun im Rahmen der Vertragserfüllung Aufschluss geben, sondern persönliche Eindrücke, die der Anwalt in den Gesprächen gewonnen hat, wiedergeben. Aufzeichnungen des Anwalts über derartige persönliche Eindrücke sind oft nützlich; sie sind im Zweifel jedoch nicht für die Einsicht durch den Mandanten bestimmt, und eine solche wäre dem Anwalt auch nicht zumutbar. Ein Anwalt, der zur Herausgabe von Handakten verpflichtet ist, braucht daher nicht auch derartige Aufzeichnungen offenzulegen. Darüber hinaus wird dem Anwalt bei der Ausführung des Mandats ein gewisser Freiraum zuzuerkennen sein, vertrauliche „Hintergrundinformationen" zu sammeln, die er auch und gerade im wohl verstandenen Interesse seines Mandanten sowie im Interesse der Rechtspflege diesem gegenüber verschweigen darf. Aufzeichnungen über derartige Vorgänge unterliegen nicht der Herausgabepflicht (BGH, aaO S. 265).

bb) Zudem bestehen Verschwiegenheitspflichten des auf Herausgabe der Handakte in Anspruch genommenen Rechtsanwalts mit Rücksicht auf Interessen seiner sonstigen Mandanten. Die Verschwiegenheitspflicht findet ihre Grundlage in dem auf einem besonderen Vertrauensverhältnis beruhenden Anwaltsvertrag (Vill, in: G. Fischer/Vill/D. Fischer/Rinkler/Chab, Handbuch der Anwaltshaftung, 4. Aufl., § 2 Rn. 339; Weinland, in: Henssler/Gehrlein/Holzinger, Handbuch der Beraterhaftung, 2018, Kap. 3 Rn. 15). Der Rechtsanwalt ist zudem berufsrechtlich gemäß § 43a Abs. 2 Satz 1 BRAO zur Verschwiegenheit verpflichtet. Diese Verschwiegenheitspflicht, die sich auf alles bezieht, was dem Anwalt in Ausübung seines Berufs bekannt geworden ist, betrifft insbesondere Kenntnisse aus einzelnen Mandatsverhältnissen, die sonstigen Mandanten nicht offenbart werden dürfen. Eine Verletzung der anwaltlichen Schweigepflicht kann eine Vertragshaftung des Rechtsanwalts aus § 280 Abs. 1 BGB, aber auch eine deliktische Haftung gemäß § 823 Abs. 2 BGB, § 203 Abs. 1 Nr. 3 StGB begründen (Heinemann, in: Greger/Vollkommer/Heinemann, Anwaltshaftungsrecht, 4. Aufl., § 15 Rn. 3; Vill, aaO § 2 Rn. 340; Weinland, aaO Kap. 3 Rn. 18).

cc) Persönliche Geheimhaltungsinteressen von an Besprechungen mit dem Anwalt beteiligten dritten Personen vermögen für diesen zumindest nicht ein uneingeschränktes Auskunftsverweigerungsrecht zu begründen. Dies hat der Bundesgerichtshof für Gespräche entschieden, die der Anwalt der späteren Schuldnerin mit deren Organmitgliedern geführt hat (BGH, Urteil vom 30. November 1989 – III ZR 112/88, BGHZ 109, 260, 271). Ein Auskunftsverweigerungsrecht kommt in einer solchen Konstellation nur dann in Betracht, wenn zwischen dem Anwalt und dem einzelnen Organmitglied eine besondere Vertrauensbeziehung bestanden hat, die individuell begründet worden ist, etwa dadurch, dass das betreffende Mitglied den Anwalt ausdrücklich um eine persönliche Beratung gebeten hat. Nur für einen solchen Ausnahmefall könnte es gebilligt werden, dass es sich bei den Beziehungen des Anwalts zu der Schuldnerin einerseits und den Organmitgliedern andererseits um zwei getrennte, rechtlich selbständige Rechtsverhältnisse gehandelt habe. An die dem Anwalt insoweit obliegende Darlegungslast sind jedoch strenge Anforderungen zu stellen, zumal eine solche Konstellation deswegen ungewöhnlich wäre, weil die Gefahr eines Interessenkonflikts mit dem ursprünglichen Auftraggeber nicht von der Hand zu weisen ist (BGH, aaO S. 272). Insoweit obliegt die Darlegungslast dem beklagten Rechtsanwalt (BGH, aaO S. 273 f.).

2. Nach diesen im Schrifttum geteilten (Heinemann, aa O § 15 Rn. 17; Vill, aaO § 2 Rn. 3 70; Fahrendorf in Fahrendorf/Mennemeyer, Die Haftung des Rechtsanwalts, 9. Aufl., Kap. 2 Rn. 684; Weinland, aaO Kap. 3 Rn. 41), weiter gültigen Grundsätzen hat die Beklagte ihrer Darlegungslast, mit Rücksicht auf Belange Dritter einer nur eingeschränkten Herausgabepflicht zu unterliegen, nicht genügt.

a) Soweit der Anwalt unter Berufung auf Verschwiegenheitspflichten die Herausgabe der Handakte verweigert, hat er den Darlegungspflichten eines Zeugen zu genügen, der ein Zeugnisverweigerungsrecht in Anspruch nimmt (vgl. § 386 Abs. 1, § 383 Abs. 1 Nr. 6 ZPO). Ist der Grund der Herausgabeverweigerung nicht ohne weiteres erkennbar, ist die Angabe näherer Tatsachen unerlässlich (RG JW 1903, 241 Nr. 15). Das Gericht muss sich auf der Grundlage der Sachverhaltsangaben, ohne dass das Geheimnis aufzudecken ist, ein Bild davon machen können, um was es geht (MünchKomm-ZPO/Damrau, 5.Aufl., §386 Rn. 2). Deshalb müssen die Angaben so weit ins Einzelne gehen, dass dem Richter ein Urteil über den Weigerungsgrund möglich ist (Stein/Jonas/Berger, ZPO, 23. Aufl., §386 Rn. 1). Handelt es sich um eine Auskunftsverweigerung aus beruflichen Gründen, bedarf es der beweisgeeigneten Darlegung, dass es sich um Tatsachen handelt, die im Rahmen der Berufsausübung anvertraut oder bekannt geworden sind. Insoweit ist in geeigneten Sachverhalten von der anerkannten Befugnis Gebrauch zu machen, eine vollständig anonymisierte Darstellung abzugeben, die keine Bezugsherstellung zu den beteiligten Personen gestattet (AnwG Köln, AnwBl. 2009, 792, 793 aE). Im Blick auf die Tatsachen, aus denen die Auskunftsverweigerung hergeleitet wird, ist nach Möglichkeit Beweis anzubieten. Im Streitfall käme die zeugenschaftliche Vernehmung von Rechtsanwalt D. als zuständigem Sachbearbeiter in Betracht, der nicht zu den vertretungsberechtigten Organen der Beklagten gehört. Diesen Darlegungsanforderungen ist entgegen der Würdigung des Berufungsgerichts unabhängig davon zu genügen, ob der Rechtsanwalt die Herausgabe der Handakte im Blick auf von ihm gefertigte persönliche Aufzeichnungen, Interessen anderer Mandanten oder dritter Personen verweigert, weil die Verschwiegenheitspflicht unterschiedslos gilt.

b) Den Anforderungen an die Spezifizierung (Wieczorek/Schütze/Ahrens, ZPO, 4. Aufl., § 386 Rn. 6) hat die Beklagte durch die bloße, nicht näher unterlegte Angabe, dass Interessen anderer Mandanten durch die Herausgabe der Akten beeinträchtigt werden können, nicht genügt. Es fehlt an jeglichen Angaben, inwiefern die Mandate der Schuldnerin Berührungspunkte zu sonstigen Mandaten der Beklagten haben können. Darum kann nach bisherigem Sach- und Streitstand nicht davon ausgegangen werden, dass die Beklagte die Herausgabe der Handakten mit Rücksicht auf die Geheimhaltungsinteressen anderer Mandanten verweigern darf.

aa) Die Vordergerichte durften im Streitfall nicht allein auf der Grundlage des Beklagtenvorbringens zu der Überzeugung gelangen, dass einer uneingeschränkten Herausgabepflicht der Akten Geheimhaltungsinteressen anderer Mandanten der Beklagten entgegenstehen. Dem Richter ist es zwar grundsätzlich erlaubt, allein aufgrund des Vortrags der Parteien und ohne Beweiserhebung festzustellen, was für wahr und was für nicht wahr zu erachten ist (§ 286 ZPO). Ein solches Verfahren darf aber nur in Ausnahmefällen angewandt werden, wenn der vorgetragene Sachverhalt beider Parteien klar, widerspruchsfrei und überzeugend ist (BGH, Urteil vom 6. Oktober 1981 – XZR 57/80, BGHZ 82, 13, 20 f.; Zöller/Greger, ZPO, 32. Aufl., § 286 Rn. 14; MünchKomm-ZPO/Prütting, 5. Aufl., § 286 Rn. 13; Prütting/Gehrlein/Laumen, ZPO, 9. Aufl., § 286 Rn. 2). Diese Voraussetzungen sind im Streitfall nicht gegeben, weil die Beklagte widersprüchlich vorgetragen hat.

(1) Die Beklagte hat sich vorgerichtlich lediglich darauf berufen, dass „in diesen Schriftstücken natürliche Personen involviert" seien, hinsichtlich derer eine Verschwiegenheitspflicht bestehe. Diese Darstellung hat die Beklagte im vorliegenden Rechtsstreit dahin ergänzt, dass der Schriftwechsel mit diesen Personen für die Schuldnerin geführt worden sei. Ferner hat sie ausgeführt, der Inhalt der Handakte betreffend das Mandat gegen S. und die R. S. GmbH & Co. KG bestehe, lasse man den Schriftwechsel mit der Schuldnerin außer Betracht, aus den erstinstanzlich und zweitinstanzlich gewechselten Schriftsätzen. Die Handakte aus dem Mandat gegen M. S. beschränke sich auf ein Anspruchsschreiben der Beklagten, durch das namens der Schuldnerin der Rücktritt von Kaufverträgen über Eigentumswohnungen erklärt worden sei, sowie ein Antwortschreiben des von M. S. beauftragten Rechtsanwalts. Erst in der mündlichen Verhandlung vor dem Amtsgericht hat die Beklagte geltend gemacht, in den Handakten seien Schriftstücke dritter Personen enthalten, zu denen ein Mandatsverhältnis bestehe.

(2) Angesichts des wechselnden, von dem Kläger bestrittenen Sachvortrags kann nicht davon ausgegangen werden, dass die herauszugebenden Handakten dritte Personen betreffende Schriftstücke enthalten, die durch ein Mandatsverhältnis mit der Beklagten verbunden sind. Zum einen ist zu berücksichtigen, dass die Beklagte zunächst lediglich ohne Bezug auf ein Mandatsverhältnis geltend gemacht hat, dass „in diesen Schriftstücken natürliche Personen involviert" seien, hinsichtlich derer eine Verschwiegenheitspflicht bestehe. Daraus kann schon nicht entnommen werden, ob die Schriftstücke von diesen Personen stammen oder diese Personen lediglich im Rahmen der Mandate schriftsätzlich erwähnt wurden. Überdies legen die erstinstanzlichen schriftsätzlichen Darlegungen der Beklagten nahe, dass die Handakten tatsächlich nur das Mandatsverhältnis zu der Schuldnerin betreffende Unterlagen aufweisen. Die Erklärung in der mündlichen Verhandlung vor dem Amtsgericht, zu dritten Personen sei ein Mandatsverhältnis begründet worden, entbehrt jeder auch nur abstrakten Konkretisierung. Da eine besondere Geheimhaltungspflicht erst nachträglich behauptet wurde, hätte sie zumindest plausibel gemacht werden müssen. Ferner kommt hinzu, dass die Beklagte von der Schuldnerin in zwei Verfahren mandatiert wurde. Es erscheint erklärungsbedürftig, dass ausgerechnet mit diesen beiden Mandaten gesonderte Mandate der Beklagten zu dritten Personen verknüpft sind.

bb) Zudem ist eine erhöhte Darlegungspflicht der Beklagten geboten, weil es die anwaltlichen Berufspflichten verletzen kann, unterschiedliche Mandate betreffende Schriftsätze in einer Handakte zu vereinigen.

cc) Gemäß § 50 Abs. 1 BRAO muss der Rechtsanwalt durch Anlegen von Handakten ein geordnetes Bild über die von ihm entfaltete Tätigkeit geben können. Um dieser Verpflichtung zu genügen, hat der Anwalt zu jedem Mandat eine eigenständige Akte anzulegen. Die Pflicht zur Anlegung der Handakte ist lückenlos (Henssler/Prütting/Offermann-Burckart, BRAO, 4. Aufl., § 50 Rn. 6, 11 f.; Feuerich/Weyland/Träger, BRAO, 9. Aufl., § 50 Rn. 1; Tauchert/Dahns in Gaier/Wolf/Göcken, Anwaltliches Berufsrecht, 2. Aufl., § 50 BRAO Rn. 3). Die Norm bezweckt die Sicherstellung der Mindestvoraussetzung einer Verwaltungsstruktur für die anwaltliche Tätigkeit einerseits und die Schaffung eines Beweismittels für den Rechtsanwalt und seinen Mandanten andererseits. Die Regelung dient dem Schutz des Mandanten, der mit der Handakte ein Beweismittel für ein etwaiges Fehlverhalten des Anwalts erhält (Tauchert/Dahns, aaO). Die Führung einer Handakte für unterschiedliche Verfahren stellt darum regelmäßig einen Organisationsmangel des Rechtsanwalts dar (vgl. BGH, Beschluss vom 14. Januar 1999 – III ZB 44/98, NJW – RR 1999, 716).

dd) Bei dieser Sachlage war es der Beklagten ohne besonderen Anlass verwehrt, andere Mandate betreffende Schriftstücke in die Handakten einzufügen, welche die Verfahren der Schuldnerin zum Gegenstand haben. Vor diesem Hintergrund bedürfte es einer eingehenden Darlegung, warum die Beklagte für die unterschiedlichen Mandate nicht gesonderte Handakten geführt hat.

III. Das angefochtene Urteil kann damit keinen Bestand haben. Es wird aufgehoben (§ 562 Abs. 1 ZPO). Da die Sache nicht zur Endentscheidung reif ist, wird sie zur neuen Verhandlung und Entscheidung an das Berufungsgericht zurückverwiesen. Dieses wird nunmehr aufgrund ergänzenden Sachvortrags der Beklagten darüber zu befinden haben, ob sie den Anforderungen an die Darlegung einer Geheimhaltungspflicht genügt hat.

Zur Prüfungspflicht des Betreibers einer Internet-Suchmaschine bei Persönlichkeitsrechtsverletzungen

(**Bundesgerichtshof**, Urteil vom 27. Februar 2018 – VI ZR 489/16 –)

Der Betreiber einer Internet-Suchmaschine (hier: Google) ist nicht verpflichtet, sich vor der Anzeige eines Suchergebnisses darüber zu vergewissern, ob dieses Persönlichkeitsrechtsverletzungen beinhaltet. Eine Pflicht

zum Handeln besteht erst dann, wenn durch einen konkreten Hinweis von einer offensichtlichen und auf den ersten Blick klar erkennbaren Verletzung des allgemeinen Persönlichkeitsrechts Kenntnis erlangt wird.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Kläger nehmen die Beklagten als Betreiber einer Internetsuchmaschine in Anspruch, es zu unterlassen, bestimmte, sie nach ihrem Vortrag in ihren Persönlichkeitsrechten verletzende Inhalte auf Drittseiten über die Suchmaschine auffindbar zu machen. Sie verlangen ferner von den Beklagten, einen entsprechenden Suchfilter einzurichten, der künftige Verletzungen verhindert, sowie eine Geldentschädigung für die bereits erfolgte Verletzung des Persönlichkeitsrechts.

Die Beklagte zu 1, die ihren Sitz in Kalifornien hat, betreibt die Internetsuchmaschine „Google". Dabei durchsucht sie mit einer Software kontinuierlich und automatisiert das Internet und übernimmt die so ermittelten Internetseiten in einen Suchindex. Die Daten gibt die Suchmaschine an die Nutzer entsprechend dem eingegebenen Suchbegriff nach einem von der Beklagten zu 1 erstellten Algorithmus als Ergebnisliste aus und verlinkt diese. Die Beklagte zu 2 ist eine Tochtergesellschaft der Beklagten zu 1 mit Sitz in Deutschland. Sie vermarktet Werbeflächen auf der Internetseite der Beklagten zu 1.

Die Kläger wandten sich an die Beklagten und monierten, dass ihr Persönlichkeitsrecht verletzende Inhalte auf bestimmten, von ihnen benannten Internetseiten über den Suchindex der Suchmaschine auffindbar gemacht würden. Diese Seiten dienten nach Auffassung der Kläger allein der Diffamierung, Kreditgefährdung und Rufschädigung.

Die Beklagte zu 1 bat daraufhin um die Übersendung der Verknüpfungen („Links") in elektronischer Form sowie um Darlegung, welche konkreten Aussagen beanstandet würden, wo genau sich die geltend gemachten Rechtsverletzungen in Bezug auf die Verknüpfungenbefänden und woraus sich diese ergäben. Die Kläger übersandten daraufhin entsprechende Angaben, verwiesen aber darauf, dass eine Differenzierung nicht möglich sei, da alle beanstandeten Beiträge Hinweise auf eine in Wahrheit nicht bestehende Beziehung der Kläger zum F-Internetforum enthielten.

Später teilte die Beklagte zu 1 mit, einige der beanstandeten Verknüpfungen entfernt zu haben. Die Kläger monierten jedoch eine Vielzahl weiterer Verknüpfungen. Sie übersandten der Beklagten zu 1 eine Abmahnung und beanstandeten mehrere hundert weitere zu löschende Verknüpfungen. Die Beklagte zu 1 teilte daraufhin wieder mit, dass (weitere) Verknüpfungen entfernt worden seien.

Die Kläger sind der Auffassung, die Beklagten seien als Betreiber der Suchmaschine mitverantwortlich für die fortwährende Verletzung ihrer Persönlichkeitsrechte. Insbesondere die Beklagte zu 1 hafte auf Unterlassung, da sie durch die Indexierung der Beiträge die unwahren und beleidigenden Aussagen erst allgemein auffindbar gemacht habe.

Das Landgericht hat die Beklagte zu 1 verurteilt, es zu unterlassen, einzelne Verknüpfungen auffindbar zu machen und die Klage im Übrigen abgewiesen. Auf die Anschlussberufung der Beklagten zu 1 hat das Oberlandesgericht unter Zurückweisung der Berufung der Kläger die Klage insgesamt abgewiesen. Mit der vom Berufungsgericht zugelassen Revision verfolgen die Kläger ihr Klagebegehren weiter.

Aus den Gründen:

Das Berufungsgericht (Urteil veröffentlicht in K&R 2017, 55) hat im Wesentlichen ausgeführt, dass den Klägern ein Unterlassungsanspruch gegen die Beklagte zu 2 weder aus dem Gesichtspunkt der Persönlichkeitsrechtsverletzung nach § 823 Abs. 1, § 1004 BGB analog, Art. 2 Abs. 1, Art. 1 GG zustehe noch wegen Verstoßes gegen das Bundesdatenschutzgesetz nach § 1004 BGB analog, § 823 Abs. 2 BGB iVm § 29 BDSG. Zwar greife die Beklagte zu 1 in das Allgemeine Persönlichkeitsrecht der Kläger ein, wenn sie durch ihre Suchmaschine Internetseiten auffindbar mache, auf denen die Behauptung aufgestellt werde, der Kläger zu 2 sei Betreiber des F-Internetforums, und auf denen es zu Beschimpfungen der Kläger komme. Dadurch werde der soziale Geltungsanspruch der Kläger beeinträchtigt. Insoweit könne sich eine Haftung der Beklagten zu 1 als mittelbare Störerin ergeben. Das Landgericht habe eine Haftung im Ausgangspukt zu Recht angenommen, wenn und soweit die Beklagte zu 1 im Einzelfall gegen reaktive Prüfpflichten verstoßen habe. Dies setze einen Hinweis auf eine klare Rechtsverletzung voraus. Weder die Vorschriften des Telemediengesetzes, noch der E-Commerce – Richtlinie (Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000, ABl. L 178/1 vom 17. Juli 2000, hiernach: „ECRL") stünden der Annahme einer solchen Prüfpflicht entgegen. Ein Unterlassungsanspruch der Kläger scheitere aber an der nicht ordnungsgemäßen Inkenntnissetzung der Beklagten zu 1, so dass keine reaktiven Prüfpflichten ausgelöst worden seien. Ein Suchmaschinenbetreiber sei zur Sperrung von Verknüpfungen nur verpflichtet, wenn die behauptete Rechtsverletzung offensichtlich erkennbar sei, der Betroffene also den Sachverhalt detailliert beschrieben habe. Diesen Anforderungen seien die Kläger nicht gerecht geworden.

Ein Unterlassungsanspruch ergebe sich ebenso wenig aus einer Verletzung des Bundesdatenschutzgesetzes (BDSG). Die Beklagte zu 1 habe die öffentlich zugänglichen Daten auf den Internetseiten erheben und als Ergebnislisten an ihre Nutzer übermitteln dürfen (§ 29 Abs. 1 Satz 1 Nr. 2 und Abs. 2 Satz 1 BDSG).

Mangels einer Verletzung des Allgemeinen Persönlichkeitsrechts der Kläger bestehe kein Anspruch auf Geldentschädigung. Der geltend gemachte Anspruch auf Einrichtung eines Suchfilters entbehre einer Anspruchsgrundlage.

Die Beklagte zu 2 sei, auch wenn es sich bei ihr um eine wirtschaftlich abhängige Tochtergesellschaft der Beklagten zu 1 handele, nicht passivlegitimiert, da sie selbst nicht Betreiberin der Suchmaschine sei.

B. Das angegriffene Urteil hält revisionsrechtlicher Nachprüfung stand.

I. Zutreffend ist das Berufungsgericht davon ausgegangen, dass sich die internationale Zuständigkeit der deutschen Gerichte für die gegen die in den USA ansässige Beklagte zu 1 gerichtete Klage, die auch in der Revisionsinstanz zu prüfen ist (Senatsurteil vom 2. März 2010 – VI ZR 23/09, BGHZ 184, 313 Rn. 9 f f. – New York Times; BGH, Urteile vom 28. November 2002 – III ZR 102/02, BGHZ 153, 82, 84 ff.; vom 20. November 2008 – I ZR 70/06, VersR 2009, 807 mwN; vom 22. Oktober 2009 – I ZR 88/07, VersR 2011, 648), nach § 32 ZPO bestimmt. Denn die Vorschriften über die örtliche Zuständigkeit (§§ 12 ff. ZPO) regeln mittelbar auch die Grenzziehung zwischen der Zuständigkeit deutscher und ausländischer Gerichte (vgl. Senatsurteil vom 3. Mai 1977 – VI ZR 24/75, NJW 1977, 1590; BGH, Urteil vom 22. November 1994 – XI ZR 45/91, NJW 1995, 1225, 1226).

1. Nach § 32 ZPO ist für Klagen aus unerlaubten Handlungen das Gericht zuständig, in dessen Bezirk die Handlung begangen ist. Zur Begründung der Zuständigkeit genügt es, wenn der Kläger schlüssig Tatsachen behauptet, aus denen sich eine im Gerichtsbezirk begangene unerlaubte Handlung ergibt (vgl. BGH,

Urteile vom 25. November 1993 – IX ZR 32/93, BGHZ 124, 237, 241; vom 28. Februar 1996 – XII ZR 181/93, BGHZ 132, 105, 110 f.). Begehungsort der deliktischen Handlung ist dabei so wohl der Handlungs- als auch der Erfolgsort, so dass eine Zuständigkeit wahlweise dort gegeben ist, wo die Verletzungshandlung begangen wurde, oder dort, wo in ein geschütztes Rechtsgut eingegriffen wurde (vgl. BGH, Urteil vom 28. Februar 1996 – XII ZR 181/93, BGHZ 132, 105, 110 f.; vom 21. April 2016 – I ZR 43/14, GRUR 2016, 1048 Rn. 18 – An evening with Marlene Dietrich). Erfasst werden neben Ansprüchen auf Schadensersatz auch Unterlassungsansprüche (vgl. Senatsurteil vom 29. März 2011 – VI ZR 111/10, AfP 2011, 265 Rn. 6 f. – www.womanineurope.com; BGH, Urteil vom 21. April 2016 – I ZR 43/14, GRUR 2016, 1048 Rn. 17 – An evening with Marlene Dietrich; Beschluss vom 17. März 1994 – I ZR 304/91, MDR 1995, 282 – Beta).

Die deutschen Gerichte sind zur Entscheidung über Klagen wegen Persönlichkeitsbeeinträchtigungen durch im Internet abrufbare Veröffentlichungen international zuständig, wenn die als rechtsverletzend beanstandeten Inhalte objektiv einen deutlichen Bezug zum Inland in dem Sinne aufweisen, dass eine Kollision der widerstreitenden Interessen – Interesse der Kläger an der Achtung ihres Persönlichkeitsrechts einerseits, Interesse der Beklagten an der Gestaltung ihres Internetauftritts und an einer Berichterstattung andererseits – nach den Umständen des konkreten Falls, insbesondere aufgrund des Inhalts der beanstandeten Meldung, im Inland tatsächlich eingetreten sein kann oder eintreten kann (vgl. Senatsurteil vom 2. März 2010 – VI ZR 23/09, BGHZ 184, 313 Rn. 15 ff. „New York Times“). Dies ist dann anzunehmen, wenn eine Kenntnisnahme von der beanstandeten Meldung nach den Umständen des konkreten Falls im Inland erheblich näher liegt, als es aufgrund der bloßen Abrufbarkeit des Angebots der Fall wäre und die von den Klägern behauptete Beeinträchtigung ihres Persönlichkeitsrechts durch Kenntnisnahme von der Meldung (auch) im Inland eintreten würde (vgl. Senat aaO).

2. Nach diesen Grundsätzen ist die internationale Zuständigkeit der deutschen Gerichte gemäß § 32 ZPO entgegen der Ansicht der Revisionserwiderung betreffend alle von der Beklagten zu 1 angebotenen Suchmaschinen-leistungen gegeben.

Ein Inlandsbezug besteht auch hinsichtlich der über www.google.com gewonnenen Suchergebnisse. Zwar weist die Revisionserwiderung darauf hin, dass die von der Beklagten zu 1 eingesetzte Technik die deutschen Nutzer der Suchmaschine www.google.com zum länderspezifischen Internetauftritt www.google.de umleite. Nach den unangegriffenen Feststellungen des Berufungsgerichts ist es jedoch möglich, von Deutschland aus die Suche über www.google.com durchzuführen und dabei deutschsprachige Ergebnisse zu erzielen. Die Beklagte zu 1 hält für die Nutzer nach der Umleitung auf den deutschlandspezifischen Internetauftritt eine Option auf der Internetseite vor, gleichwohl mit www.google.com zu suchen. Auch die bei einer Suche über www.google.com angezeigten Ergebnislisten weisen einen deutlichen Inlandsbezug auf, weil sie die angezeigten Treffer in deutscher Sprache aufführen und die in Deutschland wohnenden und hier ihrer beruflichen Tätigkeit nachgehenden Kläger namentlich genannt werden.

II. Das Berufungsgericht geht zu Recht von der Anwendbarkeit deutschen materiellen Rechts aus. Die richtige Anwendung des deutschen Internationalen Privatrechts ist in der Revisionsinstanz von Amts wegen zu prüfen (vgl. Senatsurteile vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 13; vom 15. Juli 2008 – VI ZR 105/07, BGHZ 177, 237 Rn. 8 mwN; BGH, Urteil vom 2. Oktober 1997 – I ZR 88/95, BGHZ 136, 380, 386; Zöller/Geimer, ZPO, 32. Aufl., § 293 Rn. 9 ff.).

1. Die Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates vom 11. Juli 2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht (Rom II – Verordnung) ist im Streitfall nicht anwendbar, da gemäß deren Art. 1 Abs. 2 lit. g außervertragliche Schuldverhältnisse aus der Verletzung der Persönlichkeitsrechte vom Anwendungsbereich der Verordnung ausgenommen sind.

2. Dass der von den Klägern geltend gemachte Anspruch nach deutschem Recht zu beurteilen ist, folgt aus Art. 40 Abs. 1 Satz 2 EGBGB, dem auch der Persönlichkeitsschutz einschließlich sich daraus herleitender Unterlassungsansprüche unterfällt (vgl. Senatsurteil vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 15).

a) Art. 40 EGBGB wird nicht durch § 3 Abs. 2 TMG verdrängt. Denn diese Bestimmung enthält keine Kollisionsnorm (Senatsurteil vom 8. Mai 2012 – VI ZR 217/08, VersR 2012, 994 Rn. 23 ff. nach Vorlage an den EuGH, Urteil vom 25. Oktober 2011 – Rs. C-509/09, juris – eDate Advertising).

b) Der maßgebliche Erfolgsort liegt in Deutschland. Hier wird der soziale Geltungsanspruch, den die Kläger in ihrem Lebenskreis genießen, gestört bzw. gefährdet (vgl. Senatsurteile vom 8. Mai 2012 – VI ZR 217/08, VersR 2012, 994 Rn. 31; vom 2. März 2010 – VI ZR 23/09, BGHZ 184, 313 Rn. 23; vom 3. Mai 1977 – VI ZR 24/75, NJW 1977, 1590 f.). Hier kollidiert ihr Interesse an der Unterlassung der ihr Persönlichkeitsrecht berührenden Anzeige der Suchergebnisse mit dem Interesse der Beklagten zu 1 an der Gestaltung ihres Internetauftritts und an der Ausübung ihres Geschäftsmodells.

III. Den Klägern steht gegen die Beklagte zu 1 kein Anspruch zu, es zu unterlassen, die beanstandeten Inhalte auf den von ihnen benannten Internetseiten durch Anzeige in den Suchergebnissen mit entsprechender Verlinkung auffindbar zu machen. Der Unterlassungsanspruch ergibt sich weder aufgrund einer Haftung der Beklagten zu 1 als mittelbare Störer in wegen Verletzung des Allgemeinen Persönlichkeitsrechts (§ 823 Abs. 1, § 1004 Abs. 1 BGB analog iVm Art. 2 Abs. 1, Art. 1 GG) noch aufgrund einer Verletzung datenschutzrechtlicher Schutzgesetze (§ 823 Abs. 2 BGB iVm § 4 Abs. 1, § 29 BDSG). Auch die darüber hinaus von den Klägern geltend gemachten Ansprüche auf Einrichtung eines Filters, auf Auskunft über die Identität von Verfassern der beanstandeten Interneteinträge sowie auf Zahlung einer Geldentschädigung bestehen nicht.

1. Die Kläger haben gegen die Beklagte zu 1 keinen Unterlassungsanspruch aufgrund einer Haftung als mittelbare Störerin wegen Verletzung ihres allgemeinen Persönlichkeitsrechts nach § 823 Abs. 1, § 1004 Abs. 1 BGB analog iVm Art. 2 Abs. 1, Art. 1 GG.

a) Zutreffend geht das Berufungsgericht davon aus, dass es im Streitfall nicht um die Haftung der Beklagten zu 1 als unmittelbare Störerin geht (in der Diktion des I. Zivilsenats „Täterin“; zu den unterschiedlichen Begrifflichkeiten des erkennenden Senats einerseits und des I. Zivilsenats andererseits vgl. Senatsurteil vom 28. Juli 2015 – VIZR 340/14, AfP 2015, 425 Rn. 34; v. Pentz, AfP 2014, 8, 16).

aa) Unmittelbare Störerin könnte die Beklagte zu 1 nur sein, wenn es sich bei den von den Klägern angegriffenen Suchergebnisseiten um eigene Inhalte der Beklagten zu 1 handelte, wobei zu den eigenen Inhalten eines Suchmaschinenbetreibers auch solche Inhalte gehören, die zwar von einem Dritten hergestellt wurden, die sich der Suchmaschinenbetreiber aber zu eigen gemacht hat. Von einem Zu-Eigen-Machen ist auszugehen, wenn der

in Anspruch Genommene nach außen erkennbar die inhaltliche Verantwortung für die auf seiner Internetseite veröffentlichten Inhalte übernommen hat, was aus Sicht eines verständigen Durchschnittsnutzers auf der Grundlage einer Gesamtbetrachtung aller relevanten Umstände zu beurteilen ist (Senatsurteile vom 4. April 2017 – VI ZR 123/16, VersR 2017, 895 Rn. 18; vom 1. März 2016 – VIZR 34/15, BGHZ 209, 139 Rn. 17 – jameda.de II; vom 27. März 2012 – VI ZR 144/11, AfP 2012, 264 Rn. 10 f. – RSS – Feeds; vom 30. Juni 2009 – VI ZR 210/08, AfP 2009, 494 Rn. 19 – Domainverpächter; BGH, Urteil vom 19. März 2015 – I ZR 94/13, NJW 2015, 3443 Rn. 25 – Hotelbewertungsportal). Dabei ist bei der Annahme einer Identifikation mit fremden Inhalten grundsätzlich Zurückhaltung geboten.

bb) Die von den Klägern beanstandeten Inhalte auf den Internetseiten, welche die Beklagte zu 1 durch Verlinkung auffindbar macht, sind keine eigenen Inhalte der Beklagten zu 1. Sie wurden von anderen Personen ins Internet eingestellt. Die Beklagte zu 1 hat sich die Inhalte durch Aufnahme in den Suchindex auch nicht zu Eigen gemacht. Die Beklagte zu 1 durchsucht mit Hilfe sog. crawler – Programme die im Internet vorhandenen Seiten und erstellt hieraus automatisiert und nach ihren Algorithmen einen Suchindex. Bei der Anfrage durch einen Nutzer durchsucht die Suchmaschine der Beklagten zu 1 diesen Index und liefert entsprechende Suchergebnisse. Auf der Grundlage einer Gesamtbetrachtung aller relevanten Umstände übernimmt die Beklagte zu 1 aus der Sicht eines verständigen Durchschnittsnutzers damit nicht nach außen erkennbar die Verantwortung für die nachgewiesenen Inhalte (vgl. Senatsurteil vom 1. März 2016 – VI ZR 34/15 BGHZ 209, 139 Rn. 16 – jameda.de II). Der Anzeige der Suchergebnisse entnimmt der verständige Durchschnittsnutzer lediglich dieAussage, dass sich die von ihm eingegebenen Suchbegriffe in irgendeiner Weise in den über die angegebenen Links erreichbaren Texten auf den nachgewiesenen Internetseiten befinden; er entnimmt ihr hingegen nicht, dass sich die Beklagte zu 1 mit den auffindbar gemachten Inhalten identifiziert. Dass die Beklagte zu 1 die indexierten Internetseiten inhaltlich-redaktionell überprüft hätte, ist (vgl. Senatsurteil vom 27. März 2012 – VI ZR 144/11, AfP 2012, 264 Rn. 11 – RSS-Feeds; BGH, Urteil vom 19. März 2015 – I ZR 94/13, NJW 2015, 3443 Rn. 25 ff. mwN – Hotelbewertungsportal) ist im Übrigen weder festgestellt noch von den Klägern behauptet worden.

b) Wie das Berufungsgericht weiter zutreffend angenommen hat, kommt allerdings eine Haftung der Beklagten zu 1 als mittelbare Störerin in Betracht.

aa) Grundsätzlich ist als mittelbarer Störer verpflichtet, wer, ohne unmittelbarer Störer zu sein, in irgendeiner Weise willentlich und adäquat kausal zur Beeinträchtigung des Rechtsguts beiträgt. Dabei kann als Beitrag auch die Unterstützung oder Ausnutzung der Handlung eines eigenverantwortlich handelnden Dritten genügen, sofern der in Anspruch Genommene die rechtliche und tatsächliche Möglichkeit zur Verhinderung dieser Handlung hatte (vgl. Senatsurteile vom 1. März 2016 – VI ZR 34/15, BGHZ 209, 139 Rn. 22 – jameda.de II; vom 28. Juli 2015 – VI ZR 340/14, AfP 2015, 425 Rn. 34; vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 21 mwN – Blog-Eintrag). Die Haftung als mittelbarer Störer darf nach ständiger höchstrichterlicher Rechtsprechung aber nicht über Gebühr auf Dritte erstreckt werden, welche die rechtswidrige Beeinträchtigung nicht selbst vorgenommen haben. Sie setzt deshalb die Verletzung von Verhaltenspflichten, insbesondere von Prüfpflichten, voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem als mittelbaren Störer in Anspruch Genommenen nach den Umständen des Einzelfalls eine Verhinderung der Verletzung zuzumuten ist (Senatsurteile vom 1. März 2016 – VI ZR 34/15, BGHZ 209, 139 Rn. 22 – jameda.de II; vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 22 – Blog – Eintrag; vom 30. Juni 2009 – VI ZR 210/08, AfP 2009, 494 Rn. 18 – Domainverpächter; BGH, Urteile vom 21. September 2017 – I ZR 11/16, WRP 2018, 201 Rn. 74 – Vorschaubilder III; vom 17. August 2011 – I ZR 57/09, BGHZ 191, 19 Rn. 20 – Stiftparfüm; vom 17. Dezember 2010 – V ZR 44/10, AfP 2011, 156 Rn. 15; vom 1. April 2004 – I ZR 317/01, BGHZ 158, 343, 350 – Schöner Wetten; vom 11. März 2004 – I ZR 304/01, BGHZ 158, 236, 251 – Internetversteigerung I; vom 30. April 2008 – I ZR 73/05, NJW – RR 2008, 1136 Rn. 50 – Internetversteigerung III).

bb) Für die Verhaltenspflichten eines Hostproviders, der dem unmittelbaren Störer die Internetplattform zur Verfügung stellt, hat der erkennende Senat bereits Grundsätze aufgestellt. Danach ist ein Hostprovider zur Vermeidung einer Haftung als mittelbarer Störer grundsätzlich nicht verpflichtet, die von den Nutzern in das Netz gestellten Beiträge vor der Veröffentlichung auf eventuelle Rechtsverletzungen zu überprüfen. Er ist aber verantwortlich, sobald er Kenntnis von der Rechtsverletzung erlangt. Weist ein Betroffener den Hostprovider auf eine Verletzung seines Persönlichkeitsrechts durch den Nutzer seines Angebots hin, kann der Hostprovider verpflichtet sein, künftig derartige Störungen zu verhindern (Senatsurteile vom 1. März 2016 – VI ZR 34/15, BGHZ 209, 139 Rn. 23 – jameda.de II; vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 24 – Blog-Eintrag; vgl. auch BGH, Urteile vom 17. August 2011 – I ZR 57/09, BGHZ 191, 19 Rn. 21 – Stiftparfüm; vom 12. Juli 2007 – I ZR 18/04, BGHZ 173, 188 Rn. 41 ff. – Jugendgefährdende Medien bei ebay; vom 11. März 2004 – I ZR 304/01, BGHZ 158, 236, 251 f. – Internet-Versteigerung I). Wird eine Verletzung von Persönlichkeitsrechten behauptet, wird sich eine Rechtsverletzung allerdings nicht stets ohne weiteres feststellen lassen. Denn sie erfordert eine Abwägung zwischen dem Recht des Betroffenen auf Schutz seiner Persönlichkeit aus Art. 1 Abs. 1 iVm Art. 2 Abs. 1 GG, Art. 8 Abs. 1 EMRK und dem durch Art. 5 Abs.1 GG, Art. 10 EMRK geschützten Recht jedenfalls des Providers auf Meinungs- und Medienfreiheit. Ist der Provider mit der Beanstandung eines Betroffenen konfrontiert, die so konkret gefasst ist, dass der Rechtsverstoß auf der Grundlage der Behauptung des Betroffenen unschwer bejaht werden kann, ist eine Ermittlung und Bewertung des gesamten Sachverhalts unter Berücksichtigung einer etwaigen Stellungnahme des für den beanstandeten Beitrag Verantwortlichen erforderlich (Senatsurteil vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 25 f. – Blog-Eintrag). Dies gilt auch dann, wenn die beanstandete Äußerung nicht als Tatsachenbehauptung, sondern als Werturteil zu qualifizieren ist, das Werturteil vom Betroffenen aber mit der schlüssigen Behauptung als rechtswidrig beanstandet wird, der tatsächliche Bestandteil der Äußerung, auf dem die Wertung aufbaue, sei unrichtig, dem Werturteil fehle damit jegliche Tatsachengrundlage (Senatsurteil vom 1. März 2016 – VI ZR 34/15, BGHZ 209, 139 Rn. 24 – jameda.de II).

cc) Diese Grundsätze können im Ansatz auch auf den Betreiber einer Internet-Suchmaschine übertragen werden (vgl. BGH, Urteile vom 29. April 2010 – I ZR 69/08, BGHZ 185, 291 Rn. 39 – Vorschaubilder I – und vom 21. September 2017 – I ZR 11/16, WRP 2018, 201 Rn. 60 ff. – Vorschaubilder III). An dessen Prüfpflichten sind jedoch geringere Anforderungen zu stellen.

(1) Vom Anbieter einer Suchmaschine kann vernünftigerweise nicht erwartet werden, dass er sich vergewissert, ob die

von den Suchprogrammen aufgefundenen Inhalte rechtmäßig ins Internet eingestellt worden sind, bevor er diese auffindbar macht. Einer Pflicht des Anbieters einer Suchfunktion, Nachforschungen zur Rechtmäßigkeit der Veröffentlichung der von Suchmaschinen aufgefundenen Inhalte anzustellen (proaktive Prüfungspflicht), stehen Aufgabe und Funktionsweise der Suchmaschinen entgegen. Der Zugriff einer Suchmaschine auf andere Internetseiten erfolgt nicht in der Weise, dass absichtlich und gezielt einzelne Hyperlinks auf bestimmte andere Internetseiten gesetzt werden. Suchmaschinen durchsuchen das frei zugängliche Internet in einem automatisierten Verfahren unter Einsatz von Computerprogrammen, wobei sie nicht danach unterscheiden können, ob der aufgefundene Beitrag eine Persönlichkeitsrechtsverletzung eines Dritten darstellt (vgl. BGH, Urteil vom 21. September 2017 – I ZR 11/16, WRP 2018, 201 Rn. 60 ff. – Vorschaubilder III). Eine allgemeine Kontrollpflicht wäre im Blick auf die Aufgabe von Internetsuchmaschinen unangemessen. Ohne die Hilfestellung einer solchen Suchmaschine wäre das Internet aufgrund der nicht mehr übersehbaren Flut von Daten für den Einzelnen nicht sinnvoll nutzbar. Letztlich ist damit die Nutzung des Internets insgesamt auf die Existenz und Verfügbarkeit von Suchmaschinen angewiesen. Wegen ihrer essentiellen Bedeutung für die Nutzbarmachungdes Internets dürfen keine Prüfpflichten statuiert werden, die den Betrieb von Suchmschinen gefährdeten oder unverhältnismäßig erschwerten. Die Annahme einer – praktisch kaum zu bewerkstelligenden – allgemeinen Kontrollpflicht würde die Existenz von Suchmaschinen als Geschäftsmodell, das von der Rechtsordnung gebilligt worden und gesellschaftlich erwünscht ist, ernstlich in Frage stellen (vgl. zum Vorstehenden BGH, Urteile vom 21. September 2017 – I ZR 11/16, WRP 2018, 201 Rn. 60 ff. – Vorschaubilder III – und vom 11. März 2004 – I ZR 304/01, BGHZ 158, 236, 251 f. – Internet – Versteigerung).

(2) Anders als in den bislang vom erkennenden Senat zu entscheidenden Fällen, die eine Haftung der Portalbetreiber betrafen, steht der Suchmaschinenbetreiber regelmäßig in keinem rechtlichen Verhältnis zu den Verfassern der in der Ergebnisliste nachgewiesenen Inhalte. Die Ermittlung und Bewertung des gesamten Sachverhaltes unter Berücksichtigung einer Stellungnahme des unmittelbaren Störers (notice-and-take-down-Verfahren) ist mangels bestehen den Kontakts zu den Verantwortlichen der Internetseiten regelmäßig nicht ohne weiteres möglich. In der Regel stehen dem Suchmaschinenbetreiber nur die Angaben des Betroffenen zur Verfügung, der die Löschung der Internetseite aus der Ergebnisanzeige begehrt. Die Kontaktaufnahme zum Verantwortlichen der beanstandeten Internetseite kann einen erheblichen Suchaufwand erfordern und muss nicht gelingen (kritisch hierzu Rau, K&R 2017, 60). Von einer fehlenden zeitnahen Rückmeldung könnte daher nicht ohne weiteres auf die Rechtswidrigkeit der nachgewiesenen Inhalte geschlossen werden. Eine Überspannung der Anforderungen an den Suchmaschinenbetreiber in einer Situation, in der die Rechtswidrigkeit des Eingriffs in das geschützte Rechtsgut – anders als bei Marken- oder Urheberrechtsrechtsverletzungen – nicht indiziert ist (vgl. Senatsurteil vom 8. Mai 2012 – VI ZR 217/08, AfP 2012, 372 Rn.35) und die Durchführung eines notice-and-take-down-Verfahrens nicht möglich ist, führte zu der Gefahr des Overblocking, also zu einer Neigung des Diensteanbieters, im Zweifelsfall zur Vermeidung weiterer Auseinandersetzungen die beanstandete Internetseite aus dem Suchindex zu entfernen. Dies hätte zur Folge, dass im ersten Zugriff als problematisch angesehene, aber bei weiterer Prüfung als zulässig zu beurteilende Inhalte faktisch unauffindbar gemacht würden (vgl. EuGH, Urteile vom 16. Februar 2012, Rs. C-360/10, juris Rn. 50 – SABAM; vom 24. November 2011, Rs. C-70/10, juris Rn. 52 – Scarlet Extended; siehe auch Masing, VerfBlog vom 14. August 2014, Ziffer 5: http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/). Darüber hinaus wäre, weil Links gelöscht würden, jeweils der komplette Beitrag betroffen und nicht nur der konkret als unzulässig beanstandete Teil eines Beitrags.

(3) Den Betreiber einer Suchmaschine treffen daher erst dann spezifische Verhaltenspflichten, wenn er durch einen konkreten Hinweis Kenntnis von einer offensichtlichen und auf den ersten Blick klar erkennbaren Rechtsverletzung erlangt hat (vgl. zum Umfang der Prüfpflichten eines Suchmaschinenbetreibers auch OLG Hamburg, Urteil vom 16. August 2011 – 7 U 51/10, AfP 2011, 491; LG Hamburg, Urteil vom 07. November 2014 – 324 O 660/12, NJW 2015, 796). Der Hinweis ist erforderlich, um den grundsätzlich nicht zur präventiven Kontrolle verpflichteten Diensteanbieter in die Lage zu versetzen, in der Vielzahl der indexierten Internetseiten diejenigen auffinden zu können, die möglicherweise die Rechte Dritter verletzen (vgl. BGH, Urteil vom 17. August 2011 – I ZR 57/09, BGHZ 191, 19 Rn. 21, 28 – Stiftparfüm). Ein Rechtsverstoß kann beispielsweise im oben genannten Sinn auf der Hand liegen bei Kinderpornographie, Aufruf zur Gewalt gegen Personen, offensichtlichen Personenverwechslungen, Vorliegen eines rechtskräftigen Titels gegen den unmittelbaren Störer, Erledigung jeglichen Informationsinteresses durch Zeitablauf (vgl. EuGH, Urteil vom 13. Mai 2014 – Rs. C-131/12, juris Rn. 92 ff. – Google Spain), Hassreden (vgl. EGMR, Urteil vom 16. Juni 2015 – 64569/09, NJW 2015, 2863 Rn. 153 ff. – Delfi AS/Estland) oder eindeutiger Schmähkritik.

(4) Allerdings kann die Grenze insbesondere in den beiden letztgenannten Fällen schwer zu ziehen sein. Gerade bei Schmähkritik ist die Erkennbarkeit einer offensichtlichen Rechtsverletzung für den Suchmaschinenbetreiber problematisch. Die Grenze zulässiger Meinungsäußerungen liegt nicht schon da, wo eine polemische Zuspitzung für die Äußerung sachlicher Kritik nicht erforderlich ist (vgl. BVerfG, NJW 2016, 2870 Rn. 13; BVerfGE 82, 272, 283 f.; BVerfGE 85, 1, 16). Eine Schmähkritik kann nicht bereits dann angenommen werden, wenn eine Äußerung überzogen oder ausfällig ist. Hinzutreten muss eine das sachliche Anliegen der Äußerung völlig in den Hintergrund drängende persönliche Kränkung (vgl. BVerfGE 93, 266 Ziffer 7b; BVerfGE 82, 272, 284), deren abschließende Bewertung ohne verifizierbare Erkenntnisse zum sachlichen Hintergrund selten möglich ist. Entsprechendes gilt für herabsetzende Tatsachenbehauptungen oder Werturteile mit Tatsachenkern. Denn hier kommt es maßgeblich auf den Wahrheitsgehalt der behaupteten Tatsache an (v. Pentz, AfP 2017, 102, 115). Hierzu hat der Suchmaschinenbetreiber typischerweise keine Erkenntnisse. Ist eine Validierung des Vortrags der Betroffenen somit regelmäßig nicht möglich, führt auch der Maßstab der „offensichtlich und auf den ersten Blick klar erkennbaren Rechtsverletzung“ nur in Ausnahmefällen zu einem eindeutigen Ergebnis für den Suchmaschinenbetreiber. Eine sichere und eindeutige Beurteilung, ob unter Berücksichtigung aller widerstreitenden grundrechtlich geschützten Belange und der Umstände des Einzelfalls das Schutzinteresse der Betroffenen die schutzwürdigen Belange der Internetseitenbetreiber, der Beklagten zu 1 sowie der Internetnutzer überwiegt (vgl. Senatsurteile vom 1.März 2016 – VI ZR 34/15, BGHZ 209, 139 Rn. 30; vom 17. Dezember 2013 – VI ZR 211/12, BGHZ 199, 237 Rn. 22 – Sächsische Korruptionsaffäre; vom 15. September 2015 – VI ZR 175/14, VersR

2015, 1437 Rn. 20; vom 28. Juli 2015 – VI ZR 340/14, AfP 2015, 425 Rn. 29; vom 13. Januar 2015 – VI ZR 386/13, VersR 2015, 336 Rn. 13 – Filialleiter bei Promi-Friseur; vom 30. September 2014 – VI ZR 490/12, AfP 2014, 534, 536 – Innenminister unter Druck; vom 29. April 2014 – VI ZR 137/13, AfP 2014, 325 Rn. 8 – Adoptivtochter), ist dem Suchmaschinenbetreiber im Regelfall nicht ohne weiteres möglich.

c) Nach diesen Grundsätzen wendet sich die Revision ohne Erfolg gegen die Annahme des Berufungsgerichts, dass die Kläger den Anforderungen an einen hinreichend konkreten Hinweis, der dem Suchmaschinenbetreiber eine offensichtliche und bereits auf den ersten Blick klar erkennbare Rechtsverletzung aufzeigt, nicht genügt haben.

aa) Das Berufungsgericht ist zutreffend davon ausgegagen, dass die von der Revision beanstandeten Bezeichnungen der Kläger zwar ausfallend scharf sind und ihre Ehre beeinträchtigen. Es hat jedoch weiter mit Recht angenommen, dass ihr ehrbeeinträchtigender Gehalt nicht von vornherein außerhalb jedes in einer Sachauseinandersetzung wurzelnden Verwendungskontextes steht. Denn die Äußerungen stehen ersichtlich im Zusammenhang mit der Rolle, welche die Kläger beim F-Internetforum gespielt haben sollen. Nach dem Inhalt der beanstandeten Suchergebnisse werden den Mitgliedern des F-Internetforums u.a. Stalking (Straftat iS des § 238 StGB) vorgeworfen. Darüber hinausdarf nach den Feststellungen des Berufungsgerichts auch nicht unberücksichtigt bleiben, dass es sich bei den Foren, in denen die betreffenden Äußerungen über die Kläger abgegeben wurden, in Gänze um Seiten handelt, auf denen eine eher deftige und grenzwertige Diktion vorherrscht und der Kläger zu 2 immerhin an der Erstellung des F-Internetforums mitgewirkt hat, das ebenfalls als Plattform für entsprechende Äußerungen gegen Dritte dient. Die vom Kläger zu 2 beanstandeten Begriffe fügen sich nahtlos in die auf diesen Seiten vorherrschende Wortwahl ein, was in Verbindung mit einem bestehenden Sachbezug gegen eine offensichtliche und bereits auf den ersten Blick klar erkennbare Rechtsverletzung spricht.

bb) Die Beteiligung des Klägers zu 2 an der Erstellung des F-Internetforums haben die Kläger nicht zweifelsfrei klären können. Der Kläger zu 2 räumt selbst ein, am „Aufsetzen" des F-Internetforums beteiligt gewesen zu sein; auch war eine von ihm eingerichtete E-Mail-Weiterleitung über das F-Internetforum an ihn noch Wochen nach dem Aufsetzen des Forums aktiv. Über die eigene, durch „eidesstattliche Versicherung" bekräftigte, jedoch ziemlich allgemein gehaltene und pauschale Behauptung hinaus, mit dem F-Internetforum nichts zu tun zu haben, hat der Kläger zu 2 keinerlei belastbare Indizien für die Haltlosigkeit der ihm – und zumindest mittelbar in Form der Mitwisserschaft seiner Frau, der Klägerin zu 1, – gemachten Vorwürfe aufgezeigt. Eine offensichtliche und auf den ersten Blick klar erkennbare Rechtsverletzung musste die Beklagte zu 1 den beanstandeten Äußerungen deshalb nicht entnehmen.

cc) Vor diesem Hintergrund wird die von der Revision als persönlichkeitsrechtsverletzend beanstandete Bezeichnung „Arschkriecher" auf der durch den Link in der Suchmaschine nachgewiesenen Seite nicht zusammenhanglos zur Diffamierung der Person des Klägers zu 2 verwendet, sondern weist aufgrund der Bezugnahme auf den Bekannten des Klägers zu 2 als mutmaßlichen Initiator des F-Internetforums noch eine Beziehung zur sachlichen Auseinandersetzung über die Rolle des Klägers zu 2 in diesem Forum auf. Mit der in ihrer Gesamtheit zu beurteilenden Äußerung „Der hat seinen jahrelangen Arschkriecher und Fußsoldaten... (Kläger zu 2)... ermuntert, die Seite F... ins Netz zu stellen" wird für den durchschnittlichen Rezipienten deutlich, dass nicht – ohne Sachbezug – eine im Vordergrund stehende Schmähung des Klägers zu 2 erfolgen, sondern vielmehr sein Verhalten gegenüber dem mutmaßlichen Initiator des F-Internetforums einer polemischen und überspitzten Kritik zugeführt werden sollte. Ähnliches gilt für die Bezeichnungen „Schwerstkriminelle" und „krimineller Schuft", die unter Berücksichtigung der Meinungsfreiheit der Blogger noch Teil einer sachbezogenen Auseinandersetzung mit den gegen den Kläger zu 2 und – zumindest als Mitwisserin – gegen die Klägerin zu 1 erhobenen Vorwürfen des Stalking sein konnten, das von dem vom Kläger zu 2 miterschaffenen F-Internetforum ausgegangen sein soll. Es ist insofern nicht – jedenfalls nicht aus Sicht der Beklagten zu 1 – offensichtlich und auf den ersten Blick klar erkennbar, dass sich die Äußerungen von den sachbezogenen Vorwürfen völlig gelöst hätten und die Verantwortlichkeit der Kläger nur als mutwillig gesuchter Anlass oder Vorwand genutzt würde, um die Kläger persönlich zu diffamieren. Da Mitgliedern des F-Internetforums u.a. Stalking vorgeworfen wurde und sich davon Betroffene „terrorisiert" fühlten, gilt entsprechendes für die beanstandeten Ausdrücke „Terroristen", „Bande", „Stalker", „krimineller Stalkerhaushalt" u.ä.

2. Den Klägern steht gegen die Beklagte zu 1 der von ihnen geltend gemachte Unterlassungsanspruch auch nicht nach § 1004 BGB analog, § 823 Abs. 2 BGB iVm §§ 4, 29 Abs. 1 Satz 1 Nr. 2, Abs. 2 BDSG zu. Nach diesen Vorschriften kann der Betroffene die Unterlassung einerunzulässigen Erhebung und Übermittlung von Daten verlangen. Eine Unzulässigkeit in diesem Sinne liegt im Streitfall nicht vor.

a) Das Berufungsgericht ist zunächst zutreffend von der grundsätzlichen Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG) ausgegangen. Dessen Anwendungsbereich ist nach § 1 Abs. 2 Nr. 3 BDSG, derjenige seines dritten Abschnitts nach § 27 Abs. 1 Satz 1 Nr. 1 BDSG eröffnet. Denn die Beklagte zu 1 ist als juristische Person des privaten Rechts, die nicht unter § 2 Abs. 1 bis 3 BDSG fällt, gemäß § 2 Abs. 4 Satz 1 BDSG eine nicht-öffentliche Stelle und verarbeitet personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG über die Kläger unter Einsatz von Datenverarbeitungsanlagen (Senatsurteile vom 23. September 2014 – VI ZR 358/13, BGHZ 202, 242 Rn. 12 – Ärztebewertungsportal II; vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 17 f.; siehe auch EuGH, Urteil vom 13. Mai 2014 – Rs. C-131/12, juris Rn. 28 und 33 – Google Spain; ferner Dammann, in: Simitis, BDSG, 8. Aufl., § 3 Rn. 7 ff.; BeckOK DatenSR/Buchner, 21. Ed., 1. Februar 2017, BDSG § 29 Rn. 41 f.; Stehmeier/Schimke, UFITA 2014, 661, 666 f.), hier in Form von Suchprogrammen, sog. crawlern, um die gewonnenen Daten systematisch anhand ihrer Algorithmen zu durchsuchen, zu indexieren und zu speichern. Der Begriff der personenbezogenen Daten umfasst alle Informationen, die über eine Bezugsperson etwas aussagen oder mit ihr in Verbindung zu bringen sind. Das sind nicht nur der Name oder der Geburtsort, sondern auch Meinungsäußerungen, Beurteilungen und Werturteile, die sich auf einen bestimmten oder bestimmbaren Betroffenen beziehen, die Wiedergabe von mündlichen und schriftlichen Aussagen eines Betroffenen und die Darstellung des privaten oder des beruflichen Verhaltens eines Betroffenen (vgl. Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 17; vgl. Gola/Schomerus/Körffer/Gola/Klug, BDSG, 12. Aufl., § 3 Rn. 2 ff.; Dammann, in: Simitis, BDSG, 8. Aufl., § 3 Rn. 7 ff.; Bergmann/Möhrle/Herb, BDSG, 38. Erg., § 3 Rn. 24). Dass die personenbezogenen Daten bereits im Internet veröffentlicht worden sind und von der Suchmaschine der Beklagten zu 1 nicht verändert

werden, ändert daran nichts (vgl. EuGH, Urteil vom 13. Mai 2014 – Rs. C – 131/12, juris Rn. 29 f. – Google Spain).

b) Dem Berufungsgericht ist weiter darin beizupflichten, dass einem entsprechenden Anspruch der Kläger auch das Medienprivileg nach § 57 des Rundfunkstaatsvertrages nicht entgegenstünde. Denn diese Sonderstellung der Medien ist daran gebunden, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten einer pressemäßigen Veröffentlichung dient, die Daten also ausschließlich für eigene journalistisch – redaktionelle oder literarische Zwecke bestimmt sind. Übertragen auf den Bereich der Telemedien kann mithin die reine Übermittlung von erhobenen Daten an Nutzer nicht unter den besonderen Schutz der Presse fallen, weil die bloße automatische Auflistung von redaktionellen Beiträgen noch nicht eine eigene journalistisch-redaktionelle Gestaltung darstellt (vgl. Senatsurteile vom 23. September 2014 – VI ZR 358/13, juris Rn. 13 und vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328). Dies macht auch die Revision nicht geltend.

c) Der Kläger muss sich auch nicht – wie die Revisionserwiderung meint – darauf verweisen lassen, vorrangig die verantwortlichen Betreiber der streitgegenständlichen Internetseiten in Anspruch zu nehmen. Die Haftung des Suchmaschinenbetreibers ist nach der Rechtsprechung des Europäischen Gerichtshofsgerade nicht subsidiär, da ein wirksamer und umfassender Schutz der betroffenen Personen nicht erreicht werden kann, wenn diese vorher oder parallel bei den Herausgebern der Websites die Löschung der sie betreffenden Informationen erwirken müsste (vgl. EuGH, Urteil vom 13. Mai 2014 – Rs. C-131/12, Rn. 82 ff. – Google Spain; vgl. hierzu auch OLG Celle, Urteil vom 1. Juni 2017 – 13 U 178/16, AfP 2017, 444 Rn. 15). Im Übrigen kann die Abwägung im Rahmen des Anspruches aus § 35 Abs. 2 Satz 2 Nr. 1 BDSG gegen den Suchmaschinenbetreiber zu einem anderen Ergebnis führen als im Rahmen des Anspruchs gegen den Herausgeber der Website, da sowohl die berechtigten Interessen, die die Datenverarbeitungen rechtfertigen, unterschiedlich sein können als auch die Folgen, die die Verarbeitungen für die betroffene Person, insbesondere für ihr Privatleben, haben (vgl. EuGH, aaO, Rn. 86).

d) Ein Unterlassungsanspruch der Kläger scheitert jedoch – wie das Berufungsgericht mit Recht angenommen hat – daran, dass die geschäftsmäßige Erhebung der beanstandeten Daten zum Zwecke der Übermittlung nach § 29 Abs. 1 Nr. 2 BDSG und ihre Übermittlung nach § 29 Abs. 2 Satz 1 BDSG zulässig sind.

aa) Nach § 29 Abs. 1 Nr. 2 BDSG ist das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt.

bb) Die Tatsache, dass die Beklagte zu 1 mit ihrer Suchmaschine Werbeeinnahmen generiert, führt – wie bereits der Wortlaut der Vorschrift zeigt – noch nicht dazu, die Datenerhebung als solche als Mittel für die Erfüllung eigener Geschäftszwecke im Sinne von § 28 BDSG zu qualifizieren (vgl. Simitis, BDSG, 8. Aufl., § 28 BDSG Rn. 22). Der Zweck der Datenerhebung als solcher besteht nämlich darin, die im Internet recherchierten Informationen über die Suchmaschine für die Nutzer auffindbar zu machen. Dass die Suchmaschine daneben auch als Werbeplattform dient, ist (erwünschte) Folge, dagegen nicht Zweck der Datenerhebung.

cc) Die Beklagte zu 1 hat die Daten der Kläger – nach den Feststellungen des Berufungsgerichts – aus allgemein zugänglichen Quellen entnommen. Allgemein zugänglich sind solche Quellen, die sich nach ihrer technischen Ausgestaltung und Zielsetzung dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln (vgl. Simitis, BDSG, 8. Aufl., § 28 BDSG Rn. 152). Zu den allgemein zugänglichen Quellen gehören insbesondere auch die für jedermann auffindbaren Inhalte des Internets (vgl. Gola/Schomerus, BDSG, 12. Aufl., § 28 Rn. 33a; Plath, BDSG, 2. Aufl., § 29 Rn. 56; OLG Hamburg, Beschluss vom 13. November 2009 – 7 W 125/09, juris Rn. 3; OLG Celle, Urteil vom 1. Juni 2017 – 13 U 178/16, aaO Rn. 17).

dd) Die Voraussetzung eines Unterlassungsanspruchs der Kläger, dass ihr schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung „offensichtlich" überwiegt und Grund zu der Annahme besteht, dass sie ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben, liegt nicht vor.

(1) Für das Vorliegen eines „schutzwürdigen Interesses" der Kläger ist eine Abwägung zwischen dem Schutz ihres Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK, Art. 7, Art. 8 EU-Grundrechtecharta auf der einen Seite und dem Recht der Beklagten und der Nutzer ihrer Suchmaschine auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG, Art. 10 Abs. 1 EMRK, Art. 11 EU-Grundrechtecharta auf der anderen unter Berücksichtigung der mittelbaren Drittwirkung von Grundrechten (vgl. Senatsurteile vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328; vom 23. September 2014 – VI ZR 358/13, BGHZ 202, 242 Rn. 12 – Ärztebewertungsportal II und vom 20. Februar 2018 – VI ZR 30/17 zV in BGHZ bestimmt, jeweils mwN) erforderlich.

(2) Bei der danach gebotenen Abwägung der grundrechtlich geschützten Positionen der Kläger einerseits, der Beklagten zu 1 und ihrer Nutzer andererseits greifen die oben – zur Frage des Unterlassungsanspruchs gemäß § 823 Abs. 1, § 1004 BGB analog, Art. 1 Abs. 1 iVm Art. 2 Abs. 1 GG – angestellten Überlegungen entsprechend Platz. Unter Berücksichtigung der Arbeitsweise und der besonderen Bedeutung der Suchmaschine für die Nutzbarmachung des Internets (vgl. oben unter III. 1. b) cc) (1)) erfordert das Überwiegen eines schutzwürdigen Interesses der Kläger mithin auch hier einen hinreichend konkreten Hinweis, der dem Suchmaschinenbetreiber eine offensichtliche und bereits auf den ersten Blick klar erkennbare Rechtsverletzung aufzeigt. Dies ist im Streitfall – wie oben bereits ausgeführt – nicht der Fall. Darüber hinaus wurden die beanstandeten Suchergebnisse nicht schon bei schlichter Eingabe der Namen der Kläger angezeigt (vgl. EuGH, Urteil vom 13. Mai 2014 – Rs. C-131/12, juris – Google Spain). Dies macht selbst die Revision nicht geltend. Voraussetzung für ihr Auffinden war vielmehr, dass bei der Suche bestimmte Suchphrasen und -kombinationen verwendet wurden, der Nutzer also bereits Vorkenntnisse von der Verbindung der Kläger mit dem F-Internetforum oder bestimmten, diesem nahestehenden Personen haben musste.

3. Ohne Erfolg wendet sich die Revision auch gegen die Beurteilung des Berufungsgerichts, dass den Klägern gegenüber der Beklagten zu 1 kein Anspruch auf Einrichtung eines Suchfilters zustehe, der die Suchergebnisse automatisch nach bestimmten, im Antrag wiedergegebenen Begriffskombinationen absucht und übereinstimmende Ergebnisse unterdrückt. Dabei kann wiederum dahinstehen, ob und inwieweit ein solcher Anspruch bei Persönlichkeitsrechtsverletzungen überhaupt in Be-

tracht kommt (zum Markenrecht vgl. BGH, Urteile vom 19. April 2007 – I ZR 35/04, BGHZ 172, 119 Rn. 47 – Internet – Versteigerungen II – und vom 30. April 2008 – I ZR 73/05, NJW – RR 2008, 1136 Rn. 53 – Internet – Versteigerungen III; vgl. auch EuGH, Urteile vom 24. November 2011, Rs. C-70/10, juris Rn. 35 – Scarlet Extended und vom 16. Februar 2012, Rs. C-360/10, juris Rn. 26 ff., 52 – SABAM). Denn jedenfalls müsste die Beklagte zu 1 als mittelbare Störerin erst tätig werden, wenn sie durch einen konkreten Hinweis auf eine offensichtliche und auf den ersten Blick klar erkennbare Rechtsverletzung von dieser Kenntnis erlangt hätte. Dies war nach den obigen Ausführungen nicht der Fall. Deshalb muss auch der von den Klägern diesbezüglich hilfsweise gestellte Feststellungsantrag zu 13 – wie vom Berufungsgericht zutreffend erkannt – erfolglos bleiben.

4. Rechtsfehlerfrei ist weiterhin die Beurteilung des Berufungsgerichts, dass den Klägern gegenüber der Beklagten zu 1 kein Anspruch auf Auskunft über die Identität der Verfasser beanstandeter Äußerungen zustehe.

a) Auf den allgemeinen Auskunftsanspruch nach § 242 BGB, wonach ein Anspruch auf Auskunftserteilung nach Treu und Glauben grundsätzlich in jedem Rechtsverhältnis besteht, in dem der Berechtigte in entschuldbarer Weise über Bestehen und Umfang seines Rechtes im Ungewissen und der Verpflichtete unschwer zur Auskunftserteilung in der Lage ist (BGH, Urteil vom 17. Mai 2001 – I ZR 291/98, BGHZ 148, 26 Rn. 29 – Entfernung der Herstellungsnummer II), können sich die Kläger nicht berufen. Das hierzu erforderliche Schuldverhältnis zwischen den Parteien besteht nicht, auch nicht in Form von Pflichten des mittelbaren Störers (vgl. OLG Dresden, Beschluss vom 8. Februar 2012 – 4 U 1850/11, juris Rn. 11), denn eine die mittelbare Störerstellung begründende Pflichtverletzung der Beklagten zu 1 liegt nach den rechtsfehlerfreien Feststellungen des Berufungsgerichts nicht vor.

b) Darüber hinaus zeigt die Revision keinen übergangenen Sachvortrag der Kläger auf, dass der Beklagten zu 1 die Auskunftserteilung unschwer möglich wäre. Die Beklagte zu 1 unterhält als Suchmaschinenbetreiberin – anders als ein Hostprovider – regelmäßig keine geschäftlichen Beziehungen zu den Verfassern der angegriffenen Textpassagen, aufgrund derer ihr deren Identität bekannt oder ohne weiteres ermittelbar wäre.

5. Schließlich hat das Berufungsgericht mit Recht einen Anspruch auf Zahlung einer Geldentschädigung verneint.

Ein Schadensersatzanspruch käme grundsätzlich nur in Betracht, wenn die Beklagte zu 1 als unmittelbare oder als mittelbare Störerin haften würde (vgl. BGH, Urteile vom 17. August 2011 – I ZR 57/09, BGHZ 191, 19 Rn. 47 – Stiftparfüm; vom 11. März 2004 – I ZR 304/01, BGHZ 158, 236, 253 – Internetversteigerung I). Dies ist – wie oben ausgeführt – nicht der Fall.

6. Rechtsfehlerfrei ist letztlich auch die Beurteilung des Berufungsgerichts, dass der Beklagten zu 2 die Passivlegitimation fehlt, weil sie selbst nicht Betreiberin einer Suchmaschine ist.

a) Zwar kann nach der Rechtsprechung des erkennenden Senats – wie die Revision im Ausgangspunkt zutreffend annimmt – als Störer jeder haften, der in irgendeiner Weise willentlich und adäquat kausal an der Herbeiführung einer rechtswidrigen Beeinträchtigung mitgewirkt hat (Senatsurteil vom 14. Mai 2013 – VI ZR 269/12, BGHZ 197, 213 Rn. 24 mwN – Autocomplete). Voraussetzung hierfür ist jedoch, dass der in Anspruch Genommene die rechtliche und tatsächliche Möglichkeit zur Verhinderung dieser Handlung hatte (vgl. Senatsurteile vom 28. Juli 2015 – VI ZR 340/14, AfP 2015, 425 Rn. 34 und vom 1. März 2016 – VI ZR 34/15, BGHZ 209, 139 Rn. 22). Die Beklagte zu 2 ist nach den Feststellungen des Berufungsgerichts nicht Betreiberin der Suchmaschine, sondern nur eine zum Verkauf von Online-Werbung gegründete Gesellschaft. Eine Möglichkeit der Beklagten zu 2, die Datenerfassung und Ausgestaltung der Suchindizes der Beklagten zu 1 zu beeinflussen, ist nicht festgestellt.

b) Soweit die Revision aus dem Urteil des Gerichtshofs der Europäischen Union in Sachen „Google Spain" (EuGH, Urteil vom 13. Mai 2014, Rs. C-131/12, juris) schlussfolgern will, auch die in einem Mitgliedstaat befindliche Tochtergesellschaft sei im vorliegenden Fall passivlegitimiert, ist dies der Entscheidung nicht zu entnehmen. Der Gerichtshof nimmt in seiner Entscheidung eine Zurechnung der Datenverarbeitung der in den Vereinigten Staaten von Amerikadomizilierten Suchmaschinenbetreiberin zu einer Niederlassung mit Sitz in der Europäischen Union, die für die Vermarktung der Werbung in der länderspezifischen Suchmaschine verantwortlich ist, vor, so dass die Verarbeitung personenbezogener Daten zwar nicht „von" der Niederlassung, so aber doch „im Rahmen der Tätigkeiten" der Niederlassung durchgeführt wird (vgl. Art. 4 Abs. 1 lit.a der Datenschutzrichtlinie). Dies führt zur Eröffnung des Anwendungsbereichs der Datenschutzrichtlinie und ihres umfassenden Schutzes der Grundfreiheiten und Grundrechte natürlicher Personen auch auf Suchmaschinenbetreiber, die – wie im Streitfall die Beklagte zu 1 – außerhalb der Europäischen Union ihren Sitz haben (EuGH, aaO, Rn. 51 ff., 58). Insoweit sind die Tätigkeit des Suchmaschinenbetreibers und die seiner Niederlassung untrennbar miteinander verbunden (EuGH, aaO, Rn. 56). Eine Erstreckung der Haftung auf die Niederlassung (hier: Tochtergesellschaft) geht damit aber nicht einher. Dementsprechend nahmen sowohl der Spanische Oberste Gerichtshof (Tribunal Supremo, Urteil vom 14. März 2016, Az. 964/2016, CRi 2016, 81) als auch das Tribunal de Grande Instance de Paris (Urteil vom 13. Mai 2016, Monsieur X ./. Google France et Google Inc.) an, dass die nationalen, die Suchmaschine nicht selbst betreibenden Niederlassungen in vergleichbaren Fällen nicht passivlegitimiert und die Unterlassungsklagen vielmehr gegen den Suchmaschinenbetreiber selbst zu richten seien. Entsprechendes gilt für den Streitfall.

Nach alledem war die Revision der Kläger zurückzuweisen. Der Senat hatte keine Veranlassung, den Gerichtshof der Europäischen Union gemäß Art. 267 Abs. 1 bis 3 AEUV um eine Vorabentscheidung zu ersuchen. Die im Streitfall maßgeblichen unionsrechtlichen Fragen waren – wie ausgeführt – bereits Gegenstand der Entscheidung des Gerichtshofs vom 13. Mai 2014 (Rs. C-131/12 -Google Spain) und sind damit actes éclairés (vgl. EuGH, Urteil vom 6. Oktober 1982 – C-283/81, Slg. 1982, 3415 Rn. 13 – CILFIT).

Zum Auskunftsanspruch des Betriebsrats über die von der Konzernmutter gewährten Aktienoptionen und Nachzugsaktien (Ls)

(**Bundesarbeitsgericht**, Beschluss vom 20. März 2018 – 1 ABR 15/17 –)

1. Macht ein Betriebsrat im Rahmen des ihm innerbetrieblich nach § 80 Abs. 1 Nr. 1 BetrVg zustehenden

Überwachungsrechts Auskunftsansprüche nach § 80 Abs. 2 S, 1 BetrVG geltend, so hat er darzulegen, für welche Aufgabe die verlangte Auskunft erforderlich ist.

2. Der Betriebsrat hat zur Wahrung der Grundsätze von Recht und Billigkeit im Rahmen des § 75 Abs. 1 BetrVG nicht die Aufgabe bzw. Befugnis, bei diskriminierender Maßnahmen Dritter (hier Einhaltung des Gleichheitssatzes bei der Zuteilung von Aktienoptionen durch die Konzernmutter) gegenüber den Arbeitnehmern Schutzmaßnahmen zu ergreifen, wenn diese bei Durchführung eines zwischen dem Arbeitnehmer und dem Dritten bestehenden Vertragsverhältnisses erfolgen. Die Arbeitnehmer handeln nicht „bei Ausübung ihrer Tätigkeit" für den Arbeitgeber.

(Nicht amtliche Leitsätze)

Unterlassungsanspruch bei Herstellung eines Fotos

(**Oberlandesgericht Dresden**, Urteil vom 10. Juli 2018 – 4 U 381/18 –)

1. Die (behauptete) Herstellung von Fotografien einer Person kann nicht unter Berufung auf §§ 22, 23 KUG abgewehrt werden; eine analoge Anwendung dieser Vorschriften auf die im Vorfeld der Verbreitung stattfindende Herstellung kommt nicht in Betracht.

2. Ein Unterlassungsanspruch kann sich aber aus einer Verletzung des allgemeinen Persönlichkeitsrechts ergeben.

3. Der Verletzte muss allerdings beweisen, dass es tatsächlich zur Herstellung eines Bildnisses gekommen ist; dass der Verletzer durch sein Verhalten einen solchen Eindruck erweckt, reicht für einen Unterlassungsanspruch nicht aus, sofern hierdurch die Grenze zum Stalking nicht überschritten wird.

Aus den Gründen:

1. Der von dem Kläger gegen die Beklagte geltend gemachte Anspruch auf Unterlassung der Anfertigung, Verwendung und Verbreitung von Lichtbildern oder Filmaufnahmen seiner Person und/oder seines Grundstücks ist nicht begründet.

a) Der Unterlassungsanspruch kann nicht auf die Regelungen der §§ 22 ff. KUG gestützt werden, da diese Vorschriften lediglich die Verbreitung und öffentliche Zurschaustellung eines Bildnisses, nicht aber die vom Kläger behauptete Herstellung von Fotografien oder Filmaufnahmen seiner Person betreffen. Eine analoge Anwendung der Vorschriften der §§ 22 ff. KUG auf den Fall der im Vorfeld einer Verbreitung erfolgten Herstellung von Aufnahmen scheidet schon wegen der in § 33 KUG geregelten Strafbewehrung aus (so auch Golla/Herboth, Zivilrechtlicher Bildnisschutz im Vorfeld von Weitergabe und Veröffentlichung, GRUR 2015, 648, 649 m.w.N.).

b) Unterlassungsansprüche folgen auch nicht aus dem Bundesdatenschutzgesetz (BDSG). Abgesehen, dass nach § 6 BDSG nur Löschung der erhobenen Daten begehrt werden kann, scheitern sie bereits daran, dass es sich nach dem Vortrag des Klägers um Aufnahmen handelt, die zu persönlichen bzw. privaten Zwecken gefertigt wurden und nicht für Dritte vorgesehen sind, so dass der Anwendungsbereich des BDSG gem. § 1 Abs. 2 Nr. 3 BDSG nicht eröffnet ist.

c) Der Kläger kann auch nicht mit Erfolg geltend machen, ein Unterlassungsanspruch ergäbe sich aus einer Verletzung seines allgemeinen Persönlichkeitsrechts in seiner Ausprägung als Grundrecht auf informationelle Selbstbestimmung entsprechend §§ 823 Abs. 1 BGB, § 1004 BGB analog. Zwar fällt in den Schutzbereich dieser Norm auch bereits die Anfertigung eines Bildnisses. Der Kläger hat aber den ihm danach obliegenden Beweis nicht führen können, dass die Beklagte anlässlich der Begegnung der Parteien an der Grundstücksgrenze am 14.06.2016 gegen 19:00 Uhr mittels ihres Mobiltelefons von ihm tatsächlich Foto- und oder Filmaufnahmen gefertigt hat. Der vom Landgericht hierzu vernommene Zeuge J. hat lediglich geschildert, dass die Beklagte in einem kurzen Abstand vor dem Kläger stehend ein Handy in „Fotografierstellung" gehalten hat. Er konnte jedoch nicht bestätigen, dass die Beklagte dabei Fotos des Klägers angefertigt oder ihn gefilmt hat. Es bestehen auch keine sonstigen Anhaltspunkte für die Behauptung des Klägers, die Beklagte habe ihn bei dieser Gelegenheit fotografiert oder gefilmt, denn unstreitig hat die Beklagte Aufnahmen des Klägers weder im Bekanntenkreis oder privaten Umfeld der Parteien verbreitet noch in anderer Weise veröffentlicht. Aus diesem Grund ist auch dem Vortrag der Beklagten nicht weiter nachzugehen, sie habe zum fraglichen Zeitpunkt keine Fotografien anfertigen können, da sie keinen Zugriff auf ein Mobiltelefon mit Fotofunktion gehabt habe.

d) Ein den geltend gemachten Unterlassungsanspruch begründenden Eingriff in das allgemeine Persönlichkeitsrecht folgt entgegen der Ansicht des Klägers auch nicht aus dem vom Zeugen J. geschilderten Verhalten der Beklagten, die zumindest den Eindruck erweckt haben soll, den Kläger aus einem geringen Abstand fotografiert zu haben. Ein vorbeugender, hier mangels Nachweises einer früheren Verletzungshandlung nur auf eine Erstbegehungsgefahr gestützter Unterlassungsanspruch setzt voraus, dass ernsthafte und greifbare tatsächlich Anhaltspunkte dafür vorhanden sind, der Anspruchsgegner werde sich in naher Zukunft rechtswidrig verhalten, etwa im Hinblick auf einen eskalierenden Nachbarschaftsstreit oder aufgrund objektiv Verdacht erregender Umstände (vgl. BGH, Urt. v. 16.03.2010, VI ZR 176/09, Rn. 14, – juris; OLG Köln, Urt. v. 30.10.2008, 21 U 22/08, Rn. 3, – juris; LG Berlin, Urt. v. 18.10.2016, 35 O 200/14, Rn. 32 – juris jeweils m.w.N.). Es ist im Streitfall aber nicht ersichtlich, dass eine solche konkrete Verletzungshandlung ernsthaft drohte. Die vom Kläger vorgetragenen Auseinandersetzungen reichen nicht aus, um einen massiv und über eine lange Zeit geführten Nachbarschaftsstreit zu belegen. Mit Ausnahme des vorliegenden Verfahrens gab es bis zum Vorfall vom 14.06.2016 zwischen den Parteien lediglich ein Klageverfahren um die Zulässigkeit einer Grenzbepflanzung. Nach Beendigung dieses Verfahrens stellte der Kläger Strafanzeige wegen des Vorwurfs, der Ehemann der Beklagten habe die streitige Grenzbepflanzung mittels eines Unkrautvernichtungsmittels geschädigt. Dieses Verfahren wurde gem. § 170 StPO eingestellt. Die Parteien haben auch in der mündlichen Verhandlung vor dem Senat am 10.07.2018 bestätigt, dass es außer diesen Verfahren keine weiteren Rechtsstreitigkeiten,

Anfeindungen, verbalen Auseinandersetzungen oder weitere Eskalationen zwischen ihnen gegeben habe. Auch unter Berücksichtigung des Umstands, dass es einen weiteren Streit ebenfalls um eine Grenzbepflanzung zwischen der Beklagten und deren Ehemann und dem Vater des Klägers, dem Zeugen J. gibt, der Eigentümer eines weiteren Nachbargrundstücks ist, gehen die geschilderten Streitigkeiten somit in keinem Fall über das hinaus, was als übliche Zwistigkeiten unter Grundstücksnachbarn anzusehen ist. Auch durch den Vorfall vom 14.06.2016 selbst lässt sich die drohende Gefahr weiterer Rechtsverletzungen nicht begründen. Zum einen hat der Kläger in der fraglichen Situation bzw. unmittelbar danach der Beklagten weder mitgeteilt noch sonst wie zu erkennen gegeben, dass er das Verhalten der Beklagten missbilligen und sich dadurch belästigt fühlen würde. Zum anderen hat die Beklagte auf die mittels anwaltlichen Schreibens vom 16.06.2016 gestellte Forderung des Klägers, Foto- und Filmaufnahmen von ihm zu unterlassen, sofort reagiert und mit Schreiben vom 24.06.2016 mitteilen lassen, sie könne bereits den geschilderten Sachverhalt nicht bestätigen, habe aber kein Interesse an Bildern oder Filmaufnahmen des Klägers und bestätige, auch künftig keine solche fertigen zu wollen. Auch aus diesem Grund besteht kein Anlass für die Befürchtung des Klägers, seitens der Beklagten würden dennoch weitere konkrete Verletzungshandlungen unmittelbar bevorstehen.

e) Auch soweit der Kläger einen Unterlassungsanspruch damit begründen will, die Beklagte habe den Kläger durch den Anschein, ihn zu fotografieren zumindest schikanieren wollen, liegen die Voraussetzungen gem. § 823 Abs. 2, § 1004, i.V.m. § 238 StGB nicht vor. Ein Verhalten, mit dem vorgegeben wird, den Betroffenen zu fotografieren, kann zwar unter Umständen eine Störung bzw. Belästigung darstellen. Da es sich anders als beim Nachstellen gem. § 238 StGB bzw. Stalking hier aber um einen einmaligen Vorgang von sehr kurzer Dauer gehandelt hat, der für sich genommen keine schwerwiegende Beeinträchtigung darstellt, ist das allgemeine Persönlichkeitsrecht des Betroffenen noch nicht verletzt (zur Abgrenzung: OLG Köln, Urteil vom 20. Juli 2010 – 3 U 94/09 –, juris). Schon gar nicht liegt in dem Verhalten der Beklagten ein schwerwiegender Verstoß gegen das nachbarschaftsrechtliche Rücksichtnahmegebot.

2. Die Beklagte hat jedoch keinen Anspruch auf die mit der Widerklage geltend gemachten Kosten der vorgerichtlichen Rechtsverteidigung, so dass die Berufung insoweit ohne Erfolg bleibt. Auch wenn der materiell-rechtliche Kostenerstattungsanspruch durch die Regelungen der §§ 91 ff. ZPO nicht von vornherein ausgeschlossen wird, müssen die Voraussetzungen einer materiell-rechtlichen Anspruchsgrundlage erfüllt sein (BGHZ 45, 251, 256 f.; 52, 393, 396; eingehend Hösl, Kostenerstattung bei außerprozessualer Verteidigung gegen unberechtigte Rechtsverfolgung, 2004, S. 13 ff.). Wird jemand unberechtigt als angeblicher Schuldner mit einer Forderung konfrontiert und entstehen ihm bei der Abwehr dieser Forderung Kosten, dann kommen als Anspruchsgrundlage für einen Ersatzanspruch regelmäßig vertragliche Pflichtverletzungen gemäß §§ 280, 311 BGB oder deliktischen Vorschriften gem. §§ 823, 826 BGB in Betracht (Bork, in: Stein/Jonas, ZPO, 22. Aufl., vor § 91 Rdnr. 18; Zöller/Herget, ZPO, 31. Aufl., vor § 91 Rdnr. 11), möglicherweise auch Geschäftsführung ohne Auftrag gem. §§ 677 ff. BGB. Die Voraussetzungen dieser Anspruchsgrundlagen liegen hier jedoch nicht vor. Zwischen den Parteien besteht weder eine vertragliche Beziehung noch sonst eine Sonderverbindung. Allein durch die Geltendmachung eines Anspruchs, der tatsächlich nicht besteht oder nicht weiter verfolgt wird, entsteht eine solche Sonderverbindung nicht (BGH, VersR 1996, 1113, 1114; NJW 1988, 2032). Der Kläger verletzt mit der Forderung nach Unterlassung auch nicht § 823 Abs. 1 BGB, weil er in keines der dort genannten Rechtsgüter eingegriffen und die Beklagte allenfalls einen reinen Vermögensschaden erlitten hat (vgl. Brandenburgisches Oberlandesgericht, Urteil vom 11. April 2016 – 1 U 13/15 –, juris und Hösl, a.a.O., S. 114 ff., S. 164). Mit unberechtigten Ansprüchen konfrontiert zu werden, gehört zum allgemeinen Lebensrisiko.

DS-GVO und Bildberichterstattung – Das Kunsturhebergesetz (KUG) findet auch unter Geltung der DS-GVO Anwendung

(**Oberlandesgericht Köln,** Beschluss vom 18. Juni 2018 – 15 W 27/18 –)

1. **Das Kunsturhebergesetz (KUG) findet auch nach Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) zumindest bei journalistischer Bildveröffentlichung gemäß Art. 85 DS-GVO weiterhin Anwendung.**
2. **Artikel 85 DS-GVO erlaubt nationale Gesetze mit Abweichungen von der DS-GVO zugunsten der Verarbeitung zu journalistischen Zwecken. Davon sind nicht nur neue Gesetze erfasst, sondern auch bestehende Regelungen.**
3. **Art 85 Abs. 2 DS-GVO (Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit) macht im Kern keine materiell-rechtlichen Vorgaben, sondern stellt nur auf die Erforderlichkeit zur Herbeiführung der praktischen Konkordanz zwischen Datenschutz einerseits und Äußerungs- und Kommunikationsfreiheit andererseits ab. Da Datenschutzregelungen als Vorfeldschutz letztlich immer die journalistische Arbeit beeinträchtigen, sind hier keine strengen Maßstäbe anzulegen.**
4. **Die umfangreichen Abwägungsmöglichkeiten im Rahmen des KUG erlauben dann auch eine – künftig gebotene – Berücksichtigung auch der unionsrechtlichen Grundrechtspositionen. Erwägungsgrund 153 der DS-GVO bedingt eine – national im Zuge des § 823 Abs. 1 BGB als Rahmenrecht bzw. bei §§ 22, 23 KUG ohnehin erfolgende – umfassende Abwägung der widerstreitenden Grundrechtspositionen. Entsprechend Erwägungsgrund 4 Satz 3 hat Art. 85 DS-GVO gerade den Normzweck, einen Verstoß der DS-GVO gegen die Meinung- und Medienfreiheit zu vermeiden und entsprechende Komplikationen auszuschließen.**

(Nicht amtliche Leitsätze)

Aus den Gründen:

Der Senat geht allerdings nach eigener Überprüfung aufgrund der – lückenhaften – Aktenlage derzeit davon aus, dass das Landgericht die Vorschriften des KUG zutreffend angewandt hat und dass dem Antragsteller gegen den Antragsgegner kein Unterlassungsanspruch gemäß §§ 1004 Abs. 1 S. 2, 823 Abs. 2 BGB i.V.m. § 22 KUG zusteht, da Bildnisse der Zeitgeschichte im Sinne von § 23 Abs.1 Nr. 1 KUG in Rede stehen. Das Landgericht hat hierzu unter zutreffender Anwendung der maßgeblichen höchstrichterlichen Grundsätze richtig ausgeführt. Hierauf wird zwecks Vermeidung unnötiger Wiederholung mit folgender Ergänzung verwiesen: Soweit mit dem Antrag des Antragstellers formuliert ist, es zu unterlassen, das Bildnis des Antragstellers „weiterhin kenntlich zur Schau zu stellen", so umfasst dies – als Minus – auch eine etwaige Verpixelung, auf die gegebenenfalls in Hinblick auf § 938 Abs. 1 ZPO erkannt werden könnte. Ob allerdings eine solche Verpixelung bei Würdigung der Gesamtumstände zur Wahrung der Interessen des Antragstellers im Sinne des § 23 Abs. 2 KUG erforderlich ist, ist von Antragstellerseite ebenfalls nicht glaubhaft gemacht. Denn hierfür wäre – da auch in diesem Zusammenhang auf den Gesamtkontext abzuheben ist – eine Darstellung des gesamten Beitrages nötig gewesen.

Soweit der Antragsteller sich mit der Beschwerdebegründung auf die Datenschutzgrundverordnung (DS-GVO) beruft, geht dies fehl.

Artikel 85 DS-GVO erlaubt wie die Vorgängerregelung in Art 9 der Richtlinie RL 95/46/EG nationale Gesetze mit Abweichungen von der DS-GVO zugunsten der Verarbeitung zu journalistischen Zwecken. Er enthält damit eine Öffnungsklausel, die nicht nur neue Gesetze erlaubt, sondern auch bestehende Regelungen – soweit sie sich einfügen – erfassen kann. Dies zeigt sich auch daran, dass für den Bereich des Art. 85 DS-GVO nur die Frage der nachträglichen Notifizierungspflicht strittig ist (Gierschmann u.a/Schulz/Heilmann, DS-GVO, Art. 85 Rn. 66).

Insgesamt verkennt der Antragsteller, dass die Tätigkeit des Antragsgegners durch den gerade mit Blick auf Art. 85 DS-GVO durch das 16. RundfunkänderungsG vom 8.5.2018 (GV. NRW. S. 214) neu gefassten § 48 WDR-Gesetz (vgl. auch § 46 LMG und § 12 LPresseG) geregelt worden ist, wonach sich die Verarbeitung personenbezogener Daten zu journalistischen Zwecken durch den Antragsgegner nach Maßgabe der §§ 9c und 57 des Rundfunkstaatsvertrages in der jeweils geltenden Fassung bestimmt. Diese normieren – ebenfalls mit Blick auf Art 85 DS-GVO gerade neu gefasst – in §§ 9c, 57 RStV dann das früher in § 41 BDSG a.F. enthaltene sog. „Medienprivileg". Nach den Regelungen gelten außer den Kapiteln I, VIII, X und XI der DS-GVO nur Artikel 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Artikel 24 und Artikel 32 DS-GVO und damit nicht die Regelungen, auf die der Antragsteller sich hier beruft.

Aus Sicht des Senates bestehen hiergegen keine europarechtlichen Bedenken. Art 85 Abs. 2 DS-GVO macht im Kern keine materiell-rechtlichen Vorgaben (Auernhammer/von Lewinski, DS-GVO, 5. Aufl. 2017, Art. 85 Rn. 13; Gierschmann u.a/Schulz/Heilmann, DS-GVO, Art. 85 Rn. 3, 34, 67, 72 ff.), sondern stellt nur auf die Erforderlichkeit zur Herbeiführung der praktischen Konkordanz zwischen Datenschutz einerseits und Äußerungs- und Kommunikationsfreiheit andererseits ab. Da Datenschutzregelungen als Vorfeldschutz letztlich immer die journalistische Arbeit beeinträchtigen, sind daher hier keine strengen Maßstäbe anzulegen (Auernhammer/von Lewinski, DS-GVO, 5. Aufl. 2017, Art. 85 Rn. 13; Gierschmann u.a/Schulz/Heilmann, DS-GVO, Art. 85 Rn. 61). Dies ist auch vor dem Hintergrund zu sehen, dass Art 85 DS-GVO gerade den Normzweck hat, einen sonst zu befürchtenden Verstoß der DS-GVO gegen die Meinungs- und Medienfreiheit zu vermeiden (vgl. etwa Gierschmann u.a/Schulz/Heilmann, DS-GVO, Art. 85 Rn. 1). Der Erwägungsgrund 4 S. 3 der DS-GVO will solche Komplikationen gerade ausschließen.

Mit Blick darauf sind dann Ausführungen des Landgerichts im Nichtabhilfebeschluss zum „Fortgelten" des KUG im journalistischen Bereich und das Berufen auf den zitierten Aufsatz Lauber-Rönsberg/Hartlaub, NJW 2017, 1057 ff. überzeugend. Für das Äußerungsrecht (§ 823 Abs. 1 BGB i.V.m. APR) ist auch bereits thematisiert worden, dass dieses die Abwägungs- und Ausgleichsfunktion zur Herbeiführung praktischer Konkordanz der widerstreitenden Grundrechtspositionen im hiesigen Bereich übernehmen kann (Gierschmann u.a/Schulz/Heilmann, DS-GVO, Art. 85 Rn. 8); für das KUG kann im Bereich der Bildberichterstattung nichts anderes gelten. Die umfangreichen Abwägungsmöglichkeiten im Rahmen des KUG erlauben dann auch – was künftig geboten sein dürfte – eine Berücksichtigung auch der unionsrechtlichen Grundrechtspositionen. Dass sich daraus hier etwas anderes ergeben sollte, ist weder vorgetragen noch ersichtlich. Insbesondere ist dem Senat keine Abweichung zu den – ohnehin in der Abwägung bewusst offen gehaltenen (Überblick bei Ehmann/Selmayr/Schiedermair, DS-GVO 2017, Art 85 Rn. 8 – 15 m.w.N.) – Rspr. des EuGH bzw. des EGMR ersichtlich; auch Erwägungsgrund 153 der DS-GVO wünscht in diesem Bereich nur eine – national im Zuge des § 823 Abs. 1 BGB als Rahmenrecht bzw. bei §§ 22, 23 KUG ohnehin erfolgende – umfassende Abwägung der widerstreitenden Grundrechtspositionen.

Zum Anspruch der Mutter und des Kindes auf Auskunft über Samenspender (Ls)

(**Oberlandesgericht Hamm**, Urteil vom 19. Februar 2018 – 3 U 66/16 –)

1. **Der Anspruch auf die Herausgabe von Behandlungsunterlagen gibt kein Recht auf die Einsicht in eine Kartei mit Samenspendern.**
2. **Ein Arzt ist grundsätzlich nicht verpflichtet, einem Patienten gegenüber die Richtigkeit und Vollständigkeit überreichter Behandlungsunterlagen an Eides statt zu versichern.**
3. **Trägt eine mit „falschem" Sperma, weil nicht vom richtigen Samenspender stammend, durchgeführte heterologe Insemination zu einer körperlich-psychischen Belastung der Mutter bei, kann der Mutter ein Schmerzensgeldanspruch gegen den für die Insemination verantwortlichen Arzt zustehen (vorliegend 7.500,– €).**
4. **Hinsichtlich des Anspruch des Kindes, von dem für die Insemination verantwortlichen Arzt Auskunft über die Identität eines Vaters zu erhalten, besteht kein An-**

lass, in vorliegendem Fall von dem vom BGH aufgestellten Grundsatz abzuweichen, wonach dem Auskunftsrecht des Kindes als Ausfluss des allgemeinen Persönlichkeitsrechtes gem. Art. 2 Abs. 1, 1 Abs. 1 GG der Vorrang gegenüber dem allgemeinen Persönlichkeitsrecht der Spender, denen seitens der Behandler Anonymität zugesichert worden ist, einzuräumen ist.

(Nicht amtliche Leitsätze)

Fristlose Kündigung wegen ausländerfeindlicher Facebook-Veröffentlichung (Ls)

(**Landesarbeitsgericht Sachsen**, Urteil vom 27. Februar 2018 – 1 Sa 515/17 –)

Veröffentlicht ein bei einer Straßenbahn tätiger Arbeitnehmer unter Angabe seines Namens und eines Fotos in Straßenbahnuniform auf einer rechtsradikalen Facebookseite ein Bild mit einer meckernden Ziege mit der Sprechblase „Achmed, ich bin schwanger", so rechtfertigt dies eine fristlose Kündigung durch die im Eigentum der Stadt stehende Straßenbahngesellschaft.

Verarbeitung sensitiver Daten bei Medikamentenvertrieb im Internet (Ls)

(**Landgericht Dessau-Roßlau**, Urteil vom 28. März 2018 – 3 O 29/17 –)

1. **Um dem Erfordernis der Ausdrücklichkeit einer Einwilligung (§ 4a Abs. 3 BDSG) Genüge zu tun, bedarf es einer detaillierten Aufzählung der in § 3 Abs. 9 BDGS augezählten Datenkatgeorien, der Darlegung des Verarbeitungszwecks, sowie der Benennung des konkreten Verarbeitungszwecks.**
2. **Während Apotheker einer Geheimhaltungspflicht unterliegen, trifft dies nicht auf Internet-Handelsplattformen zu, sodas für die Erhebung personenbezogener Gesundheitsdaten während des Bestellvorgangs eine Rechtfertigung auf Basis von § 28 Abs. 7 BDSG ausgeschlossen ist.**

Alles in einem – Datenschutz und IT-Sicherheit

Handbuch Datenschutz und IT-Sicherheit

Herausgegeben von **Dr. Uwe Schläger** und **Jan-Christoph Thode**

2018, XXXVI, 627 Seiten, fester Einband, € (D) 94,–, ISBN 978-3-503-17727-1

Auch als eBook erhältlich

Mit dem 25. Mai 2018 sind **Datenschutz-Grundverordnung (DSGVO) und das neue BDSG** geltendes Recht. So werden neben erweiterten **Informations-, Rechenschafts- bzw. Meldepflichten** u. a. Datenschutz-Folgenabschätzungen oder das Führen eines Verarbeitungsverzeichnisses relevant.

Doch muss auch die Eignung **organisatorischer und technischer Sicherheitsmaßnahmen** regelmäßig nachgewiesen werden. Um (Persönlichkeits-)Rechte zu wahren und kostspielige Bußgelder zu vermeiden.

Hier setzt das neue Handbuch an, das **juristische und IT-sicherheitsrelevante Fragen erstmals konsequent verknüpft**.

Online informieren und bestellen:
www.ESV.info/17727

ESV ERICH SCHMIDT VERLAG

Auf Wissen vertrauen

Erich Schmidt Verlag GmbH & Co. KG
Genthiner Str. 30 G · 10785 Berlin · Tel. (030) 25 00 85-265
Fax (030) 25 00 85-275 · ESV@ESVmedien.de · www.ESV.info

Berichte, Informationen, Sonstiges

Bitkom: Jeder zweite Social-Media-Nutzer kann Werbung von Inhalt nur schwer unterscheiden

Bitkom – Pressemitteilung vom 16.07.2018

Vor allem Jüngere haben Probleme, Werbung in sozialen Netzwerken zu erkennen.

Banner, Werbe-Videos, Pop-Ups und Influencer, die ein Produkt in die Kamera halten: Werbung in sozialen Netzwerken ist allgegenwärtig. Doch viele Social-Media-Nutzer haben mittlerweile Schwierigkeiten, zwischen Werbung und inhaltlichen Beiträgen zu unterscheiden. So sagt knapp jeder zweite Nutzer (48 Prozent), dass er Werbung von Inhalt nur schwer unterscheiden kann. Unter den jüngeren Nutzem im Alter von 14 bis 29 Jahren sind es sogar 56 Prozent, unter den 50- bis 64-Jährigen und bei der Generation 65 Plus dagegen nur jeweils 40 Prozent. Das ist das Ergebnis einer repräsentativen Studie im Auftrag des Digitalverbands Bitkom, bei der 1.212 Internetnutzer ab 14 Jahren befragt wurden, darunter 1.011 Nutzer von sozialen Netzwerken. „Gerade Online-Werbung will unterhalten und ist oft so auf den Nutzer zugeschnitten, dass er von ihr einen konkreten Nutzen hat und sie gar nicht als Werbung wahrnimmt“, sagt Linda van Rennings, Social-Media-Expertin beim Bitkom. „Insbesondere Surfanfänger sollten daher früh über die verschiedenen Werbeformen wie etwa Produktplatzierungen aufgeklärt werden. Hier sind nicht zuletzt auch die Schulen gefragt, Kinder darauf vorzubereiten, Werbung besser einzuordnen.“

Acht von zehn Social-Media-Nutzer (78 Prozent) haben das Gefühl, dass Werbung in sozialen Netzwerken in letzter Zeit zugenommen hat. Allerdings sind auch sechs von zehn Befragten (60 Prozent) der Meinung, dass Werbung in sozialen Netzwerken in Ordnung ist, weil dadurch die Netzwerke kostenlos zur Verfügung stehen. Bei den 14- bis 29-Jährigen sagen das sogar zwei Drittel (66 Prozent). Drei von zehn Befragten (29 Prozent) geben an, dass sie auf Werbung in sozialen Netzwerken nicht verzichten möchten, weil sie dadurch immer wieder Angebote oder Themen entdecken, die sie sonst nicht gefunden hätten. Mehr als ein Drittel der Befragten (35 Prozent) meint außerdem, dass Werbung in sozialen Netzwerken besser zu den eigenen Interessen passt als herkömmliche Online-Werbung.

Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für einen kindgerechten Datenschutz im Umgang mit digitalen Medienangeboten

Empfehlung 1:

Anbieter digitaler Medien und Dienste, die insbesondere auch Minderjährige ansprechen, sind aufgefordert, die Datenschutzbelange dieser Zielgruppe in besonderem Maße zu berücksichtigen.

Empfehlung 2:

Der besonderen Schutzbedürffigkeit Minderjähriger ist durch eine entsprechende Gestattung von Produkten und Dienstleistungen besondere Rechnung zu tragen. Informationspflichten sind kindgerecht verständlich darzustellen.

Empfehlung 3:

Medienanbieter und -dienste, die sich entweder geziert an Minderjährige wenden oder jedenfalls nicht ausschließen können, dass ihr Angebot auch von Kindern und Jugendlichen unter 16 Jahren in Anspruch genommen wird, sind verpflichtet, für eine umfassende Transparenz und Sicherheit der Datenverarbeitung zu sorgen.

Empfehlung 4:

Datenschutzhinweise einschließlich Informationen zu den erforderlichen Einwilligungen sind in einfacher und für Minderjährige leicht verständlicher Sprache abzufassen und an exponierter Stelle zu platzieren.

Empfehlung 5:

Eraehungsberechtigte, Lehrkräfte und alte sonstigen in die Betreuung von Kindern und Jugendlichen eingebundenen gesellschaftfichen Kräfte sind aufgerufen, gerade in Zeiten der durch die Digitalisierung ermöglichten Freiheiten sowohl für den besonderen Wert personenbezogener Infonnationen als auch für das Risiko der hohen Vertetzbarkeit der eigenen Persönlichkeit zu sensibilisieren.

Empfehlung 6:

Insbesondere staatlichen Institutionen obliegt es, Kinder und Jugendliche alteregerecht und umfassend auf die digitale Welt und die datenschutzrechtlichen Risiken vorzubereiten und ihnen Chancen und Risiken einer selbstbewusst-kritischen Teilhabe an den vielfältigen medialen Angeboten zu vermitteln.

Empfehlung 7:

Auf Bundes- und Landesebene sollten Informations- und Aufklärungskampagnen von Verbänden und Institutionen für kindgerechten Datenschutz initiiert und stärker unterstützt werden. Hierzu gehören auch die verschiedenen Initiativen der Landesdatenschutzfbehörden.

Empfehlung 8:

Der Umgang mit digitalen Medien und die Vermittlung entsprechender Kom-

petenzen im Bereich des Datenschutzes sollte fester Bestandteil des schulischen Bildungsangebots sein.

Empfehlung 9:

Eltern sollten durch Informationsinitiativen dabei unterstützt werden, ihren Kindern insbesondere bei der Ersterkundung digitaler Medien die notwendige Hilfestellung auch im Bereich des Datenschutzes zu geben.

Gesetzesentwurf für das 2. DS-AnPUG liegt vor

Mit Stand vom 21. Juni 2017 hat das Bundesministerium des Innern, für Bau und Heimat den Referentenentwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) vorgelegt.

Die mit dem im Referentenentwurf vorgelegten Änderungsvorschläge vorwiegend im bereichsspezifischen Datenschutz sind umfassend, unter anderem aufgeführt werden Anpassungen bei den Begriffsbestimmungen, den Verweisungen, den Rechtsgrundlagen für die Datenverarbeitung und den Betroffenenrechten.

Insgesamt betrifft das Änderungsgesetz 153 Gesetze, betroffen sind zum Beispiel das Antiterrordateigesetz, das Rechtsextremismus-Datei-Gesetz, das Informationsfreiheitsgesetz, das BSI-Gesetz, das De-Mail-Gesetz, das E-Government-Gesetz, das Bundesmeldegesetz, das Gendiagnostikgesetz, das Infektionsschutzgesetz, das Visa-Warndateigesetz, das Bundeszentralregistergesetz, das Strafgesetzbuch, die Abgabenordnung, die Bundeshaushaltsordnung, das Medizinproduktegesetz, das Energiewirtschaftsgesetz, das Messstellenbetriebsgesetz, das Sozialgesetzbuch und das Telekommunikationsgesetz.

Für das aktuelle BDSG sieht der Referentenentwurf Änderungen bei folgenden Normen vor:

- § 4 BDSG – Videoüberwachung öffentlich zugänglicher Räume, (zu einer möglichen Europarechtswidrigkeit des § 4 BDSG wird sich nicht geäußert),
- § 9 BDSG – Zuständigkeit,
- § 16 BDSG – Befugnisse,
- § 22 BDSG – Verarbeitung besonderer Kategorien personenbezogener Daten,
- Neueinführung des § 86 BDSG – Verarbeitung personenbezogener Daten für Zwecke staatlicher Auszeichnungen und Ehrungen.

Der Gesetzesentwurf wurde am 5.9.2018 von der Bundesregierung beschlossen und liegt inzwischen dem Bundesrat vor.

Beschluss der DSK zu Facebook Fanpages

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Düsseldorf, 5. September 2018

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-210/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben.

Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DS-GVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DS-GVO erfüllt werden.

Seit dem Urteil des EuGH sind drei Monate vergangen. Zwar hat Facebook einige Änderungen in seinem Angebot – zum Beispiel bezüglich der Cookies – vorgenommen, doch weiterhin werden auch bei Personen, die keine Facebook-Nutzerinnen und Nutzer sind, Cookies mit Identifikatoren gesetzt, jedenfalls wenn sie über die bloße Startseite einer Fanpage hinaus dort einen Inhalt aufrufen.

Auch werden nach wie vor die Fanpage-Besuche von Betroffenen nach bestimmten, teilweise voreingestellten Kriterien im Rahmen einer sogenannten Insights-Funktion von Facebook ausgewertet und den Betreiberinnen und Betreibern zur Verfügung gestellt.

Der EuGH hat unter anderem hervorgehoben, dass „die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst."

Offizielle Verlautbarungen vonseiten Facebooks, ob und welche Schritte unternommen werden, um einen rechtskonformen Betrieb von Facebook-Fanpages zu ermöglichen, sind bisher ausgeblieben. Eine von Facebook noch im Juni 2018 angekündigte Vereinbarung nach Art. 26 DS-GVO (Gemeinsam für die Verarbeitung Verantwortliche) wurde bislang nicht zur Verfügung gestellt. Die deutschen Datenschutzaufsichtsbehörden wirken daher auf europäischer Ebene auf ein abgestimmtes Vorgehen gegenüber Facebook hin.

Auch Fanpage-Betreiberinnen und Betreiber müssen sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Art. 26 DS-GVO ist der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten wird, rechtswidrig.

Daher fordert die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden. Dazu gehört insbesondere, dass die gemeinsam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellen.

Eine gemeinsame Verantwortlichkeit bedeutet allerdings auch, dass Fanpage-Betreiberinnen und Betreiber (unabhängig davon, ob es sich um öffentliche oder nicht-öffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zudem können Betroffene ihre Rechte aus der DS-GVO bei und gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DS-GVO).

Insbesondere die im Anhang aufgeführten Fragen müssen deshalb sowohl von Facebook als auch und von Fanpage-Betreiberinnen und Betreibern beantwortet werden können.

Literaturhinweise

Silke Jandt/Roland Steidle (Hrsg.), **Datenschutz im Internet, Rechtshandbuch zu DS-GVO und BDSG,** Nomos Verlag, Baden-Baden, 2018, 532 S., 89,- €

Mit dem neuen Datenschutzrecht gelten komplett neue Rechtsgrundlagen auch für die internetspezifischen Datenschutzvorschriften. Jeder Anbieter von Dienstleistungen rund um das Internet, jeder Nutzer des Internet und jeder Rechtsberater, in Unternehmen und Kanzleien, muss das neue Recht kennen, anwenden und in datenschutzkonforme Verfahren und Verträge überführen. Auch für Aufsichtsbehörden und Verbraucherschutzorganisationen bilden die europäische Datenschutz-Grundverordnung, das neue BDSG und der Entwurf der E-Privacy-Verordnung den verbindlichen Maßstab.

Das von Jandt und Steidle herausgegebene, von insgesamt 13 Autoren mitverfasste Handbuch Datenschutz behandelt alle datenschutzrechtlichen Aspekte des neuen Rechts:

- Technische und strukturelle Grundlagen (auch zum „Internet of Things“ und zum Online-Tracking).
- Rechtliche Grundlagen (z.B. Anwendungsvorrang, Abgrenzung zur E-Privacy-VO).
- Zulässigkeit der Verarbeitung von Daten nach neuem Recht.
- Neue Vorgaben zur Einwilligung inkl. Kopplungsverbot.
- Verarbeitung biometrischer Daten.
- Neue Vorgaben der Auftragsdatenverarbeitung inkl. Besonderheiten für Webdienste.
- Pflichten der Verantwortlichen nach neuem Recht, bspw. Informationspflichten, DSFA.
- Internationale Datenverarbeitung.
- Technischer und organisatorischer Datenschutz inkl. privacy by design und privacy by default.
- Rechte der Betroffenen.
- Sanktionen.
- Rechtsschutz für die Betroffenen (Beschwerde, gerichtliche Durchsetzbarkeit/ Schadensersatzansprüche).

Alle praxisrelevanten Themen werden berücksichtigt

Die sektorenspezifische Darstellung nimmt sich aller wichtigen Themen der modernen Verarbeitungspraxis von personenbezogenen Daten rund um das Internet an:

- Zulässigkeitsvorschriften oder Beschränkungen nach der E-Privacy-VO.
- Internetspezifische Datenverarbeitungen:
  Web- und Cloud-Angebote inkl. Online-Marketing | Social Networks | Suchmaschinen | Webanalyse | Office-Tools | Datenverarbeitung zur Netz- und Informationssicherheit | Datenverarbeitung zur Betrugsverhinderung | Kommunikations- und Over the Top Dienste| Messenger | Big Data.

Das Handbuch ist auf die Praxis ausgerichtet, greift aber auch die wissenschaftlichen Diskussionen rund um den Datenschutz im Internet auf und führt sie weiter.

(Schriftleitung)

Gernot Sydow (Hrsg.), **Europäische Datenschutzgrundverordnung,** Handkommentar, Nomos Verlag, Baden-Baden, 2. Aufl. 2018, 1638 S., 128,- €.

Die 2. Auflage des Handkommentars zur Datenschutzgrundverordnung ermöglicht eine gezielte Vorbereitung und Auseinandersetzung mit dem neuen Rechtsrahmen. Die Neuauflage zeigt auf, wo die Praxisprobleme liegen, wann welche Regelungen gelten.

Besonderen Schwerpunkt legt der Kommentar auf die Bereiche:

- Verhältnis der DS-GVO zum neuen BDSG.
- Anwendungsbereich der Datenschutzgrundverordnung.
- Recht auf Vergessenwerden.
- Einwilligungs-Erlaubnisfragen rund um die personenbezogene Datenverarbeitung in und durch Unternehmen.
- Arbeitnehmerdatenschutz.
- Rechtschutzmöglichkeiten.

Die ausführliche Einleitung vermittelt auf einen Blick grundlegendes Orientierungswissen über den neuen Rechtsrahmen und die Abgrenzungsfragen zum neuen BDSG.

Die Beiträge der Kommentierung stammen von 23 Autoren. An Umfang hat der Text gegenüber der Ersten Auflage um rund 200 Seiten zugenommen, was vorrangig durch die Berücksichtigung des neuen BDSG bedingt ist, wobei dessen Normen im Kontext mit den einschlägigen Bestimmungen der DS-GVO abgehandelt werden.

(Schriftleitung)

Paul Voigt/Axel von dem Busche, **EU-Datenschutz-Grundverordnung (DS-GVO),** Springer Verlag, Berlin, 2018, 531 S., 69,99 €

Dieses Praktikerhandbuch enthält in zehn 326 Seiten füllenden Kapiteln Hinweise zur praktischen Umsetzung der EU-Datenschutz-Grundverordnung (DS-GVO) bzw. des BDSG nF sowie eine systematische Analyse der neuen Vorschriften. Es legt den Schwerpunkt auf praktischen Fragestellungen, einschließlich Vorschlägen zur Umsetzung der neuen gesetzlichen Regelungen. Zahlreiche Praxishinweise und Beispiele zum Verständnis der Auswirkungen der neuen Regelungen. Insoweit widmen sich die Autoren unter anderem den organisatorischen und materiellen Datenschutzanforderungen, den Rechten der betroffenen Personen, der Rolle der Aufsichtsbehörden, der Rechtsdurchsetzung und den Bußgeldern nach der Verordnung, sowie nationalen Besonderheiten. Zusätzlich gewährt das Handbuch einen kompakten Überblick zu den Konsequenzen der Neuregelung für ausgewählte Verarbeitungssituationen mit hoher Praxisrelevanz, wie Cloud Computing, Big Data und Internet of Things. Die Darstellung zum Beschäftigtendatenschutz umfasst jedoch nur 6 Seiten. Die den Anhang des Buches ausmachenden rund 200 Seiten enthalten eine Gegenüberstellung der Vorschriften der Verordnung mit den korrespondierenden des BDSG 2018.

(Schriftleitung)

Sebastian Rogge, **Die Zukunft der Netzneutralität im Internet,** Internetrecht und Digitale Gesellschaft (IDG), Band 11, Duncker & Humblodt, Berlin, 2018, 312 S., Print: 94,90 €, Print & E-Book: 113,90 €

Netzneutralität steht für einen unterschiedslosen Datentransport und gewährleistet den diskriminierungsfreien Zugang zum Internet. Um die von den Telekommunikationsnetzbetreibern forcierte Abkehr von diesem Prinzip entbrannte in der EU eine hitzige Debatte. Die Europäische Kommission versuchte, die widerstreitenden Interessen der Marktakteure per Verordnung in Einklang zu bringen. Dies gelang jedoch nur teilweise.

Sebastian Rogge zeigt auf, inwieweit die mit der Netzneutralität verknüpften Ziele bereits vor Erlass der Verordnung europarechtlich adressiert waren und welche Auswirkungen der nun gewählte Regulierungsansatz hat. Die Grundrechtecharta legt dem europäischen Normgeber diverse Schutzpflichten auf. Die Missbrauchsaufsicht steht kartellrechtswidrigen Absprachen und der Marktmacht der Netzbetreiber entgegen. In der Praxis sind diese Instrumente jedoch nicht geeignet, einen umfassenden Schutz zu gewährleisten. Auch die Verordnung schließt die identifizierten Schutzlücken nicht effektiv.

(Redaktion)

Stefan Bucher, **Sachqualität und Veräußerung von Dateien – Der Online-Handel mit E-Books, Musik- und Filmdateien,** Internetrecht und Digitale Gesellschaft (IDG), Band 12, Duncker & Humblodt, Berlin, 2018, 225 S., Print: 69,90 €, Print & E-Book: 83,90 €

Die klassischen Vertriebswege für Literatur-, Musik- oder Filmprodukte in Form gedruckter Bücher, CDs bzw. DVDs oder Blu-Rays werden mittlerweile zunehmend durch den Download von E-Books, Musik- oder Filmdateien über das Internet verdrängt. Vor diesem Hintergrund untersucht die Arbeit die sachenrechtliche Dimension des Online-Handels mit elektronischen Medien. Zunächst wird die Rechtsnatur von E-Books, Musik- und Filmdateien untersucht, und dabei insbesondere deren Sachqualität im Sinne von § 90 BGB nachgegangen. Die Arbeit widmet sich sodann der Frage, ob sich der Download von Dateien unter die Übereignungstatbestände der §§ 929 ff. BGB einordnen lässt. Dabei werden relevante Aspekte des Urheber-, Erb-, Kreditsicherungs- und Zwangsvollstreckungsrechts in die Betrachtung einbezogen. Der Autor entwickelt ein neues Konzept des Sachbegriffs und der Übergabe, das erlaubt, den Online-Handel mit Mediendateien mit dem herkömmlichen Instrumentarium des BGB zu bewältigen.

(Redaktion)

Mannheim ist Lebensfreude, Wirtschaftskraft und Inspiration: Es pulsiert, es wächst, es lockt und es begeistert. Doch die Quadratestadt überzeugt auch als innovative Arbeitgeberin auf ganzer Linie – mit vielseitigen Berufen, die vermeintlich Unvereinbares in Einklang bringen: Offenheit und Zukunftsorientierung treffen hier auf große Jobsicherheit; gesellschaftlich relevante, sinnhafte und abwechslungsreiche Tätigkeiten auf eine ausgewogene Work-Life-Balance. Begleiten Sie uns auf unserem Weg zu einer der modernsten Stadtverwaltungen Deutschlands!

Für das Rechtsamt suchen wir zum nächstmöglichen Zeitpunkt die/den

BEAUFTRAGTE/N FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT

-Entgeltgruppe E 14 TVöD / Besoldungsgruppe A 14 LBesO-
unbefristet mit der regelmäßigen wöchentlichen Arbeitszeit
(zzt. 39/41 Stunden)

IN MANNHEIM² WIRD DIE ZUKUNFT GEMACHT

Ihre Aufgaben

Sie nehmen die gesetzlichen Aufgaben der/des Datenschutzbeauftragten für die Stadt Mannheim und ggf. für weitere Körperschaften wahr. Insbesondere beraten und unterstützen Sie die Verwaltungsspitze und die Dienststellen in allen Fragen mit datenschutzrechtlicher Relevanz. Sie überwachen die Einhaltung der Vorgaben zum Datenschutz. Zur Sicherstellung der gesetzlichen Vorgaben führen Sie Schulungen zum Datenschutz durch. Sie schreiben die gesamtstädtischen Datenschutzregelungen fort; bei Projekten mit datenschutzrelevanten Fragen wirken Sie mit. Zur Gewährleistung von Datensicherheit im IT-Bereich arbeiten Sie mit dem IT-Sicherheitsbeauftragten der Stadt Mannheim zusammen.
Als Informationsfreiheitsbeauftragte/r beraten und koordinieren Sie die Dienststellen, um auf eine rechtmäßige und fristgerechte Bearbeitung von Anträgen nach LIFG, UVwG und anderen Vorschriften über die Informationsfreiheit hinzuwirken. Dabei berücksichtigen Sie neben der Öffentlichkeitswirksamkeit dieser Vorgänge auch entgegenstehende öffentliche und private Belange (z.B. Datenschutz, Schutz geistigen Eigentums, Betriebs- und Geschäftsgeheimnisse) sowie den Bezug zu wirtschaftswissenschaftlichen oder technischen Fragestellungen.
Daneben sind Sie Ansprechpartner/in für die Aufsichtsbehörden in den Bereichen Datenschutz und Informationsfreiheit.

Ihr Profil

Sie sind Volljurist/in und sollten die juristische Ausbildung mit zwei Prädikatsexamina abgeschlossen haben. Neben vertieften Kenntnissen im Datenschutzrecht verfügen Sie idealerweise über eine mehrjährige Berufserfahrung in diesem Bereich.
Mit den besonderen Anforderungen einer Kommunalverwaltung sind Sie vertraut. Verständnis für Fragen der Informations- und Telekommunikationstechnik setzen wir voraus. Wir erwarten eine Persönlichkeit mit einem hohen Maß an analytischem Denkvermögen, hoher kommunikativer Kompetenz und sicherem Auftreten. Entscheidungskraft und überdurchschnittliche Einsatzbereitschaft runden Ihr Profil ab. Vorkenntnisse im Recht der Informationsfreiheit sowie Lehrerfahrung sind willkommen.
Die Stadt Mannheim hat sich auf Leitlinien für Führung, Kommunikation und Zusammenarbeit verpflichtet (nachzulesen im Internet unter www.mannheim.de/leitlinien) und wir erwarten von unseren Mitarbeitern/innen, dass sie diese aktiv leben.
Sie bringen die hierzu erforderliche Befähigung mit.

Unser Angebot

Neben beruflicher Sicherheit und Familienfreundlichkeit, einem attraktiven, vielfältigen Arbeitsumfeld, zuverlässigen Strukturen und einer abwechslungsreichen Tätigkeit, bei der Sie einen wichtigen Beitrag zum Gemeinwohl leisten, bieten wir Ihnen ein gutes Arbeitsklima sowie flexible Arbeitszeiten.

Für Beschäftigte halten wir ein eigenständiges Angebot zur Kinderbetreuung im „Stadtnest²" vor. Die Stadt Mannheim setzt sich für Chancengleichheit ein. Daneben würden wir es begrüßen, wenn Sie Ihren Wohnsitz in Mannheim nehmen würden.

Fachliche Fragen beantwortet Ihnen gerne Frau Braun unter der Rufnummer 0621/293-9446, Personalfragen Frau Holzmann unter der Rufnummer 0621/293-9623.

Wir freuen uns auf Ihre Online-Bewerbung bis spätestens **01.12.2018** über unser Bewerbungsportal auf der Homepage www.mannheim.de/jobs.

Weitere Informationen finden Sie unter:
www.mannheim.de/jobs
ONLINE-BEWERBUNG ERWÜNSCHT

STADT MANNHEIM²

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.

Conrad, Sebastian, **Kann die künstliche Intelligenz den Menschen entschlüsseln?,** DuD 2018, 54
Erörtert wird, welche Folgen die „künstliche Intelligenz" für die Gesellschaft haben kann und wie den möglichen zukünftigen Entwicklungen rechtlich begegnet werden kann.

Gola, Peter/Klug, Christoph, **Die Entwicklung des Datenschutzrechts im 1. Halbjahr 2018**, NJW 2018, 2608
Der Beitrag enthält den halbjährlichen erscheinenden Übersichtsaufsatz über aktuelle Rechtsprechung und Literatur.

Laoutoumai, Sebastian/Hoppe, Adrian, **Setzt die DSGVO das UWG Schachmatt?,** K&R 2018, 533
Der europäische Gesetzgeber hat mit der DSGVO den Versuch gestartet, ein europaweit einheitliches Datenschutzniveau zu schaffen. Ob auch Zivilgerichte über das Recht des unlauteren Wettbewerbs (Wettbewerbsrecht) bei der Auslegung der Normen der DSGVO hinzugezogen werden können, hängt maßgeblich mit der Frage zusammen, ob Verstöße gegen die DSGVO über das Wettbewerbsrecht geahndet werden können. Dieser Frage geht der Beitrag auf den Grund.

Lezzi, Lukas/Oberin, Jutta Sonja, **Gemeinsam Verantwortliche in der konzerninternen Datenverarbeitung,** ZD 2018, 398
Der Beitrag zeigt die nach der DS-GVO bestehenden Möglichkeiten der Kooperation bei der Datenverarbeitung im Konzern in Form der reinen Datenübermittlung, der Auftragsdatenverarbeitung oder der gemeinsamen Verantwortlichkeit nebst den insoweit zu treffenden Vereinbarungen auf. Beispielhaft wird auch der letztgenannte Fall konkret im Themengebiet Human Ressources angesprochen.

Pfrang, Sebastian, **Die „nicht-dateimäßige" Verarbeitung von Beschäftigtendaten,** DuD 2018, 380
Der Autor gibt Erläuterungen zur Anwendung des § 26 Abs. 7 BDSG bei „nicht-dateimäßiger" Verarbeitung von Beschäftigtendaten.

Schrader, Peter/Thoms, Tina/Mahler, Maike, **Auskunft durch den Arbeitnehmer: Was darf er? Was muss er?**, NZA 2018, 965
Dargestellt werden insbesondere im Rahmen von Mitarbeiterbefragungen bestehende Pflichten der Beschäftigten zur Teilnahme und Auskunftserteilung.

Schwarz, Lea-Christina, **Datenschutzrechtliche Zulässigkeit des Pre-Employments Screenings – Rechtliche Grundlagen und Einschränkungen der Bewerberüberprüfung durch Arbeitgeber**, ZD 2018, 358
Vornehmlich im Rahmen von Compliance-Strukturen besteht ein Interesse, Bewerber einer Vorfeldprüfung u.a. im Hinblick auf einschlägige strafrechtliche Verurteilungen in mit Art. 10 DS-GVO vereinbarer Weise zu überprüfen.

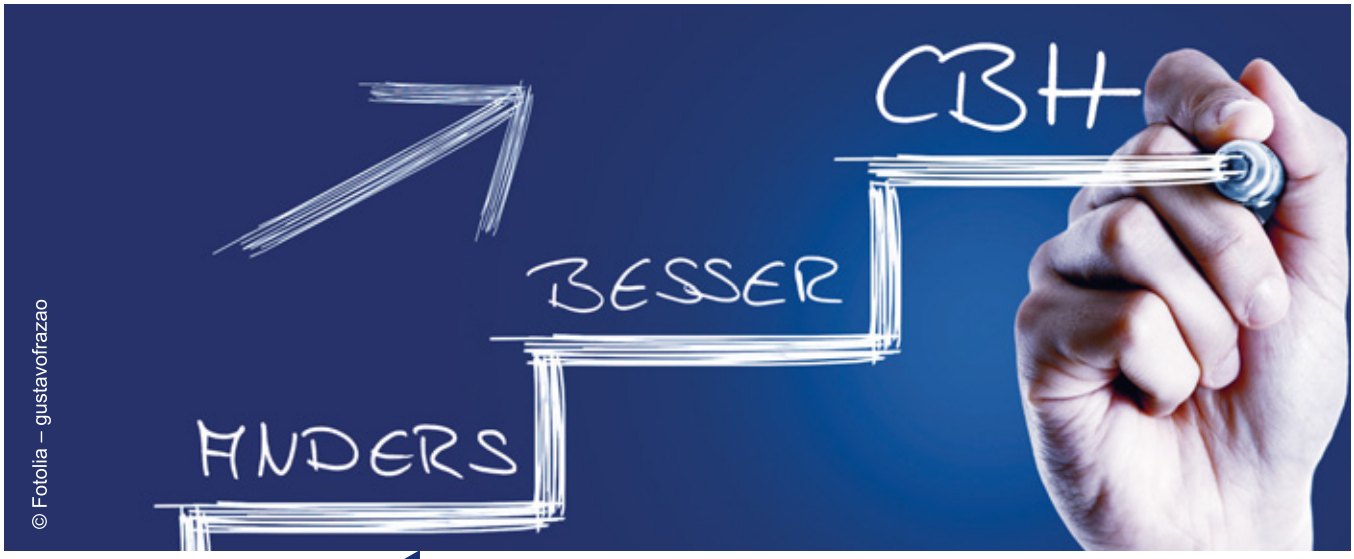
Wojak, Stefanie, **Intelligente Kollektiv-Algorithmen in der Personalverwaltung,** DuD 2018, 553
Auch hinsichtlich der zu erwartenden Weiterentwicklung der Methoden künstlicher Intelligenz fragt die Autorin an Hand von Beispiele nach, ob die Erfüllung unternehmerischer Aufgaben der Personalverwaltung durch die fortschreitende Verwendung autonom agierender Algorithmen beeinflusst werden kann und darf.

Gola, Peter, **Der Beschäftigtendatenschutz in den novellierten Landesdatenschutzgesetzen – Anregungen für den Bundesgesetzgeber?,** ZD 2018, 486
Bis auf Bayern haben alle Bundesländer in ihre zwischenzeitlich DS-GVO-konform novellierten Landesdatenschutzgesetze Bestimmungen zum Beschäftigtendatenschutz aufgenommen bzw. fortgeschrieben, die vom Umfang und der Regelungsmaterie recht unterschiedlich ausgefallen sind. Der Beitrag stellt als Übersichtsaufsatz die Regelungen dar und vergleicht sie mit der Bundesregelung in § 26 BDSG.

Gehen Sie zur Datenschutzimpfung

Wer mit einer Erkältung zum Arzt geht, der möchte in erster Linie seine Bazillen loswerden. Weil man vor der Behandlung aber noch Informationen über die Grippe los wird, muss sich der Arzt erstmal mit dem Datenschutz des Patienten befassen. Das ist keine Schikane, sondern Datenschutzrecht und das tritt neben die Pflichten aus dem Arztvertrag. Unterlässt der Arzt die Dateninfo und schwärzt ihn ein Patient an, dann kann das teuer werden. Dabei geht es in der Regel gar nicht darum, ob der Arzt untersuchen darf. Das muss er ja. Zweck, Umfang und Aufklärung über die Untersuchung ergeben sich schon aus dem Behandlungsvertrag. Das Tückische sind die neuen Zusatzpflichten des Datenschutzes. Patienten müssen über all das, was mit den erhobenen Daten geschieht, informiert werden, und diese Informationen sind zu dokumentieren. Nicht vom Arztvertrag erfasst ist etwa die Abrechnung durch einen privaten Abrechnungsdienst. Ob der Patient alles gelesen hat, muss der Arzt sich wohl nicht unterschreiben lassen. Es dürfte reichen, dass die erfolgte Unterrichtung im Praxiscomputer vermerkt wird.

In der Praxis selbst ist Diskretion angebracht. Ob der Fußpilz bei Herrn Schmitz ähnlich schlimm juckt wie die Hämorriden letztes Jahr, bespricht man besser nicht beim Check In. Datenschutzfreundlich zu sein, bedeutet unpersönlich zu sein. Wer das als Arzt ernst nehmen will, der kann Nummern verteilen. Herr Schmitz, dessen Krankengeschichte das Wartezimmer ja von der Begrüßung kennt, wird zur Nummer 12 und geht in Zimmer drei. Natürlich ist es auch kein Gewinn, wenn man den Fußpilz ohne Namensnennung in Zimmer drei schickt. Zum Glück lässt die Aufsicht hoffen. Aus Bayern heißt es auf die Frage: „Dürfen Patientinnen und Patienten in der Praxis oder am Telefon noch mit dem Familiennamen angesprochen werden oder muss anonymisiert werden?“ offiziell: „Ja, an dieser Praxis sozial- und grundrechtsadäquaten Praxis hat sich auch durch den Erlass der DS-GVO nichts geändert.“ Es lebe der Datenschutz mit Augenmaß und die Datenschutzimpfung. Die gibt es bei der GDD.



© Fotolia – gustavofrazao

CBH
RECHTSANWÄLTE

Datenschutz mit Augenmaß - für Ihren Vorteil im Wettbewerb

CBH ist eine der führenden Wirtschaftskanzleien in Deutschland.

Mit mehr als 90 Rechtsanwältinnen und Rechtsanwälten sind wir an den Standorten Köln, Berlin, Hamburg, München, Stuttgart und Cottbus vertreten.

Wir beraten Sie in unseren strategischen Schwerpunkten Unternehmen und Finanzen, Personal und Sozialwesen, Geistiges Eigentum, Medien und IT, Bau und Immobilien sowie Verwaltung und Wirtschaft.

Im Fachbereich IT decken wir das gesamte Spektrum IT-rechtlicher Angelegenheiten ab und konzentrieren uns unter u.a. auf datenschutzrechtliche Fragen - insbesondere die Auswirkungen der Datenschutzgrundverordnung. Unser Handout zur DSGVO finden Sie unter www.dsgvo-eu.de.

Als Ansprechpartner im datenschutzrechtlichen Bereich stehen Ihnen RA und FA für IT Recht Dr. Sascha Vander, LL.M. (s.vander@cbh.de) sowie RA Niklas Kinting (n.kinting@cbh.de) gerne zur Verfügung.

The LEGAL 500 EMEA LEADING FIRM 2018 · TOP WIRTSCHAFTSKANZLEI 2018 BAURECHT · TOP WIRTSCHAFTSKANZLEI 2018 MARKENRECHT · TOP WIRTSCHAFTSKANZLEI 2018 PATENTRECHT

CBH Rechtsanwälte
Cornelius Bartenbach Haesemann & Partner
Partnerschaft von Rechtsanwälten mbB
Köln | Berlin | Hamburg | München | Stuttgart | Cottbus
Bismarckstraße 11 - 13 | 50672 Köln
Fon +49 221 95190-0 | Fax +49 221 9519095
koeln@cbh.de | www.cbh.de

SecuPedia

Das Portal für Sicherheits-Informationen

Umfassendes und redaktionell geprüftes **Sicherheits-Wissen** und **aktuelle Sicherheitsinformationen** von und für Sicherheits- und IT-Sicherheitsverantwortliche.

Diese Verbände und Unternehmen ermöglichen als Sponsoren die Sicherheitsplattform:

ZVEI Die Elektroindustrie · ASW Landesverband · VdS · BDSW · BDGW · BHE · security essen · itsa · VSW · ASW Norddeutschland

dormakaba · GEUTEBRÜCK · tenable · NTT Security · ESSER by Honeywell · SALTO inspired access · WISAG

DATAKONTEXT

www.secupedia.info