ISSN 0178-8930

G 20 470

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

3/2017

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

Kurzbeiträge

Rechtsprechung

Aus dem Inhalt

33. Jahrgang
Juni 2017
Seiten 109–162

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

GDD-FACHTAGUNG

Fortbildungs-
veranstaltung
gem. § 4f BDSG/
Art. 38 DS-GVO

Datenschutz in Deutschland:

Zusammenwirken von BDSG (neu) und DS-GVO

TERMIN/ORT

12.07.2017 in STUTTGART*

10.00–17.00 Uhr

ZIELGRUPPE

Datenschutzbeauftragte, Datenschutzverantwortliche in Wirtschaft und Verwaltung, Fach- und Führungskräfte im Personalwesen, Mitarbeitervertretungen sowie Betriebsräte

***Weitere Termine:** 30.08.2017 Hannover • 07.09.2017 Berlin • 09.10.2017 München • 18.10.2017 Düsseldorf • 06.11.2017 Hamburg

Sichern Sie sich Ihren fachlichen Vorsprung!

Jetzt informieren und anmelden unter www.datakontext.com

DATAKONTEXT

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT GmbH · Postfach 41 28 · 50217 Frechen · Tel.: 02234/98949-40 · Fax: 02234/98949-44
Internet: www.datakontext.com · E-Mail: tagungen@datakontext.com

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

33. Jahrgang 2017
Heft 3
Seiten 109–162

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Beilagenhinweis GDD-Mitteilungen 3/2017; DATAKONTEXT, Frechen

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

Urheber- und Verlagsrechte:

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

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

Erscheinungsweise
6 x jährlich

Bezugspreis

Jahresabonnement	€ 139,–
Einzelheft	€ 25,–

MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

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

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

Verlag
DATAKONTEXT GmbH, Frechen
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-30
Telefax: (0 22 34) 9 89 49-32
www.datakontext.com
Geschäftsführung: Dr. Karl Ulrich;
Hans-Günter Böse
HRB 337678

Satz
alka mediengestaltung gmbh
Ottostraße 6, 53332 Bornheim-Sechtem

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

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

Zeitschrift für
Datenschutz-, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
33. Jahrgang 2017 Heft 3
Seiten 109–162

RDV
Recht der Datenverarbeitung

33. Jahrgang · Juni 2017 · Seiten 109–162

Editorial

Datenschutz und Sicherheit

Fleißig war er ja, der Bundesgesetzgeber, in den letzten Monaten vor Ablauf der Legislaturperiode bei der Verabschiedung datenschutzrelevanter Gesetze. Dabei ging es nicht nur um den Schutz von Persönlichkeitsrechten; dies gilt im Wesentlichen für die am 27.04.2017 verabschiedete Neufassung des BDSG. Gleichzeitig wurden dem Staat neue Eingriffsbefugnisse eingeräumt.

Nach dem „Gesetz zur Förderung des elektronischen Identitätsnachweises" können nunmehr Verfassungsschutz, der MAD und der BND das Lichtbild des Personalausweises grundsätzlich zur Erfüllung ihrer Aufgaben im automatisierten Verfahren abrufen. Zu diesen Aufgaben gehört nicht nur die Strafverfolgung oder die Abwehr konkreter Gefahren. Polizeibehörden führen Verkehrskontrollen aus und betreiben Videoüberwachungsanlagen.

Zukünftig könnten im Rahmen der „intelligenten Videoüberwachung" alle Menschen identifizieret werden, die sich in einem Bahnhof, auf einem Flughafen, in einem Einkaufszentrum oder auf einem öffentlichen Platz aufhalten. Das am 09.03.2017 verabschiedete „Gesetz zur Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz)" gibt die Grundlage.

Infolge des am 16.05.2017 in Kraft getretenen „Gesetzes zur Verbesserung der Fahndung bei besonderen Gefahrenlagen und zum Schutz von Beamtinnen und Beamten der Bundespolizei durch den Einsatz von mobiler Videotechnik" sollen Bundespolizisten durch die Ausrüstung mit sog. Bodycams besser vor gewalttätigen Übergriffen geschützt werden. Das Gesetz regelt auch den Einsatz von automatischen Kennzeichen-Lesesystemen im Straßenverkehr. Im Gefahrenfall kann die Bundespolizei durch den Einsatz dieser Technik leichter nach Straftätern fahnden.

Europäisches Recht umgesetzt wird mit dem am 27.04.2017 verabschiedeten „Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681(Fluggastdatengesetz – FlugDaG)." Zukünftig werden jährlich Fluggastdaten von etwa 170 Millionen Passagieren unterschiedslos erfasst und über 5 Jahre gespeichert. Der EuGH wird nun entscheiden haben, ob und wie die neu einzurichtenden europäischen Fluggastzentralen personenbezogene Daten verdachtslos analysieren und speichern dürfen.

Am 1. Juli 2017 beginnt für Telekommunikationsanbieter erneut die Pflicht, Verkehrs- und Standortdaten auf Vorrat zu speichern und für Abfragen der Sicherheitsbehörden bereit zu halten. Die weitere Zukunft der Vorratsspeicherung von Daten wird vermutlich erneut vom Bundesverfassungsgericht und dem Europäischen Gerichtshof entschieden. Letzterer hatte bereits angedeutet, dass eine umfassende anlasslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer in Bezug auf alle elektronischen Kommunikationsmittel nicht mit den Vorgaben der Grundrechtecharta vereinbar sei.

Ebenfalls am 27. April 2017 hat der Bundestag das umstrittene Gesetz zur Neustrukturierung des Bundeskriminalamts beschlossen. Rechtsanwälte sind von Überwachungsmaßahmen nunmehr absolut ausgenommen. Dies gilt jedoch nicht für Psychotherapeuten und Ärzte als Berufsgeheimnisträger. Für den Datenschutz gilt jedoch anderes. Nach § 29 BDSG n.F. haben hier die Datenschutzaufsichtsbehörden keine detaillierten Kontrollrechte bei Geheimhaltungsberechtigten mehr.

Prof. Peter Gola

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

Termin	Thema	Ort	Kontakt
07.-09.08.2017	GDD-Sommer-Workshop	Timmendorfer Strand	GDD e.V. und DATAKONTEXT
31.08.2017	IT-SecurityCircles – Retter in der Not!	Köln	GDD e.V. und DATAKONTEXT
04.09.2017	Datenschutz-Schwachstellen und die erheblichen Bußgeld-risiken nach der DS-GVO vermeiden	Köln	GDD e.V. und DATAKONTEXT
05.09.2017	Beschäftigtendatenverarbeitung: Zulässigkeit und Organisation	Köln	GDD e.V. und DATAKONTEXT
05.09.2017	Personalprozesse datenschutzkonform organisieren	Stuttgart	GDD e.V. und DATAKONTEXT
11.-15.09.2017	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Bonn	GDD e.V. und DATAKONTEXT
12.09.2017	IT-Sicherheit für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
19.09.2017	Datenschutz Aktuell	Stuttgart	GDD e.V. und DATAKONTEXT
19.09.2017	Datenschutz bei Unternehmensaktionen	Köln	GDD e.V. und DATAKONTEXT
25.09.2017	ISO 27001 und Datenschutz	Köln	GDD e.V. und DATAKONTEXT
26.09.2017	Einsatz mobiler Endgeräte	Köln	GDD e.V. und DATAKONTEXT
27.09.2017	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Köln	GDD e.V. und DATAKONTEXT
28.09.2017	Big Data-Analysen und der Datenschutz	Köln	GDD e.V. und DATAKONTEXT
09.-10.10.2017	Datenschutz Kompakt	Frankfurt/M.	GDD e.V. und DATAKONTEXT
09.-11.10.2017	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Berlin	GDD e.V. und DATAKONTEXT
16.10.2017	Kundendatenschutz nach der DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
16.10.2017	Grenzüberschreitender Datenverkehr unter neuen Spielregeln	Köln	GDD e.V. und DATAKONTEXT
17.10.2017	Datenschutz und Videoüberwachung – was geht und was geht nicht?	Berlin	GDD e.V. und DATAKONTEXT
25.10.2017	Hacker-Tools für Datenschutzbeauftragte	Berlin	GDD e.V. und DATAKONTEXT
02.11.2017	IT-SecurityCircles – was tun, wenn's brennt oder knallt?	Berlin	GDD e.V. und DATAKONTEXT
06.-07.11.2017	IT-SecurityCircles – sicher durch die Brandung...	Frankfurt/M.	GDD e.V. und DATAKONTEXT
07.-08.11.2017	Datenschutz-Management – Teil 3	Berlin	GDD e.V. und DATAKONTEXT
08.11.2017	Grundlagen der Auftragsverarbeitung (AV)	Köln	GDD e.V. und DATAKONTEXT
13.11.2017	IT-SecurityCircles – Home-Office – sweet Home-Office?	Leipzig	GDD e.V. und DATAKONTEXT
14.11.2017	Prüfung von SAP-Systemen durch Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT

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

Aufsätze

Prof. Peter Gola/Dr. Stephan Pötters

Die Verarbeitung von Beschäftigtendaten im Rahmen betriebsverfassungsrechtlicher Aufgaben nach § 26 Abs. 1 S. 1 BDSG-n.F.

Das Gesetzgebungsverfahren zur Verabschiedung des Datenschutz-Anpassungs- und -Umsetzungsgesetzes, dessen Schwerpunkt eine die DS-GVO ergänzende Neufassung des BDSG ist, abgeschlossen. Der Beschäftigtendatenschutz enthält in § 26 BDSG-n.F. eine bereichsspezifische Regelung, die umfangreicher ausfällt als die jetzige Regelung des § 32 BDSG. Der Beitrag widmet sich den für die Verarbeitung von Beschäftigtendaten für Zwecke der Kollektivvertretungen neuen Zulässigkeitstatbeständen. Diese geben der Beachtung von schutzwürdigen Interessen von Beschäftigten Raum, ohne die berechtigten Informationsansprüche des Betriebs- bzw. Personalrats zu reduzieren.

I. Das neue BDSG auf der Zielgeraden

Am 1.2.2017 wurde vom Bundeskabinett das DS-AnpUG verabschiedet und damit in das Gesetzgebungsverfahren eingebracht.[1] Der Bundestag hat das Gesetz am 27.04.2017 verabschiedet.[2] Der Bundesrat hat die Zustimmung am 12.05.2017 erteilt.

Im Mittelpunkt des Gesetzes steht ein neues BDSG, mit dem die DS-GVO ergänzt und präzisiert werden soll. Enthalten soll das neue BDSG (nachfolgend: BDSG-n.F.) auch eine bereichsspezifische Norm zum Beschäftigtendatenschutz, die sich im Wesentlichen auf die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO stützt. Die vorgesehene Regelung in § 26 BDSG-n.F. wird damit § 32 BDSG als bisherige lex regia des Beschäftigtendatenschutzes ablösen. Sie lautet:

§ 26 BDSG-n.F. Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

1. *Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.*
2. *Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.*
3. *Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen*

1 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU), BR-Drs. 110/17 vom 02.02.2017.

2 BT-Drs. 18/11325.

Person an dem Ausschluss der Verarbeitung überwiegt. Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 22 Absatz 2 gilt entsprechend.

4. *Die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.*
5. *Der Verantwortliche muss geeignete Maßnahmen ergreifen um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.*
6. *Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.*
7. *Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.*

II. Wesentliche Regelungen des neuen § 26 BDSG-n.F.

Mit dieser Norm würde der Regelungsgehalt von § 32 BDSG im Kern unverändert fortgeführt. § 26 Abs. 1 S. 1 BDSG-n.F. erlaubt weiterhin die Verarbeitung von Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses, sofern die Erforderlichkeit gegeben ist. Die Terminologie wurde im Vergleich zu § 32 Abs. 1 S. 1 BDSG leicht geändert und an die DS-GVO angepasst. So ist etwa nur noch von der „Verarbeitung" die Rede, nicht mehr von der „Erhebung", „Verarbeitung" oder „Nutzung". Im Übrigen wird die unnötig komplizierte Sprache der bisherigen Regelung übernommen.[3] Ebenso wird leider auch die wenig gelungene und in der Rechtsprechung[4] zuletzt vermehrt für Unsicherheit sorgende Regelung für Datenverarbeitungen zur Aufklärung eines Straftatverdachts (jeweils Abs. 1 S. 2) beibehalten. Der Gesetzgeber hat die Gelegenheit für eine Klarstellung verpasst, welche Regelung bei der Aufklärung sonstiger schwerwiegender Pflichtverletzungen eingreift. Ebenso wurde die einschränkende Rechtsprechung des BAG zum Anwendungsbereich von § 32 Abs. 1 S. 2 BDSG nicht aufgegriffen. Nach Ansicht der Erfurter Richter ist die Anwendbarkeit dieser Vorschrift aufgrund der erhöhten Anforderungen (Einschränkung des Kreises der Betroffenen[5]; Dokumentationspflicht) nur gerechtfertigt, wenn es sich um eine besonders eingriffsintensive Überwachungsmaßnahme vergleichbar einer Videoüberwachung handelt.[6] So sei etwa die Anhörung des Arbeitnehmers zur Vorbereitung einer Verdachtskündigung keine solche Überwachungsmaßnahme. Sie könne daher nach § 32 Abs. 1 S. 1 BDSG gerechtfertigt werden.

Hinzugetreten ist in § 26 Abs. 1 S. 1 BDSG-n.F. ein zweiter Erlaubnistatbestand, nach dem auch die *„zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten"* erforderlichen Verarbeitungen gestattet werden. Der Gesetzgeber sieht diese Regelung offensichtlich als notwendig an, da er die allgemeinen Informationspflichten des BetrVG nicht als der DS-GVO vorrangige Normen betrachtet. Zugleich dürfte er hiermit beabsichtigt haben, zusammen mit § 26 Abs. 4 BDSG-n.F. eine klarstellende Regelung mit Blick auf die Öffnungsklauseln der DS-GVO zu schaffen.

III. Öffnungsklauseln der DS-GVO mit Relevanz für den Beschäftigtendatenschutz

Die Rechtsetzungsbefugnis des nationalen Gesetzgebers, die grundsätzlich unmittelbar und zwingend geltende DS-GVO um nationale Regelungen zum Beschäftigtendatenschutz zu ergänzen, ergibt sich aus in der Verordnung enthaltenen Öffnungsklauseln, die sowohl Regelungsaufträge als auch in das Ermessen des nationalen Gesetzgebers gestellte Regelungsmöglichkeiten enthalten. Mit Blick auf den Beschäftigtendatenschutz ist vor allem der vom Gesetzgeber in Bezug genommene[7] Art. 88 DS-GVO[8] die einschlägige Regelung, auf die sich nationale Rechtsvorschriften stützen können.

Weitere Öffnungsklauseln mit Relevanz für Beschäftigtendaten sind Art. 9 Abs. 2 lit. b) DS-GVO sowie Art. 9 Abs. 4 DS-GVO für den Umgang mit sensiblen Daten, ferner Art. 6 Abs. 1 lit. c) („rechtliche Verpflichtung") und Art. 6 Abs. 1 lit. e) DS-GVO. Soweit es um Beschäftigungsverhältnisse im öffentlichen Dienst geht, d.h. um die Erledigung der öffent-

3 So etwa die unnötige Wendung „oder nach Begründung des Beschäftigungsverhältnisses", vgl. zum insofern noch besseren Referentenentwurf Thüsing, BB 2016, 2165.

4 S. etwa einerseits LAG Baden-Württemberg v. 20.07.2016 – 4 Sa 61/15, ZD 2017, 88; LAG Hamm v. 17.06.2016 – 16 Sa 1711/15, ZD 2017, 140 (m. Anm. Tiedemann); andererseits BAG v. 22.09.2016 – 2 AZR 848/15, BB 2017, 571 (m. Anm. Glugla); vgl. hierzu Fuhlrott/Schröder, NZA 2017, 278; Wybitul, NZA 2017, 413 (416); Gola/Thüsing/Schmidt, DuD 2017, 244 (247).

5 Es muss ein Verdacht gegen den Betroffenen selbst oder zumindest im Hinblick auf einen „räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern" bestehen, BAG 21.11.2013 – 2 AZR 797/11, NZA 2014, 243; vgl. bereits vor Geltung von § 32 BDSG: BAG v. 21.06.2012 – 2 AZR 153/11, NZA 2012, 1025.

6 BAG v. 12.02.2015 – 6 AZR 845/13, NZA 2015, 741, 747, Rn. 71 ff.; zustimmend Lunk, AP BBiG § 22 Nr. 1; Fuhlrott/Oltmanns, DB 2015, 1719; vgl. auch ErfK/Franzen, BDSG, § 32 Rn. 31; weitere Beispiele aus der Rechtsprechung für Anwendungsfälle des § 32 Abs. 1 S. 2 BDSG sind: Die heimliche Beobachtung durch einen Detektiv zur Krankenkontrolle mit heimlicher Fertigung von Videoaufnahmen (LAG Hamm v. 11.07.2013 – 11 Sa 312/13, ZD 2014, 204), die Spinddurchsuchung (BAG v. 20.06.2013 – 2 AZR 546/12, NZA 2014, 143), die Einsicht in als privat markierte Einträge im elektronischen Kalender des Arbeitnehmers (LAG Rheinland-Pfalz v. 25.11.2014 – 8 Sa 363/14, ZD 2015, 488), die heimliche Installation und Anwendung eines Computerkontrollprogramms zum Zwecke des Nachweises, dass nachträglich durchgeführte Änderungen im elektronischen Arbeitszeitkonto eines Arbeitnehmers von dessen Computer aus durchgeführt worden sind (ArbG Augsburg v. 04.10.2012 – 1 BV 36/12, juris).

7 BR-Drs. 110/17, S. 96: „Die Öffnungsklausel des Artikels 88 der Verordnung (EU) 2016/679 lässt nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext zu. Mit § 26 hat der Gesetzgeber hiervon Gebrauch gemacht."

8 Zur Vereinbarkeit des §26 BDSG-n.F. mit den Anforderungen des Art. 88 DS-GVO vgl. Gola/Thüsing/Schmidt, DuD 2017, 244.

lichen Aufgaben und die dazu ggf. auszuübende öffentliche Gewalt gestattet Art. 6 Abs. 1 lit. e) i.V.m. Abs. 2 DS-GVO den Mitgliedsstaaten spezifischere Regelungen zu erlassen.[9] Der ausdrückliche Einbezug der besonderen Verarbeitungssituationen des Kapitels IX, zu denen auch der Beschäftigtendatenschutz zählt, verdeutlicht die spezielle Regelungskompetenz nicht nur des Bundes, sondern auch der Bundesländer.[10] Hinsichtlich der in § 26 BDSG-n.F. ebenfalls erwähnten Beamten wäre die Bezugnahme auf diese Ermächtigungsnorm korrekt gewesen.

IV. Der Geltungsbereich des § 26 BDSG-n.F.

Erlaubt wird in § 26 BDSG-n.F. die Verarbeitung personenbezogener Daten von betroffenen Personen in ihrer Rolle als „Beschäftigte". Wer zu dem Kreis der besonders geschützten Beschäftigten zählen soll, regelt § 26 Abs. 8 BDSG-n.F., wobei dies die bereits in § 3 Abs. 11 BDSG aufgezählten Personenkreise inklusive der nunmehr auch erwähnten Leiharbeitnehmer sind.

Sodann wird der Anwendungsbereich auf das Vorfeld bzw. auf die Zeit nach Ende des Arbeits- bzw. Beschäftigungsverhältnisses erstreckt, indem Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, genannt werden.

Am Ende der Aufzählung, also nach der Benennung der Bewerber und Ausgeschiedenen folgen wie bislang in § 3 Abs. 11 Nr. 8 BDSG die Beamten, Richter, Soldaten und Zivildienstleistenden. Kaum erkennbar ist der Nutzen, der für Beamte in der Einbeziehung in § 26 BDSG-n.F. bestehen soll, da § 26 BDSG-n.F. ebenso wie das insgesamt subsidiäre BDSG-n.F. gegenüber tatbestandsmäßig spezifischen Rechtsvorschriften des Bundes grundsätzlich zurücktritt (s. § 1 Abs. 2 S. 1 BDSG-n.F.). Nach § 1 Abs. 2 S. 1 BDSG-n.F. kommt § 26 BDSG-n.F. somit für Beamtendaten nicht zum Tragen, soweit das Personalaktenrecht abschließend[11] bereichsspezifisch geregelt ist – dies ist insbesondere bei §§ 106 ff. BBG der Fall.

In sachlicher Hinsicht knüpft § 26 Abs. 7 BDSG-n.F. ebenfalls an die bisherige Regelung des § 32 Abs. 2 BDSG an, indem sämtliche Verarbeitungen personenbezogener Daten erfasst werden. Somit sind abweichend von Art. 2 Abs. 1 DS-GVO nicht allein dateigebundene oder automatisierte Verarbeitungsformen am Beschäftigtendatenschutz zu messen, sondern jedwede Form der Informationsgewinnung.[12] Dies gilt auch für bei der Mitarbeitervertretung stattfindende Verarbeitungen.

V. Datenverarbeitung des Arbeitgebers mit der Zweckbestimmung des § 26 Abs. 1 S. 1 Zulässigkeitsalternative 2 BDSG-n.F.

1. Der Vorrang der Informationsregelungen des BetrVG

Das neue BDSG ist ebenso wie das alte als „Auffanggesetz" konzipiert; es tritt gegenüber spezifischen Rechtsvorschriften des Bundes grundsätzlich zurück (§ 1 Abs. 2 S. 1 BDSG-n.F.). Das bedeutet, dass die Erlaubnisnorm des § 26 Abs. 1 S. 1 BDSG-n.F. mit ihrer Gestattung von Datenverarbeitungen, die zur Erfüllung von Rechten und Pflichten der Interessenvertretungen erforderlich sind, nicht zum Zuge kommt, wenn sich die diesbezügliche Befugnis bzw. Verpflichtung bereits aus dem Betriebsverfassungs- oder Bundespersonalvertretungsgesetz oder auch einer Betriebsvereinbarung ergibt.

Durch § 1 Abs. 2 S. 2 BDSG-n.F. wird jedoch ergänzend klargestellt, dass die jeweilige bereichsspezifische Spezialregelung nur vorrangig ist, wenn eine Tatbestandskongruenz vorliegt. Diese ist im Einzelfall nach den Tatbeständen des jeweiligen bereichsspezifischen Gesetzes zu beurteilen. Eine Norm außerhalb des BDSG rechtfertigt im Übrigen eine Datenverarbeitung nur, wenn sie eine konkrete Aussage bezüglich der Art der Daten und ihrer Zweckbestimmung trifft. Es genügt also nicht, dass lediglich abstrakt eine Aufgabe oder Zuständigkeit beschrieben wird, zu deren Erfüllung ggf. personenbezogene Daten benötigt werden.[13] Inwieweit im Einzelfall die Bestimmungen des BetrVG/BPersVG über Informationspflichten des Arbeitgebers gegenüber der Mitarbeitervertretung Vorrang vor § 26 Abs. 1 S. 1 BDSG-n.F. haben, ist unter diesen Vorgaben zu klären.

Dieser Vorrang kann für Bestimmungen bejaht werden, die sowohl die Art der personenbezogenen Information als auch die Art und Weise des Informationsflusses regeln. Eine solche konkrete, das BDSG verdrängende Bundesvorschrift stellt u.a. § 80 Abs. 2 S. 2 Halbs. 2 BetrVG dar, der dem Betriebsrat ein Recht auf Einsicht in Bruttolohn- und Gehaltslisten gibt.[14] Gewährt werden kann nur die Einsichtnahme. Ein Online-Zugriffsrecht steht dem Betriebsrat nicht zu und kann ihm auch nicht freiwillig eingeräumt werden.[15] Die Erforderlichkeit der Maßnahme ist vorgegeben und eventuelle entgegenstehende Wünsche von einzelnen Beschäftigten sind irrelevant, d.h. Individualrechte haben gegenüber dem kollektivrechtlich begründeten Einsichtsrecht zurückzustehen.

Eine Prüfung des BDSG entfällt in einem solchen Fall nach derzeitigem und zukünftigen Recht – also § 32 BDSG bzw. § 26 BDSG-n.F. – infolge seiner Subsidiarität (§ 1 Abs. 3 S. 1 BDSG; § 1 Abs. 2 S. 1 BDSG-n.F.). Wenn das BAG[16] gleichwohl festhält, dass, wenn der Arbeitgeber einem Betriebsratsmitglied nach § 80 Abs. 2 S. 2 Halbs. 2 BetrVG Einsicht in die Gehaltslisten gewährt, es sich um eine nach § 32 Abs. 1 BDSG zulässige Datennutzung handele, so ist dies eine überflüssige Begründungsschleife, denn auf § 32 Abs. 1 S. 1 BDSG kommt es in diesem Fall nicht an.

9 Maier, DuD 2017, 169.

10 Roßnagel, DuD 2017, 290 (292).

11 Vgl. zum alten BDSG, BVerwG, RDV 2004, 272.

12 S. z.B. BAG v. 20.06.2013 – 2 AZR 546/12, NZA 2014, 143: Spinddurchsuchung durch den Arbeitgeber; vgl. hierzu Becker-Schäufler, BB 2015, 629; Wybitul/Pötters, BB 2014, 437.

13 Vgl. z.B. Kort, RDV 2012, 8 (9); Dix, in: Simitis (Hrsg.), BDSG, § 1 Rn. 170.

14 Vgl. Jordan/Bissels/Löw, BB 2010, 2889 (2891).

15 Generell zum Onlinezugriff zur Erfüllung von Informationspflichten: BAG v. 16.08.2011 – 1 ABR 22/10, ZD 2012, 180 (m. Anm. Tiedemann).

16 BAG v. 14.01.2014 – 1 ABR 54/12, RDV 2014, 277.

Ein weiteres Beispiel einer vorrangigen Regelung gibt § 99 Abs. 1 S. 1 BetrVG, nach dem im Rahmen der Mitbestimmung über eine Einstellung oder Versetzung dem Betriebsrat die Bewerbungsunterlagen aller Interessenten vorzulegen sind, nebst evtl. Schriftstücke, die der Arbeitgeber im Rahmen des Bewerbungsverfahrens über die Bewerber erstellt und bei seiner Auswahlentscheidung berücksichtigt hat.[17]

Keine das BDSG verdrängende Regelung beinhalten jedoch die allgemeinen Informationspflichten des § 80 Abs. 2 S. 1 Halbs. 1 und S. 2 Halbs. 1 BetrVG bzw. § 68 Abs. 2 S. 1 und 2 BPersVG, die nur pauschal zur Weitergabe erforderlicher Informationen zur Wahrnehmung der Aufgaben der Mitarbeitervertretung und zur Vorlage diesbezüglicher Unterlagen verpflichten. Eine Aussage dazu, ob und wann hiervon auch bestimmte personenbezogene Daten erfasst werden und wie die „Vorlage" zu erfolgen hat, ist nicht erkennbar.[18] Inzwischen hat sich auch das BAG[19] von der früher vertretenen Auffassung eines apodiktischen Vorrangs von § 80 Abs. 2 BetrVG verabschiedet, wenn es im Rahmen der Unterrichtungsverpflichtung über die sensiblen Daten des Eingliederungsmanagements § 28 Abs. 6 Nr. 1 BDSG prüft – was sich dogmatisch verbieten würde, wenn BDSG-Normen durch § 80 Abs. 2 BetrVG präkludiert würden.

Aus dem Gesagten ergibt sich auch, dass, da das BPersVG keine ausdrücklichen Regelungen zur Einsichtnahme in Bruttolohn und Gehaltslisten oder zur Vorlage sämtlicher Bewerbungsunterlagen kennt, für diese der Mitarbeitervertretung gleichwohl zugestandenen Informationen[20] künftig § 26 Abs. 1 S. 1 BDSG-n.F. als Erlaubnistatbestand heranzuziehen sein wird.

2. Erforderlichkeit als Maßstab

Kommt mangels vorrangiger Regelung im Betriebsverfassungs- bzw. Bundespersonalvertretungsgesetz oder in einer Betriebsvereinbarung[21] demnächst § 26 Abs. 1 S. 1 BDSG-n.F. zur Anwendung, so muss die Datenverarbeitung, d.h. die Offenlegung von Beschäftigtendaten gegenüber der Mitarbeitervertretung die Kriterien der „Erforderlichkeit" erfüllen. In diesem Merkmal steckt im Ergebnis eine Verhältnismäßigkeitsprüfung. Neben der Geeignetheit der Datenverarbeitung zur Verwirklichung des vom Verantwortlichen verfolgten Zwecks darf es also keine milderen, d.h. das Recht auf Schutz personenbezogener Daten (Art. 8 EU-GRCh) weniger beeinträchtigenden Mittel geben. Schließlich ist eine Abwägung der Rechte und Interessen des Verantwortlichen und der betroffenen Personen im Wege praktischer Konkordanz vorzunehmen.[22]

Mit Blick auf Datenverarbeitungen durch die Interessenvertretungen der Beschäftigten ist demnach zunächst erforderlich, dass die Datenverarbeitung der Erfüllung der Aufgaben der Stelle dient. Bereits an dem Aufgabenbezug fehlt es z.B., wenn der Betriebsrat Auskunft über außerhalb seiner Zuständigkeit erteilte oder beabsichtigte Abmahnungen begehrt.[23]

Zu beachten ist ferner – als Ausprägung der Erforderlichkeit – das Gebot der Datensparsamkeit (derzeit noch § 3a BDSG) bzw. der Datenminimierung nach Art. 5 Abs. 1 lit. c) DS-GVO. Ggf. muss sich die Mitarbeitervertretung jedenfalls im ersten Schritt mit anonymisierten oder pseudonymisierten Angaben zur Erfüllung ihrer Kontrollpflicht nach § 80 Abs. 1 BetrVG begnügen.[24] Insoweit wird die Entscheidung des BVerwG[25], nach der es genügt, dem Personalrat zwecks Überwachung der Einhaltung der Arbeitszeitregelungen zumindest als ersten Schritt die Arbeitszeitdaten in anonymisierter Form zur Verfügung zu stellen, eher der Regelung des § 26 Abs. 1 S. 1 BDSG-n.F. gerecht als die gegenteilige Auffassung des BAG.[26]

Eine personenbezogene Offenlegung von Beschäftigtendaten ist sodann unter dem Aspekt der Verhältnismäßigkeit an eventuell entgegenstehenden Interessen des Betroffenen zu messen. Geht es um von der DS-GVO besonders geschützte sensible Daten des Art. 9 Abs. 1 DS-GVO, so erlaubt § 26 Abs. 3 BDSG-n.F. deren Offenlegung unter der Vorgabe, dass sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht erforderlich ist, wobei entgegenstehenden Interessen des Beschäftigten sogar ausdrücklich Rechnung zu tragen ist. Auch im Rahmen von Abs. 1 ist aber stets eine Interessenabwägung durchzuführen.

„Dabei sind die Interessen des Arbeitgebers – und auch der Mitarbeitervertretung – an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt".[27] Beispielhaft stellt Kort[28] insoweit zutreffend die Entscheidung des LAG Hessen[29] zur Information des Betriebsrats über individuelle Zielvereinbarungen in Frage.

Die bislang vertretene Auffassung, dass das BDSG nicht zur Einschränkung der Rechte führt, die das BetrVG oder das Personalvertretungsrecht der Mitarbeitervertretung gewährt,[30] kann nur noch gelten, sofern man den Begriff der Erforderlichkeit in § 80 Abs. 2 BetrVG/§ 68 Abs. 1 S. 1 und 2 BPersVG und in § 26 Abs. 1 S. 1 BDSG-n.F. einheitlich datenschutzkonform interpretiert.[31] Die Ansicht, der Arbeitgeber sei nicht verpflichtet oder berechtigt, sich gegenüber dem Überwachungsrecht des Betriebsrats auf Interessen und Grundrechte der Arbeitnehmer und speziell deren Recht auf Schutz personenbezogener Daten zu berufen[32], kann in dieser generel-

17 Vgl. zuletzt BAG v. 14.04.2015 – 1 ABR 58/13, NZA 2015, 1081.

18 Vgl. Gola/Schomerus, BDSG, § 4 Rn. 8; Jordan/Bisels/Löw, BB 2010, 1889.

19 BAG v. 07.02.2012 – 1 ABR 46/10, RDV 2012, 192.

20 Vgl. Gräfl, in: Richardi/Dörner/Werber, BPersVG, § 68 Rn. 82 und 86 ff. mit Nachweisen der Rechtsprechung.

21 Hierzu Wybitul/Sörup/Pötters, ZD 2015, 559.

22 S. auch für § 26 BDSG-n.F., Wybitul, NZA 2017, 413 (415).

23 BAG v. 17.09.2013 – 1 ABR 26/12.

24 Vgl. Gola/Pötters, DS-GVO, Art. 5 Rn. 23.

25 BVerwG v. 19.03.2014 – 6 P.1.13, RDV 2014, 212.

26 BAG v. 06.05.2003 – 1 ABR 13/02, RDV 2004, 77.

27 So die Gesetzesbegründung zu § 26 BDSG-n.F., BR-Drs. 110/17, S. 96 zu § 26 Abs. 3.

28 ZD 2017, 3 (5).

29 LAG Hessen v. 24.11.2015 – 16 TABV 106/15, juris.

30 Vgl. z.B. BVerwG v. 23.01.2002 – 6 P 5/01, RDV 2002, 188: „Im Übrigen gilt das an die Voraussetzungen des § 68 Abs. 2 BPersVG, insbesondere an den Maßstab der Erforderlichkeit gebundene Informationsrecht der Personalvertretung als bereichsspezifische Regelung des Dienstrechts".

31 Vgl. auch Wybitul, NZA 2017, 413 (415).

len Aussage keinen Bestand mehr haben. Dem Beschäftigten steht zwar kein Selbstbestimmungsrecht zu, jedoch das Recht, dass seine gegenläufigen Interessen berücksichtigt werden.[33]

Ob entgegenstehende schutzwürdige Interessen der betroffenen Personen bestehen, ist zunächst im Rahmen einer allgemeinen, die Interessen aller betroffenen Mitarbeiter berücksichtigenden Abwägung zu prüfen. Ggf. ist diese aber auch nur in einem Einzelfall gefordert, wenn der Beschäftigte aus Gründen, die sich aus seiner besonderen Situation ergeben, Widerspruch gegen die Verarbeitung einlegt. Art. 21 Abs. 1 S. 1 DS-GVO muss auch hier gelten. Insoweit wird der Auffassung des BVerwG[34], nach der eine schwangere Mitarbeiterin ggf. schutzwürdige Interessen haben kann, dass ihre Schwangerschaft der Mitarbeitervertretung – zunächst – nicht mitgeteilt wird, der Regelung des § 26 Abs. 1 S. 1 BDSG-n.F. nunmehr eher entsprechen als die eine solche den Einzelfall berücksichtigende Interessenabwägung ablehnende Auffassung im Rahmen des BetrVG.[35] Das BAG wird insofern seine Entscheidung[36] zur personenbezogenen Information des Betriebsrats über die für ein Eingliederungsmanagement in Betracht kommenden Beschäftigten zu überdenken haben.[37]

VI. Datenverarbeitungen der Mitarbeitervertretung

Die Erlaubnisnorm des § 26 Abs. 1 S. 1 Alt. 2 BDSG-n.F. hat nicht nur Bedeutung für Verarbeitungen des Arbeitgebers, sondern auch für solche der Mitarbeitervertretung. Auch dort stattfindende Verarbeitungen von Beschäftigtendaten sind gestattet, wenn sie zur Erfüllung von Rechten und Pflichten der Interessenvertretung erforderlich sind. Das gilt unabhängig von der Frage, ob die Mitarbeitervertretung – so wie bisher von der herrschenden Meinung[38] angenommen – Teil des Betriebes oder der Dienstelle ist[39] oder nunmehr doch aufgrund der ihr vom BAG in Interpretation des BetrVG eingeräumten eigenständigen Verantwortlichkeit über die bei ihr stattfindenden Datenverarbeitungen die Funktion eines (Co-)Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO hat.[40]

Unabhängig hiervon erfordert die unter der Regie der Mitarbeitervertretung stattfindende Datenverarbeitung eine Rechtsgrundlage. Auch hier ist also, sofern nicht Spezialvorschriften eingreifen, nach § 26 Abs. 1 S. 1 BDSG-n.F. eine Erforderlichkeitsprüfung vorzunehmen. Somit muss in Zukunft das BetrVG mit den Vorgaben der DS-GVO und des § 26 BDSG-n.F. entgegen der aktuell weit verbreiteten gegenteiligen Auffassung[41] in Einklang stehen.[42]

Maßgebend für die eigenständige Verarbeitung der in der Regel vom Arbeitgeber bereit gestellten Beschäftigtendaten[43] ist der Aufgabenbezug und die ggf. befristete Zweckbestimmung der Information. Eine Verarbeitung von Personaldaten durch die Mitarbeitervertretung kann nur dann und so lange in Betracht kommen, wie Unterlagen dem Betriebs- bzw. Personalrat – zeitweise oder auf Dauer – im Rahmen seiner kollektivrechtlich begründeten Informationsansprüche überlassen werden.

Dürfen Daten, die von der Mitarbeitervertretung zur Wahrnehmung ihrer Beteiligungsrechte immer wieder benötigt werden, ihr in Kopie auf Dauer belassen werden,[44] so können sie auch automatisiert geführt werden. Um ihren Pflichten sachgemäß nachkommen zu können, benötigt die Mitarbeitervertretung z.B. einen Überblick, wen sie vertritt. Nach Auffassung der Aufsichtsbehörden[45] und einiger Landesgesetzgeber[46] gehört hierzu die Kenntnis von Name, Funktion nebst Bewertung, Besoldungs-, Vergütungs- und Lohngruppe, Geburts-, Einstellungs- und letztes Beförderungsdatum, Beurlaubung und Ermäßigung der Arbeitszeit. In welchem Rhythmus diese Aufstellungen aktualisiert werden, müssen die Beteiligten miteinander vereinbaren. Der Datenbestand darf sich jedoch weder von der Quantität noch von der Qualität her derart gestalten, dass die Datei zu einem Personalinformationssystem wird, d.h. einer ganz oder in Teilen automatisiert geführten Personalakte gleichkommt. Dem stehen § 83 Abs. 2 S. 2 BetrVG bzw. § 68 Abs. 2 S. 2 BPersVG entgegen, nach denen die Personalaktenführung allein dem Arbeitgeber/Dienstherrn zusteht und die Einsichtnahme von Mitgliedern der Mitarbeitervertretung an die Zustimmung des Beschäftigten geknüpft ist.[47] Gehen die Datenverarbeitungen durch die Mitarbeitervertretung über das für ihre Aufgaben Erforderliche hinaus, bedürfen sie der Einwilligungen der Beschäftigten.[48]

Die Verpflichtung zur Schaffung geeigneter Garanitien gemäß § 26 Abs. 3 und § 26 Abs. 5 BDSG-n.F. gilt auch für die DV der Mitarbeitervertretung.

32 BAG v. 07.02.2012 – 1 ABR 46/10, RDV 2012, 192; Fitting, BetrVG, § 80 Rn. 61; Buschmann, in: D/K/K/W, BetrVG, § 80 Rn. 76; Düwell, CuA 5/2013, 17.

33 So vom Ergebnis her auch Thüsing, in: Richardi, BetrVG § 80 Rn. 58a, mit Nachweisen positiver und negativer Literatur.

34 BVerwG v. 29.08.1990 – 6 P 30/87, NJW 1991, 373.

35 Vgl. bei Fitting, BetrVG, § 80 Rn. 61.

36 BAG v. 07.02.2012 – 1 ABR 46/10, RDV 2012, 192.

37 Vgl. bereits Taeger, in: Taeger/Gabel (Hrsg.), BDSG, § 4 Rn. 39; Kort, ZD 2016, 3.

38 Zur Rechtsprechung: BAG, Beschlüsse v. 12.08.2009 – 7 ABR 15/08; v. 11.11.1997 – 1 ABR 21/97.

39 Dies ist aber nur der Fall bei „aufgabenbezogener" Tätigkeit, vgl. Kort, NZA2010,1267 (1268).

40 Die Frage offen lässt Wybitul, BB 2017, 181, 184; Gola, in: Gola (Hrsg.), DS-GVO Art. 4 Rn 55.

41 Vgl. z.B. Kort, NZA Beilage 2/2016, 62 (64); aus der Rechtsprechung zuletzt LAG Baden-Württemberg v. 17.01.2017 – 19 TaBV 3/16, Rn. 55: „Das Bundesdatenschutzgesetz steht einer Weitergabe von Informationen an den Betriebsrat nicht entgegen. Das Bundesdatenschutzgesetz verdrängt das Betriebsverfassungsgesetz nicht. Gesetzliche Vorschriftendes § 80 Abs. 1 S. 1 BetrVG, welche die Information des Betriebsrats und damit auch die Weitergabe von personenbezogenen Daten vorschreiben, gehen dem Bundesdatenschutzgesetz vor."

42 Vgl. auch Wybitul, NZA 2017, 413 (415).

43 Zur Befugnis eigener Datenerhebung der Mitarbeitervertretung Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn. 2154 ff.

44 Zum Stellenplan BVerwG v. 23.01.2002 – 6 P 5/01, RDV 2002, 188.

45 22. Tätigkeitsbericht (1993) des Hess. LDSB, Ziff. 23; 17. Tätigkeitsbericht LDSB des Saarlands (1997/98), S. 105 ff.

46 § 65 Abs. 3 LPVG Baden-Württemberg.

47 Vgl. im Einzelnen Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn. 2159 ff.

48 Insofern wirft Kort, NZA 2010, 1267 (1271), zu Recht die Frage auf, ob die Mitarbeitervertretung im Falle nicht-aufgabenbezogener Datenverarbeitung „Dritter" ist.

VII. Fazit

§ 26 Abs. 1 S. 1 BDSG-n.F. enthält einen Erlaubnistatbestand für die im Rahmen der Regelungen des Betriebsverfassungs- bzw. des Bundespersonalvertretungsgesetzes erforderlichen Verarbeitungen von Beschäftigtendaten durch Arbeitgeber und Mitarbeitervertretung. Er gibt der Beachtung von schutzwürdigen Interessen von Beschäftigten Raum, ohne die berechtigten Informationsansprüche des Betriebs- bzw. Personalrats zu reduzieren.

Daneben können spezifische Erlaubnistatbestände des Betriebsverfassungsrechts Datenverarbeitungen rechtfertigen. Solche Regelungen sind wie bislang nach dem geltenden BDSG vorrangig gegenüber den allgemeinen Vorschriften des BDSG. Dieser Vorrang kann jedoch nur für Bestimmungen bejaht werden, die sowohl die Art der personenbezogenen Information als auch die Art und Weise des Informationsflusses regeln. Beispiele hierfür sind § 80 Abs. 2 S. 2 Halbs. 2 BetrVG und § 99 Abs. 1 S. 1 BetrVG.

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

Dr. Stephan Pötters
Dr. Stephan Pötters ist Rechtsanwalt bei Seitz Rechtsanwälte Steuerberater in Köln. Schwerpunkte seiner Beratung sind das Arbeits- und Datenschutzrecht.

Prof. Gregor Thüsing/Dr. Maximilian Schmidt/Dr. Gerrit Forst

Das Schriftformerfordernis der Einwilligung nach § 4a BDSG im Pendelblick zu Art. 7 DS-GVO

Die Einwilligung ist und bleibt wichtiges Instrument des Datenschutzrechts – ihre wirksame Erteilung vorausgesetzt, vermag sie rechtssicher Datenverarbeitungen zu legitimieren. Mit Geltung der DS-GVO werden sich die Voraussetzungen der Einwilligung aber wesentlich verändern. Dieser Beitrag soll aufzeigen, warum die Schriftlichkeit künftig zu Recht nicht mehr konstitutive Bedingung einer wirksamen Erteilung nach Art. 7 Abs. 1 DS-GVO sein wird.

I. Die Schriftlichkeit der Einwilligung zwischen BDSG und DS-GVO

Die Einwilligung ist als originärer Ausdruck informationeller Selbstbestimmung wesentliches Instrument des Datenschutzrechts. Grundsätzlich soll es dem von einer Datenverarbeitung Betroffenen überlassen sein zu entscheiden, ob und wem er welche personenbezogenen Daten zur Verfügung stellt. Doch wie ist diese Entscheidung verfahrenstechnisch abzusichern? Diese Frage lässt sich nur beantworten, wenn man sich den Sinn und Zweck gesetzlicher Formerfordernisse im Allgemeinen ins Bewusstsein ruft (dazu unter II.), die gleichsam als Metarecht auch für das Datenschutzrecht Geltung beanspruchen. Das BDSG sieht in Konkretisierung dieser allgemeinen Grundsätze in § 4a unter anderem die Schriftlichkeit der Erklärung vor. Seit jeher ist umstritten, welche Schriftlichkeit hiermit gemeint sein mag (dazu unter III. und IV.): Die des § 126 Abs. 1 BGB oder doch eine datenschutzrechtlich spezifische Schriftform? Der vergleichende Pendelblick zur ab Mai 2018 geltenden Datenschutz-Grundverordnung wird erhellen, dass die zu § 4a Abs. 1 S. 3 BDSG herrschende Meinung überholt werden wird – zu Recht, wie die Autoren dieser Zeilen befinden. Dass der deutsche Gesetzgeber mit § 26 BDSG-n.F. im Beschäftigtendatenschutz den alten Streit um die Schriftform im Arbeitsrecht am Leben hält, ist dabei den Besonderheiten des Beschäftigungsverhältnisses geschuldet (zu beidem unter V.).

II. Sinn und Zweck gesetzlicher Formerfordernisse

Nähert man sich der Frage um Formerfordernisse, lassen sich ausgehend von der grundsätzlichen Formfreiheit privater Rechtsgeschäfte Funktionen benennen, die in bestimmten Fällen die Anordnung einer gesetzlich vorgeschriebenen Form rechtfertigen. Bei diesen Ausnahmen handelt es sich regelmäßig um Bestimmungen, die den Betroffenen vor der über-

eilten Bindung bei bedeutenden oder riskanten Geschäften schützen sollen.[1] Neben der so beschriebenen Warnfunktion können Schriftformvorschriften dazu dienen, den Vertragsschluss von bloßen Vorverhandlungen deutlich zu trennen, den Inhalt des Geschäfts zu fixieren und klarzustellen sowie den Beweis für dessen Inhalt zu erleichtern (Klarstellungs- und Beweisfunktion).[2] Ein Minus zur Beweisfunktion gesetzlicher Formerfordernisse ist die Dokumentationsfunktion: Die Information durch ein Medium, das die dauerhafte Verfügbarkeit und Abrufbarkeit einer Erklärung gewährleistet, steht im Vordergrund der Textformerfordernisse.[3]

So wurden Sinn und Zweck gesetzlicher Formerfordernisse bereits in den Motiven zum BGB bildlich dargestellt.[4] Schon vor Inkrafttreten des Bürgerlichen Gesetzbuches – in einer Zeit, in der die Form als „Zwillingsschwester der Freiheit"[5] betitelt wurde – hoben die Rechtslehrer als praktische Seite des Formzwangs bereits die Abschlussklarheit sowie die Warn- und Beweisfunktion hervor und betonten den damit verbundenen Vorteil für die Rechtssicherheit.[6]

Der Grundsatz der Formfreiheit lässt dem Erklärenden die Wahlfreiheit, in welcher Art und Weise er seinen Willen äußern will – vor dem Hintergrund der Privatautonomie bildet demgegenüber der gesetzliche Formzwang die Ausnahme, die der Rechtfertigung bedarf.[7] Aus den Gründen zur Rechtfertigung des Formzwangs ergibt sich jedoch auch, dass die gesetzlichen Formvorschriften zwingend sind. Damit ordnet § 125 S. 1 BGB an, dass ein Rechtsgeschäft, welches der durch Gesetz vorgeschriebenen Form ermangelt, nichtig ist. Die Voraussetzungen der Schriftform, soweit sie für privatrechtliche Verträge und Willenserklärungen angeordnet wird, sind in § 126 BGB normiert.

III. Die Rechtslage nach § 4a BDSG

Eine datenschutzrechtlich relevante Erklärung ist die Einwilligung, welche in § 4a BDSG ihre Regelung findet. § 4a Abs. 1 S. 3 BDSG bestimmt, dass die Einwilligung der Schriftform bedarf, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. § 126 Abs. 1 BGB schreibt zur Erfüllung eines gesetzlichen Formerfordernisses vor, dass „die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens" unterzeichnet wird. Die Schriftform führt zur Entstehung einer Urkunde.[8] Dieser im Gesetz nicht näher erläuterte Begriff wird von der Literatur als die schriftliche Verkörperung einer Gedankenerklärung definiert, die sich auf einem Medium befindet, das geeignet ist, Schriftzeichen dauerhaft festzuhalten.[9]

Die datenschutzrechtliche Kommentarliteratur sieht recht einmütig für die datenschutzrechtliche Einwilligung das Schriftformerfordernis des § 126 Abs. 1 BGB zur Anwendung berufen, bleibt jedoch eine Begründung weitgehend schuldig.[10] Die Rechtsprechung hat sich mit dieser Problematik im Rahmen des Datenschutzrechts – soweit ersichtlich – bisher noch nicht näher beschäftigt.[11] Im Schrifttum wird von der Anwendbarkeit der §§ 125, 126 BGB – beispielsweise bei Fragestellungen der Auftragsdatenverarbeitung – ausgegangen.[12] Dies ist jedoch keineswegs zwingend, denn der Schriftlichkeitsbegriff des BDSG kann ein anderer sein als der des BGB.[13] Ein ausdrücklicher gesetzlicher Hinweis der datenschutzrechtlichen Regelung auf das BGB fehlt. Inwieweit die Normierung des Schriftformerfordernisses, die § 126 Abs. 1 BGB enthält, auf die Einwilligung nach § 4a BDSG Anwendung findet, ist also sorgfältig zu prüfen. Dabei sind stets die eigenständigen Formzwecke, die einer Regelung innewohnen, zu erforschen und zu berücksichtigen.

1. Allgemeine Ansicht: Anwendbarkeit nur auf privatrechtliche Vorschriften

§ 126 BGB gilt für alle Schriftformerfordernisse des BGB sowie anderer privatrechtlicher Gesetze.[14] Über das BGB hinaus findet diese Vorschrift also grundsätzlich nur im Privatrecht Anwendung. Außerhalb von öffentlich-rechtlichen Verträgen gilt § 126 BGB für die öffentlich-rechtliche Schriftform nicht,[15] und zwar grundsätzlich auch nicht analog.[16] Damit kommt der Frage, ob das BDSG dem Privatrecht

1 MüKomm/Einsele, BGB, 5. Aufl. 2006, § 125 Rn. 8; Staudinger/Hertel, BGB, Neub. 2004, § 125 Rn. 35; Larenz/Wolf, BGB AT, 9. Aufl. 2004, § 27 Rn. 4; Bamberger/Roth/Wendtland, BGB, Stand 2010, § 125 Rn. 1.

2 MüKomm/Einsele, BGB, § 125 Rn. 9; Larenz/Wolf, BGB AT, 9. Aufl. 2004, § 27 Rn. 4.

3 MüKomm/Einsele, BGB, § 125 Rn. 9.

4 Mugdan, Materialien zum BGB, Nachdruck 1899, Bd. 1, S. 451 Rn. 179: „Die Notwendigkeit der Beobachtung einer Form ruft bei den Beteiligten eine geschäftsmäßige Stimmung hervor, weckt das juristische Bewusstsein, fordert zu besonnenen Überlegungen heraus und gewährleistet die Ernstlichkeit der gefassten Entschließung. Die beobachtete Form ferner stellt den rechtlichen Charakter der Handlung klar, dient, gleich dem Gepräge einer Münze, als Stempel des fertigen juristischen Willens und setzt die Vollendung des Rechtsakts außer Zweifel. Die beobachtete Form sichert endlich den Beweis des Rechtsgeschäftes seinem Bestande und Inhalte nach für alle Zeit; sie führt auch zur Verminderung oder doch zur Abkürzung und Vereinfachung der Prozesse."

5 V. Ihering, Geist des römischen Rechts auf den verschiedenen Stufen seiner Entwicklung, 4. Aufl. 1894, Teil 2 Abt. 1 S. 471.

6 V. Ihering, a.A.O., S. 472; v. Savigny, System des heutigen römischen Rechts, 1840, Bd. 1 S. 219; dazu: Hagen, DNotZ 2010, 644.

7 Flume, BGB AT, 4. Aufl. 1992, Bd. 2 § 15, S. 246; Larenz/Wolf, BGB AT, 9. Aufl. 2004, § 27 Rn. 3.

8 Larenz/Wolf, BGB AT, 9. Aufl. 2004, § 27 Rn. 32.

9 Staudinger/Hertel, BGB, Neub. 2004, § 126 Rn. 108; Larenz/Wolf, BGB AT, 9. Aufl. 2004, § 27 Rn. 32; Spindler/Schuster/Spindler/Weber, Recht der elektronischen Medien, 2008, § 126 BGB Rn. 2; Bamberger/Roth/Wendtland, BGB, Stand 2010, § 126 Rn. 3.

10 D/K/W/W/Däubler, BDSG, 3. Aufl. 2009, § 4a Rn. 11; Gola/Schomerus, BDSG, 10. Aufl. 2010, § 4a Rn. 13; Simitis/Simitis, BDSG, 6. Aufl. 2006, § 4a Rn. 33; Taeger/Gabel/Taeger, BDSG, 2010, § 4a Rn. 32; ErfK/Wank, 11. Aufl. 2011, § 4a BDSG Rn. 3.

11 Allein zur Pflicht zur Hervorhebung OLG Koblenz, Urteil vom 26. März 2014 – 9 U 1116/13, Rn. 58. § 126 BGB offenbar für anwendbar hält AG Elmshorn, Urt. v. 25.04.2005 – 49 C 54/05, Juris Rn. 37, jedoch ohne Begründung.

12 Gola/Schomerus, BDSG, 10. Aufl. 2010, § 11 Rn. 17; D/K/W/W/Wedde, BDSG, 3. Aufl. 2009, § 11 Rn. 32; Simitis/Walz, BDSG, 6. Aufl. 2006, § 11 Rn. 49ff.

13 So Thüsing, Arbeitnehmerdatenschutz und Compliance, 2010, Rn. 123.

14 BVerwG v. 25.11.1970 – IV C 119/68, NJW 1971, 1054; RG v. 27.6.1910 – VI 297/08, RGZ 74, 69 (70); MüKomm/Einsele, BGB, 5. Aufl. 2006, § 126 Rn. 3; Staudinger/Hertel, BGB, Neub. 2004, § 126 Rn. 7; Bamberger/Roth/Wendtland, BGB, Stand 2010, § 126 Rn. 1.

15 BVerwG v. 25.11.1970 – IV C 119/68, NJW 1971, 1054; MüKomm/Einsele, BGB, 5. Aufl. 2006, § 126 Rn. 5; Staudinger/Hertel, BGB, Neub. 2004, § 126 Rn. 11.

16 Bamberger/Roth/Wendtland, BGB, 41. Ed. (01.11.2016), § 126 Rn. 1 m.w.N.

oder dem öffentlichen Recht zuzuordnen ist, entscheidende Bedeutung zu. Diese Zuordnung liegt keineswegs auf der Hand – die stärkeren Argumente sprechen wohl aber für eine öffentlich-rechtliche Verortung der allgemeinen Regelungen des Datenschutzrechts.

Das BDSG schützt den Betroffenen vor Missbrauch von Daten durch datenverarbeitende Stellen. Der in § 1 normierte Zweck des Gesetzes besteht darin, zu verhindern, dass der Einzelne in seinem Persönlichkeitsrecht beeinträchtigt wird. Das BDSG ist damit ein Eingriffsgesetz, mit dem Eingriffe in das Grundrecht auf informationelle Selbstbestimmung legitimiert werden können.[17] Folglich ist den Normen ein öffentlich-rechtlicher Charakter nicht grundsätzlich abzusprechen.

Die Regelung in § 4a BDSG enthält entsprechende Verfahrensbedingungen, die verhindern sollen, dass der Datenschutz allzu leicht unterlaufen wird.[18] Dazu zählt neben der Einsichtsfähigkeit und vorherigen Information des Betroffenen, dem Bestimmtheitserfordernis und der Freiwilligkeit der Entscheidung auch die Schriftform der Erklärung. Aus dem bisher Gesagten ergibt sich nun, dass dieses Schriftformerfordernis nicht automatisch den Anforderungen des BGB unterworfen werden kann. Vielmehr handelt es sich bei der Regelung des § 4a Abs. 1 S. 3 BDSG um eine dem öffentlichen Recht zuzuordnende Norm. Mithin findet § 126 Abs. 1 BGB hier keine Anwendung.

2. Herrschende Meinung: Keine Anwendbarkeit auf rechtsgeschäftsähnliche Handlungen

Darüber hinaus könnte eine Anwendbarkeit des § 126 BGB auf das Schriftformerfordernis des § 4a BDSG aufgrund des Rechtscharakters der Einwilligungserklärung ausscheiden.

Das BGB enthält im 3. Abschnitt des ersten Buches detaillierte Vorschriften über Willenserklärungen, die konstitutiv für ein Rechtsgeschäft sind. Dafür gilt explizit auch die Regelung über die Schriftform in § 126 BGB. Keine ausdrückliche Regelung enthält das Gesetz demgegenüber für rechtsgeschäftsähnliche Handlungen. Während ein Rechtsgeschäft aus einer oder mehreren Willenserklärungen besteht, die allein oder in Verbindung mit anderen Tatbestandsmerkmalen eine Rechtsfolge herbeiführen, weil sie gewollt ist, sind geschäftsähnliche Handlungen auf einen tatsächlichen Erfolg gerichtete Erklärungen, deren Rechtsfolgen kraft Gesetzes eintreten.[19] Gemeinsam ist Willenserklärungen und geschäftsähnlichen Handlungen, dass die Rechtsfolge an einen Erklärungstatbestand anknüpft, wodurch sie sich von Realakten abgrenzen lassen. Eine Willenserklärung führt jedoch Rechtsfolgen herbei, weil sie erklärt und gewollt sind. Darin unterscheidet sie sich von geschäftsähnlichen Handlungen, welche kraft Gesetzes eintretende Rechtsfolgen auslösen.[20] Regelmäßig ermöglichen oder verhindern sie den Eintritt gesetzlich angeordneter Folgen des Tätigwerdens oder Untätigbleibens.[21] Ausgehend von dieser Definition erfolgt die rechtliche Einordnung der Einwilligung übereinstimmend als geschäftsähnliche Erklärung.[22]

Nach der Ansicht der Rechtsprechung gilt die gesetzliche Schriftform des § 126 Abs. 1 BGB jedoch nur für Rechtsgeschäfte.[23] Dem ist zuzustimmen. Die Norm enthält zwar ihrem Wortlaut nach eine solche Beschränkung auf Rechtsgeschäfte nicht. Sie ergibt sich aber aus dem systematischen Zusammenhang mit § 125 S. 1 BGB: Danach ist ein „Rechtsgeschäft", welches der durch Gesetz vorgeschriebenen Form ermangelt, nichtig.[24] Der Gegenstand, an den sich diese Anforderungen richten, muss aufgrund des inneren Zusammenhangs der beiden Normen ebenfalls ein Rechtsgeschäft sein. Hinzu kommt, dass beide Vorschriften des BGB im Abschnitt über „Rechtsgeschäfte" und unter dem Titel „Willenserklärungen" stehen.[25] Eine direkte Anwendung des § 126 Abs. 1 BGB auf rechtsgeschäftsähnliche Handlungen scheidet somit aus. Dies gilt mithin auch für eine Geltung im Rahmen des § 4a Abs. 1 S. 3 BDSG.

3. § 126 Abs. 1 BGB findet im Datenschutzrecht keine Anwendung

Somit kann die Schriftform des BGB nicht in das BDSG übernommen werden. Dies mag nicht der herrschenden Meinung entsprechen, doch kommt etwa *Plath* über einen Umweg zu in der Praxis wohl vergleichbaren Ergebnissen, allein unter Heranziehung der Ausnahmeklausel des § 4a Abs. 1 S. 3 BDSG.[26] *Plath* nimmt also an, dass die Schriftform des § 126 Abs. 1 BGB grundsätzlich gelte, aber in vielen Fällen „unangemessen" und „nicht praktikabel" sei.[27] Daher dürften die „besonderen Umstände" nach § 4a Abs. 1 S. 3 BDSG nicht eng, sondern müssten besonders weit ausgelegt werden.[28] Stringenter, da nicht mit Ausnahmen begründet, sondern einer sauberen Auslegung, ist die Anwendung eines eigenständigen Schriftlichkeitsbegriff im Rahmen des § 4a Abs. 1 S. 3 BDSG.

IV. Eigenständiger Schriftlichkeitsbegriff des BDSG

Dieser Schriftlichkeitsbegriff ist nach dem Sinn und Zweck der vorgeschriebenen Schriftlichkeit zu bestimmen.

1. Technikoffener Schriftlichkeitsbegriff des BDSG

Der eigenständige Schriftlichkeitsbegriff des BDSG erhellt sich daraus, dass das Schriftlichkeitserfordernis auf Art. 17

17 D/K/W/W/Weichert, BDSG, 3. Aufl. 2009, § 1 Rn. 5.

18 Simitis/Simitis, BDSG, 6. Aufl. 2006, § 4a Rn. 9.

19 Medicus, BGB AT, 10. Aufl. 2010, Rn. 195 ff.; Larenz/Wolf, BGB AT, 9. Aufl. 2004, § 22 Rn. 14.

20 BAG. v. 11.10.2000 – 5 AZR 313/99, NJW 2001, 989 m.w.N.

21 BAG v. 11.06.2002 – 1 ABR 43/01, NJW 2003, 843 (844).

22 Däubler, Gläserne Belegschaften, 5. Aufl. 2010, Rn. 138; Simitis/Simitis, BDSG, 6. Aufl. 2006, § 4a Rn. 20; ErfK/Wank, 11. Aufl. 2011, § 4a BDSG, Rn. 1.

23 BAG v. 11.06.2002 – 1 ABR 43/01, NJW 2003, 843 (844); a.A. MüKomm/Einsele, BGB, 5. Aufl. 2006, § 126 Rn. 4; Röger, NJW 2004, 1764; Ulrici, NJW 2003, 2053.

24 BAG v. 11.6.2002 – 1 ABR 43/01, NJW 2003, 843 (844).

25 Köhler, AcP 182 (1982), 126 (151).

26 So etwa Plath/Plath, BDSG/DSGVO, 2. Aufl. 2017, § 4a BDSG Rn. 14.

27 So etwa Plath/Plath, BDSG/DSGVO, 2. Aufl. 2017, § 4a BDSG Rn. 14.

28 So jedenfalls auch Wybitul: Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO, NZA 2017, 413, 417.

Abs. 4 EG-Datenschutz-Richtlinie zurückzuführen ist. Schriftlichkeitserfordernisse im Gemeinschaftsrecht sind nach der Rechtsprechung des EuGH autonom europäisch auszulegen.[29] Dabei ist der Zweck der Vorschrift maßgeblich zur Auslegung heranzuziehen. Art. 17 Abs. 4 EG-Datenschutz-Richtlinie benennt als Zweck der Schriftform ausdrücklich die Beweissicherung. Diese kann aber auch ohne Unterschrift gewährleistet werden, es genügt etwa die Textform.

In den Gesetzesmaterialien zur 2. BDSG-Novelle finden sich keine Ausführungen zu dieser Problematik. Dies mag daran liegen, dass man der verbreiteten Ansicht im Schrifttum folgen wollte, oder aber daran, dass man es nicht als Problem gesehen hat. Jedenfalls wird aber auch dort deutlich, dass es dem Gesetzgeber im Wesentlichen darauf ankam, *dass* die erforderlichen Angaben fixiert werden, weniger aber, *wie* diese zu fixieren sind.

Dies spricht alles für einen technikoffenen Ansatz. Überzeugend ist dabei ein zweiter Blick auf die Gesetzgebungsgeschichte des BDSG. Das Gesetz entstand mit dem Ziel einer Legitimation und gleichzeitigen Begrenzung staatlicher Maßnahmen, die personenbezogene Daten der Bürger betrafen. Hintergrund war die Feststellung, dass sich im Rahmen der elektronischen Datenverarbeitung die spezifische Gefahren aus der Kürzung inhaltlicher Angaben (sog. Kontextverlust), aus der Geschwindigkeit und großen Zahl der Abruf- und Kombinationsmöglichkeiten, den dadurch bedingten verstärkten Kontrollmöglichkeiten, ferner aus dem „Verewigungseffekt", der „Scheinobjektivität" und dem dadurch auf den Betroffenen ausgeübten „Konformitätsdruck" ergeben.[30] Vor diesem Hintergrund spiegelt das Bestreben, personenbezogene Daten einem rechtlichen Schutz zugänglich zu machen, wohl wie kaum ein anderes Rechtsgebiet die Entwicklung der modernen Industriegesellschaft zur Informationsgesellschaft wider.[31] Zunächst ließe sich somit schlussfolgern, dass der gesetzliche Datenschutz ein technikbezogenes Recht ist. Ein zweiter Blick erhellt jedoch, dass gerade die allgemeinen Generalklauseln, die der gesetzlichen Kodifizierung des Datenschutzes immanent sind,[32] die Reaktion und Anpassung auf neue technische Entwicklungen ermöglichen.

So wurde auch zuletzt im Rahmen des aktuellen Gesetzesvorhabens, welches einen umfassenden Arbeitnehmerdatenschutz in das BDSG integrieren soll, in der zugehörigen Regierungsbegründung unter der Überschrift „Nachhaltigkeit" deutlich gemacht, dass „die Regelungen technikneutral ausgestaltet sind und so die Gewähr bieten, zukünftige technische Entwicklungen mit zu umfassen".[33]

2. Effektiver Schriftlichkeitsnachweis

Ausgehend von der Feststellung, dass die Regelung des § 4a Abs. 1 S. 3 BDSG in erster Linie dem Zweck der Beweissicherung und Dokumentation dient, ist also anhand entsprechender Wertungskriterien zu bestimmen, wie dieser Nachweis praktisch und technisch ausgestaltet werden kann.

Als erstes Kriterium ist der Schutz vor Erheblichkeit der rechtlichen Wirkung einer Erklärung zu nennen.[34] Die Anordnung eines Formzwangs ist also wesentlich durch die Qualität der Rechtsfolgen, die an die Erklärung geknüpft sind, bedingt: Je erheblicher sie ausfallen, desto eher spricht dies für eine höhere Formstrenge. So kann beispielsweise der Widerspruch nach § 613a IV BGB zum Verlust des Arbeitsplatzes führen und ist damit auch in der Form an besonders hohe Anforderungen zu knüpfen.[35] Dagegen führt die Verwendung personenbezogener Daten regelmäßig nicht zu existentiellen Beeinträchtigungen des Arbeits- und Sozialllebens des Einzelnen. Vielmehr ermöglicht sie oftmals erst die Teilhabe am gesellschaftlichen und technischen Fortschritt. Inwieweit der Einzelne seine Daten – z.B. einem Vertragspartner – preisgeben möchte, kann er von Fall zu Fall entscheiden, ohne im Grundsatz eine Entscheidung über die Beteiligung am Wirtschaftsverkehr zu treffen. Außerdem ist die Einwilligung jederzeit widerruflich.[36] Obgleich die Einwilligung als gleichwertige Möglichkeit der Rechtfertigung im System des Verbots mit Erlaubnisvorbehalt steht, ist die Erheblichkeit der rechtlichen Wirkung einer einzelnen Erklärung für den Betroffenen damit als überschaubar einzustufen. Sie ist in Textform zu fixieren, bedarf jedoch nicht zwingend der eigenhändigen Unterschrift, solange der Einzelne erkennbar zugestimmt hat.

Des Weiteren ist auf die rechtliche Verbindlichkeit der Erklärung abzustellen.[37] Auch hier gilt: Je höher die Rechtsverbindlichkeit einer Erklärung, desto stärker fällt das Bedürfnis nach Formstrenge aus.[38] Die eigenhändige Unterschrift ist insbesondere dann als nicht notwendig anzusehen, wenn die Rechtsfolgen einer Erklärung leicht rückgängig zu machen sind. Bei der Einwilligung in datenverarbeitende Maßnahmen ist von der verantwortlichen Stelle stets die Möglichkeit des Widerrufs im Auge zu behalten. Bereits erfolgte Verarbeitungsprozesse werden nicht unwirksam, für die Zukunft gelten jedoch ausschließlich die gesetzlichen Erlaubnistatbestände. Auch unter diesem Gesichtspunkt ist eine schriftliche Fixierung unerlässlich. Der Schwerpunkt liegt aber wohl auf der genauen zeitlichen Niederschrift, der Bestimmtheit des Datenumfangs und auch der Festhaltung des Zwecks der Erhebung, Verarbeitung oder Nutzung.

Weiteres Kriterium für die Beantwortung der Frage, welche Anforderungen einem Formzwang zugrunde zu legen sind, ist die Schutzbedürftigkeit der Rechtssicherheit.[39] Letztere ist immer und nur dann besonders hoch, wenn der Erklärende und der Erklärungsempfänger als Beteiligte oder

29 EuGH v. 29.04.1982 – Rs. C-66/81, Slg. 1982, 1363 Rn. 19 ff. – Butterreinfett.

30 Küttner/Griese, Personalbuch, 17. Aufl. 2010, Datenschutz Rn. 1; Hold, RDV 2006, 249 (251); MüHdbArbR/Reichold, 3. Aufl. 2009, § 88 Rn. 1.

31 Hoeren/Sieber/Helfrich, Multimedia-Recht, 22. Aufl. 2009, Teil 16.1 Rn. 1.

32 Vgl. dazu Franzen, RdA 2010, 257 (261).

33 BR-Drucks. 535/10, S. 24.

34 Vgl. dazu ausführlich Gotthardt/Beck, NZA 2002, 876 (879).

35 BR-Drucks. 14/7769, S. 20.

36 Erwägungsgrund 30 der EG-Datenschutz-Richtlinie 95/46/EG.

37 Gotthardt/Beck, NZA 2002, 876 (879).

38 BT-Drucks. 14/4987, S. 18.

39 Gotthardt/Beck, NZA 2002, 876 (879).

aber ein Dritter regelmäßig ein Interesse an einer Fälschung der Erklärung haben werden.[40] In diesen Fällen einer besonderen Manipulationsgefahr besteht zuvorderst das Bedürfnis, die Identität des Erklärenden im Rechtsverkehr einwandfrei offen zu legen. Dabei dürfen jedoch die praktischen Bedürfnisse des Datenschutzrechts nicht verkannt werden. Nicht zuletzt die EG-Datenschutz-Richtlinie wurde unter der Prämisse geschaffen, den Datenfluss für Unternehmen zu erleichtern.[41] Damit dient die Einwilligung als Alternative zu den gesetzlichen Erlaubnistatbeständen, auch und gerade der Steigerung der flexiblen Rechtsgestaltung.

Festzuhalten bleibt darüber hinaus, dass das Hauptmotiv für die Anordnung des Formzwangs nach § 4a Abs. 1 S. 3 BDSG in der Sicherstellung einer ausreichenden Information und Dokumentation zu sehen ist.[42] Nach dem bisher Gesagten kommt damit grundsätzlich auch eine Speicherung in elektronischer Form in Betracht.

3. Nachrangig: Effektiver Übereilungsschutz

Daneben kann der schriftlichen Niederlegung einer Erklärung insbesondere eine Warn- und / oder eine Beweisfunktion zukommen. Die Erklärung der Einwilligung stellt sich als Ausübung des Selbstbestimmungsrechts des Einzelnen dar.[43] Im Datenschutzrecht ist sie – so gesehen – manifestes Zeichen der verfassungsrechtlich garantierten informationellen Selbstbestimmung.[44] Wird die Einwilligung mit einem Schriftlichkeitserfordernis versehen, ist sie gleichzeitig als gesetzlicher Schutz davor anzusehen, die persönlichen Rechtspositionen – oder in diesem Fall Daten – nicht vorschnell preiszugeben.

Dazu dienen im Falle des BDSG aber insbesondere auch die weiteren Voraussetzungen für eine wirksame Einwilligung. Zunächst muss die Erklärung vor dem fraglichen Vorgang der Datenerhebung, -verarbeitung oder -nutzung abgegeben werden. Zu diesem Zeitpunkt muss auch die Einsichtsfähigkeit des Betroffenen gegeben sein. Der Einwilligende muss also die Konsequenzen seines Handelns übersehen; auf die Geschäftsfähigkeit kommt es dagegen nicht an.[45] Nicht zuletzt entscheidend ist die Freiwilligkeit der Erklärung. Grundlage dafür ist die EG-Datenschutz-Richtlinie, die in Art. 2 lit. h) eine wirksame Einwilligung nur dann annimmt, wenn diese „ohne Zwang" abgegeben wurde. De facto ist man sich aber einig, dass die Existenz eines informationellen, wirtschaftlichen oder gesellschaftlichen Ungleichgewichts, wie es häufig zwischen Arzt und Patient, Bank und Kunden oder Arbeitgeber und Arbeitnehmer auftritt, nicht von vornherein jede „freiwillige" Einwilligung ausschließt.[46] Zu einer Unwirksamkeit der abgegeben Erklärung – und damit auch zur Unzulässigkeit der datenschutzrechtlich relevanten Maßnahme über die gesetzliche Rechtfertigung hinaus – führen jedoch die Missachtung des Kopplungsverbots, Fälle der „Überrumpelung" oder das In-Aussicht-Stellen von Nachteilen bei fehlender Einwilligung.[47]

Ausgehend von der rechtssystematischen Erwägung, dass eine Einwilligung grundsätzlich immer möglich ist,[48] wird sie hier schon an weitere Bedingungen geknüpft, die sie als Erlaubnisvorbehalt im Verbotssystem des BDSG verankern. Für die Schriftform nach § 4a Abs. 1 S. 3 BDSG bleibt damit vorrangig die Funktion der Beweissicherung und der Dokumentation.

Die Einwilligung nach § 4a Abs. 1 BDSG bietet die Möglichkeit einer Rechtfertigung datenschutzrechtlich relevanter Maßnahmen, die einem Verbot mit Erlaubnisvorbehalt unterliegen. Verwendet ein Unternehmen dann als verantwortliche Stelle auf dieser Grundlage personenbezogene Daten, tritt dies neben die gesetzliche Rechtfertigung. Von der Folge, ordnungswidrig zu handeln und der Bußgeldvorschrift des § 43 BDSG zu unterfallen, entbindet das datenverarbeitende Unternehmen jedoch ausschließlich die wirksame Einwilligung. Diese setzt neben einer Reihe wichtiger Bedingungen – wie der Freiwilligkeit der Erklärung – auch die Schriftform voraus. Die Schriftform dient damit nicht zuletzt dem Beweis dieser Rechtfertigung für die datenverarbeitende Stelle.

4. Kriterien eines effektiven Übereilungsschutzes

Sinn und Zweck der Warnfunktion der Schriftform erfordern es, dass die Art der Erteilung einer Einwilligung „bei den Beteiligten eine geschäftsmäßige Stimmung hervorruft, zu besonnenen Überlegungen herausfordert und die Ernstlichkeit der gefassten Entschließung gewährleistet."[49] Entscheidend ist insoweit, dass dem Einzelnen deutlich wird, dass er eine rechtserhebliche Erklärung abgibt und damit wirksam über sein Recht auf informationelle Selbstbestimmung sowie die in Rede stehenden Daten disponiert. Der „Akt des Schreibens" darf sich mithin qualitativ nicht von der auf Papier gesetzten Unterschrift unterscheiden. Wird etwa ein Verfahren verwendet, bei dem ein optisches und haptisches Erlebnis erzeugt wird, das der rechtlichen Verbindlichkeit der Erklärung in gleichem Maße Gewicht verleiht, wie eine Unterschrift auf Papier, stehen der Schriftlichkeit dieser Erklärung keine Bedenken entgegen.

Darüber hinaus dürfte jedenfalls derzeit noch der Einsatz elektronischer Schreibunterlagen gegenüber dem herkömmlichen Papierverfahren die Ausnahme bilden. Die mit der

40 BT-Drucks. 14/4987, S. 18.

41 Roßnagel/Abel, Hdb. Datenschutzrecht, 2003, Kap. 2.7 Rn. 45; D/K/W/W, BDSG, 3. Aufl. 2009, Einl. Rn. 82; Taeger/Gabel/Taeger/Schmidt, BDSG, Einführung, Rn. 34.

42 Wie dies künftig auch die DS-GVO regelt, s. unten IV.

43 Buchner, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 231; Gola/Schomerus, BDSG, 10. Aufl. 2010, § 4a Rn. 2; Schack, AcP 195 (1995), 595 (597).

44 Simitis/Simitis, BDSG, 6. Aufl. 2006, § 4a Rn. 2.

45 D/K/W/W/Däubler, BDSG, 3. Aufl. 2009, § 4a Rn. 5; Gola/Schomerus, BDSG, 10. Aufl. 2010, § 4a Rn. 10; Simitis/Simitis, BDSG, 6. Aufl. 2006, § 4a Rn. 20; ErfK/Wank, 11. Aufl. 2011, § 4a BDSG Rn. 1

46 D/K/W/W/Däubler, BDSG, 3. Aufl. 2009, § 4a Rn. 23; Gola/Schomerus, BDSG, 10. Aufl. 2010, § 4a Rn. 9; Taeger/Gabel/Taeger, BDSG, 2010, § 4a Rn. 49.

47 D/K/W/W/Däubler, BDSG, 3. Aufl. 2009, § 4a Rn. 24-26; Schaar, MMR 2001, 641; Simitis/Simitis, BDSG, 6. Aufl. 2006, § 4a Rn. 63; Tinnefeld, NJW 2001, 3081.

48 Taeger/Gabel/Taeger, BDSG, 2010, § 4a Rn. 4; v. Uckermann, DuD 1979, 163.

49 Mugdan, Materialien zum BGB, Nachdruck 1899, Bd. 1, S. 451 Rn. 179.

Form verbundene Warnfunktion muss deshalb bei einer elektronischen Unterschrift noch stärker zu Tage treten als bei der Unterzeichnung eines Papiers. Wer verspürt bei der Unterzeichnung eines ihm gereichten Dokuments schon noch eine „geschäftsmäßige Stimmung", ein In-Sich-Gehen, gleichsam eine Walpurgisnacht des Rechtsbindungswillens? Die Realität ist doch die, dass Verträge unterzeichnet werden und sich die Parteien hinterher fragen, was im Kleingedruckten steht. Anderenfalls wären die zahlreichen Widerrufsvorschriften des BGB überflüssig, der Verbraucher bedürfte keines Schutzes, wird er doch durch die Schriftform stets und allerorten auf die Folgen seines Tuns hingewiesen. Die Unterschrift ist so alltäglich geworden, dass sie den Reiz des Besonderen verloren hat. Einem pawlowschen Hund gleich greift der moderne Mensch bei jedem Vertragsschluss wie selbstverständlich zu Stift und Papier. Der elektronischen Unterschrift hingegen haftet noch immer der Reiz des Neuen an – und ihr bringt man deshalb auch ein – hier durchaus positiv verstandenes, eben gesundes – Misstrauen entgegen.

Dementsprechend gilt es zur Wahrung der Schriftlichkeit i.S.d. BDSG behutsam vorzugehen. Daraus, dass § 126 Abs. 1 BGB keine Anwendung findet, kann nicht geschlossen werden, dass nun jedes irgendwie unterschriebene Dokument formwahrend wirkt. Vielmehr sind die Zwecke vorrangig der Nachweisfunktion, aber auch des Übereilungsschutzes mit der im elektronischen Verkehr notwendigen effektiven Einholung von Einwilligungen in Einklang zu bringen.

V. Das künftige Recht der DS-GVO: Art. 7 DS-GVO

Dass dieser technikbezogene Ansatz den Betroffenen bei Erteilung einer Einwilligung verfahrensmäßig effektiv schützt, ohne zugleich den Datenverkehr unnötig zu belasten, zeigt die Neuregelung in Art. 7 Abs. 1 DS-GVO. Diese geht deutlich weg von der Schriftform des § 126 Abs. 1 BGB und wählt den Weg einer Nachweispflicht.

1. Bloße Nachweispflicht im Rahmen des Art. 7 Abs. 1 DS-GVO

Ganz im Sinne der primären Nachweisfunktion legt Art. 7 Abs. 1 DS-GVO dem Verantwortlichen eine Nachweispflicht bei Berufung auf eine Einwilligung auf. Dieser trägt die Beweislast für das Vorliegen einer Einwilligung, was dem Verbot mit Erlaubnisvorbehalt nach Art. 6 Abs. 1 DS-GVO entspricht: Wer sich auf eine Ausnahme vom grundsätzlichen Verbot der Datenverarbeitung beruft, hat das Vorliegen der Voraussetzungen nachzuweisen. Art. 7 Abs. 1 DS-GVO konkretisiert für Einwilligungen damit das Prinzip der Rechenschaftspflicht, das in Art. 5 Abs. 2 DS-GVO Eingang gefunden hat.[50] Letztlich geht es um die Transparenz von Datenverarbeitungen.[51] Schriftlichkeit – sei es nach § 126 Abs. 1 BGB oder nach eigenständiger Bestimmung im Rahmen des § 4a Abs. 1 S. 3 BDSG – wird künftig also nicht mehr zur Wirksamkeitsvoraussetzung einer Einwilligung erhoben. Dies mag man mit Blick auf den Übereilungsschutz kritisch sehen, doch wirkt insoweit gerade die jederzeitige Widerruflichkeit der Einwilligung entlastend: Je weniger bedeutend eine Erklärung ist, desto geringer können die Formanforderungen ausfallen. Zudem wird der Wegfall des Schriftformzwanges nicht zu einem Weggehen von schriftlichen Erklärungen – oder zumindest elektronisch vom Betroffenen angeklickten Buttons – führen. Der sorgsame Datenverarbeiter wird sich aufgrund seiner Nachweispflicht aus Art. 7 Abs.1 DS-GVO und seiner weitergehenden Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO davor hüten, ohne jede Art von dauerhaft in Zeichen verkörperter Bestätigung auf Grundlage einer Einwilligung Daten zu verarbeiten. Zu bedrohlich sind die Sanktionsmechanismen, die die DS-GVO zum Individualrechtsschutz eingebaut hat.[52] Faktisch dürfte dieser „sanfte Druck" mehr als ein normierter Schriftlichkeitszwang erreichen: Verantwortliche werden die effektivste Einholung von Einwilligungen zur Vermeidung unnötiger Transaktionskosten und zur Abwendung von Strafen wählen – das mag mal ein Button auf einer Homepage, mal eine E-Mail, mal aber auch klassisch ein Stück Papier sein.

2. Abweichung in § 26 BDSG-n.F. für den Beschäftigtendatenschutz

Im Beschäftigtendatenschutz sieht der nationale Gesetzgeber aber Handlungsbedarf und hat mit § 26 BDSG-n.F. die Schriftform für Einwilligungen im Beschäftigungskontext festgeschrieben. Nimmt man die dargestellten Zwecke in den Blick, präsentiert sich dieser Vorschlag als durchaus nachvollziehbar. Zwar trifft auch den Arbeitgeber (richtiger wäre Beschäftigenden), wie jeden anderen Datenverarbeiter auch, die Nachweispflicht des Art. 7 Abs. 1 DS-GVO. Das Beschäftigungsverhältnis ruft aber nach weitergehenden Regelungen, wenn eine Einwilligung in Rede steht, weil es naheliegend ist, dass der Arbeitgeber seine meistens bestehende wirtschaftliche Überlegenheit anderenfalls dazu nutzt, den Beschäftigten zur Abgabe der Einwilligung zu bewegen.[53] Die Diskussion um die Freiwilligkeit der Einwilligung in solchen Zwangslagen ist eines der prominentesten Kinder des Datenschutzrechts, doch es wird mit den Jahren immer reifer. Statt „Alles-oder-Nichts-Lösungen", wie dem vollständigen Ausschluss der Einwilligung in Beschäftigungsverhältnissen,[54] sieht der Entwurf nun eine abgestufte Regelung mit Abwägungskriterien vor – gut so! Dass man als weitere Zutat die Schriftlichkeit implementiert, kann nur begrüßt werden. Zwar sollte auch künftig wie dargelegt nicht die Schriftform des § 126 Abs. 1 BGB unbesehen angewendet werden, und der Gesetzgeber sollte dies auch in der

50 Plath/Plath, BDSG/DSGVO, Art. 7 DSGVO Rn. 3.

51 Paal/Pauly, DSGVO, 1. Aufl. 2017, Art. 7 Rn. 6.

52 Vgl. Behling, ZIP 2017, 697.

53 Ausführlich Schmidt, Datenschutz für „Beschäftigte", 2016, S. 298.

54 Der schon vor dem Inkrafttreten der DS-GVO unionsrechtlich unzulässig war (Forst, RDV 2010, 150 ff.) und es auch in Zukunft sein wird, weil Art. 88 DS-GVO es den Mitgliedstaaten nicht erlaubt, die allgemeinen Grundsätze (wie Art. 7 DS-GVO) im Beschäftigungsverhältnis gänzlich abzubedingen.

Begründung klarstellen. Schließlich dürfte gerade das Einholen von Einwilligungen in elektronischer oder in Textform in der betrieblichen Praxis eher den Regelfall darstellen.[55]

Doch selbst wenn der Gesetzgeber nicht klarstellend tätig wird, hat der Entwurf vorgesorgt: Schließlich soll mit § 26 Abs. 2 S. 3 BDSG-n.F. wiederum ein Abweichen von der Schriftlichkeit im Falle des Vorliegens besonderer Umstände zulässig sein. Ob diese Ausnahme von der Ausnahme – gleichsam als legislatorisches Überdruckventil – erforderlich ist, um zu verhindern, dass der deutsche Gesetzgeber den ihm durch Art. 88 DS-GVO gesteckten Regelungsspielraum überschreitet, braucht hier nicht vertieft zu werden. Besonderheiten im Sinne des § 26 Abs. 2 S. 3 BDSG-n.F. könnten sich gegenüber der allgemeinen Regelung in Art. 7 DS-GVO jedenfalls auch aus den für Beschäftigungsverhältnisse insgesamt spezifischen Umständen ergeben.[56] Es kommt also auf eine Gesamtbetrachtung des Beschäftigungsverhältnisses an. Ein Beschäftigter, der vollständig von zuhause aus am PC arbeitet und keinerlei Schriftverkehr mit seinem Arbeitgeber pflegt, wird eine Einwilligung sicherlich via E-Mail erklären können und muss hierfür nicht einen Brief frankieren und zum Arbeitgeber schicken. Alles andere wäre nicht nur praxisfern, sondern widerspräche auch den Zielen des Schriftformgebotes. Entsprechendes gilt für einen Bewerber, der sich in einem vollständig online durchzuführenden Bewerbungsprozess auf eine Stelle bewirbt.

VI. Von der Schriftlichkeit zur Nachweispflicht

Die Evolution des Datenschutzrechts geht mit der DS-GVO unaufhaltsam weiter und bringt für Einwilligungen eine praxisgerechte Lösung. Mit Fokussierung auf die Nachweisfunktion wird mit Art. 7 Abs. 1 DS-GVO eine Nachweispflicht implementiert, ohne dass eine Einwilligung allein aufgrund mangelnder Schriftlichkeit unwirksam ist. Bis dahin wird im Rahmen von § 4a Abs. 1 S. 3 BDSG der Streit weitergehen, ob Schriftlichkeit die Schriftform des § 126 Abs.1 BGB meint. Doch auch danach wird jedenfalls dem datenschutzrechtlich aktiven Arbeitsrechtler mit Geltung des § 26 Abs. 2 BDSG-n.F. dieser Streit erhalten bleiben – Ende offen.

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

Dr. Maximilian Schmidt
ist Wissenschaftlicher Mitarbeiter am Institut für Arbeitsrecht und das Recht der Sozialen Sicherheit. Neben zahlreichen Veröffentlichungen zum Arbeits- und Datenschutzrecht hat er sich in seiner Dissertation mit Grundlagenfragen des Beschäftigtendatenschutzrechtes auseinandergesetzt.

PD Dr. Gerrit Forst LL.M. (Cambridge)
ist Rechtsanwalt im Düsseldorfer Büro von Hengeler Mueller und berät Unternehmen zu Fragen des Wirtschaftsrechts.

55 Wybitul, NZA 2017, 413, 417.
56 Wybitul, NZA 2017, 413, 417.

Dr. Sebastian J. Golla

Säbelrasseln in der DS-GVO: Drohende Sanktionen bei Verstößen gegen die Vorgaben zum Werbedatenschutz

Dieser Beitrag betrachtet die drohenden Konsequenzen bei Verstößen gegen die Vorgaben der DS-GVO zum Werbedatenschutz. Neben den in Kapitel VIII DS-GVO („Rechtsbehelfe, Haftung und Sanktionen") genannten Sanktionen nimmt er mögliche Schadensersatzansprüche sowie aufsichtsbehördliche Eingriffsbefugnisse in den Blick. Auch die Wettbewerbsaufsicht durch das Bundeskartellamt und die Klagebefugnisse von Verbraucherverbänden werden kurz in die Betrachtung miteinbezogen.

I. Die DS-GVO: Eine Revolution im Sanktionsrecht?

Im Datenschutzrecht klafft zwischen den rechtlichen Vorgaben und ihrer Befolgung eine so große Lücke „wie in fast keinem anderen Rechtsgebiet."[1] Ähnlich defizitär wie die Befolgung der Regelungen erscheint ihre Durchsetzung bzw. die Sanktionierung von Verstößen – sei es durch Bußgelder, zivilrechtliche Sanktionen oder aufsichtsbehördliche Maßnahmen.[2]

Die Neuregelung durch die DS-GVO legt einen Schwerpunkt auf die Sanktionierung von Datenschutzverstößen.[3] Insbesondere aufgrund des hohen Bußgeldrahmens in Art. 83 DS-GVO wurde dem Aspekt der Sanktionierung auch eine besondere Aufmerksamkeit in der fachlichen und öffentlichen Diskussion zuteil.[4] Die Durchsetzungsmechanismen der DS-GVO erhielten auch bereits Vorschusslorbeeren: So kündigte Jan Phillip Albrecht, Berichterstatter für die DS-GVO im Europäischen Parlament, an, die DS-GVO werde die Welt verändern und mit ihrer Anwendung vom 4. Mai 2018 an werde das Durchsetzungsdefizit im Datenschutzrecht beendet.[5]

Solche Ankündigungen sind Grund genug, die Sanktionen nach der DS-GVO einmal im Gesamtpaket unter die Lupe zu nehmen. Dieser Beitrag betrachtet nicht nur die in Kapitel VIII DS-GVO („Rechtsbehelfe, Haftung und Sanktionen") genannten Sanktionen als drohende Konsequenzen bei Verstößen gegen die Vorgaben der DS-GVO zum Werbedatenschutz, sondern auch mögliche Schadensersatzansprüche sowie aufsichtsbehördliche Eingriffe als Sanktionen im weiteren Sinne. Die Darstellung erfolgt geordnet nach den wichtigsten Akteuren, die Sanktionen herbeiführen können. Sie konzentriert sich auf den Bereich des Werbedatenschutzes, in dem auch verstärkt die wettbewerbs- und kartellrechtliche Sanktionierung von Datenschutzverstößen eine Rolle spielt. Daher werden auch die Wettbewerbsaufsicht durch das Bundeskartellamt und die Klagebefugnisse von Verbraucherverbänden kurz in die Betrachtung miteinbezogen.

II. Aufsichtsbehördliche Sanktionen

1. Die Datenschutzaufsicht

Der in der Praxis wichtigste Akteur bei der Sanktionierung von Verstößen gegen den (Werbe-)Datenschutz sind derzeit die Datenschutzaufsichtsbehörden. Auch Art. 57 Abs. 1 lit. a) DS-GVO benennt die Durchsetzung der DS-GVO als zentrale Aufgabe der Aufsichtsbehörden.

Nach geltendem Recht können Aufsichtsbehörden Datenschutzverstöße sanktionieren, indem sie diese formell beanstanden, Anordnungen nach § 38 Abs. 5 BDSG treffen, oder nach § 43 BDSG Bußgelder verhängen. Dazu können sie weitere Maßnahmen ergreifen, die zumindest faktisch Sanktionswirkung haben, aber keine echten Sanktionsmittel sind – beispielsweise die Erwähnung von Datenschutzverstößen im öffentlichen Tätigkeitsbericht.[6]

In der DS-GVO sind die wesentlichen Sanktionsmöglichkeiten als „Abhilfebefugnisse" in Art. 58 Abs. 2 geregelt. Zentral sind als Sanktionsinstrumente besonders die Verwarnung (Art. 58 Abs. 2 lit. b) DS-GVO), die Anweisung zur Herstellung datenschutzkonformer Zustände (Art. 58 Abs. 2 lit. d) DS-GVO), die Untersagung der Datenverarbeitung (Art. 58 Abs. 2 lit. f) DS-GVO) sowie die Verhängung von Bußgeldern (Art. 58 Abs. 2 lit. i) i.V.m. Art. 83 DS-GVO). Eine Öffnungsklausel in Art. 58 Abs. 6 S. 1 DS-GVO gibt den Mitgliedsstaaten darüber hinaus die Möglichkeit zur Regelung weiterer Befugnisse.[7]

a) Die Verwarnung

Die Verwarnung nach Art. 58 Abs. 2 lit. b) DS-GVO lässt sich als „erste Stufe des datenschutzrechtlichen Sanktionsregimes"[8] und gewissermaßen als „Gelbe Karte" der Aufsichts-

1 Becker, JZ 2017, 170 (173).

2 Vgl. Golla, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, 2015, S. 209 ff. m.w.N.

3 Vgl. insbesondere ErwGr 11 und 13.

4 Vgl. SZ vom 15.12.2015, EU plant hohe Bußgelder bei Datenschutz-Verstößen, online abrufbar unter www.sueddeutsche.de/digital/datenschutz-hohe-bussgelder-fuer-firmen-bei-verstoessen-1.2782319 (zuletzt abgerufen am 17. April 2017).

5 „From 24 May 24 2018 [...] the lack of enforcement in the field of data protection provisions will end.", Albrecht, European Data Protection Law Review 2016, 287.

6 Während die Erwähnung eines Unternehmens in Zusammenhang mit einem Datenschutzverstoß in einem Tätigkeitsbericht „Prangerwirkung" haben kann (Weichert, RDV 2005, 1 (2)), dürfte die zielgerichtete Verwendung des Berichtes als Sanktionsinstrument dessen Hauptfunktion – als Informationsinstrument – widersprechen; vgl. von Lewinski, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, § 26 Rn. 15.

7 Derzeit ist für die geplante Neuregelung des BDSG keine signifikante Ausweitung sanktionierender Befugnisse nach Art. 58 Abs. 6 DS-GVO vorgesehen; vgl. BT-Drs. 18/11235, S. 108.

8 Martini/Wenzel, PinG 2017, 92.

behörden begreifen.[9] Der Sanktionscharakter geht u.a. aus ErwGr 150 S. 7 DS-GVO hervor, der von „andere[n] Sanktionen" im Zusammenhang mit Geldbußen und Verwarnungen spricht. Nach ErwGr 148 S. 2 DS-GVO kann die Verwarnung „[i]m Falle eines geringfügigeren Verstoßes oder falls [eine] voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde" insbesondere als milderes Mittel im Vergleich zu einer Geldbuße ausgesprochen werden. Wann ein Verstoß dabei als geringfügig anzusehen ist, dürfte nach den Kriterien aus Art. 83 Abs. 2 S. 2 DS-GVO zu bewerten sein.[10]

Im Gegensatz zu einer Geldbuße setzt eine Verwarnung lediglich einen objektiven Rechtsverstoß, nicht aber dessen Vorwerfbarkeit voraus.[11] Grundsätzlich umfasst Art. 58 Abs. 2 lit. b) DS-GVO dabei sämtliche Verstöße gegen die Verordnung. Ähnlich wie die formelle Beanstandung eines Datenschutzverstoßes nach § 25 Abs. 1 BDSG[12] entfaltet die Verwarnung keine unmittelbare materielle Rechtsfolge gegenüber der datenverarbeitenden Stelle oder ihrem Adressaten,[13] sondern ist „nur eine negative Beurteilung".[14] Die Verwarnung ist gegenüber der Beanstandung nach BDSG sogar insofern milder, als erstere keine Pflicht zur Stellungnahme des Adressaten zur Folge hat.[15] Insofern lässt sich über den Sanktionscharakter der Verwarnung auch zumindest dann streiten, wenn sie lediglich gegenüber der verantwortlichen Stelle und nicht öffentlich erfolgt.[16] Da die Verwarnung aber jedenfalls eine verbindliche Feststellung bzgl. des Rechtsverstoßes enthält, lässt sie sich als feststellender Verwaltungsakt einordnen.[17] Eine bestimmte Form ist für die Verwarnung nicht vorgegeben; praktisch dürfte sie aber in der Regel schriftlich erfolgen.

Die Anzahl der öffentlich bekannten formellen Beanstandungen von Datenverstößen nach dem BDSG war bislang sehr überschaubar.[18] Es bleibt abzuwarten, ob die Verwarnung gem. Art. 58 Abs. 2 lit. b) DS-GVO gegenüber dieser Praxis an Bedeutung gewinnt.

b) Anweisungen bzgl. der Datenverarbeitung

Durch Anweisungen gem. Art. 58 Abs. 2 lit. c) – e) DS-GVO können Aufsichtsbehörden mittelbar Einfluss auf die Datenverarbeitung nehmen. Hierzu gehört insbesondere die Befugnis gem. Art. 58 Abs. 2 lit. d) DS-GVO, Verantwortliche und Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge in Einklang mit den Vorgaben der DS-GVO zu bringen. Dabei kann die Aufsichtsbehörde auch konkrete Vorgaben machen, wie die Konformität mit der DS-GVO herzustellen ist.

Art. 58 Abs. 2 lit. d) DS-GVO entspricht damit weitgehend der Anordnungsbefugnis nach § 38 Abs. 5 S. 1 BDSG im geltenden Recht.[19] Diese Befugnis gilt zwar zumindest auf dem Papier als wichtig, um den Vollzug der Regelungen des Datenschutzrechts sicherzustellen;[20] in der Praxis aber erwecken die Berichte der Aufsichtsbehörden den Eindruck, dass von den Eingriffsmöglichkeiten nach § 38 Abs. 5 BDSG im Hinblick auf materielle Datenschutzverstöße nur in wenigen Einzelfällen Gebrauch gemacht wird.[21] Dies könnte u.a. mit dem erhöhten Aufwand verbunden sein, den der Erlass eines Verwaltungsaktes für die Aufsichtsbehörden im Vergleich mit informellem Verwaltungshandeln verursacht.

c) Untersagung der Datenverarbeitung

Eine überaus einschneidende Anordnung, die die Aufsichtsbehörden treffen können, ist nach Art. 58 Abs. 2 lit. f) DS-GVO die Beschränkung oder vollständige Untersagung einer Datenverarbeitung.[22] Da Art. 58 Abs. 2 lit. f) DS-GVO keine besonderen Voraussetzungen formuliert, erscheint die Regelung weitergehender als der korrespondierende § 38 Abs. 5 S. 2 BDSG im geltenden Recht, der ausdrücklich einschränkende Voraussetzungen formuliert.[23]

Allerdings dürfte bei der Anwendung von Art. 58 Abs. 2 lit. f) DS-GVO zumindest der Grundsatz der Verhältnismäßigkeit besonders zu beachten sein.[24] In diesem Zusammenhang ist ErwGr 129 S. 5 DS-GVO zu beachten, wonach die Maßnahmen der Aufsichtsbehörden „geeignet, erforderlich und verhältnismäßig sein" sollen, „wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind". Vor der Untersagung eines Datenverarbeitungsvorgangs wird daher vor allem genauestens zu prüfen sein, ob der Verarbeiter nicht

9 Die Warnung nach Art. 58 Abs. 2 lit. a) DS-GVO bezieht sich hingegen auf einen noch nicht erfolgten, erst bevorstehenden Datenschutzverstoß.

10 Martini/Wenzel, PinG 2017, 92 (94).

11 Martini/Wenzel, PinG 2017, 92 (93).

12 § 25 BDSG sieht die Beanstandung gegenüber öffentlichen Stellen vor, entsprechende Regelungen finden sich in den Landesdatenschutzgesetzen. Auch gegenüber privaten Stellen wird die Möglichkeit der Beanstandung allerdings angenommen und hergeleitet „aus der Notwendigkeit einer Abschlussverfügung bei Aufsichtsmaßnahmen, wenn Rechtsverstöße festgestellt werden, die nicht mit den Mitteln des [§ 38 Abs. 5 BDSG] geahndet werden sollen"; Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5. Aufl. 2016, § 38 Rn. 29.

13 Vgl. zu § 25 BDSG Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 25 Rn. 2; zu Art. 58 Abs. 2 lit. a) DS-GVO, Körffer, in: Paal/Pauly, Datenschutz-Grundverordnung, 2. Aufl. 2016, Art. 58 Rn. 18.

14 Schiedemair, in: BeckOK Datenschutzrecht, 19. Ed. 2017, § 25 BDSG Rn. 10; vgl. zu Art. 58 Abs. 2 lit. a) DS-GVO von Lewinski, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, Art. 58 Rn. 24 („Tadel"); Martini/Wenzel, PinG 2017, 92 (93) („Missbilligung").

15 Diese Pflicht ergibt sich im geltenden Recht aus § 25 Abs. 1 S. 1 i.V.m. Abs. 3 BDSG.

16 Golla, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, 2015, S. 205.

17 Martini/Wenzel, PinG 2017, 92 (96). Die Beanstandung ordnet die Rechtsprechung hingegen mangels Regelungswirkung nicht als Verwaltungsakt ein; BVerwG, Beschl. v. 05.02.1992 – 7 B 15/92, CR 1993, 242.

18 Aus ihren Berichten geht hervor, dass die meisten Landesdatenschutzbeauftragten von dem Instrument der Beanstandung – wenn überhaupt – nur vereinzelt Gebrauch machen; Vgl. LfD Baden-Württemberg, Bericht 2010/2011, S. 114, 122, 129; LfDI NRW, Bericht 2011/2012, S. 20; LfDI Rheinland-Pfalz, Bericht 2010/2011, S. 54, 93, 95.

19 Vgl. zu Unterschieden Körffer, in: Paal/Pauly, Datenschutz-Grundverordnung, 2. Aufl. 2016, Art. 58 Rn. 20.

20 Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 38 Rn. 25; Grittmann, in: Taeger/Gabel, BDSG, 2. Aufl. 2013, § 38 Rn. 36.

21 Vgl. Ehmann, ZD 2014, 493 (494).

22 Als besonderen Fall der Untersagung einer Datenverarbeitung regelt Art. 58 Abs. 2 lit. j) DS-GVO die Befugnis, die Aussetzung der Übermittlung von Daten in Drittländer anzuordnen.

23 Insbesondere muss ein schwerwiegender Verstoß oder Mangel vorliegen.

24 Körffer, in: Paal/Pauly, Datenschutz-Grundverordnung, 2. Aufl. 2016, Art. 58 Rn. 23.

durch eigene Maßnahmen die Rechtskonformität der Verarbeitung herstellen kann.

d) Bußgelder

Eine besondere Aufmerksamkeit gebührt den in Art. 83 DS-GVO geregelten Geldbußen. Diese können Aufsichtsbehörden auch neben weiteren Anordnungen nach Art. 58 Abs. 2 DS-GVO verhängen.[25] Hier stellt nicht nur der hohe Bußgeldrahmen von bis zu 20.000.000 Euro oder 4 % des weltweiten Umsatzes des vergangenen Jahres bei Unternehmen ein Novum dar.

Die Regelung intendiert eine tendenziell strengere Verhängung von Geldbußen, als dies bisher praktisch nach dem BDSG und § 47 Abs. 1 OWiG geschehen ist.[26] Insbesondere aus ErwGr. 148 S. 2, wonach „[i]m Falle eines geringfügigeren Verstoßes oder falls [eine] voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, […] anstelle einer Geldbuße eine Verwarnung erteilt werden" kann, scheint sich implizit zu ergeben, dass die Verhängung einer Geldbuße bei einem Datenschutzverstoß der Regelfall sein soll.

Abs. 1 und Abs. 2 regeln konkrete Kriterien für die Verhängung von Geldbußen. Besonders der sehr detaillierte Katalog in Abs. 2, der sich an die kartellrechtliche Praxis der Kommission bei der Verhängung von Bußgeldern anlehnt,[27] ist insofern aufschlussreich. Die Kriterien des Art. 83 Abs. 2 DS-GVO beziehen sich auf den Verstoß selbst (lit. a), b) und g)), das Verhalten des Täters vor dem Verstoß (lit. d), e), i) und j)) sowie das Verhalten nach dem Verstoß (lit. c), f) und h)). Außerdem ermöglicht die Auffangregelung in lit. k), über die ausdrücklich genannten Kriterien hinaus weitere erschwerende oder mildernde Umstände in die Abwägung miteinzubeziehen. Genauere Leitlinien für die Aufsichtsbehörden zur Festsetzung von Geldbußen sollen nach Art. 70 Abs. 1 lit. k) DS-GVO erst ausgearbeitet werden.[28]

Der Adressatenkreis von Art. 83 DS-GVO ist zwar nicht ganz eindeutig geregelt, allerdings legen Abs. 2 lit. d) und Abs. 3 der Vorschrift nahe, dass grundsätzlich nur Verantwortliche (Art. 4 Nr. 7) und Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) als Adressaten in Betracht kommen, soweit nicht andere Adressaten ausdrücklich genannt sind.[29] Damit ist der persönliche Anwendungsbereich der Vorschrift enger als jener von § 43 BDSG. Insbesondere sind Mitarbeiter von verantwortlichen Stellen nicht umfasst.

Das Spektrum der mit Bußgeld bedrohten Datenschutzverstöße nach Art. 83 Abs. 4 – Abs. 6 DS-GVO ist noch weiter als nach § 43 BDSG. Die Regelung bezieht Verstöße gegen beinahe 50 Normen mit ein. Noch größer als bei § 43 BDSG[30] ist im Zusammenhang mit Art. 83 DS-GVO die Problematik der mangelnden Bestimmtheit der Normen.[31] Die von den Bußgeldtatbeständen in Bezug genommenen Verhaltensnormen weisen zum Teil Unklarheiten auf, aufgrund derer etwa ihre Adressaten nicht bestimmt werden können und auch unklar bleibt, welches Verhalten im Einzelnen verboten und damit bußgeldbedroht ist. Dies betrifft unter anderem mögliche Verstöße gegen den Werbedatenschutz.

Es ist davon auszugehen, dass in der Praxis Art. 83 Abs. 5 lit. a) DS-GVO – nicht nur im Bereich der Werbung – zu dem zentralen Bußgeldtatbestand bei materiellen Datenschutzverstößen werden wird. Die Vorschrift erfasst Verstöße gegen „die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9" und ist damit das Pendant zu § 43 Abs. 2 Nr. 1 BDSG im geltenden Recht. Die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten beurteilt sich nach Art. 6 DS-GVO, der mehrere Erlaubnistatbestände zur Verarbeitung personenbezogener Daten vorsieht.

Hierbei könnte Art. 6 Abs. 1 lit. f) DS-GVO zum „zentralen Erlaubnistatbestand für die Datenverarbeitung im werbewirtschaftlichen Bereich"[32] werden. Diese Vorschrift bringt allerdings eine große Rechtsunsicherheit mit sich, die sich vor allem im Bußgeldbereich verheerend auswirken könnte.[33] Nach Art. 6 Abs. 1 lit. f) DS-GVO kommt es für die Beurteilung der Rechtmäßigkeit einer Datenverarbeitung entscheidend auf eine Abwägung zwischen den Interessen des Verantwortlichen und des Betroffenen an. Zwar kann nach ErwGr 47 S. 7 DS-GVO „[d]ie Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung […] als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden." Erstens ist jedoch schon unklar, welche Maßnahmen von dem Begriff der Direktwerbung umfasst sind.[34] Hiervon „jedwede Datenverarbeitung im Sinne von Art. 4 Nr. 2 zu werblichen Zwecken"[35] als umfasst zu sehen erscheint zumindest als riskant, da der Zusatz „Direkt-" insbesondere auf personalisierte Ansprachen zu zielen scheint.[36] Zweitens sagt die Anerkennung eines berechtigten Interesses an der Direktwerbung noch nichts über Interessen auf Betroffenenseite aus, die der Rechtmäßigkeit dieser Datenverarbeitung entgegenstehen können.[37] Auch die Beantwortung der Frage, welche entgegenstehenden Interessen hierbei zu berücksichtigen sind, wirft Schwierigkeiten auf. So bleibt unklar, ob bei den entgegenstehenden Interessen im Rahmen der DS-GVO auch die wettbewerbsrechtliche Zulässigkeit berücksichtigt werden kann.[38]

25 Vgl. Art. 58 Abs. 2 lit. i) DS-GVO.

26 Golla, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, Art. 83 Rn. 4.

27 Vgl. Leitlinien für das Verfahren zur Festsetzung von Geldbußen gemäß Artikel 23 Absatz 2 Buchstabe a) der Verordnung (EG) Nr. 1/2003, Ziffern 27 ff.

28 Rost, RDV 2017, 13 (19).

29 Golla, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, Art. 83 Rn. 3.

30 Vgl. hierzu von Lewinski, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, Vor. zu § 43 BDSG Rn. 7 ff.

31 Diese Problematik wird auch von Seiten der Aufsichtsbehörden gesehen; vgl. Rost, RDV 2017, 13 (15).

32 Tavanti, RDV 2016, 295 (296); vgl. auch Schulz, in: Gola, DS-GVO, 2017, Art. 6 Rn. 62 f.

33 Vgl. Kring/Marosi, K&R 2016, 773, 776.

34 Piltz, K&R 2016, 557 (565).

35 Tavanti, RDV 2016, 295 (297).

36 Piltz, K&R 2016, 557 (565).

37 Vgl. Tavanti, RDV 2016, 295 (297).

38 Dagegen Schulz, in: Gola, DS-GVO, 2017, Art. 6 Rn. 67; Tavanti, RDV 2016, 295 (298).

Die Verhängung eines Bußgeldes erfordert im Übrigen ein Verschulden des Verantwortlichen bzw. des Auftragsverarbeiters.[39] Dies setzt schon das auch im Unionsrecht verankerte Schuldprinzip voraus.[40]

In der Rechtsfolge drohen Geldbußen von bis zu 20.000.000 Euro oder 4 % des weltweiten Umsatzes des vergangenen Jahres bei Unternehmen. Umstritten ist die praktisch überaus relevante Frage, wie der Begriff des Unternehmens zu verstehen ist – im Sinne von Art. 4 Nr. 18 DS-GVO (als eine natürliche oder juristische Person) oder Art. 101, 102 AEUV (funktional, im Sinne einer eine wirtschaftliche Tätigkeit ausübenden Einheit, die auch aus mehreren Personen bestehen kann).[41] Hierbei scheint sich – vor allem bei den Aufsichtsbehörden[42] – das funktionale Verständnis durchzusetzen.[43] Dies entspricht auch dem eindeutigen Willen des Verordnungsgebers, der in ErwGr 150 S. 3 zum Ausdruck kommt.

2. Die Wettbewerbsaufsicht durch das Bundeskartellamt

An Fahrt gewonnen hat zuletzt die Diskussion um die Frage, ob auch die Kartellaufsicht bei bestimmten Datenschutzverstößen einschreiten kann.[44] Anstoß hierfür gab die Eröffnung eines Verfahrens durch das Bundeskartellamt gegen Facebook wegen Verdachts auf Marktmachtmissbrauch durch Datenschutzverstöße.[45] Ein Kartellverfahren kann zu Verfügungen mit Sanktionswirkung gem. §§ 32 ff. GWB sowie Bußgeldern führen.

Als möglicher Marktmissbrauch in Form eines Konditionenmissbrauchs gem. § 19 Abs. 1, Abs. 2 Nr. 2 GWB durch Facebook steht dabei die Ausgestaltung der Vertragsbestimmungen zur Verwendung von Nutzerdaten im Raum. So besteht laut Bundeskartellamt der Verdacht, dass Facebook eine marktbeherrschende Stellung missbraucht, um von seinen Kunden durch (datenschutz-)rechtswidrige Einwilligungserklärungen Daten zu erlangen, die letztlich zu Werbezwecken verwendet werden. Hierbei sind allerdings bereits grundlegende Fragen unklar, die nicht spezifisch datenschutzrechtlich sind – so etwa die Bestimmung eines möglichen Marktes und dessen Beherrschung durch Facebook.[46]

Der Ausgang des Verfahrens ist bislang noch nicht abzusehen. Den Neuerungen durch die DS-GVO gegenüber dem BDSG dürfte in diesem Verfahren und der kartellrechtlichen Sanktionierung aber keine entscheidende Bedeutung zukommen. Mit der immer größeren Rolle, die (personenbezogene) Daten in der digitalen Ökonomie spielen, dürfte sich aber die Frage nach der Bedeutung von Datenschutzverstößen im Kartellrecht künftig vermehrt stellen. Diese Entwicklung ist ebenso im Auge zu behalten wie die Fortentwicklung des Kartellrechts für digitale Märkte[47] und die Frage nach dem künftigen Verhältnis von Datenschutz- und Kartellaufsicht.[48]

III. Strafrechtliche Konsequenzen

Die DS-GVO harmonisiert die Strafbarkeit von Datenschutzverstößen nicht.[49] Art. 84 DS-GVO lässt den Mitgliedsstaaten bei der Regelung solcher Sanktionen, die nicht schon in Kapitel VIII DS-GVO geregelt sind, einen weiten Spielraum. Darunter fällt auch die Möglichkeit strafrechtlicher Sanktionen, auf die ErwGr 149 DS-GVO näher eingeht.

Vor diesem Hintergrund haben die Regelungen der DS-GVO auf das Datenschutzstrafrecht nur mittelbare Auswirkungen. Es ist davon auszugehen, dass der Gesetzgeber ähnlich dem bisherigen § 44 Abs. 1 BDSG in der Neufassung des BDSG eine Strafnorm vorsehen wird, die zu weiten Teilen implizit auf Verhaltensnormen der DS-GVO verweist. Während §§ 44 Abs. 1 i.V.m. 43 Abs. 2 BDSG die Verhaltensnormen des BDSG durch das Merkmal „unbefugt" in den Tatbestand einbeziehen, geschieht dies bezüglich der DS-GVO in § 42 BDSG-neu in der Fassung des aktuellen Regierungsentwurfs[51] durch das Merkmal „ohne hierzu berechtigt zu sein".

Neue Probleme entstehen hier vor allem mit Blick auf das strafrechtliche Bestimmtheitsgebot aus Art. 103 Abs. 2 GG. Dass die Auslegung der nationalen Strafnorm im Wesentlichen anhand der Regelungen der DS-GVO zu erfolgen haben wird, führt für Normadressaten zu zusätzlichen Schwierigkeiten. Schon aus dem Tatbestand wird nicht klar, dass die maßgeblichen Verbote vor allem aus dem Unionsrecht folgen könnten.[52] Zudem entstehen durch die DS-GVO – wie bereits erwähnt – verstärkt normative Unklarheiten. Naturgemäß wird auch die Klärung unbestimmter Rechtsbegriffe durch die Rechtsprechung des EuGH und die Bereitstellung

39 So auch Becker, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 83 Rn. 11; Piltz, K&R 2017 85 (92); a.A. Härting, Datenschutz-Grundverordnung, 2016, Rn. 253.

40 Ferner legt Art. 83 Abs. 3 DS-GVO dies nahe; vgl. Golla, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017 Art. 83 Rn. 9.

41 Vgl. Faust/Spittka/Wybitul, ZD 2016, 120 ff.; Gola, K&R 2017, 145 (146 f.); Piltz, K&R 2017 85 (92).

42 Bayerisches Landesamt für Datenschutzaufsicht, Sanktionen nach der DS-GVO, abrufbar unter https://www.lda.bayern.de/media/baylda_ds-gvo_7_sanctions.pdf (zuletzt abgerufen am 17. April 2017); LfDI Berlin, Bericht 2016, S. 32; Rost, RDV 2017, 13 (15 ff.); Schönefeld/Thomé, PinG 2017, 126 (127).

43 Dieterich, ZD 2016, 260 (264); Becker, in: Plath, BDSG/DSGVO, 2. Aufl. 2016; Art. 83 Rn. 23; Golla, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, Art. 83 Rn. 25 f.

44 Podszun/de Toma, NJW 2016, 2987 (2992 ff.); Rempe, K&R 2017, 149 ff.; Telle, WRP 2016, 814 ff.; Wiedmann/Jäger, K&R 2016, 217 ff.

45 Bundeskartellamt, Meldung vom 2. März 2016, abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html (zuletzt abgerufen am 17. April 2017).

46 Vgl. Rempe, K&R 2017 149 (150 ff.).

47 Vgl. die 9. GWB-Novelle (BT-Drs. 18/10207), der der Bundesrat am 31. März 2017 zugestimmt hat (BR-Drs. 207/17 (B)), womit diese voraussichtlich in nächster Zeit in Kraft treten wird.

48 Dazu Kieck, PinG 2017, 37 ff.; vgl. auch Podszun/de Toma, NJW 2016, 2987 (2994).

49 Eine Harmonisierung des Datenschutzstrafrechts wäre durch das Regelungsinstrument der Verordnung auch nicht zulässig gewesen. Die für den Bereich des Datenschutzes in Betracht kommenden strafrechtlichen Regelungskompetenzen aus Art. 83 Abs. 1 und 2 AEUV beschränken sich auf den Erlass von Richtlinien.

50 Golla, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, Art. 84 Rn. 1 f.

51 BT-Drs. 18/11325.

52 Eine ähnliche Regelungstechnik verwendet im geltenden Recht u.a. § 326 Abs. 2 Nr. 2 StGB. Demnach macht sich strafbar, wer bestimmte Abfälle „entgegen einem Verbot oder ohne die erforderliche Genehmigung in den, aus dem oder durch den Geltungsbereich [des StGB] verbringt." Als Verbote sind hierbei Einfuhr- und Ausfuhrverbote für Abfall einschlägig, die sich aus EU-Verordnungen ergeben. Für den Normadressaten wird dies aus der Lektüre von § 326 Abs. 2 Nr. 2 StGB nicht klar. Aus diesem Grunde wird diese Vorschrift zu Recht kritisiert; vgl. Heger, in: Böse, Europäisches Strafrecht, 2013, § 5 Rn. 79.

von Auslegungshilfen durch den Europäischen Datenschutzausschuss mehr Zeit in Anspruch nehmen als vergleichbare Prozesse auf nationaler Ebene.

Daneben bietet die DS-GVO auch Stoff für eine weitere Diskussion im Datenschutzstrafrecht. Seit der Entscheidung Berliner Stadtreinigung II[53], in der der BGH die Garantenstellung eines Compliance-Officers bejahte, wird verstärkt die Frage gestellt, ob und inwiefern bei Datenschutzverstößen eine strafrechtliche Verantwortlichkeit des betrieblichen Datenschutzbeauftragten wegen Unterlassens angenommen werden kann.[54] Hier deutet die Beschreibung der Aufgaben des Datenschutzbeauftragten in Art. 39 Abs. 1 lit. b) DS-GVO, der von einer Überwachung der Einhaltung der Verordnung spricht, zwar verstärkt auf eine Garantenstellung hin.[55] Mangels einer Rechtsprechungspraxis zu der Frage bleiben die Konsequenzen dieser Neuerung aber im Ergebnis unklar.

IV. Zivilrechtliche Ansprüche von Privatpersonen

Darüber hinaus können sich Datenverarbeiter bei Verstößen gegen die Vorgaben der DS-GVO zum Werbedatenschutz zivilrechtlichen Ansprüchen ausgesetzt sehen.[56] Diese können zunächst direkt von den Betroffenen ausgehen, die wegen der rechtswidrigen Verarbeitung personenbezogener Daten Schadensersatz oder Unterlassung verlangen können. Nach geltendem Recht können sich Unterlassungsansprüche aus § 1004 BGB analog und § 7 BDSG sowie Schadensersatzansprüche vor allem aus §§ 7, 8 BDSG und § 823 Abs. 2 BGB ergeben.[57] Praktisch sind diese Schadensersatzansprüche wegen Datenschutzverstößen nur von geringer Bedeutung.[58]

Art. 82 DS-GVO regelt das Recht auf Schadensersatz grundlegend neu und wird mit Anwendungsbeginn der DS-GVO als eigene Anspruchsgrundlage zur Anwendung kommen.[59] Der Anspruch steht bei einer rechtswidrigen Datenverarbeitung nur den nach der DS-GVO betroffenen Datensubjekten zu, nicht aber beispielsweise Wettbewerbern.[60] Er richtet sich gegen Verantwortliche und Auftragsverarbeiter. Tatbestandlich kann dabei grundsätzlich jeder Verstoß gegen die DS-GVO einen Schadensersatzanspruch auslösen.[61] Die Haftung ist nur dann ausgeschlossen, wenn der Verantwortliche oder Auftragsverarbeiter „nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist."[62]

Während die h.M. dies im Zusammenhang mit § 7 BDSG noch ablehnte,[63] umfasst Art. 82 DS-GVO ausdrücklich auch den Ersatz immaterieller Schäden. Der Begriff des Schadens in Art. 82 DS-GVO ist weit zu verstehen, wie auch ErwGr 146 S. 3 nahelegt. Dies entspricht dem Ziel der Verordnung, eine wirksame Sanktionierung von Datenschutzverstößen zu erreichen.[64] Mit Art. 82 DS-GVO wird im Ergebnis die Position von Betroffenen, die Schadensersatzansprüche wegen Datenschutzverstößen geltend machen, gestärkt. Ob dies zu einer erhöhten Relevanz der Vorschrift gegenüber § 7 BDSG führt, erscheint noch offen.[65] Eher zweifelhaft erscheint, ob die vorgenommenen Änderungen das grundsätzliche Phänomen der „rationalen Apathie"[66] jener Betroffenen ausgleichen können, denen durch die Verfolgung eines Datenschutzverstoßes nach eigener Einschätzung mehr Aufwand zu entstehen scheint als sie daraus Nutzen ziehen können.

V. Durchsetzung durch Verbraucherverbände

Bei der zivilrechtlichen Durchsetzung des Datenschutzrechts spielen auch die Verbraucherverbände eine wichtige Rolle. Diese können nicht nur Betroffene in Zivilprozessen vertreten,[67] sondern auch – möglicherweise weniger von einer „rationalen Apathie" befallen – eigenständig klagen.

Nach § 8 Abs. 3 Nr. 3 UWG sind sie berechtigt, Beseitigungs- und Unterlassungsansprüche bei nach §§ 3 und 7 UWG unzulässigen geschäftlichen Handlungen geltend zu machen. Welche Verstöße gegen das Datenschutzrecht im Werbebereich unzulässige geschäftliche Handlungen sind, ist allerdings unklar. Ein Verstoß gegen Vorschriften des Datenschutzrechts ist als Verstoß gegen § 3a UWG anzusehen, soweit man diese als dazu bestimmt einordnet, „im Interesse der Marktteilnehmer das Marktverhalten zu regeln." Zum Teil wird eine solche Bestimmung der Vorschriften des Datenschutzrechts gänzlich abgelehnt, zum Teil zumindest in Bezug auf einzelne Vorschriften angenommen.[68] Es zeichnet sich aber die Tendenz ab, dass zumindest Regelungen des Werbedatenschutzes wie etwa § 28 Abs. 3 BDSG als zur Regelung des Marktverhaltens bestimmt angesehen werden,[69] da der „Umgang mit Daten in einer datengetriebenen Marketingökonomie [...] integraler Bestandteil des Werbens"[70] ist.

53 BGH, Urt. v. 17.07.2009 – 5 StR 394/08, NJW 2009, 3173 ff.

54 Vgl. Barton, RDV 2010, 247 ff.; Bongers/Krupna, ZD 2013, 594 (597 f.); Marschall, ZD 2014, 66 ff. sowie ausführlich Hantschel, Die strafrechtliche Unterlassungsverantwortlichkeit eines betrieblichen Datenschutzbeauftragten, 2015.

55 Vgl. Nolde, PinG 2017, 114 (119).

56 Vgl. zu vertraglichen und deliktischen Schadensersatzansprüchen gegen betriebliche Datenschutzbeauftragte, für die § 7 BDSG und Art. 82 DS-GVO keine Anwendung finden, Bongers/Krupna, ZD 2013, 594 (595 ff.).

57 Weitere Schadensersatzansprüche wegen Datenschutzverstößen kommen einerseits im vertraglichen und vorvertraglichen Bereich nach § 280 BGB, andererseits deliktsrechtlich etwa nach den §§ 823 Abs. 1, 826 und 839 BGB in Betracht; vgl. Eßer, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, § 7 Rn. 29 ff.; Niedermeier/Schröcker, RDV 2002, 217 (219).

58 Vgl. Eßer, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, § 7 Rn. 3; von Lewinski, PinG 2013, 12 (14).

59 Eßer, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, Art. 82 Rn. 1.

60 Frenzel, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 82 Rn. 7.

61 Piltz, K&R 2017, 85 (91).

62 Die Einordnung als Gefährdungshaftung oder verschuldensabhängige Haftung mit vermutetem Verschulden ist hierbei streitig; vgl. Bergt, in: Kühling/Buchner, DS-GVO, 2017, Art. 82 Rn. 51 m.w.N.

63 BGH, Urt. v. 29.11.2016 – VI ZR 530/15, NJW 2017, 800 ff.; OLG Zweibrücken, Urt. v. 21.02.2013 – 6 U 21/12, BeckRS 2013, 03840; Eßer, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, § 7 Rn. 24; Gola/Piltz, RDV 2015, 279 (280); Simitis, in: Simitis, BDSG, 8. Aufl. 2014, § 7 Rn. 32 m.w.N.; a.A. Niedermeier/Schröcker, RDV 2002, 217 (224).

64 Vgl. Frenzel, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 82 Rn. 10.

65 Eßer, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017 Art. 82 Rn. 3.

66 Von Lewinski, PinG 2013, 12.

67 Vgl. § 79 Abs. 2 S. 2 Nr. 3 ZPO.

68 Vgl. Forgó, in: BeckOK Datenschutzrecht, 19 Ed. 2017, Grundlagen und bereichsspezifischer Datenschutz, Werbung Rn. 98 f.; Podszun/de Toma, NJW 2016, 2987 (2989 f.).

Dazu sind Verbraucherverbände seit der am 24. Februar 2016 in Kraft getretenen Reform des UKlaG[71] als anspruchsberechtigte Stellen gem. § 3 Abs. 1 Nr. 1 UKlaG befugt, bei Verstößen gegen diverse Datenschutzvorschriften gem. § 2 Abs. 1, Abs. 2 Nr. 11 UKlaG auf Unterlassung und Beseitigung zu klagen.[72] Diese Klagebefugnis gilt insbesondere bei der Erhebung, Verarbeitung und Nutzung von Daten für Zwecke der Werbung.[73] Die neue Befugnis der Verbraucherverbände hat zwar nicht zu einer „Klagewelle" geführt,[74] wohl aber zu einzelnen Verfahren.[75]

Mit der DS-GVO ändert sich die Rolle der Verbraucherverbände nicht grundlegend.[76] Insbesondere bleibt es bei deren Klagebefugnissen nach nationalem Recht.[77] Die DS-GVO lässt dem mitgliedsstaatlichen Gesetzgeber insofern einen weiten Spielraum. Nach Art. 80 Abs. 2 DS-GVO können Mitgliedstaaten Einrichtungen, Organisationen oder bestimmten Vereinigungen[78] das Recht einräumen, Beschwerden bei den Datenschutzaufsichtsbehörden einzulegen und die in Art. 78 und 79 DS-GVO aufgeführten Rechte in Anspruch zu nehmen, wenn die Rechte eines Betroffenen nach ihrer Ansicht verletzt worden sind. Dies deckt die im UKlaG geschaffene Verbandsklagebefugnis ab.[79]

VI. Fazit: Die Praxis muss es zeigen

Das Instrumentarium zur Sanktionierung von Datenschutzverstößen verändert sich mit der DS-GVO vor allem durch die Neuregelung der Bußgelder in Art. 83 DS-GVO erheblich. Andere Regelungen mit Sanktionsbezug wie die Anordnungsbefugnisse des Art. 58 Abs. 2 DS-GVO und der Anspruch auf Schadensersatz nach Art. 82 DS-GVO erfahren vergleichsweise geringe Veränderungen zum geltenden Recht, die aber die Position von Aufsichtsbehörden und Betroffenen (zumindest auf dem Papier) durchaus stärken.

Vor allem mit Blick auf die Bußgeldregelung wird die Rechtsunsicherheit bei Beurteilung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten nicht nur der Werbebranche noch einiges Kopfzerbrechen bereiten. Wenn Art. 6 Abs. 1 f) DS-GVO als zentrale Grundlage für die Verarbeitung personenbezogener Daten zu Werbezwecken dienen soll, ist die weitere Konkretisierung der Voraussetzungen etwa durch die Rechtsprechung oder zumindest durch Hinweise von den Aufsichtsbehörden dringend notwendig.

Ob mit Geltung der DS-GVO deutlich mehr Bußgelder verhängt werden und ob diese deutlich höher ausfallen als bisher, bleibt mit Spannung abzuwarten.[80] In den letzten Jahren hat die Verhängung von Bußgeldern auf Grundlage des BDSG zugenommen.[81] Auch die Datenverarbeitung zu Werbezwecken geriet dabei ein ums andere Mal in das Visier der Aufsichtsbehörden.[82] Die künftige Entwicklung hängt auch davon ab, mit welchem Ergebnis Koordinationsprozesse zwischen den zuständigen Aufsichtsbehörden verlaufen.[83] Aufgrund der begrenzten personellen Ausstattung der Aufsichtsbehörden dürfte es jedenfalls unrealistisch sein, dass die Aufsichtsbehörden sämtliche Datenschutzverstöße, die ihnen zur Kenntnis gelangen, mit Bußgeldern sanktionieren.[84] Auch ob die Obergrenzen der Sanktionen ausgereizt werden, ist ohne Spekulation kaum vorherzusagen. Bei den umsatzbezogenen Geldbußen im Kartellrecht jedenfalls hat die Kommission den oberen Rahmen bislang nicht ausgereizt. Insofern erscheint es zumindest unwahrscheinlich, dass Geldbußen im zweistelligen Millionenbereich für Datenschutzverstöße bald an der Tagesordnung sein werden.

Ob die DS-GVO also tatsächlich zu einer „Revolution" bei der Durchsetzung und Sanktionierung im Datenschutz recht führen wird, bleibt abzuwarten. Mit Blick auf die grundlegenden Ursachen der bestehenden Defizite bei

69 Vgl. Podszun/de Toma, NJW 2016, 2987 (2991) („wohl weitgehender Konsens, dass Datenschutzregelungen, die sich explizit auf Werbung beziehen, als Marktverhaltensregelungen anzusehen sind"); Schwichtenberg, PinG 2017, 104 (105) jeweils m.w.N. aus der Rechtsprechung.

70 Podszun/de Toma, NJW 2016, 2987 (2991).

71 Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts vom 7. Februar 2016, BGBl. I, S. 233.

72 Vgl. hierzu Halfmeier, NJW 2016, 1126 ff.; Ritter/Schwichtenberg, VuR 2016, 96 ff.; Schulz, ZD 2014, 510 ff.

73 Umfasst sind gem. § 2 Abs. 2 Nr. 11 UKlaG Verstöße gegen solche Vorschriften, die die Zulässigkeit „der Erhebung personenbezogener Daten eines Verbrauchers durch einen Unternehmer oder der Verarbeitung oder der Nutzung personenbezogener Daten, die über einen Verbraucher erhoben wurden, durch einen Unternehmer" regeln, „wenn die Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden".

74 Weichert, Verbraucherverbandsklage bei Datenschutzverstößen, 2017, S. 15 (abrufbar unter http://www.netzwerk-datenschutzexpertise.de/dokument/verbandsklagerecht-datenschutz, zuletzt abgerufen am 17. April 2017).

75 So führt beispielsweise die Verbraucherzentrale Sachsen nach eigenen Angaben derzeit drei Verfahren auf Grundlage von § 2 Abs. 2 Nr. 11 UKlaG; vgl. Tweet von Katja Henschler (Verbraucherzentrale Sachsen) vom 22. März 2017 http://tinyurl.com/n4csdm9 (zuletzt abgerufen am 17. April 2017).

76 Schwichtenberg, PinG 2017, 104 (106).

77 Härting, Datenschutz-Grundverordnung, 2016, Rn. 246.

78 Hiervon umfasst ist gem. Art. 80 Abs. 1 DS-GVO jede Vereinigung „ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist". Hierunter fallen typischerweise auch Verbraucherverbände; Becker, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 80 Rn. 2.

79 Vgl. Halfmeier, NJW 2016, 1126 (1129).

80 Die Aufsichtsbehörden beginnen hier erst, sich zu positionieren. Deutlich machte ihre Position etwa bereits die Berliner Datenschutzbehörde in ihrem Tätigkeitsbericht 2016 (S. 34): „Unsere Bußgeldpraxis wird sich durch die neuen Bestimmungen deutlich ändern. Insbesondere müssen Unternehmen bei Verstößen gegen die DS-GVO mit erheblich höheren Bußgeldern rechnen."

81 Von Lewinski, in: Auernhammer, DSGVO BDSG, 5. Aufl. 2017, Vor. zu § 43 BDSG Rn. 2; Weiß, PinG 2017, 97 (99).

82 Vgl. etwa LfD Bremen, Bericht 2014, S. 88; ULD Schleswig-Holstein, Bericht 2010, S. 94; LfDI Berlin, Bericht 2016, S. 156.

83 Ähnlich Piltz, K&R 2017, 85 (93).

84 Nach Spindler, ZD 2016, 114 „kann es nicht verwundern, dass Aufsichtsbehörden mit nicht mehr als 50-100 Personen allenfalls punktuell und auf Beschwerden hin tätig werden können; eine flächendeckende Überwachung ist hier nicht zu erwarten und kann von den Behörden im Rahmen ihres Budgetrahmens nicht geleistet werden, außer man möchte Mammutaufsichtsbehörden einrichten."

der Durchsetzung des Datenschutzrechts erscheint dies zumindest zweifelhaft. Während es auch nach geltendem Recht an Sanktionsnormen nicht mangelt, dürfte neben der Ausstattung der Aufsichtsbehörden und einem geringen Interesse der Betroffenen auch die Unbestimmtheit der Normen ursächlich für die defizitäre Durchsetzung sein. Diese Ursachen werden jedoch durch die Geltung der DS-GVO nicht beseitigt.

Dr. Sebastian J. Golla
Der Autor ist wissenschaftlicher Mitarbeiter an der Johannes Gutenberg-Universität Mainz.

Kurzbeiträge

Datenschutzrechtliche Aspekte des „neuen" § 203 StGB

Rechtsanwalt Dr. Georg Wronka, Bonn*

I. Vorbemerkung

§ 203 StGB begründet die Strafbarkeit für das unbefugte Offenbaren fremder Geheimnisse durch bestimmte, im Einzelnen bezeichnete Personen wie etwa Ärzte, Rechtsanwälte, Notare, Apotheker, Psychologen oder betriebliche Datenschutzbeauftragte. Zwischen der Strafrechtsnorm und dem Datenschutzrecht besteht eine enge Verbindung. Deutlich wird dies z.B. in § 203 Abs. 2 Satz 2 StGB, der eine Gleichstellung von personenbezogenen Daten, wie sie in § 3 Abs. 1 BDSG definiert sind, mit einem Geheimnis nach § 203 Abs. 1 StGB vorsieht. So wird denn auch das durch § 203 StGB primär geschützte Rechtsgut in den Verfassungsnormen der Art. 1 und 2 GG verortet, also der gleichen Quelle, aus der sich auch das Datenschutzrecht ableitet[1]. Daran ändert die geplante und als Regierungsentwurf unlängst auf den parlamentarischen Beratungsweg gebrachte Änderung der Bestimmung nichts[2]. Mit ihr sollen – das ist der Kern der neuen Regelung – die Möglichkeiten der schweigepflichtigen Personen erweitert werden, sich im Rahmen ihrer Berufstätigkeit der Unterstützung externer Personen zu bedienen, ohne strafrechtliche Risiken einzugehen. Dieses Ziel soll namentlich durch einen neu gefassten § 203 Abs. 3 StGB erreicht werden[3].

Der neuen Bestimmung zufolge wird der „Kreis der Wissenden oder zum Wissen Berufenen"[4] um den eigentlichen Geheimnisträger gesetzlich definiert und erweitert und gleichzeitig gegenüber den „berufsmäßig tätigen Gehilfen" – also den in der Praxis, Kanzlei usw. tätigen Mitarbeitern des Berufsgeheimnisträgers – abgegrenzt. Während der dem internen Personal eröffnete Zugriff auf die geheimhaltungsbedürftigen Tatsachen tatbestandlich kein „Offenbaren" sein soll, stellt ihre Bekanntgabe an solche Externe, die an der beruflichen Tätigkeit des Schweigepflichtigen „mitwirken", sehr wohl ein „Offenbaren" dar, dieses wird aber nicht als unbefugt, also nicht rechtswidrig angesehen[5].

Ausweislich der Begründung soll der Schweigepflichtige durch die Ausweitung des „geschlossenen Geheimnisträgerkreises"[6] ermächtigt werden, straflos etwa auf informationstechnische Anlagen und Systeme zur externen Speicherung von Daten durch darauf spezialisierte Unternehmen – expli-

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

1 „Ihre verfassungsrechtliche Legitimation bezieht die Vorschrift aus Art. 2 I i.V.m. 1 I GG", Lackner/Kühl, StGB, 26. Aufl., § 203 Rn. 1; zur Diskussion differenzierender Ansätze vgl. Lenckner, in: Schönke/Schröder, Strafgesetzbuch, 27. Aufl., § 203 Rn. 5.

2 „Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen", BR-Drucks. 163/17 vom 17.02.2017. Es handelt sich bei der Gesetzesvorlage um ein Artikelgesetz, das mit der gleichen Zielsetzung neben Änderungen des StGB auch solche der BRAO, BNotO, PatAnwO und anderer Gesetze vorsieht.

3 Die künftige Fassung soll lauten (gekürzt):
„Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; …"

4 RegE Begründung, A. Allgemeiner Teil, Abschnitt I 1a.

5 RegE Begründung, A. Allgemeiner Teil, Abschnitt II 1c.

6 RegE Begründung, A. Allgemeiner Teil, Abschnitt I 1a.

zit angesprochen wird die Speicherung in einer Cloud – zugreifen zu können. Zu den beispielhaft („insbesondere") aufgeführten Fällen[7] gehören weiterhin neben dem mit der Einrichtung, dem Betrieb und der Wartung von IT-Anlagen befassten Personenkreis u.a. externe Schreibdienste, die Aktenvernichtung, die Durchführung von Buchführungsarbeiten oder das Rechnungswesen.

Aus datenschutzrechtlicher Perspektive stehen zwei Fragen im Vordergrund:

- Reflektiert die strafrechtliche Regelung eine datenschutzrechtlich erfasste Datenumgangsform und ggf. welche?
- Welches Zulässigkeitsregime ist zu beachten? Geht von § 203 Abs. 3 StGB (neu) eine das BDSG verdrängende Wirkung aus und in welchem Umfang?

II. Offenbaren von Geheimnissen als Datenweitergabe

Geheimnisse sind solche Tatsachen, die nur einem Einzelnen oder einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung der Geschützte ein subjektives Interesse hat[8] oder haben könnte[9]. Offenbart wird eine geheimhaltungsbedürftige Tatsache, wenn sie einem Dritten mitgeteilt wird, der sie zuvor noch nicht oder nicht sicher kannte[10], bzw. wenn sie „in irgendeiner Weise an einen anderen gelangt ist".[11] Ob der andere sie auch tatsächlich zur Kenntnis nimmt oder nur die Möglichkeit der Kenntnisnahme erhält, weil sie ungehindert seinem Zugriff ausgesetzt wird, ist dabei nach wohl h.M. irrelevant[12]. Durch den gleichen Inhalt definiert sich auch der Begriff des Bekanntgebens durch Weitergeben einer (personenbezogenen) Information gem. § 3 Abs. 4 Satz 2 Nr. 3a BDSG[13], d.h. dass das strafrechtliche Offenbaren und die datenschutzrechtliche Weitergabe eine identische Bedeutung haben.

Die Feststellung eines Weitergabe-Tatbestands trifft allerdings noch keine Aussage über die datenschutzrechtliche „Qualität" des Empfängers, die darüber entscheidet, ob dieser als „Dritter" oder als Auftragsdatenverarbeiter einzustufen ist (§ 3 Abs. 8 BDSG).

Betrachtet man unter diesem Gesichtspunkt den Katalog der Beispiele in der Begründung zum § 203 StGB-Änderungsgesetz, die von der vorgesehenen Fassung des dritten Absatzes (Satz 2) erfasst werden sollen, erscheint der Geheimnis-Empfängerkreis nicht so ohne weiteres einordenbar. Nach den Erläuterungen soll es sich um solche Stellen handeln, die zwar nicht „in die Sphäre des Berufsgeheimnisträgers eingegliedert" sind, gleichwohl in seine Tätigkeit „in irgendeiner Weise eingebunden werden". Bestimmte Aufgaben, die von ihnen wahrgenommen werden, dürften wohl in aller Regel nach Maßgabe der Auftragsdatenverarbeitung erledigt werden; dazu gehören etwa die Aktenvernichtung, der externe Schreib- und Telefondienst (Call-Center) oder die Inanspruchnahme externer IT-Dienstleistungen (vgl. auch § 11 Abs. 5 BDSG). Wenn aber im gleichen Zug auch das „Rechnungswesen" und die „Mitwirkung an der Erfüllung von Buchführungs- und steuerrechtlichen Pflichten des Berufsgeheimnisträgers" genannt werden[14], mag durchaus zweifelhaft sein, ob diese Stellen nicht als Dritte angesehen werden müssen, die selbst unmittelbar datenschutzrechtlich verantwortlich sind (Stichwort: Funktionsübertragung).

Ein Datentransfer in die eine wie die andere Empfängerkategorie steht in jedem Fall unter dem „Verbot mit Erlaubnisvorbehalt" (§ 4 Abs. 1 BDSG) – im Fall der Weitergabe an einen Dritten in der Verarbeitungsform der Übermittlung, bei einer Auftragsdatenverarbeitung als Datennutzung[15]. Erforderlich ist m.a.W. in beiden Fällen eine datenschutzrechtliche Legitimationsnorm. Sie ergibt sich möglicherweise nicht zwangsläufig und vor allem nicht abschließend aus der strafrechtlichen Weitergabebefugnis; vgl. dazu nachfolgend.

III. § 203 Abs. 3 StGB (neu) als vorrangige Rechtsvorschrift i.S. von § 1 Abs. 3 BDSG

Mit der Frage, auf welche Rechtsgrundlage sich der Arzt, Rechtsanwalt oder Apotheker bei der Übermittlung bzw. Nutzung der Geheimnis-Daten stützen kann, sind sehr praktische Überlegungen verbunden. Er muss entscheiden, wer im Einzelfall noch zu seinen „Mitwirkenden" zu zählen ist, ob und mit welchem der an seiner beruflichen Tätigkeit Mitwirkenden ggf. Verträge über Auftragsdatenverarbeitung abzuschließen sind, in welchen Fällen er (weiterhin) eine Einwilligung der Betroffenen benötigt[16] und ob ihn Informationspflichten gegenüber Patienten, Mandanten oder Kunden treffen (vgl. § 4 Abs. 3 BDSG).

1. Subsidiarität des BDSG

Das BDSG ist als Auffanggesetz konzipiert, dessen Bestimmungen nach seiner „gestuften Regelungstechnik"[17] erst dann zum Tragen kommen, wenn kein bereichsspezifisches Sonderrecht existiert. Im Schrifttum besteht durchweg Ei-

7 RegE Begründung, A. Allgemeiner Teil, Abschnitt II 1a.

8 Samson, in: Systematischer Kommentar zum Strafgesetzbuch, § 203 Rn. 26; Kargl, in: Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 3. Aufl., § 203 Rn. 6; Ciernak/Pohlit, in: Müchener Kommentar zum Strafgesetzbuch, 2. Aufl., § 203 Rn. 11.

9 Lenckner, in: Schönke/Schröder, § 203 Rn. 19.

10 Kargl, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 19; Schünemann, Strafgesetzbuch (Leipziger Kommentar), § 203 Rn. 41; OLG Köln, NJW 1980, 898.

11 Lenckner, in: Schönke/Schröder, § 203 Rn. 19.

12 Str. bei EDV-Servicearbeiten, wenn das Wartungs-/Technikpersonal mit den auf der EDV-Anlage oder dem IT-Netzwerk gespeicherten Daten in Kontakt kommen kann. Vgl. zum Meinungsstand Kargl in Kindhäuser/Neumann/Paeffgen, § 203 Rn. 21; Ciernak/Pohlit, in: Münchener Kommentar, § 203 Rn. 52; Schünemann, in: Leipziger Kommentar, § 203 Rn. 41; Preuß, DuD 2016, 802 (804).

13 Dammann, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl., § 3 Rn. 146: „Die Weitergabe ist erfolgt, sobald der Empfänger die Möglichkeit hat, unbehindert vom Weitergebenden die Information zur Kenntnis zu nehmen. Ob und wann er das tatsächlich tut, ist gleichgültig."

14 RegE Begründung, A. Allgemeiner Teil, Abschnitt II 1a.

15 Die Zuleitung personenbezogener Daten an einen Auftragnehmer stellt eine Nutzung dar; Dammann, in: Simitis, § 3 Rn. 195; Plath/Schreiber, in: Plath, BDSG-DSGVO, 2. Aufl., § 3 Rn. 54. Die verbreitete These von der angeblichen Privilegierung der Auftragsdatenverarbeitung gegenüber einer Übermittlung lässt sich deshalb nur bedingt halten.

16 Vgl. RegE Begründung, A. Allgemeiner Teil, Abschnitt II 1a.

17 Gusy, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 1 BDSG Rn. 78.

nigkeit darüber, dass eine Verdrängungs- bzw. Vorrangwirkung bestimmten Rechtsvorschriften nur dann zukommt, wenn der Anwendungsbereich konkurrierender Normen „deckungsgleich" ist und die bereichsspezifische Vorschrift eindeutig Belange des Datenschutzrechts regelt[18]. Ob und wann insoweit § 203 StGB als vorrangig geltende Norm in Betracht zu ziehen ist, wird bislang durchweg bei § 1 Abs. 3 Satz 2 BDSG unter dem Aspekt einer gesetzlichen Geheimhaltungspflicht diskutiert. Einer solchen sollen die meisten der in § 203 Abs. 1 StGB genannten Personenkreise nicht unterliegen[19]. Sie wird namentlich für das Arzt- oder Patientengeheimnis abgelehnt, da die allgemeine ärztliche Schweigepflicht nur berufs- bzw. standesrechtlich festgelegt sei und nicht auf staatlich kodifiziertem Recht basiere. Die Frage wird sich indes unter einem anderen Vorzeichen neu stellen, wenn die Novelle des § 203 Abs. 3 StGB in Kraft getreten ist.

Die künftig dem Geheimnisträger eingeräumte Befugnis zur Weitergabe von ihm anvertrauten personenbezogenen Angaben an Außenstehende beruht zwar auf einer Strafrechtsnorm und betrifft zunächst auch nur strafrechtliche Rechtsfolgen. Gleichwohl wäre nicht nachvollziehbar, wenn die datenschutzrechtliche Rechtfertigung von der datenschutzrechtlichen abweichen würde, wenn sie sich auf den gleichen faktischen Vorgang, nämlich ein Weitergeben, bezieht. Es wäre paradox anzunehmen, dass eine Datenweitergabe zwar strafrechtlich ausdrücklich gestattet, datenschutzrechtlich aber verboten ist und zudem noch Rechtsfolgen nach den §§ 43, 44 BDSG auslösen könnte. Es bedarf insoweit noch nicht einmal des Rückgriffs auf die „Einheit der Rechtsordnung", um von einer tatbestandlichen Kongruenz von Strafrechts- und Datenschutznormen im Hinblick auf die Erlaubnis des Datenumgangs – bezogen auf den Kreis der „Mitwirkenden" – auszugehen, so dass § 203 Abs. 3 Satz 2 StGB die Zulässigkeitsnormen des BDSG (§§ 4, 28 ...) verdrängt. Entscheidend ist also nicht auf das Arzt- usw. -geheimnis abzustellen, sondern unmittelbar auf die gesetzliche Regelung des Offenbarungs-/Weitergabetatbestandes.

2. Konsequenzen

Mit dem Vorliegen der Voraussetzungen für die Weitergabebefugnis nach § 203 Abs. 3 Satz 2 (neu) entfällt jede Prüfung durch den Geheimhaltungsverpflichteten, ob eine Einwilligung vom Betroffenen eingeholt werden muss oder die Tatbestandsmerkmale des § 28 BDSG (insbesondere auch hinsichtlich Abs. 7) erfüllt sind. Fraglich ist, ob die Fälle, die nach den datenschutzrechtlichen Kriterien als Auftragsdatenverarbeitung einzustufen wären, auch weiterhin nach den für dieses datenschutzrechtliche Konstrukt geltenden Regeln zu behandeln sind und z.B. Verträge nach § 11 Abs. 2 BDSG erfordern, oder ob dieses Institut in Gänze von § 203 Abs. 3 Satz 2 StGB (neu) verdrängt wird.

Auch wenn in der Begründung des Gesetzentwurfs die datenschutzrechtlich ggf. unterschiedlich zu behandelnden Empfängerkategorien des ausgeweiteten ärztlichen Hilfspersonals auf eine Stufe gestellt werden, bleibt es bei der durch das BDSG festgelegten Grundordnung: Der Zulässigkeitsvorrang des § 203 Abs. 3 Satz 2 StGB (neu) bezieht sich nur auf die Erlaubnis der Nutzung als solcher, also darauf, überhaupt Auftragsdatenverarbeitung durchführen zu dürfen. Die weiteren Anforderungen des § 11 BDSG werden dadurch nicht abbedungen. Der Arzt, Apotheker usw. kommt also nicht umhin, je nach Eigenart der für ihn handelnden Personen mit diesen ggf. auch Verträge gem. § 11 Abs. 2 StGB abzuschließen

Nur kurz anzusprechen ist ferner, inwieweit (pars pro toto) der Arzt den Patienten über sein „back office" informieren muss. Da nach wohl überwiegender Meinung die Unterrichtung des Betroffenen bei der Datenerhebung keine Zulässigkeitsbedingung in dem Sinn darstellt, dass die unterbliebene Aufklärung in jedem Fall zur Unzulässigkeit der Erhebung und nachfolgenden Verarbeitung sowie Nutzung führt, konsumiert die Erlaubnis des § 203 Abs. 3 Satz 2 StGB (neu) nicht die Verpflichtung nach § 4 Abs. 3 BDSG. Da der Patient kaum wissen wird, dass, und vor allem an wen seine Daten aus der Praxis heraus gelangen, wird der Arzt ihn in geeigneter Form darauf hinweisen müssen – eine Pflicht, die ihn unabhängig davon trifft, welche datenschutzrechtliche Eigenschaft dem Empfänger (Dritter oder Auftragnehmer) zukommt.

IV. Neues Datenschutzrecht

Das Prinzip der Subsidiarität des „allgemeinen" Datenschutzrechts gegenüber bereichsspezifischen Normen bleibt auch erhalten, wenn ab dem 25. Mai 2018 das „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU"[20] und die EU-Datenschutzgrundverordnung (DS-GVO)[21] zu beachten sind. § 1 Abs. 2 des „neuen BDSG" sieht das bisherige Subordinationsverhältnis weiterhin expressis verbis vor. Kollisionen mit der DS-GVO sind nicht zu befürchten[22], da sich die DS-GVO nicht auf § 203 Abs. 3 StGB auswirkt[23].

18 Plath, in: Plath, § 1 Rn. 36; Dix, in: Simitis, § 1 Rn. 170: "Nur die deckungsgleiche, tatbestandskongruente Norm geht dem BDSG vor"; Schmidt, in: Taeger/Gabel, Kommentar zum BDSG, 2010, § 1 Rn. 33: „Tatbestandskongruenz"; ebenso Gola/Schomerus, BDSG, 12. Aufl., § 1 Rn. 24; Topp, Datenschutz in der Steuerverwaltung, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 8.12 Rn. 25: „Das BDSG tritt nur insoweit zurück, wie es sich mit der Sondervorschrift ... überlappt."

19 Vgl. etwa Dix, in: Simitis, § 1 Rn. 180; Gola/Schomerus, § 1 Rn. 25; Gusy, in: Wolff/Brink, § 1 BDSG Rn. 85 f; Schmidt, in: Taeger/Gabel, § 1 Rn. 37.

20 Gesetzentwurf der Bundesregierung, BR-Drucksache 110/17 vom 02.02.2017.

21 Verordnung (EU) 2016/679, ABl. L 119/1 vom 04.05.2016.

22 Vgl. die „Rückzugsregelung" in § 1 Abs. 5 BDSG (neu).

23 Insoweit fehlt die EU-Gesetzgebungskompetenz; vgl. auch Art. 2 Abs. 2 DS-GVO.

Aus den aktuellen Berichten der Aufsichtsbehörden (30): Umgang mit dem Internet

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter*

Medienprivileg im Internet

Der zum 3. 3. 2017 vorgelegte 7. TB (2015/2016) des BayLDA erörtert auf Grund mehrfacher Beschwerden, inwieweit im öffentlich zugänglichen Bereich des Internets erfolgende Veröffentlichungen von einem Betroffenen hinzunehmen sind (Ziff. 7.3), wobei die die Bandbreite an Telemediendiensten, in denen es zu solchen Veröffentlichungen kommt, vielfältig war.

So schreiben sich Personen auf eigener Homepage oder in Blogs ihren Frust über Mitmenschen und negative Erfahrungen mit Behörden oder kommunalen Mandatsträgern von der Seele und wollen die ganze Welt an ihrem Schicksal teilhaben lassen. Bürgerinitiativen wollen via Internet die Öffentlichkeit gezielt auf bestimmte Anliegen aufmerksam machen und prangern nicht selten in diesem Zusammenhang das Verhalten einzelner namentlich genannter Personen an.

Aus datenschutzrechtlicher Sicht stellte sich für das BayLDA in jedem Einzelfall die Frage, ob der konkrete Telemediendienst für sich das sog. „Medienprivileg" des § 41 Abs. 1 BDSG beanspruchen kann, mit der Folge, dass er dann von den Bestimmungen des BDSG weitgehend freigestellt ist, das LDA als Aufsichtsbehörde nicht mehr zuständig wäre und betroffene Personen die Frage einer vermeintlichen Beeinträchtigung ihres Persönlichkeitsrechts zivilrechtlich klären lassen müssten. Eindeutig zu klären, ob der für den Telemediendienst Verantwortliche als „Unternehmen und Hilfsunternehmen der Presse" anzusehen ist oder er einer „journalistisch-redaktionellen Tätigkeit" nachkommt, stieß ggf. auf Schwierigkeiten. Eine Rückfrage beim Deutschen Presserat, der ebenfalls in seiner täglichen Arbeit mit diesen Fragen zu kämpfen hat, bestätigte dies. Da eine pauschale Antwort nicht möglich ist, bedurfte jeder Einzelfall einer gesonderten Betrachtung.

Unstrittig war dabei, dass ein Diensteanbieter u.a. nicht dadurch zu einem Presseunternehmen wird, dass er sich selbst ohne weiteren Nachweis als Journalist, Redakteur usw. bezeichnet. Ferner kann auch die schlichte Veröffentlichung von behördlichem Schriftverkehr nicht als journalistisch-redaktionelle Tätigkeit gesehen werden. Andernfalls könnte sich letztlich jeder Verein, jedes Unternehmen und jede Privatperson, die über eine eigene Homepage die Öffentlichkeit über die eigenen Aktivitäten und Erfahrungen informiert, auf das Medienprivileg berufen. Nötig sind zumindest „formale" Indizien, wie beispielsweise der Besitz eines Presseausweises oder die Mitgliedschaft in einem Presseverband, die für den Status eines „Journalisten" sprechen. Ferner muss die Aufbereitung des Internetauftritts ein Mindestmaß an journalistisch-redaktioneller Bearbeitung aufweisen.

In einem Gerichtsverfahren, bei dem das LDA beteiligt war, hat beispielsweise das Bundesverwaltungsgericht (Beschluss v. 29. 10. 2015 – 1 B 32.15) festgestellt, dass es für die Annahme eines Presseunternehmens nicht genügt, *„wenn der Vorstand einer Wählervereinigung seine allerdings von der Meinungsäußerungsfreiheit geschützten Beiträge zur Unterrichtung der Öffentlichkeit und zur öffentlichen Auseinandersetzung auf der Website veröffentlicht. Denn es fehlt insoweit an einer eigenständigen, vom sonstigen Handeln des Vorstandes abgegrenzten, autonomen redaktionellen Stelle innerhalb des Vereins, die diese Informationsbearbeitung zu einer Verarbeitung „allein" bzw. „ausschließlich" zu eigenen journalistischen Zwecken werden lassen könnte. Das Berufungsgericht nimmt zu Recht an, dass das sog. Medienprivileg kein allgemeines Meinungsprivileg enthält. (…) Insbesondere folgt aus dem Umstand, dass journalistische Tätigkeiten nicht Medienunternehmen vorbehalten sind, nicht, dass jegliche Verbreitung von Informationen, Meinungen oder Ideen in der Öffentlichkeit „allein zu journalistischen Zwecken" erfolgt."*

Somit wird es auch künftig nur Einzelfallentscheidungen zu Fragen der Anwendbarkeit des „Medienprivilegs" geben können.

Veröffentlichung von Fotos im Internet

Als Dauerbrenner bezeichnet das LDA auch die ähnlich gelagerte Problematik der uneingewilligten Veröffentlichungen von Fotos im Internet (7. TB, Ziff. 7.7). Das LDA erinnert daran, dass das Veröffentlichen von Fotos von Personen im Internet grundsätzlich der Einwilligung der abgebildeten Personen bedarf. Einschlägige Rechtsvorschriften sind die §§ 22 und 23 Kunsturheberrechtsgesetz (KUG). Ausnahmen von diesem Grundsatz werden in § 23 KUG geregelt. Danach dürfen ohne Einwilligung verbreitet und zur Schau gestellt werden

- Bildnisse aus dem Bereich der Zeitgeschichte,
- Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen,
- Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben oder
- Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

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

Abzuwägen bleibt dabei jeweils, ob nicht ein berechtigtes Interesse des Abgebildeten verletzt wird.

An zwei konkreten Beschwerden wird sodann verdeutlicht, wo im Einzelfall die Schwierigkeiten bei der Anwendung dieser Vorschriften liegen können: Im ersten Fall wurde auf der Homepage einer Arztpraxis mit einem Foto das aus fünf Personen bestehende Praxisteam vorgestellt. Von einer Person, die zum Zeitpunkt der Eingabe bereits seit längerer Zeit nicht mehr in dieser Arztpraxis tätig war, wurde eine Löschung des Fotos gefordert. Der Fall war nach Ansicht des LDA in seiner rechtlichen Bewertung eindeutig. Die Aufnahme und die Veröffentlichung des Fotos bedurften einer Einwilligung der fotografierten Personen, da ein Ausnahmetatbestand des § 23 KUG nicht einschlägig war. Das LDA ging dann offensichtlich davon aus, dass die Einwilligung mit der Teilnahme an der Fotoaktion erklärt wurde, da das Team der Arztpraxis sich offensichtlich der Tatsache, dass ein Foto angefertigt wird und wohl auch des Zwecks, nämlich einer Veröffentlichung auf der Homepage der Arztpraxis, bewusst gewesen war. Nachdem eine der Personen nach dem Ausscheiden aus der Praxis ihre Einwilligung widerrufen hat, war das besagte Foto zu löschen bzw. zu überarbeiten (vgl. hierzu aber auch BAG, Urt. v. 19.02.2015 – 8 AZR 1011/13). Dieser Forderung des LDA kam der Arzt nach, indem er das Bild durch eine aktualisierte Fotografie seines Teams ersetzte.

Im anderen Fall war ein Bild Gegenstand einer Beschwerde, das ebenfalls fünf Personen zeigte. Der Beschwerdeführer, der im Rahmen eines Jugend-Fußballturniers als Schiedsrichter fungiert hatte, fand sich auf der Homepage eines der teilnehmenden Vereine wieder, die neben zwei Sponsoren des stattgefundenen Fußballturniers das Schiedsrichtergespann zeigte. Während der Eingabeführer nicht in die Richtung des Fotografen blickt, ist es offensichtlich, dass die vier weiteren Personen in die Kamera blicken und sich zumindest des Fotografiertwerdens bewusst sind. Das LDA erkannte hier einen „Grenzfall", da für Fotos von einer öffentlichen Sportveranstaltung grundsätzlich die Ausnahme des § 23 Abs. 1 Nr. 3 KUG („Bilder von Versammlungen) herangezogen werden kann.

Mit der Veröffentlichung der Daten Dritter auf privaten Internetseiten befasste sich auch der LfD Bremen in seinem im März vorgelegten Bericht (39. TB, 2016, Ziff. 11.2). Der LfD weist zunächst darauf hin, dass es zur Veröffentlichung von personenbezogenen Daten auf privaten Internetseiten, also zum Beispiel von Namen, persönlichen Daten und auch ganzen Dokumenten, entweder der Einwilligung der Personen, auf die sich die Daten beziehen, oder einer Rechtsvorschrift bedarf, die eine Veröffentlichung im Internet erlaubt oder anordnet. Solche Rechtsvorschriften finden sich in den Datenschutzgesetzen, sind aber immer an Bedingungen geknüpft, die zur Veröffentlichung erfüllt sein müssen. Häufig ist als Bedingung eine positive Abwägung zwischen den Rechten und Interessen der beziehungsweise des Verantwortlichen und der oder des Betroffenen erforderlich.

In einigen Fällen, in denen personenbezogene Daten auf privaten Internetseiten veröffentlicht wurden, war kein überwiegendes Interesse der Verantwortlichen festzustellen. Auch lagen keine Einwilligungen zur Veröffentlichung vor. Die Verantwortlichen verwiesen auf Nachfrage und teils aufgrund der Aufforderung zur Löschung der Daten zum Teil – nach Auffassung des LfD unzutreffend – darauf, dass die Veröffentlichungen durch das Medienprivileg und durch die Meinungsäußerungsfreiheit erlaubt würden.

Nach einem Urteil des BGH vom 23.06.2009 (VI ZR 196/08) kann das Medienprivileg zwar auch auf die Veröffentlichung von Internetseiten Anwendung finden, da es nicht nur für Druckerzeugnisse gelte, sondern für die „Presse" im verfassungsrechtlichen Sinn, also auch für die „elektronische Presse". Dies gelte allerdings lediglich, wenn die Veröffentlichung unter den Pressebegriff des Grundgesetzes falle. Internetseiten, zum Beispiel Weblogs und Microblogging-Angebote, könnten hierunter fallen, wenn es sich um professionelle journalistisch-redaktionell gestaltete Angebote handelt, wenn also das jeweilige Angebot den Eindruck vermittelt, dass Tatsachen umfassend recherchiert und dabei verschiedene Informationsquellen genutzt werden, das Angebot einen gewissen Grad an organisatorischer Verfestigung aufweist, die Kontinuität gewährleistet und Informationen ausgewählt, gewichtet und für den Nutzer aufgearbeitet werden. Diese Angebote seien dabei in ein besonderes Regelwerk von Rechten und Pflichten, den Pressekodex, eingebunden. Die aufgrund der Eingaben untersuchten Internetseiten genügten diesen Anforderungen nicht.

Auch die Meinungsäußerungsfreiheit rechtfertigt die Veröffentlichung personenbezogener Daten nur im Ausnahmefall. Das Grundrecht auf Meinungsäußerung ist nicht schrankenlos gewährt. Nach dem genannten Urteil des Bundesgerichtshofs muss eine Person gegenüber denjenigen, die unter Berufung auf die Meinungsäußerungsfreiheit ihre personenbezogenen Daten veröffentlichen, zwar grundsätzlich Einschränkungen ihres Rechts auf informationelle Selbstbestimmung hinnehmen. Dies gelte aber nur, wenn und soweit solche Beschränkungen von hinreichenden Gründen des Gemeinwohls oder überwiegenden Rechtsinteressen Dritter getragen würden und bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe die Grenze des Zumutbaren noch gewahrt sei.

In den vom LfD bearbeiteten Fällen überwogen das Rechtsinteresse und die die Veröffentlichung rechtfertigenden Gründe Dritter nicht. Eine Veröffentlichung im Internet bedeute nämlich, dass die Daten einer weltweiten Öffentlichkeit für den Betroffenen unkontrollierbar zur Verfügung gestellt werden und auch durch Suchmaschinen zugänglich sind. Es handele sich deshalb um intensive Eingriffe in das Persönlichkeitsrecht. Zur Schilderung des jeweiligen Sachverhalts auf den Internetseiten hätte jeweils auch eine anonymisierte Darstellung genügt. In den fraglichen Fällen wurden die personenbezogenen Daten auf den privaten Internetseiten gelöscht oder die Veröffentlichungen derartig durch technische Maßnahmen eingeschränkt, dass die Daten nur noch von Mitgliedern des persönlichen oder familiären Bereichs abgerufen werden können.

Das Haushaltsprivileg

Mit dem letztgenannten Hinweis gibt der LfD zumindest einen Hinweis darauf, dass Veröffentlichungen im Internet auch deshalb nicht den Regelungen das BDSG oder DS-GVO unterliegen können, weil sie unter das sog. Haushaltsprivileg des § BDSG bzw. des Art. 2 Abs. 2 lit. c DS-GVO fallen. Das BDSG bzw. die Verordnung gilt danach nicht für Verarbeitungen, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden. Zu dem typisch persönlich familiären Bereich gehören Freizeit, Urlaub, privater Konsum oder Sport. Nach ErwGr. 18 können zu solchen „freien" Verarbeitungen auch Onlineaktivitäten und die Nutzung sozialer Netze zählen. Letzteres kann aber nur gelten, wenn der Kreis der Empfänger auf einen engen Familien- und Freundeskreis beschränkt ist.

Veröffentlichung des Wählerverzeichnisses für Betriebsratswahlen im Intranet

Für die Betriebsratswahlen veröffentlichte der Wahlvorstand eines Klinikverbundes das Wählerverzeichnis mit den Daten der insgesamt über 600 Beschäftigten im Intranet des Konzerns. Das Wählerverzeichnis enthielt die Angaben Vorname, Name, Funktion und Geschäftsbereich. Neben den Beschäftigten der vier Standorte des Klinikverbunds konnten auch Beschäftigte anderer Betriebe und Unternehmen, die das Intranet ebenfalls nutzen, Zugang zu den Beschäftigtendaten erhalten. Auch konnten die Wählerlisten beliebig geladen und verschickt beziehungsweise an Dritte übermittelt werden. Der LfD Bremen (39. TB, 2016 Ziff. 12.3) hat diese Verfahren beanstandet. Die Argumente des Wahlvorstands, er habe das Wählerverzeichnis im Intranet veröffentlicht, weil viele Beschäftigte, die an der Betriebsratswahl teilnehmen könnten, an verschiedenen Standorten arbeiten und so ohne weiteres prüfen könnten, ob sie in das Wählerverzeichnis eingetragen sind, überzeugte ihn nicht.

Der LfD machte geltend, dass sich die Betriebsratswahl nur auf die Beschäftigten des Klinikverbunds erstrecke, nicht jedoch auf die Beschäftigten der übrigen Gesellschaften, die das Intranet ebenfalls nutzen. Insoweit handelte es sich um eine unzulässige Datenübermittlung an Dritte. Hinzuweisen ist insoweit noch darauf, dass die Publikation des Wählerverzeichnisses im Betrieb eine Rechtsgrundlage in § 2 Abs. 4 Wahlordnung hat. Die Regelung erstreckt sich nicht nur auf eine Veröffentlichung durch Aushang, sondern erlaubt auch auf die Nutzung im Betrieb vorhandener Informations- und Kommunikationstechnik zur Veröffentlichung des Verzeichnisses „im Betrieb".

Rechtsprechung

Zur Vereinbarkeit von arbeitgeberseitigen Überwachungsmaßnahmen nebst Kündigung mit der Europäischen Menschenrechtskonvention (Ls)

(**Europäischer Gerichtshof für Menschenrechte**, Urteil vom 12. Januar 2016 – Von: 61496/08 – Bărbulescu v. Rumänien)

1. **Artikel 8 der Europäischen Menschenrechtskonvention soll Individuen vor willkürlichen Eingriffen von Hoheitsträgern schützen.**
2. **Artikel 8 der Europäischen Menschenrechtskonvention besagt jedoch nicht, dass der Staat von solchen Eingriffen keinen Gebrauch machen darf. Vielmehr muss eine gerechte Abwägung zwischen privaten und öffentlichen Interessen oder Konventionsrechten erfolgen.**
3. **Es ist nicht unbillig, wenn ein Arbeitgeber überprüfen möchte, ob seine Arbeitnehmer die beruflichen Aufgaben während der Arbeitszeit erledigen können. Er kann daher überprüfen, ob ein Arbeitnehmer ihm einen ausschließlich für dienstliche Zwecke zur Verfügung gestellten Yahoo-Instant-Messenger-Dienst für private Zwecke nutzt.**
4. **Wertet ein nationales Gericht vom Arbeitgeber überwachte Gesprächsverläufe seines Arbeitnehmers als Beweismittel aus, um den Inhalt der Nachrichten zu überprüfen, stellt dies keinen Eingriff in Artikel 8 der Europäischen Menschenrechtskonvention dar, wenn das Gericht das Protokoll nur in dem Umfang nutzt, um zu beweisen, dass der Yahoo-Messenger während der Arbeitszeit auch zu privaten Zwecken vom Arbeitnehmer genutzt wurde und dabei nur notwendige Details seiner privaten Gespräche verwendet und insbesondere die Art der Kommunikation und die Identität der Personen, mit denen kommuniziert, nicht öffentlich macht.**

Zur Unzulässigkeit von Werbe-E-Mails an geschäftliche E-Mail-Adressen

(**Bundesgerichtshof**, Urteil vom 14. März 2017 – VI ZR 721/15 –)

1. **Die ohne wirksame Einwilligung an eine geschäftliche E-Mail-Adresse versandte Werbe-E-Mail stellt einen Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb dar (Fortführung von BGH, Urteil vom 12. September 2013 – I ZR 208/12, GRUR 2013, 1259).**

2. **Eine wirksame Einwilligung in den Empfang elektronischer Post zu Werbezwecken setzt u.a. voraus, dass der Adressat weiß, dass seine Erklärung ein Einverständnis darstellt, und dass klar ist, welche Produkte oder Dienstleistungen welcher Unternehmen sie konkret erfasst. Eine vorformulierte Einwilligungserklärung ist an den §§ 305 ff. BGB zu messen (Fortführung von BGH, Urteil vom 25. Oktober 2012 – I ZR 169/10, GRUR 2013, 531).**

3. **Zur Anwendbarkeit von § 28 Abs. 1 Nr. 2 BDSG, wenn der zur Unterlassung von Werbung mittels elektronischer Post Verpflichtete die E-Mail-Adresse des Betroffenen gegen dessen Willen nutzen möchte, um sie zu Lösch- oder Sperrzwecken an seine Werbepartner weiterzuleiten.**

Sachverhalt:

Der Kläger nimmt die Beklagte wegen unerbetener E-Mail-Werbung auf Unterlassung und Erstattung vorgerichtlicher Rechtsanwaltskosten in Anspruch. Er ist Handelsvertreter, die Beklagte betreibt einen Verlag. Die Beklagte hatte unter anderem die Z. GmbH und die P. AG damit beauftragt, Werbe-E-Mails mit Verlagsangeboten zu versenden. Für deren E-Mail-Marketing-Kampagnen gibt es verbindliche Vorgaben der Beklagten. Der Kläger erhielt am 21. und 25. März 2013 unter seiner geschäftlich genutzten E-Mailadresse ...@gmx.de von der Z. GmbH Werbe-E-Mails für (Print-) Produkte der Beklagten. Er mahnte die Beklagte daraufhin ab.

Die Beklagte teilte dem Kläger mit, dass sie keine entsprechende Unterlassungserklärung abgeben werde, weil er in die fragliche Werbung beim Herunterladen eines Free-Ware-Programmes eingewilligt habe. Er werde in die interne Liste gesperrter E-Mail-Adressen, die sogenannte interne „Robinson Liste“, aufgenommen. Der Kläger widersprach jeglicher Erhebung und Speicherung seiner personenbezogenen Daten, auch für angebliche Sperrzwecke, soweit diese nicht auf Namen und Anschrift beschränkt seien. Insbesondere widersprach er der Erhebung und/oder Speicherung von jeglichen Mail-, Telefon- und Faxkontaktdaten, um eine Weitergabe dieser Daten an die Werbepartner zu verhindern. Nach Klageerhebung erhielt er unter der genannten E-Mail-Adresse von der P. AG und der Firma N. weitere Werbe-E-Mails für Produkte der Beklagten.

Der Kläger verlangt, die Beklagte zu verurteilen, es bei Meidung eines Ordnungsgeldes, ersatzweise Ordnungshaft zu unterlassen, ihm gegenüber Werbung per elektronische Nachricht ohne seine vorherige ausdrückliche Einwilligung zu betreiben und/oder betreiben zu lassen. Das Amtsgericht hat der Klage hinsichtlich des Unterlassungsantrages stattgegeben und dem Kläger einen Teil der vorgerichtlichen Rechtsanwaltskosten zugesprochen. Auf die Berufung der Beklagten hat das Landgericht die Klage insgesamt abgewiesen, die Anschlussberufung des Klägers hat es zurückgewiesen. Mit der vom Berufungsgericht zugelassenen Revision verfolgt der Kläger sein Begehren weiter.

Aus den Gründen:

Das Berufungsgericht hält die Berufung für zulässig und begründet. Der Geltendmachung des Unterlassungsanspruchs stehe gemäß § 242 BGB der Einwand des Rechtsmissbrauchs bzw. widersprüchlichen Verhaltens entgegen.

Der Kläger habe zwar grundsätzlich einen Unterlassungsanspruch gegen die Beklagte wegen unerbetener E-Mail-Werbung gemäß §§ 1004, 823 Abs. 1 bzw. § 831 BGB. Die von der Beklagten verpflichteten Werbedienstleister hätten zur Durchführung ihrer Werbemaßnahmen E-Mail-Adressen von Dritten erworben. Letztere sollten die erforderliche Werbeeinwilligung von den späteren Werbungsempfängern als Gegenleistung für einen Software-Download oder als Bedingung für die Teilnahme an einem Gewinnspiel erhalten haben. Auch auf der Grundlage dieses Vortrags der Beklagten habe der Kläger keine wirksame Einwilligung zum Erhalt der streitgegenständlichen Werbe-E-Mails erteilt, denn es müsse eine Einwilligung für den konkreten Fall erteilt werden, aus der Erklärung müsse hinreichend klar hervorgehen, welche konkreten Unternehmen für welche konkreten Produkte werben dürften. Die Einwilligungserklärung benenne aber nicht die Produkte, für die geworben werden solle. Eine produktoffene Werbeeinwilligung sei grundsätzlich unwirksam. Auch die Tatsache, dass der Kläger in Bezug auf die Z. GmbH seine Einwilligung quasi als Gegenleistung für den kostenlosen Download von Software erteilt haben solle, helfe der Beklagten nicht darüber hinweg, dass die Einwilligung auch

in einem solchen Fall produktbezogen hätte gefasst werden müssen.

Der Unterlassungsanspruch scheitere jedoch aufgrund des Rechtsmissbrauchs des Klägers, weil dieser durch das Verbot der Weitergabe seiner E-Mail-Adresse an die werbenden Vertriebspartner der Beklagten verhindere, dass er von diesen keine weiteren Werbe-E-Mails für Produkte der Beklagten unter der genannten E-Mail-Adresse erhalte. Die Weitergabe der E-Mail-Adresse durch die Beklagte erscheine aber erforderlich, weil sie zwar die in Rede stehende E-Mail-Werbung veranlasst habe, zur Einhaltung eines gegen sie gerichteten Unterlassungsgebotes aber darauf angewiesen sei, dass Dritte, nämlich ihre Vertriebspartner, die Verwendung der E-Mail-Adresse zu Werbezwecken unterließen. Um diese entsprechend anzuweisen, benötige sie die entsprechende E-Mail-Adresse, an die die E-Mail-Werbung bisher gesandt worden sei, da nur dies die weitere Versendung zu unterbinden geeignet sei. Nur die Mitteilung des Empfängernamens, dessen Weitergabe der Kläger ausdrücklich erlaubt habe, genüge hierfür regelmäßig nicht, da die Werbedienstleister die Empfängeradressen nicht zwingend unter dem Namen des jeweiligen Inhabers registrierten. Es sei nicht nachvollziehbar, warum der Kläger sich der Weitergabe zu Sperrzwecken widersetze. Die Verwendung der erforderlichen Informationen könne der Beklagten nicht mit der Begründung abgesprochen werden, sie müsse sich ohnehin rechtstreu verhalten. Durch den Widerspruch vereitele der Kläger selbst die Durchsetzung des von ihm angestrebten Unterlassungsgebots und verlange letztlich von der Beklagten Unmögliches. Die einzig theoretisch denkbare Handlungsoption der Beklagten sei, jegliche E-Mail-Werbung durch die bisherigen Vertriebspartner einzustellen. Dies erscheine aber unverhältnismäßig, weil damit das grundsätzlich lautere Modell der E-Mail-Werbung durch Werbedienstleister unmöglich gemacht werde. Auch die Berufung auf Datenschutz und den Grundsatz der Datensparsamkeit vermöchten den Widerspruch des Klägers nicht zu rechtfertigen. Widersprüchlich sei das Verhalten des Klägers auch, weil er die behauptete Abgabe einer Einwilligung in E-Mail-Werbung durch die Beklagte im Wege des Double-Opt-In-Verfahrens (DOI-Verfahren) nicht wirksam bestritten habe. Diese Einwilligung sei lediglich deshalb nicht rechtswirksam, weil sie als produktunabhängige „Generaleinwilligung" den gesetzlichen Anforderungen nicht genüge.

Diese Erwägungen halten revisionsrechtlicher Überprüfung nicht in vollem Umfang stand.

Dem Kläger steht gegen die Beklagte gemäß § 1004 Abs. 1 Satz 2, § 823 Abs. 1, § 831 BGB ein Anspruch auf Unterlassung der Zusendung elektronischer Post mit werblichem Inhalt wegen eines rechtswidrigen Eingriffs in sein Recht am eingerichteten und ausgeübten Gewerbebetrieb zu, soweit nicht die Voraussetzungen der Ausnahmeregelung des § 7 Abs. 3 UWG erfüllt sind.

1. Mit dem Unterlassungsantrag erstrebt der Kläger die Unterlassung der Zusendung von Werbung der Beklagten per elektronische Post durch die Beklagte selbst oder durch Dritte auf ihre Veranlassung ohne vorherige ausdrückliche Einwilligung. Das Begehren ist nicht beschränkt auf die derzeit der Beklagten und deren Werbepartnern bekannte geschäftliche E-Mail-Adresse des Klägers, sondern bezieht sich auf alle etwaigen gegenwärtigen oder zukünftigen geschäftlich genutzten E-Mail-Adressen des Klägers. Dies hat das Berufungsgericht zutreffend erkannt.

2. Ein Unterlassungsanspruch kann hier allerdings nicht auf § 7 Abs. 1, Abs. 2 Nr. 3 UWG gestützt werden. Gemäß § 7 Abs. 1 UWG ist eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, unzulässig. Dies gilt insbesondere für Werbung, deren Versand erfolgt, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht. Gemäß § 7 Abs. 2 Nr. 3 UWG ist eine unzumutbare Belästigung stets anzunehmen bei Werbung unter Verwendung von elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt. Dabei sind Marktteilnehmer gemäß § 2 Abs. 1 Nr. 2 UWG neben Mitbewerbern und Verbrauchern alle Personen, die als Anbieter oder Nachfrager von Waren oder Dienstleistungen tätig sind, also auch der als Handelsvertreter tätige Kläger.

Von einem Verstoß gegen diese Regelung betroffene Verbraucher und sonstige Marktteilnehmer sind aber nach der abschließenden Regelung des § 8 Abs. 3 UWG nicht berechtigt, selbst Ansprüche auf Unterlassung gemäß § 8 Abs. 1 UWG geltend zu machen (h.M.; vgl. zum „Verbraucher" Senat, Urteil vom 15. Dezember 2015 – VI ZR 134/15, NJW 2016, 870 Rn. 9; Köhler/Feddersen, in: Köhler/Bornkamm, UWG, 35. Aufl., § 8 UWG Rn. 3.4; vgl. zur Ablehnung individueller Ansprüche Gesetzesentwurf der Bundesregierung zum Entwurf eines Gesetzes gegen den unerlaubten Wettbewerb vom 22. August 2003, BT – Drucks. 15/1487 S. 22). Der Kläger ist unstreitig nicht Mitbewerber der Beklagten. Im Übrigen steht die Klagebefugnis gemäß § 8 Abs. 3 Nr. 2 bis 4 UWG nur Wirtschafts- und Verbraucherverbänden und den Industrie- und Handelskammern oder Handwerkskammern zu.

3. Das von der Beklagten veranlasste Zusenden der Werbe-E-Mails durch ihre Werbepartner stellt aber einen rechtswidrigen Eingriff in das Recht des Klägers am eingerichteten und ausgeübten Gewerbebetrieb dar.

a) Hier kommen die Maßstäbe des § 7 UWG zur Vermeidung von Wertungswidersprüchen auch im Rahmen der Prüfung eines Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb gemäß § 823 Abs. 1 BGB zur Anwendung (vgl. BGH, Urteil vom 21. April 2016 – I ZR 276/14, GRUR 2016, 831 Rn. 16; Urteil vom 20. Mai 2009 – I ZR 218/07, GRUR 2009, 980 Rn. 14; Köhler, in: Köhler/Bornkamm, UWG, 35. Aufl., § 7 Rn. 14; Koch, in: Ullmann, jurisPK – UWG, 4. Aufl., § 7 Rn. 359). Gegenstand des Schutzes ist die Verhinderung des Eindringens des Werbenden in die geschäftliche Sphäre, insbesondere die Ungestörtheit der Betriebsabläufe des sonstigen Marktteilnehmers; es soll verhindert werden, dass dem Marktteilnehmer Werbemaßnahmen gegen seinen erkennbaren und mutmaßlichen Willen aufgedrängt werden (vgl. BGH, Urteil vom 21. April 2016 – I ZR 276/14, GRUR 2016, 831 Rn. 16). Verhindert werden soll darüber hinaus, dass die belästigende Werbung zu einer Bindung von Ressourcen des Empfängers führt (BGH, Urteil vom 1. Juni 2006 – I ZR 167/03, GRUR 2007, 164 Rn. 9). Unverlangt zugesendete E-Mail-Werbung erfolgt betriebsbezogen und beeinträchtigt den Betriebsablauf im Unternehmen des Empfängers. Das Verwenden von E-Mails mit unerbetener Werbung, die der Empfänger jeweils einzeln sichten muss und bei denen ein Widerspruch erforderlich ist, um eine weitere Zusendung zu unterbinden, führt zu einer nicht unerheblichen Belästigung (vgl. BGH, Urteil vom 12. September 2013 – I ZR 208/12, GRUR 2013, 1259 Rn. 15; Urteil vom 20. Mai 2009 – I ZR 218/07, GRUR 2009, 980 Rn. 10 ff.). So liegt es auch im Streitfall.

b) Die Werbe-E-Mails der Z. GmbH für die Printprodukte der Beklagten waren nicht durch eine vorherige Einwilligung des Klägers gedeckt.

aa) Die Beklagte hat eine Einwilligung des Klägers behauptet. Danach habe der Kläger am 25. Februar 2013 seine E-Mail-

Adresse an die Freeware-Plattform www.f...-a...de übermittelt, um dort ein Softwareprogramm herunterladen zu können. Unterhalb des Eingabefeldes für die E-Mail-Adresse sei er darauf hingewiesen worden, dass die eingegebene E-Mail-Adresse für den Betreiber der Seite sowie dessen Sponsoren für werbliche Zwecke freigegeben werde und er in unregelmäßigen Abständen Werbung per E-Mail erhalten werde. Der Kläger habe durch Drücken der Enter-Taste die Nutzungsbedingungen bestätigt. Zusätzlich habe die Plattform eine Double-Opt-In-E-Mail mit dem Betreff „Downloadlink für B. [die ausgewählte Freeware]" an das E-Mail-Postfach des Klägers gesendet, in welcher dieser auf die werbliche Nutzung der übermittelten E-Mail ein weiteres Mal mit folgendem Text hingewiesen worden sei:

„Sobald der Link bestätigt wird, startet der Download und Sie stimmen den unter www.f...-a...de hinterlegten Nutzungsbedingungen zu, die auch ein Einverständnis in werbliche Informationen von uns sowie den F. A. Sponsoren enthalten."

§ 4 (Werbeeinverständnis) der allgemeinen Geschäftsbedingungen der Seite habe folgenden Inhalt gehabt:

„Mit der Angabe seiner persönlichen Daten erklärt der Nutzer sein Einverständnis, dass er von F. M. Limited und den hier genannten Sponsoren Werbung per E-Mail an die vom Nutzer angegebene E-Mail-Adresse erhält. Der Nutzer kann der werblichen Nutzung seiner Daten durch F. M. Limited jederzeit durch eine E-Mail an Info@f...-m...com widersprechen".

Die Verlinkung hinter dem Wort „hier" habe zu einer Sponsorenliste geführt, welche die Z. GmbH sowie 25 weitere Unternehmen enthalten habe.

bb) Auch wenn man diesen – bestrittenen – Vortrag der Beklagten unterstellt, liegt keine wirksame Einwilligung vor, da aus der vorformulierten Einwilligungserklärung, wie das Berufungsgericht im Ergebnis zutreffend erkannt hat, nicht hinreichend klar hervorgeht, für welche konkreten Produkte die Unternehmen werben dürfen. Die Einwilligungserklärung hält einer Kontrolle nach den §§ 305 ff. BGB nicht stand. Sie ist gemäß § 307 Abs. 1 Satz 1 und 2, Abs. 3 Satz 2 BGB als unangemessene Benachteiligung des Klägers unwirksam, denn sie verstößt gegen das Transparenzgebot.

(1) Bei der vorformulierten Einwilligungserklärung handelt es sich um eine Allgemeine Geschäftsbedingung im Sinne des § 305 Abs. 1 Satz 1 BGB. Grundsätzlich kann die Einwilligungserklärung auch in Allgemeinen Geschäftsbedingungen wirksam erteilt werden (vgl. nur BGH, Urteil vom 25. Oktober 2012 – I ZR 169/10, GRUR 2013, 531 Rn. 21).

(2) Einer Transparenzkontrolle dieser vorformulierten Einwilligungserklärung steht nicht entgegen, dass es sich hier um eine Leistungsbeschreibung handeln könnte, wenn man davon ausginge, dass zwischen dem Betreiber der Plattform und dem Kläger ein entgeltlicher Vertrag zustande gekommen ist, bei dem die Leistung in der Gewährung des Herunterladens und der Nutzung von Software und die Gegenleistung in dem Einverständnis mit dem Empfang von Werbung des Plattformbetreibers und der Weitergabe der E-Mail-Adresse an andere Unternehmen mit dem Einverständnis, von diesen Werbung zu erhalten (vgl. Härting, in: Härting, Internetrecht, 5. Aufl., Rn. 480 ff., 769 ff.; Härting/Schätzle, ITRB 2006, 186, 187), also in der Zurverfügungstellung von personenbezogenen Daten für Werbezwecke, einem „Bezahlen mit eigenen Daten" besteht (vgl. Schmidt-Kessel/Erler/Grimm/Kramme, GPR 2016, 54, 57 f.; vgl. auch Faust, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag 2016 S. A 59). § 307 Abs. 1 Satz 2 BGB findet auch auf Leistungsbeschreibungen Anwendung (§ 307 Abs. 3 Satz 2 BGB; vgl. Becker, JZ 2017, 170, 173; Staudinger/Michael Coester (2013) BGB, § 307 Rn. 288).

(3) Die vorformulierte Einwilligungserklärung ist nicht hinreichend konkret gefasst und erfüllt nicht die Voraussetzungen des hier maßgeblichen § 7 Abs. 2 Nr. 3 UWG. Sie verstößt gegen das Transparenzgebot gemäß § 307 Abs. 1 Satz 2 BGB, das den Verwender Allgemeiner Geschäftsbedingungen verpflichtet, die Rechte und Pflichten seines Vertragspartners möglichst klar und durchschaubar darzustellen (BGH, Urteil vom 9. Dezember 2014 – X ZR 147/13, NJW – RR 2015, 618 Rn. 22; Urteil vom 3. Juni 1998 – VIII ZR 317/97, NJW 1998, 3114, 3116 mwN).

Mit § 7 Abs. 2 Nr. 2 Fall 1 UWG wurde die Bestimmung des Art. 13 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) umgesetzt. Der Begriff der „Einwilligung" ist deshalb richtlinienkonform zu bestimmen. Art. 2 Abs. 2 Buchst. f der Richtlinie verweist für die Definition der Einwilligung auf Art. 2 Buchst. h 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. Einwilligung ist „jede Willensbekundung, die ohne Zwang für den konkreten Fall und in Kenntnis der Sachlage erfolgt". Sie wird in Kenntnis der Sachlage erteilt, wenn der Verbraucher weiß, dass seine Erklärung ein Einverständnis darstellt und worauf sie sich bezieht. Die Einwilligung erfolgt für den konkreten Fall, wenn klar ist, welche Produkte oder Dienstleistungen welcher Unternehmen sie konkret erfasst (vgl. BGH, Urteil vom 25. Oktober 2012 – I ZR 169/10, GRUR 2013, 531 Rn. 23, 24 mwN; vgl. zu § 7 Abs. 2 Nr. 2 Fall 1 UWG BGH, Urteil vom 18. Juli 2012 – VIII ZR 337/11, NJW 2013, 291 Rn. 57 zu Werbeanrufen). Dies gilt entsprechend für die Werbung mittels elektronischer Post, für die § 7 Abs. 2 Nr. 3 UWG ebenfalls eine „vorherige ausdrückliche Einwilligung" des Adressaten fordert (vgl. Art. 13 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation; Micklitz/Schirmbacher, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl., § 7 UWG Rn. 99, 100, Leible, in: Münchener Kommentar zum Lauterkeitsrecht, 2. Aufl., § 7 UWG Rn. 175; Köhler, in: Köhler/Bornkamm, UWG, 35. Aufl., § 7 UWG Rn. 186; Ohly, in: Ohly/Sosnitza, UWG, 7. Aufl., § 7 UWG Rn. 66; Schöler, in: Harte-Bavendamm/Henning-Bodewig, UWG, 4. Aufl., § 7 UWG Rn. 298, 303).

Diesen Anforderungen wird die von der Beklagten behauptete Einwilligung nicht gerecht. Selbst wenn im Streitfall die Liste der „Sponsoren" abschließend und ohne Erweiterungsmöglichkeit bestimmt wäre, bleibt offen, für welche Produkte und Dienstleistungen diese werben. Aus ihren Firmen allein kann nicht auf die zur zukünftigen Bewerbung anstehenden Produkte geschlossen werden. Deren Zusammensetzung und Umfang kann wechseln oder erweitert werden. Soweit es sich wie im Streitfall bei den Sponsoren auch um Marketingunternehmen handelt, die selbst für Kunden Werbekampagnen entwerfen und durchführen, wird der Kreis der beworbenen Unternehmen und Produkte gänzlich unübersehbar.

Die Klausel enthält folglich eine (verdeckte) Generaleinwilligung, ohne dass dem Kunden dies in der gebotenen Klarheit verdeutlicht wird. Er muss durch die Klauselfassung vielmehr den Eindruck gewinnen, dass es sich um eine beschränkte Einwilligung handelt, die sich nur auf die Produkte oder die Pro-

duktart des Plattformbetreibers, nämlich „Free-Ware“, bezieht. Ob die Einwilligungserklärung aus diesem Grund auch als überraschende Klausel gemäß § 305c Abs. 1 BGB anzusehen und sie zudem gemäß § 307 Abs. 2, Abs. 1 Satz 1 BGB unwirksam ist, kann angesichts des Verstoßes gegen das Transparenzgebot dahinstehen.

c) Der Eingriff in das Recht des Klägers am eingerichteten und ausgeübten Gewerbebetrieb ist auch im Übrigen rechtswidrig.

Die aufgrund seines Charakters als Rahmenrecht erforderliche Abwägung der widerstreitenden Interessen der Parteien geht zu Lasten der Beklagten aus, wie schon der Wertung des § 7 Abs. 2 UWG zu entnehmen ist. Unabhängig davon überwiegt das Interesse des Klägers das Interesse der Beklagten, dem Kläger Werbung mit elektronischer Post ohne sein Einverständnis zuzuleiten. Auch hier gilt, dass der Schutz der geschäftlichen Sphäre, insbesondere die Ungestörtheit der Betriebsabläufe, vorrangig gegenüber dem wirtschaftlichen Gewinnstreben von anderen Unternehmen oder Gewerbetreibenden ist und dass die berechtigten Interessen der gewerblichen Wirtschaft, ihre Produkte werbemäßig anzupreisen, es angesichts der Vielfalt der Werbemethoden nicht erfordern, mit der Werbung in die internen Betriebsabläufe einzudringen (vgl. BGH, Urteil vom 27. Januar 2000 – I ZR 241/97, GRUR 20, 818, 819 zu Telefonwerbung).

4. Die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr wird durch das festgestellte rechtsverletzende Verhalten der Beklagten indiziert (Senat, Urteil vom 15. Dezember 2015 – VI ZR 134/15, AfP 2016, 149 Rn. 23; BGH, Urteil vom 12. September 2013 – I ZR 208/12, VersR 2014, 1462 Rn. 25 f. mwN – Empfehlungs-E-Mail). Die Abgabe einer strafbewehrten Unterlassungserklärung hat die Beklagte nach den Feststellungen des Berufungsgerichts abgelehnt.

5. Danach kann es im Streitfall dahinstehen, ob das Fehlen von Individualansprüchen auf Unterlassung unzulässiger Werbung mittels elektronischer Post nach § 8 Abs. 3, Abs. 1 UWG i.V.m. § 7 UWG ein Umsetzungsdefizit hinsichtlich Art. 13 der Datenschutzrichtlinie für elektronische Kommunikation darstellt. Art. 13 Abs. 1 ordnet an, dass die Verwendung von elektronischer Post für die Zwecke der Direktwerbung nur bei vorheriger Einwilligung der Teilnehmer oder Nutzer gestattet ist und Art. 13 Abs. 6 fordert, dass die Mitgliedsstaaten sicherstellen, dass beeinträchtigte Personen gegen solche Verstöße gerichtlich vorgehen können (vgl. dazu Heese, JZ 2016, 529, 531; Ohly, in: Ohly/Sosnitza, UWG, 7. Aufl., § 7 Rn. 9; Köhler, GRUR 2012, 1073, 1080). Eine Schutzlücke besteht jedenfalls hier nicht, weil sich ein solcher Individualanspruch wie dargestellt dem Deliktsrecht entnehmen lässt (vgl. Köhler, in: Köhler/Bornkamm, UWG, 35. Aufl., § 1 Rn. 39; Antwort der Bundesregierung auf die kleine Anfrage der Abgeordneten Gerold Reichenbach u.a. vom 27. Juli 2011 – BT-Drucks. 17/6689 S. 3).

6. Zu Unrecht ist das Berufungsgericht jedoch zu dem Ergebnis gelangt, dass der Unterlassungsanspruch insgesamt aufgrund eines Rechtsmissbrauchs des Klägers gemäß § 242 BGB scheitere, weil dieser durch das Verbot der Weitergabe seiner E-Mail-Adresse an die Werbepartner der Klägerin verhindere, dass er von diesen keine weiteren Werbe-E-Mails für Produkte der Beklagten jedenfalls unter der hier benannten E-Mail-Adresse erhalte. Die Geltendmachung des Unterlassungsanspruchs ist zumindest bezogen auf Werbung für Produkte der Beklagten, die den Kläger unter einer anderen als der bekannten E-Mail-Adresse erreichen kann, nicht ausgeschlossen. Für Werbung, die an die bekannte E-Mail-Adresse gerichtet wird, kann sich dies nach den bisher getroffenen Feststellungen anders darstellen.

a) Die Rechtsordnung missbilligt widersprüchliches Verhalten einer Partei im Grundsatz nicht (vgl. BGH, Urteil vom 15. November 2012 – IX ZR 103/11, WM 2013, 47 Rn. 12; Bamberger/Roth/Sutschet, BGB, 3. Aufl., § 242 Rn. 106; Palandt/Grüneberg, BGB, 76. Aufl., § 242 Rn. 55). Nach gefestigter Rechtsprechung des Bundesgerichtshofs kann eine Rechtsausübung aber dann unzulässig sein, wenn sich objektiv das Gesamtbild eines widersprüchlichen Verhaltens ergibt, weil das frühere Verhalten mit dem späteren sachlich unvereinbar ist und die Interessen der Gegenpartei im Hinblick hierauf vorrangig schutzwürdig erscheinen (vgl. BGH, Urteil vom 31. Januar 1975 – IV ZR 18/74, BGHZ 64, 5, 9; vom 12. November 2008 – XII ZR 134/04, NJW 2009, 1343 Rn. 41, BGH, Urteil vom 15. November 2012 – IX ZR 103/11, WM 2013, 47 Rn. 12).

b) Die Voraussetzungen dieses engen Ausnahmetatbestandes liegen – bezogen auf den gesamten Unterlassungsanspruch – nicht vor.

aa) Wie dargestellt, hat der Kläger einen Anspruch gegenüber der Beklagten, es zu unterlassen, ihm selbst oder auf ihre Veranlassung durch andere ohne vorherige ausdrückliche Einwilligung Werbung für ihre Produkte zuzusenden, gleichgültig an welche – gegenwärtige oder zukünftige – geschäftlich genutzte E-Mail-Adresse. Wie das Berufungsgericht zutreffend erkannt hat, bezieht sich die Weigerung des Klägers, seine E-Mail-Adresse an die Werbepartner der Beklagten weiterleiten zu lassen, nur auf seine derzeit bestehende Adresse ...@gmx.de. Mit seiner Weigerung wird also allenfalls die weitere Übersendung von Werbung an diese – bekannte – E-Mail-Adresse verhindert. Sie betrifft folglich nur einen Ausschnitt des Unterlassungsanspruchs des Klägers. Hinsichtlich des weitergehenden Unterlassungsanspruchs lässt sich schon objektiv kein widersprüchliches Verhalten des Klägers feststellen. Auch eine etwaige Unmöglichkeit oder besondere Erschwerung im Sinne von § 275 Abs. 1 und 2 BGB ist weder geltend gemacht noch sonst erkennbar, denn zu seiner Erfüllung genügt es insoweit nicht, wenn die Beklagte und ihre Werbepartner die bekannte E-Mail-Adresse des Klägers nicht mehr nutzen.

bb) Nach der ständigen Rechtsprechung des Bundesgerichtshofs erschöpft sich die Verpflichtung zur Unterlassung einer Handlung, durch die wie im Streitfall ein fortdauernder Störungszustand geschaffen wurde, nicht in bloßem Nichtstun. Vielmehr umfasst sie auch die Vornahme möglicher und zumutbarer Handlungen zur Beseitigung der Störungsquelle, wenn allein dadurch dem Unterlassungsgebot Folge geleistet werden kann (vgl. Senatsurteil vom 11. November 2014 – VI ZR 18/14, AfP 2015, 33 Rn. 16 zur titulierten Unterlassungsverpflichtung; BGH, Urteile vom 22. Oktober 1992 – IX ZR 36/92, BGHZ 120, 73, 76 f.; vom 18. September 2014 – I ZR 76/13, GRUR 2015, 258 Rn. 64; Beschluss vom 25. Januar 2007 – I ZB 58/06, NJW – RR 2007, 863 Rn. 17, jeweils mwN). Dementsprechend hat der Unterlassungsschuldner, um bestehende Gefahrenlagen zu beseitigen und künftige Verletzungen zu verhindern, erforderlichenfalls auf Dritte einzuwirken, wenn und soweit er auf diese – rechtlich oder tatsächlich – Einfluss nehmen kann (vgl. Senatsurteil vom 15. September 2015 – VI ZR 175/14, BGHZ 206, 347 Rn. 32; vom 28. Juli 2015 – VI ZR 340/14, WM 2015, 1664 Rn. 40; BGH, Urteil vom 18. September 2014 – I ZR 76/13, GRUR 2015, 258 Rn. 70; OLG Köln, GRUR – RR 2008, 365; MMR 2010, 782, 783; Ott, WRP 2007, 605, 608; Feddersen, in: Teplitzky, Wettbewerbsrechtliche Ansprüche und Verfahren, 11. Aufl., 57. Kap. Rn. 26; Köhler, in: Köhler/Bornkamm, UWG, 35. Aufl., § 12 Rn. 6.7).

cc) Nach diesen Grundsätzen ist die Beklagte verpflichtet, für ihr eigenes Unternehmen und durch Einwirkung auf ihre Werbepartner für die Zukunft sicher zu stellen, dass Werbung für ihre Produkte an geschäftliche E-Mail-Adressen des Klägers nur versandt wird, wenn eine gesetzesmäßige Einwilligung vorliegt, es sei denn, der Ausnahmetatbestand des § 7 Abs. 3 UWG wäre erfüllt. Die dazu voraussichtlich erforderliche (Um)Gestaltung der Anforderungen an wirksame Einwilligungen im Hause der Beklagten und bei ihren Werbepartnern kann ohnehin nicht durch die Sperrung einzelner E-Mail-Adressen erreicht werden. Dem Einwand, dass die Umgestaltung der vertraglichen Bedingungen und damit wohl auch der entsprechenden Internetseiten derjenigen Anbieter, die sich die Einwilligungen erteilen lassen, einen erheblichen Aufwand bedeuten kann, ist nach dem Rechtsgedanken des § 275 Abs. 2 Satz 2 BGB entgegen zu halten, dass die Beklagte die Situation zu vertreten hat, deren Beseitigung sie als wirtschaftlich unzumutbar ansieht (vgl. BGH, Beschluss vom 14. November 2013 – V ZR 302/12, juris). Spätestens seit der Veröffentlichung der Entscheidung des VIII. Zivilsenates vom 18. Juli 2012 (VIII ZR 337/11, ZIP 2012, 2064) war die erforderliche Produktbezogenheit als Wirksamkeitsvoraussetzung der Einwilligung zumindest für Allgemeine Geschäftsbedingungen bekannt.

c) Lediglich soweit sich der Unterlassungsanspruch des Klägers auf den Versand von Werbung an seine bereits bekannte E-Mail-Adresse ...@gmx.de bezieht, könnten seiner Geltendmachung aufgrund der Weigerung des Klägers, einer Weitergabe der E-Mail-Adresse an die Werbepartner zu Sperrzwecken zuzustimmen, gemäß § 275 BGB oder § 242 BGB Unmöglichkeit bzw. Unzumutbarkeit entgegenstehen. Nur insoweit kommt eine Teilabweisung des Unterlassungsanspruchs in Betracht. Da die Beklagte bereits im vorliegenden Erkenntnisverfahren geltend gemacht hat, dass ihr die erforderlichen Maßnahmen wegen der Weigerung des Klägers unmöglich oder unzumutbar seien, kann die Frage nach den unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes gebotenen Handlungen entgegen der Ansicht der Revision auch nicht dem Vollstreckungsverfahren überlassen werden (vgl. nur BGH, Beschluss vom 29. September 2016 – I ZB 34/15, WM 2017, 145 Rn. 29).

aa) Eine etwaige Unmöglichkeit gemäß § 275 BGB oder Unzumutbarkeit gemäß § 242 BGB scheidet allerdings von vornherein aus, wenn der Widerspruch des Klägers gegen die Weiterleitung seiner E-Mail-Adresse zu Sperrzwecken ganz oder teilweise unbeachtlich wäre, § 28 Abs. 1 Nr. 2 BDSG. Nach dieser Vorschrift ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen (vgl. Plath, BDSG, 2. Aufl., § 28 Rn. 47; Gola/Schomerus, BDSG, 12. Aufl., § 28 Rn. 24; Taeger/Gabel, BDSG, 2. Aufl., § 28 Rn. 55; Simitis, BDSG, 8. Aufl. § 28 Rn. 104 ff.) der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Dabei kann die Interessenabwägung grundsätzlich auch dann zugunsten der verantwortlichen Stelle ausfallen, wenn der Betroffene der Datenverarbeitung (ausdrücklich) widersprochen hat (Plath, aaO Rn. 54; Simitis, aaO Rn. 109; Taeger/Gabel, aaO Rn. 63).

Es ist ein berechtigtes Interesse der Beklagten, ihre sich aus dem bestehenden Unterlassungsanspruch ergebende Verpflichtung zur Folgenbeseitigung zu erfüllen. Daher erscheint es vorliegend nicht ausgeschlossen, dass eine zur Wahrung dieses berechtigten Interesses der Beklagten erforderliche und nach der gebotenen Interessenabwägung zulässige Maßnahme – die beispielsweise in der einmaligen Weitergabe der Adresse nur zum Zwecke ihrer Löschung aus den von den Werbepartnern der Beklagten verwendeten Verzeichnissen liegen könnte – der Beklagten trotz des Widerspruchs des Klägers eine ausreichende Folgenbeseitigung ermöglicht. Dazu sind Feststellungen bislang nicht getroffen worden.

bb) Nur wenn und soweit der Widerspruch des Klägers in Bezug auf die Verwendung seiner E-Mail-Adresse zu Sperrzwecken zu beachten ist, er mithin eine effektive Durchsetzung seines Unterlassungsanspruchs bezogen auf Werbe-E-Mails an die bekannte E-Mail-Adresse verhindert oder in erheblichem Maße erschwert, könnte der Einwand der Unmöglichkeit oder des Rechtsmissbrauchs durchgreifen. Auch zu Handlungsmöglichkeiten der Beklagten zur Umsetzung des Unterlassungsgebotes insoweit, möglicherweise ohne Weiterleitung der E-Mail-Adresse des Klägers, beispielsweise lediglich unter Verwendung seines Namens, sind aber bisher keine ausreichenden Feststellungen getroffen worden.

C. Gemäß § 563 Abs. 1 Satz 1 ZPO ist das Berufungsurteil aufzuheben und die Sache an das Berufungsgericht zurückzuverweisen. Eine Entscheidung in der Sache selbst (§ 563 Abs. 3 ZPO) kommt nicht in Betracht, weil dem angefochtenen Urteil wie dargelegt notwendige Feststellungen fehlen.

Pflicht zur Teilnahme an einem das Fahrverhalten von Busfahrern erfassenden elektronischen Warn- und Berichtssystem

(**Bundesarbeitsgericht**, Urteil vom 17. November 2016 – 2 AZR 730/15 –)

1. **Die Erfassung des Fahrverhaltens von Busfahrern durch ein elektronisches Warn- und Leitsystem kann nach § 32 Abs. 1 Satz 1 BDSG zulässig sein.**
2. **Ist die Zulässigkeit nach § 32 Abs. 1 S. 1 BDSG gegeben, kann dahinstehen, ob auch allein die diesbezüglichen Regelungen einer Betriebsvereinbarung eine die Datenverarbeitung gestattende Rechtsvorschrift iSd. § 4 Abs. 1 BDSG sein können.**
3. **Nach Beendigung des Arbeitsverhältnisses kann ein Anspruch auf Entfernung von Abmahnungen nach §§ 242, 1004 Abs. 1 Satz 1 BGB nur dann bestehen, wenn es objektive Anhaltspunkte dafür gibt, dass die Abmahnung dem Arbeitnehmer noch schaden kann (BAG 19. April 2012 – 2 AZR 233/11 – Rn. 51).**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien streiten über die Wirksamkeit einer außerordentlichen Kündigung mit Auslauffrist sowie die Entfernung von Abmahnungen aus der Personalakte des Klägers.

Die Beklagte betreibt öffentlichen Nahverkehr. Der Kläger war bei ihr seit Oktober 1989 als Busfahrer beschäftigt. Auf das Arbeitsverhältnis fand aufgrund arbeitsvertraglicher Bezugnahme der Spartentarifvertrag für Nahverkehrsbetriebe (TV-N NW) vom 25. Mai 2001 Anwendung. Nach dessen § 20 Abs. 6 Unterabs. 1 kann das Arbeitsverhältnis nach einer Betriebszugehörigkeit von mehr als 15 Jahren durch den Arbeitgeber nur noch „aus einem wichtigen Grund (§ 626 Abs. 1 BGB)“ gekündigt werden.

Die Beklagte schloss mit ihrem Betriebsrat im Jahre 2014 eine Betriebsvereinbarung über den Einsatz des sog. RIBAS-Systems (BV) auf ihren Fahrzeugen. Dieses wertet elektronisch Fahrereignisse aus und informiert die Busfahrer durch eine Warnleuchte über hochtouriges Fahren, Leerlaufzeitüberschreitungen, scharfes Bremsen, überhöhte Beschleunigung und Geschwindigkeitsüberschreitungen. Die Daten werden aufgezeichnet und gespeichert.

Nach der BV sind alle Fahrer zur Teilnahme am RIBAS-System verpflichtet. Fahrer, die nicht an dem vorgesehenen personalisierten Berichts- und Prämiensystem teilnehmen wollen, erhalten einen anonymisierten Systemschlüssel. Aufgrund von Einwendungen des Landesdatenschutzbeauftragten hatten die Betriebsparteien die BV entsprechend angepasst.

Der Kläger stimmte einer Teilnahme am personalisierten Berichts- und Prämiensystem nicht zu. Ihm wurde Ende August 2014 der anonymisierte RIBAS-Schlüssel zur Nutzung übergeben. Das entsprechende Empfangsbekenntnis sandte er nicht zurück. In einem von der Beklagten veranlassten Gespräch Mitte Oktober 2014 teilte er mit, er habe seinen Teamleiter so verstanden, dass er wählen könne, ob er – überhaupt – an dem System teilnehme.

Ende Oktober 2014 führten der Fachbereichsleiter Personal und der Leiter des Omnibusbetriebs ein weiteres Gespräch mit dem Kläger. Sie erläuterten ihm das RIBAS-System und wiesen auf die Beteiligung des Landesdatenschutzbeauftragten hin. Der Kläger wurde aufgefordert, den anonymisierten RIBAS-Schlüssel ab sofort zu verwenden. Dem kam er auch nach einer entsprechenden Schulung nicht nach. Die Beklagte mahnte den Kläger deshalb im Dezember 2014 ab und wies ihn darauf hin, dass er sich zur Vermeidung arbeitsrechtlicher Konsequenzen vor jeder Fahrt im System anzumelden habe.

Eine erneute Einweisung in das System lehnte der Kläger ab. Er nutzte seinen RIBAS-Schlüssel im Januar 2015 an sechs Arbeitstagen, an elf Arbeitstagen wiederum nicht. Ende Januar 2015 führte der Kläger ein Gespräch mit seinem Teamleiter. Diesem erklärte er, sich zu der Angelegenheit nicht mehr äußern und sie gerichtlich klären lassen zu wollen.

Anfang Februar 2015 erteilte die Beklagte dem Kläger eine weitere Abmahnung. Bei der Übergabe des Schreibens wies sie den Kläger darauf hin, sie erwarte – unabhängig von seiner Ankündigung, eine gerichtliche Klärung herbeizuführen – die Einhaltung des in der BV geregelten Verfahrens. Der Kläger setzte den RIBAS-Schlüssel weiterhin nicht ein. Die Beklagte erteilte ihm deshalb unter dem 26. Februar 2015 eine dritte Abmahnung und forderte ihn noch einmal eindringlich auf, sich vor jedem Dienstantritt im System anzumelden. Beide Schreiben gingen dem Kläger am 4. März 2015 zu. Am 5. und am 6. März 2015 meldete er sich erneut nicht im System an.

Die Beklagte hörte den Betriebsrat mit Schreiben vom 10. März 2015 zu ihrer Absicht an, das Arbeitsverhältnis der Parteien außerordentlich fristlos, hilfsweise außerordentlich mit einer sozialen Auslauffrist von sechs Monaten zum Schluss eines Kalendervierteljahres zu kündigen. Der Betriebsrat erklärte am Folgetag seine Zustimmung zu den beabsichtigten Kündigungen.

Mit Schreiben vom 12. März 2015, das dem Kläger am selben Tag zuging, kündigte die Beklagte das Arbeitsverhältnis der Parteien außerordentlich zum 13. März 2015, hilfsweise außerordentlich mit Auslauffrist zum 30. September 2015.

Dagegen hat sich der Kläger rechtzeitig mit der vorliegenden Kündigungsschutzklage gewandt. Er hat gemeint, ein wichtiger Grund zur außerordentlichen Kündigung liege nicht vor. Er sei nicht zur Teilnahme am RIBAS-System verpflichtet gewesen. Die BV sei unwirksam. Er habe nicht schuldhaft gehandelt, sondern sich in einem gut begründeten und vertretbaren Verbotsirrtum befunden. Der Lauf der Frist des § 626 Abs. 2 BGB habe überdies bereits mit seiner Erklärung begonnen, den Schlüssel bis zu einer gerichtlichen Klärung nicht zu bedienen. Die ausgesprochenen Abmahnungen seien zu Unrecht erfolgt und aus seiner Personalakte zu entfernen.

Aus den Gründen:

Die Revision ist unbegründet. Das Landesarbeitsgericht hat die außerordentliche Kündigung mit Auslauffrist zu Recht als wirksam angesehen (II.). Ein Anspruch des Klägers auf Entfernung der ihm erteilten Abmahnungen aus der Personalakte besteht nicht (III.).

II. Die Würdigung des Landesarbeitsgerichts, für die außerordentliche Kündigung mit sozialer Auslauffrist habe ein wichtiger Grund iSd. § 20 Abs. 6 Unterabs. 1 TV-N NW, § 626 Abs. 1 BGB vorgelegen, hält einer revisionsrechtlichen Überprüfung stand.

1. Nach dem kraft einzelvertraglicher Bezugnahme anwendbaren § 20 Abs. 6 Unterabs. 1 TV-N NW konnte das Arbeitsverhältnis der Parteien durch die Beklagte nur noch aus wichtigem Grund iSd. § 626 Abs. 1 BGB gekündigt werden. Der Kläger war im Zeitpunkt der Kündigung weit mehr als 15 Jahre beschäftigt.

2. Die Tarifbestimmung verweist im Zusammenhang mit dem Begriff des wichtigen Grundes auf die Regelung des § 626 Abs. 1 BGB. Deren Verständnis ist deshalb auch für die Auslegung der Tarifnorm maßgebend (vgl. BAG 13. Mai 2015 – 2 AZR 531/14 – Rn. 26; 31. Juli 2014 – 2 AZR 407/13 – Rn. 23). Nach § 626 Abs. 1 BGB kann das Arbeitsverhältnis aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, aufgrund derer dem Kündigenden unter Berücksichtigung der Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung nicht zugemutet werden kann.

a) Dafür ist zunächst zu prüfen, ob der Sachverhalt ohne seine besonderen Umstände „an sich“, dh. typischerweise als wichtiger Grund geeignet ist. Alsdann bedarf es der Prüfung, ob dem Kündigenden die Fortsetzung des Arbeitsverhältnisses unter Berücksichtigung der konkreten Umstände des Falls und unter Abwägung der Interessen beider Vertragsteile jedenfalls bis zum Ablauf der Kündigungsfrist zumutbar ist oder nicht (BAG 13. Mai 2015 – 2 AZR 531/14 – Rn. 28; 31. Juli 2014 – 2 AZR 407/13 – Rn. 25). Ein wichtiger Grund iSd. § 626 Abs. 1 BGB liegt auch im Verhältnis zu einem Arbeitnehmer, dessen Arbeitsverhältnis ordentlich nicht gekündigt werden kann, dann vor, wenn es dem Arbeitgeber unter Berücksichtigung aller Umstände des Einzelfalls – objektiv – nicht zuzumuten ist, den Arbeitnehmer auch nur bis zum Ablauf der (fiktiven) ordentlichen Kündigungsfrist weiter zu beschäftigen. In diesem Fall wäre eine außerordentliche Kündigung auch dann gerechtfertigt, wenn die ordentliche Kündigung nicht ausgeschlossen wäre (BAG 13. Mai 2015 – 2 AZR 531/14 – Rn. 42).

b) Darüber hinaus kann ein pflichtwidriges Verhalten, das bei einem Arbeitnehmer ohne Sonderkündigungsschutz nur eine ordentliche Kündigung rechtfertigen würde, unter Umständen gerade wegen der infolge des Ausschlusses der ordentlichen Kündigung langen Bindungsdauer ebenfalls einen wichtigen Grund

iSd. § 626 Abs. 1 BGB zur außerordentlichen Kündigung durch den Arbeitgeber darstellen. Zwar wirkt sich der Sonderkündigungsschutz insofern zum Nachteil für den Arbeitnehmer aus. Dies ist jedoch im Begriff des wichtigen Grundes gem. § 626 Abs. 1 BGB angelegt. Dieser richtet sich nach der Zumutbarkeit einer Fortsetzung des Dienstverhältnisses bis zum Ablauf der Kündigungsfrist oder der vereinbarten Beendigung des Dienstverhältnisses. Zur Vermeidung eines Wertungswiderspruchs muss in einem solchen Fall allerdings zugunsten des Arbeitnehmers zwingend eine der fiktiven ordentlichen Kündigungsfrist entsprechende Auslauffrist eingehalten werden. Der Arbeitnehmer, dessen Arbeitsverhältnis vom Arbeitgeber ordentlich nicht gekündigt werden kann, darf im Ergebnis nicht schlechter gestellt sein, als wenn er dem Sonderkündigungsschutz nicht unterfiele (BAG 13. Mai 2015 – 2 AZR 531/14 – Rn. 44; 15. November 2001 – 2 AZR 605/00 – zu II 5 a, b der Gründe, BAGE 99, 331).

3. Von diesen Grundsätzen ist auch das Landesarbeitsgericht ausgegangen und hat sie ohne Rechtsfehler auf den Streitfall angewandt.

a) Der Kläger hat es wiederholt vorsätzlich unterlassen, den für Fahrer, die nicht an dem personalisierten System teilnehmen, vorgesehenen anonymisierten RIBAS-Schlüssel zu verwenden. Er hat dadurch beharrlich seine arbeitsvertragliche Leistungspflicht verletzt. Dies ist „an sich" geeignet, einen wichtigen Grund für eine außerordentliche Kündigung iSd. § 626 Abs. 1 BGB zu bilden.

aa) Die Pflicht zur Verwendung des Schlüssels folgt aus § 77 Abs. 4 Satz 1 BetrVG iVm. § 4 BV. Nach § 4 Abs. 1 BV ist die Anmeldung eines jeden Fahrers an das RIBAS-System „zwingend erforderlich". Gem. § 4 Abs. 2 Satz 4 BV bleibt die „Pflicht zur generellen Teilnahme am System" bestehen, auch wenn der Fahrer seine Zustimmung zur Datenerhebung im personalisierten System nicht erteilt. Dafür erhält der Fahrer nach § 4 Abs. 2 Satz 2 BV einen anonymisierten Schlüssel.

bb) Die gem. § 77 Abs. 4 Satz 1 BetrVG auch für den Kläger begründete Pflicht zur Teilnahme am RIBAS-System steht mit höherrangigem Recht im Einklang. Sie verletzt insbesondere nicht § 75 Abs. 2 Satz 1 BetrVG iVm. Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG.

(1) Zu dem durch Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrecht gehört das Recht auf informationelle Selbstbestimmung. Dieses garantiert die Befugnis, selbst über die Preisgabe und Verwendung persönlicher Daten zu befinden (BVerfG 11. März 2008 – 1 BvR 2074/05 ua. – BVerfGE 120, 378; BAG 21. November 2013 – 2 AZR 797/11 – Rn. 45, BAGE 146, 303). Der Achtung dieses Rechts dient zudem Art. 8 Abs. 1 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) (BAG 21. November 2013 – 2 AZR 797/11 – aaO; BGH 15. Mai 2013 – XII ZB 107/08 – Rn. 14). Die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) über die Anforderungen an eine zulässige Datenverarbeitung konkretisieren und aktualisieren den Schutz des Rechts auf informationelle Selbstbestimmung. Sie regeln, in welchem Umfang im Anwendungsbereich des Gesetzes Eingriffe durch öffentliche oder nichtöffentliche Stellen iSd. § 1 Abs. 2 BDSG in diese Rechtspositionen zulässig sind (vgl. BAG 21. November 2013 – 2 AZR 797/11 – aaO).

(2) Danach ist das Recht des Klägers auf informationelle Selbstbestimmung durch die in § 4 BV begründete Verpflichtung, zumindest mithilfe des anonymisierten Schlüssels am RIBAS-System teilzunehmen, nicht verletzt. Zwar hat der Kläger in die damit verbundene Erhebung, Verarbeitung und Nutzung personenbezogener Daten nicht iSd. § 4 Abs. 1 BDSG eingewilligt. Diese ist aber gem. § 32 Abs. 1 Satz 1 BDSG und damit durch eine Rechtsvorschrift iSd. § 4 Abs. 1 BDSG gerechtfertigt. Es bedarf demnach keiner Entscheidung, ob auch allein die Regelungen der BV eine die Datenerhebung, -verarbeitung oder -nutzung gestattende Rechtsvorschrift iSd. § 4 Abs. 1 BDSG sein können.

(a) Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses ua. dann erhoben, verarbeitet oder genutzt werden, wenn dies für dessen Durchführung erforderlich ist. Um personenbezogene Daten iSd. § 3 Abs. 1 BDSG handelt es sich auch bei einer zunächst anonymisierten Erhebung, Verarbeitung oder Nutzung, wenn die Anonymisierung ohne unangemessenen Aufwand aufgehoben werden kann. Es genügt, wie ein Umkehrschluss aus § 3 Abs. 6 BDSG ergibt, dass die betroffene Person ohne besondere Schwierigkeiten bestimmbar ist (Gola/ Schomerus, BDSG 12. Aufl. § 3 Rn. 10; Simitis/Dammann, BDSG 8. Aufl. § 3 Rn. 23; Plath/Schreiber, BDSG § 3 Rn. 15; Erbs/Kohlhaas, Strafrechtliche Nebengesetze, Stand 2015 § 3 BDSG Rn. 3; zum Begriff der personenbezogenen Daten iSd. RL 95/46/EG EuGH 19. Oktober 2016 – C-582/14 – Rn. 49). So liegt der Fall hier. Nach den Feststellungen des Landesarbeitsgerichts kann der Anonymisierungsschutz im RIBAS-System im Grundsatz ohne großen Aufwand durch Hinzuziehung der Dienstpläne aufgehoben werden. Eine entsprechende Personalisierung ist auch – in Abstimmung mit dem Betriebsrat – nach § 10 Satz 3 BV zur Ermittlung von Schulungsbedarf vorgesehen, sofern im anonymisierten Fahrdatenbestand erhebliche Überschreitungen der Grenzwerte im Vergleich zu durchschnittlichen Ergebnissen erkennbar werden.

(b) § 32 Abs. 1 Satz 1 BDSG kodifiziert die von der Rechtsprechung aus dem verfassungsrechtlich geschützten allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) abgeleiteten allgemeinen Grundsätze zum Datenschutz im Beschäftigungsverhältnis (BT-Drs. 16/13657 S. 21). Dabei nimmt die Gesetzesbegründung zur Konkretisierung des Maßstabs der Erforderlichkeit einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Durchführung oder Beendigung eines Beschäftigungsverhältnisses auf die Entscheidungen des Bundesarbeitsgerichts vom 22. Oktober 1986 (– 5 AZR 660/85 –) und 7. September 1995 (– 8 AZR 828/93 –) Bezug. Diesen zufolge dürfe sich der Arbeitgeber bei seinen Beschäftigten nicht nur über Umstände informieren oder Daten verwenden, um seine vertraglichen Pflichten ihnen gegenüber erfüllen zu können, wie zB Pflichten im Zusammenhang mit der Personalverwaltung, Lohn- und Gehaltsabrechnung, sondern auch, um seine im Zusammenhang mit der Durchführung des Beschäftigungsverhältnisses bestehenden Rechte wahrzunehmen, zB durch Ausübung des Weisungsrechts oder durch Kontrollen der Leistung oder des Verhaltens des Beschäftigten (BT-Drs. 16/13657 aaO).

(c) Erforderlichkeit iSd. § 32 Abs. 1 Satz 1 BDSG setzt damit ein berechtigtes Interesse des Arbeitgebers an der Datenerhebung, -verarbeitung oder -nutzung voraus, das aus dem bestehenden Arbeitsverhältnis herrühren muss. Es muss ein Zusammenhang mit der Erfüllung der vom Arbeitnehmer geschuldeten vertraglichen Leistung, seiner sonstigen Pflichtenbindung oder mit der Pflichtenbindung des Arbeitgebers bestehen (BAG 7. September 1995 – 8 AZR 828/93 – zu II 2 c aa der Gründe, BAGE 81, 15). Die Datenerhebung, -verarbeitung oder -nutzung darf ferner keine übermäßige Belastung für den Arbeitnehmer

darstellen. Sie muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen. Greift eine Maßnahme in das allgemeine Persönlichkeitsrecht des Arbeitnehmers ein, muss der Eingriff einer Abwägung der beiderseitigen Interessen nach dem Grundsatz der Verhältnismäßigkeit standhalten (BAG 7. September 1995 – 8 AZR 828/93 – zu II 2 c bb der Gründe, aaO; 22. Oktober 1986 – 5 AZR 660/85 – zu B I 2 a der Gründe, BAGE 53, 226). Dieser verlangt, dass der Eingriff geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen (BAG 15. April 2014 – 1 ABR 2/13 (B) – Rn. 41, BAGE 148, 26; 29. Juni 2004 – 1 ABR 21/03 – zu B I 2 d der Gründe, BAGE 111, 173). Es dürfen keine anderen, zur Zielerreichung gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkenden Mittel zur Verfügung stehen. Die Verhältnismäßigkeit im engeren Sinne ist gewahrt, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht (BVerfG 4. April 2006 – 1 BvR 518/02 – zu B I 2 b dd der Gründe, BVerfGE 115, 320; BAG 15. April 2014 – 1 ABR 2/13 (B) – aaO).

(d) Danach hat das Landesarbeitsgericht zu Recht angenommen, die Verpflichtung des Klägers, zumindest mit dem anonymisierten Schlüssel am RIBAS-System teilzunehmen, greife nicht unverhältnismäßig in sein Recht auf informationelle Selbstbestimmung ein. Dies gilt auch dann, wenn die Betriebsparteien hinsichtlich Eignung und Erforderlichkeit des Eingriffs entgegen der Auffassung des Landesarbeitsgerichts (ebenso BAG 29. Juni 2004 – 1 ABR 21/03 – zu B I 2 d aa und bb der Gründe, BAGE 111, 173) nicht über einen vergleichbaren Beurteilungsspielraum wie der Gesetzgeber verfügen.

(aa) Das berechtigte Interesse der Beklagten an der Verwendung des RIBAS-Systems besteht darin, dass die bei ihr beschäftigten Busfahrer zu einer vorausschauenden und sparsamen Fahrweise angehalten werden sollen (§ 2 BV). Das betrifft unmittelbar die von ihnen geschuldete Arbeitsleistung und damit die Durchführung des Beschäftigungsverhältnisses iSd. § 32 Abs. 1 Satz 1 BDSG. Die verfolgten Ziele einer Reduzierung des Kraftstoffverbrauchs sowie einer Steigerung der Kundenzufriedenheit sind, wie das Landesarbeitsgericht zutreffend erkannt hat, nicht unbillig oder unrechtmäßig, sondern ökonomisch vernünftig und liegen zudem im ökologischen Interesse der Allgemeinheit. Das System hält die Busfahrer nicht, wie die Revision meint, in Bezug auf ihr Bremsverhalten zu einem straßenverkehrswidrigen Verhalten an. Dass es darauf hinweist und es aufzeichnet, wenn ein Fahrer scharf gebremst hat, heißt nicht, er solle auch dann nicht entsprechend reagieren, wenn die Verkehrssituation es erfordert.

(bb) Die Teilnahme der Busfahrer am RIBAS-System ist zur Erreichung dieser Ziele geeignet. Das Landesarbeitsgericht verweist zu Recht darauf, dass das System sowohl die Selbstkontrolle fördert als auch Erkenntnisse über einen etwaigen Schulungsbedarf aufgrund des Vergleichs von Fahrleistungen mit den durchschnittlichen Grenzwerten ermöglicht.

(cc) Zur Erreichung der verfolgten Ziele ist die Teilnahme aller Busfahrer, auch die des Klägers, erforderlich. Das RIBAS-System soll Durchschnittswerte ermitteln und bei erheblichen Abweichungen einen hierdurch begründeten konkreten Schulungsbedarf identifizieren. Dafür müssen alle Busfahrer – zumindest anonymisiert – daran teilnehmen. Dem trägt die nach § 4 Abs. 1 BV vorgesehene, für alle Busfahrer verpflichtende Teilnahme am System Rechnung. Ein anderes gleichermaßen geeignetes und der Beklagten zumutbares, das informationelle Selbstbestimmungsrecht des Klägers weniger berührendes Mittel ist nicht ersichtlich. So wäre eine ausschließlich freiwillige Teilnahme oder die Beschränkung auf eine elektronische Signalgebung unmittelbar im Anschluss an ein Fahrmanöver ohne eine weitere Speicherung der Daten zur Ermittlung von Schulungsbedarf nicht ausreichend. Durch ein Mitfahren von Fahrtrainern mag zwar Schulungsbedarf identifiziert werden können. Es ersetzte aber nicht den Erkenntnisgewinn durch die Ermittlung der Durchschnittswerte aller Fahrer und regte auch nicht in gleicher Weise zur Selbstkontrolle des Fahrverhaltens an wie das RIBAS-System. Ausschließlich vorbeugende Schulungen hätten diesen Effekt ebenso wenig. Der Einwand des Klägers, eine Ausrüstung der Busse mit technischen „Begrenzungsmechanismen“ betreffend „Verzögerung, Drehzahl und Geschwindigkeit“ wäre eine mildere, ebenso effektive Möglichkeit gewesen, lässt nicht erkennen, dass dadurch in gleich geeigneter Weise wie durch das RIBAS-System eine vorausschauende und sparsame Fahrweise gefördert werden könnte. Der Kläger macht nicht mit einer Verfahrensrüge geltend, hierzu bereits in den Vorinstanzen vorgetragen zu haben. Entsprechendes gilt für seine Behauptung, es wäre auch eine Kombination aus den von ihm benannten alternativen Maßnahmen möglich gewesen.

(dd) Die Verhältnismäßigkeit im engeren Sinne ist gewahrt. Die Beeinträchtigung des informationellen Selbstbestimmungsrechts des Klägers steht nicht außer Verhältnis zu den von der Beklagten legitimerweise verfolgten Interessen. Es liegt keine Dauerüberwachung in dem Sinne vor, dass die Busfahrer – wie bei einer Videoüberwachung – in ihrem gesamten Verhalten während der Arbeitszeit kontrolliert würden. Gespeichert werden allein die Daten zu den fraglichen Fahrmanövern und dies im Grundsatz auch nur zur Ermittlung der Durchschnittswerte. Dem einzelnen Fahrer zugeordnet werden die Daten lediglich dann, wenn er dem zugestimmt hat oder es in seiner Fahrleistung erhebliche Abweichungen vom Durchschnitt gibt. Dadurch ermöglicht das System in erster Linie eine Selbstkontrolle der Busfahrer. Eine personalisierte Leistungskontrolle ist dagegen, wenn der Fahrer ihr nicht durch Teilnahme am Prämiensystem zugestimmt hat, nur aus gegebenem Anlass und ausschließlich zur Ermittlung von Schulungsbedarf zulässig. Ob im Einzelfall die Voraussetzungen für eine Personalisierung gegeben wären, ist dabei nach § 10 Satz 3 BV in Abstimmung mit dem Betriebsrat festzustellen und unterläge ggf. gesonderter Überprüfung. Die Vorgabe, die Personalisierung dürfe nur bei einer erheblichen Überschreitung der Grenzwerte erfolgen, trägt dem Maßstab des § 32 Abs. 1 Satz 1 BDSG im Grundsatz hinreichend Rechnung. Zudem ordnet § 11 BV an, dass die Bestimmungen des BDSG einzuhalten sind. Daraus folgt nicht etwa eine besondere Missbrauchsgefahr, wie die Revision zu Bedenken gibt, sondern die Garantie eines Schutzstandards entsprechend dem Gesetz. In Bezug genommen sind damit insbesondere auch die Verantwortung der Beklagten für eine Auftragsdatenverarbeitung nach § 11 BDSG sowie die Ansprüche auf Löschung oder Sperrung von Daten gem. § 35 BDSG.

cc) Die den Inhalt der von ihm zu erbringenden Arbeitsleistung als Busfahrer ausgestaltende Pflicht zur Teilnahme am RIBAS-System hat der Kläger beharrlich und vorsätzlich verletzt. Er ist seiner Verpflichtung, sich im System anzumelden, wiederholt nicht nachgekommen, obwohl er von der Beklagten mehrfach darauf hingewiesen wurde, dass dies für eine ordnungsgemäße Vertragserfüllung unerlässlich sei. Der Kläger hat es bewusst in Kauf genommen, dadurch nachhaltig seine arbeitsvertraglichen Leistungspflichten zu verletzen. Er unterlag insofern keinem unverschuldeten Rechtsirrtum.

(1) Der Geltungsanspruch des Rechts bewirkt, dass der Schuldner das Risiko eines Rechtsirrtums grundsätzlich selbst trägt und es nicht dem Gläubiger überbürden kann (BAG 22. Oktober 2015 – 2 AZR 569/14 – Rn. 43, BAGE 153, 111; 19. August 2015 – 5 AZR 975/13 – Rn. 31, BAGE 152, 213). Ein unverschuldeter Rechtsirrtum liegt nur vor, wenn der Schuldner seinen Irrtum auch unter Anwendung der zu beachtenden Sorgfalt nicht erkennen konnte. Dabei sind strenge Maßstäbe anzulegen. Es reicht nicht aus, dass er sich für seine eigene Rechtsauffassung auf eine eigene Prüfung und fachkundige Beratung stützen kann. Ein Unterliegen in einem möglichen Rechtsstreit muss zwar nicht undenkbar sein (BAG 12. November 1992 – 8 AZR 503/91 – zu I 1 der Gründe, BAGE 71, 350). Gleichwohl liegt ein entschuldbarer Rechtsirrtum nur dann vor, wenn der Schuldner damit nach sorgfältiger Prüfung der Sach- und Rechtslage nicht zu rechnen brauchte; ein normales Prozessrisiko entlastet ihn nicht (BAG 22. Oktober 2015 – 2 AZR 569/14 – aaO; 29. August 2013 – 2 AZR 273/12 – Rn. 34; BGH 6. Dezember 2006 – IV ZR 34/05 – zu II 1 a aa der Gründe; 27. September 1989 – IVa ZR 156/88 -).

(2) Hier hat der Kläger das Risiko, mit seiner Einschätzung falsch liegen zu können, nicht verkannt. Er hat lediglich gemeint, die Teilnahme am RIBAS-System zumindest so lange verweigern zu können, bis die Rechtslage durch die Gerichte geklärt sei. Damit hat er es bewusst darauf ankommen lassen, sich pflichtwidrig zu verhalten. Die Beklagte hatte ihn mehrfach auf ihre Sichtweise hingewiesen sowie darauf, dass der Landesdatenschutzbeauftragte in die Ausgestaltung der BV einbezogen gewesen war. Für den Kläger stritt auch nicht etwa eine höchstrichterliche Entscheidung in einem vergleichbaren Fall (zu einer solchen Konstellation BAG 19. August 2015 – 5 AZR 975/13 – Rn. 31 f., BAGE 152, 213). Unerheblich ist, ob er mit seinem Vorbringen, einen Rechtsanwalt um Rechtsauskunft gebeten zu haben, in der Revision noch gehört werden könnte. Selbst dies zu Gunsten des Klägers unterstellt, läge kein unverschuldeter Rechtsirrtum vor. Der Kläger behauptet insbesondere nicht, der Rechtsanwalt habe ihn dahingehend beraten, es bestehe kein Risiko für eine andere rechtliche Bewertung durch die Gerichte.

b) Die Interessenabwägung des Landesarbeitsgerichts ist revisionsrechtlich nicht zu beanstanden.

aa) Eine außerordentliche Kündigung mit notwendiger Auslauffrist kam grundsätzlich in Betracht. Das Landesarbeitsgericht hat angenommen, der Beklagten wäre bei einem ordentlich kündbaren Arbeitnehmer die Einhaltung der Kündigungsfrist von sechs Wochen zum Quartalsende zumutbar gewesen. Dies steht aufgrund seiner Entscheidung, die außerordentliche fristlose Kündigung der Beklagten habe das Arbeitsverhältnis der Parteien nicht aufgelöst, rechtskräftig fest. Die Würdigung, ein bestimmter Lebenssachverhalt könne eine Kündigung materiell nicht begründen, nimmt an der Rechtskraftwirkung der Entscheidung gem. § 322 ZPO teil (BAG 20. Dezember 2012 – 2 AZR 867/11 – Rn. 27).

bb) Bei der Würdigung, eine Fortsetzung des Arbeitsverhältnisses noch bis zum Eintritt des ordentlich nicht mehr kündbaren Klägers in den Ruhestand sei der Beklagten jedoch nicht zuzumuten gewesen, hat das Landesarbeitsgericht alle relevanten widerstreitenden Interessen berücksichtigt und in vertretbarer Weise gegeneinander abgewogen. Auch die Revision zeigt insoweit keinen Rechtsfehler auf.

(1) Zwar hat das Landesarbeitsgericht nicht ausdrücklich gewürdigt, welche „Nachteile“ der Beklagten aus der Weigerung des Klägers entstehen. Es hat aber ihrem Interesse, das RIBAS-System, wie nach der BV vorgesehen, umfänglich und damit auch im Verhältnis zum Kläger zur Anwendung zu bringen, erkennbar ein hohes Gewicht beigemessen. Dies ergibt sich aus seinen Erwägungen zur Schutzwürdigkeit der verfolgten Interessen bei der Prüfung der Verhältnismäßigkeit des dadurch bewirkten Eingriffs in das allgemeine Persönlichkeitsrecht des Klägers und entspricht der durch die Betriebsparteien vorgenommenen Wertung, die Anmeldung eines jeden Fahrers an das RIBAS-System sei „zwingend erforderlich“ (§ 4 Abs. 1 BV). Auch für langjährig Beschäftigte war danach keine Ausnahme vorgesehen. Der Nachteil, das RIBAS-System gegenüber dem Kläger zumindest für die Dauer eines Rechtsstreits darüber nicht und damit nicht in der von den Betriebsparteien vorgesehenen Weise unter Einbeziehung aller Busfahrer effektiv nutzen zu können, wog nach der revisionsrechtlich nicht zu beanstandenden Abwägung des Landesarbeitsgerichts selbst unter Berücksichtigung der langjährigen Betriebszugehörigkeit des Klägers besonders schwer. Dabei hat das Landesarbeitsgericht zu Recht berücksichtigt, dass die Weigerung des Klägers beharrlich war und, wie die erfolglos gebliebenen Abmahnungen gezeigt haben, nicht mehr zu erwarten stand, dass er durch eine erneute Abmahnung zu vertragstreuem Verhalten angehalten werden könnte. Soweit der Kläger geltend macht, die Beklagte habe zumindest die Durchführung des Gütetermins in dem schon anhängigen Rechtsstreit gegen die erteilten Abmahnungen abwarten müssen, verkennt er, dass es auch nach seinem Vorbringen keinen Anhaltspunkt dafür gab, er werde bereits im Anschluss an diesen Termin seine Weigerungshaltung aufgeben. Vielmehr hatte er ausdrücklich angekündigt, zunächst eine gerichtliche „Klärung“ herbeiführen zu wollen, die jedoch in einem Gütetermin noch nicht zu erwarten stand.

(2) Die vom Kläger erhobene Verfahrensrüge, das Landesarbeitsgericht habe auf bestrittenen Vortrag zu der Frage abgestellt, weshalb eine Unterbrechung der Zündung vor Dienstantritt des nächsten Fahrers auf Dauer keine zumutbare Alternative sei, ist – ungeachtet seiner Entscheidungserheblichkeit für die Revision – unzulässig. Der Kläger legt schon nicht dar, an welcher Stelle welches Schriftsatzes oder in welcher Weise in der mündlichen Verhandlung er das entsprechende Vorbringen der Beklagten bestritten habe. Es kann daher dahinstehen, ob er dies nicht ohnehin nur mit einem Tatbestandsberichtigungsantrag nach § 320 ZPO hätte geltend machen können.

(3) Den Umstand, dass der Kläger sich in einem – wenn auch nicht unverschuldeten – Rechtsirrtum in Bezug auf die Pflicht, am RIBAS-System teilzunehmen, befunden hat, hat das Landesarbeitsgericht ebenfalls vertretbar gewürdigt. Es hat den Irrtum deshalb nicht ausschlaggebend zu seinen Gunsten gewertet, weil es dem Kläger zumutbar gewesen sei, den anonymisierten Schlüssel zumindest unter dem Vorbehalt einer gerichtlichen Prüfung zunächst zu nutzen. Auch dies begegnet mit Blick darauf, dass es sich um ein kollektiv eingeführtes und zudem unter Beteiligung des Landesdatenschutzbeauftragten etabliertes System handelte, keinen durchgreifenden Bedenken.

4. Die Beklagte hat die Kündigungserklärungsfrist gem. § 626 Abs. 2 BGB gewahrt. Grund für die Kündigung war, dass der Kläger sich wiederholt nicht im RIBAS-System angemeldet hatte. Zuletzt war dies am 5. und 6. März 2015 der Fall gewesen. Die Kündigung ging dem Kläger am 12. März 2015 und damit innerhalb von zwei Wochen zu.

III. Der Kläger hat keinen Anspruch aus §§ 242, 1004 Abs. 1 Satz 1 BGB auf Entfernung der Abmahnungen vom 18. Dezember 2014, 5. Februar 2015 und 26. Februar 2015 aus seiner Personalakte. Ein Anspruch auf Löschung von in den Abmahnungen

enthaltenen personenbezogenen Daten nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG, weil deren Kenntnis zur Erfüllung der Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sei, hat der Kläger nicht geltend gemacht.

1. Nach Beendigung des Arbeitsverhältnisses kann ein Anspruch auf Entfernung von Abmahnungen nach §§ 242, 1004 Abs. 1 Satz 1 BGB nur dann bestehen, wenn es objektive Anhaltspunkte dafür gibt, dass die Abmahnung dem Arbeitnehmer noch schaden kann (BAG 19. April 2012 – 2 AZR 233/11 – Rn. 51). Dafür hat der Kläger nach den Feststellungen des Landesarbeitsgerichts keine Tatsachen vorgetragen. Eine Verfahrensrüge erhebt er insoweit nicht.

2. Aus der Entscheidung des Bundesarbeitsgerichts vom 16. November 2010 (- 9 AZR 573/09 – BAGE 136, 156) ergibt sich kein anderer Maßstab. Dies hat das Landesarbeitsgericht zutreffend erkannt. Auch danach ist das Recht auf Einsicht in die Personalakte von der Frage zu trennen, unter welchen Voraussetzungen ein Anspruch darauf besteht, bestimmte Inhalte daraus entfernen zu lassen (BAG 16. November 2010 – 9 AZR 573/09 – Rn. 42, aaO).

Keine fristlose Kündigung wegen Änderung des XING-Profils in „Freiberufler" bei vereinbartem Ablauf des Arbeitsverhältnisses (Ls)

(**Landesarbeitsgericht Köln**, Urteil vom 7. Februar 2017 – 12 Sa 745/16 –)

1. **Die falsche Angabe des beruflichen Status als Freiberufler kann ohne Hinzutreten weiterer Umstände keine fristlose Kündigung wegen unerlaubter Konkurrenztätigkeit rechtfertigen.**
2. **Dies gilt insbesondere, wenn eine solche Angabe eine spätere Konkurrenztätigkeit nach bereits vereinbarten Ende des Arbeitsverhältnisses lediglich vorbereiten soll.**
3. **Die Grenze der zulässigen Vorbereitungshandlung wird erst bei einer aktiv nach außentretenden Werbung überschritten; so Z.B. wenn in der Xing-Rubrik „Ich suche" Wünsche nach freiberuflichen Mandaten geäußert werden.**

(Nicht amtliche Leitsätze)

Information des Betriebsrats über die Zuteilung von Aktienoptionen

(**Landesarbeitsgericht Baden-Württemberg**, Beschluss vom 17. Januar 2017 – 19 TaBV 3/16 –)

Bei der Zuteilung von Aktienoptionen und Nachzugsaktien durch eine US-amerikanische Muttergesellschaft an Mitarbeiter eines deutschen Tochterunternehmens hat der Betriebsrat kein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 10 BetrVG. Gem. § 80 Abs. 2 Satz 1 iVm. § 80 Abs.1 und § 75 Abs. 1 BetrVG hat der Betriebsrat gleichwohl einen Anspruch auf Auskunft gegen die deutsche Konzerntochter, welchen Mitarbeitern in welchem Umfang Aktienoptionen und Nachzugsaktien gewährt werden. Denn der Betriebsrat kann seiner in § 75 Abs. 1 BetrVG übertragenen Aufgabe, die Einhaltung der Grundsätze von Recht und Billigkeit und insbesondere der Gleichbehandlung zu überwachen, nur dann nachkommen, wenn er die entsprechenden Auskünfte erhält. Falls die Arbeitgeberin keine eigene Kenntnis über die Zuteilung der Aktienoptionen und Nachzugsaktien hat, ist sie verpflichtet, sich die Informationen bei der Muttergesellschaft zu beschaffen.

Sachverhalt:

Die Beteiligten streiten darüber, ob die Arbeitgeberin verpflichtet ist, dem Betriebsrat Auskünfte im Zusammenhang mit an ihre Mitarbeiter von der US-amerikanischen Konzernobergesellschaftausgegebene Aktienoptionen (Stock Options) und Nachzugsaktien (Deferred Stock) zu erteilen.

Die am 1. Januar 2010 gegründete Arbeitgeberin betreibt im Rahmen eines Betriebsführungsvertrags ua. ein Werk in R., in dem der beteiligte Betriebsrat gebildet ist. Sie gehört zum weltweit tätigen Chemie- und Technologiekonzern D., dessen Obergesellschaft The D. Company (T.) ihren Sitz in den USA hat.

In der D.-Gruppe gibt es für Mitarbeiter ab einer bestimmten Führungsebene als zusätzliche Vergütungskomponente neben der Grundvergütung und einer variablen Vergütung ein von T. aufgelegtes „Long Term Incentives"-Programm. Dieses sieht die Gewährung von Stock Options und Deferred Stock vor. Den Bezugsrahmen und die Verteilungsparameter legt T. jährlich fest; die Arbeitgeberin selbst gewährt keine Aktien. Arbeitsvertragliche Abreden mit der Arbeitgeberin existieren nicht. Die Zuteilung der Stock Options und Deferred Stock erfolgt seit 2009 im Zusammenhang mit der Leistungseinstufung des jeweiligen Mitarbeiters automatisiert in einem elektronischen Gehaltsfindungsprozess („Pay Planing Process – PPP"). Im PPP können die jeweiligen Vorgesetzten innerhalb eines bestimmten Zeitfensters von der im System vorgegebenen Leistungsbeurteilung nach oben oder unten abweichende Eingaben machen. Zudem können sie Mitarbeiter hinzufügen oder herausnehmen. T. muss diesen Änderungen nicht folgen. Wegen der nach Sparten gegliederten Organisation des Konzerns sind die Vorgesetzten, die für bei der Arbeitgeberin angestellte Mitarbeiter auf das System zugreifen, zum Teil selbst nicht bei dieser angestellt. Umgekehrt können bei der Arbeitgeberin beschäftigte Vorgesetzte auch auf den PPP von Mitarbeitern anderer Konzerngesellschaften einwirken.

Der Betriebsrat hat in dem von ihm eingeleiteten Beschlussverfahren Auskunftsansprüche über die Zuteilung der Stock Options und der Deferred Stock und die Einflussnahme der Arbeitgeberin hierauf geltend gemacht. Er hat die Auffassung vertreten, dass ihm nach § 80 Abs. 2 Satz 1 BetrVG darüber Auskunft zu erteilen sei, für welche Mitarbeiter die Gewährung von Deferred Stock und Stock Options seitens T. vorgeschlagen wurden, in welchen Fällen und mit welcher Begründung die Vorgesetzten abweichende Vorschläge unterbreitet hätten und inwieweit T. den abweichenden Vorschlägen gefolgt sei. Nur durch eine entsprechende Auskunft könne sie beurteilen, ob die Grundsätze der Lohngerechtigkeit gewahrt würden und ob ggf. ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 10 BetrVG bestehe.

Aus den Gründen:

Der Betriebsrat kann Auskunft verlangen, welchen Mitarbeitern ab dem Jahr 2016 Deferred Stock und/oder Stock Options gewährt werden. Der Auskunftsanspruch folgt aus § 80 Abs. 2 Satz 1 BetrVG i.V.m § 80 Abs. 1, 75 Abs. 1 BetrVG.

1. Nach § 80 Abs. 2 Satz 1 BetrVG ist der Arbeitgeber verpflichtet, den Betriebsrat zur Durchführung seiner gesetzlichen Aufgaben rechtzeitig und umfassend zu unterrichten. Mit dieser Verpflichtung geht ein entsprechender Anspruch des Betriebsrats einher. Zu den Aufgaben des Betriebsrats iSv. § 80 Abs. 2 Satz 1 BetrVG gehören dessen allgemeine Aufgaben gemäß dem Katalog des § 80 Abs. 1 BetrVG, die vom Vorliegen besonderer Mitwirkungs- oder Mitbestimmungsrechte unabhängig sind. Zu ihnen gehört ferner die Wahrnehmung von Beteiligungsrechten nach dem Betriebsverfassungsgesetz. Der Unterrichtungsanspruch nach § 80 Abs. 2 Satz 1 BetrVG besteht nicht nur dann, wenn solche allgemeinen Aufgaben oder Beteiligungsrechte bereits feststehen. Die Unterrichtung soll es dem Betriebsrat vielmehr auch ermöglichen, anschließend in eigener Verantwortung zu prüfen, ob sich Aufgaben iSd. Betriebsverfassungsgesetzes ergeben und er zu ihrer Wahrnehmung tätig werden muss. Dafür genügt eine gewisse Wahrscheinlichkeit für das Bestehen von Aufgaben. Die Grenzen des Auskunftsanspruchs liegen dort, wo ein Beteiligungsrecht oder eine sonstige Aufgabe offensichtlich nicht in Betracht kommt. Erst dann kann nicht mehr davon gesprochen werden, dass die begehrte Auskunft zur Durchführung von Aufgaben des Betriebsrats erforderlich sei. Aus diesen Grundsätzen folgt eine zweistufige Prüfung daraufhin, ob überhaupt eine Aufgabe des Betriebsrats gegeben und ob im Einzelfall die begehrte Information zur Aufgabenwahrnehmung erforderlich ist (st. Rspr. vgl. etwa BAG 19. Februar 2008 – 1 ABR 84/06 – Rn. 15 und 16; 10. Oktober 2006 – 1 ABR 68/05 – Rn. 18; 6. Mai 2003 – 1 ABR 13/02 – Rn. 47; 21. Oktober 2003 – 1 ABR 39/02 – Rn. 56 und 58).

Zu den Aufgaben des Betriebsrats iSv. § 80 Abs. 2 Satz 1 BetrVG gehören auch die allgemeinen Aufgaben nach dem Katalog des § 80 Abs. 1 BetrVG. Diese Aufgaben sind vom Vorliegen besonderer Mitwirkungs- oder Mitbestimmungsrechte unabhängig (BAG 21. Oktober 2003 – 1 ABR 39/02 – Rn. 56). Die Aufgabe des Betriebsrats nach § 80 Abs. 2 Satz 1 BetrVG besteht jedenfalls nach § 80 Abs. 1 Nr. 1 BetrVG in der Verpflichtung, darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze und Tarifverträge angewendet werden. Dabei sind nach § 75 Abs. 1 Satz 1 BetrVG die Grundsätze von Recht und Billigkeit und als deren wichtigste Ausprägung der Gleichbehandlungsgrundsatz zu beachten (BAG aaO Rn. 60).

2. Nach diesen rechtlichen Maßstäben besteht kein Auskunftsanspruch nach § 80 Abs. 2 Satz 1 BetrVG i.V.m. § 87 Abs. 1 Nr. 10 BetrVG. Das Arbeitsgericht hat zu Recht festgestellt, dass das Beteiligungsrecht offensichtlich nicht gegeben ist (a)). Zudem wären die begehrten Informationen nicht erforderlich zur Ausübung eines etwaigen Mitbestimmungsrechtes nach § 87 Abs. 1 Nr. 10 BetrVG, weil weder ersichtlich noch dargelegt ist, inwieweit das Beteiligungsrecht bei der Zuteilung von Deferred Stock und Stock Options durch die Konzernobergesellschaft ausgeübt werden könnte (b)).

a) Vorliegend besteht schon – offensichtlich – kein Mitbestimmungsrecht des Betriebsrates bei der Gewährung von Deferred Stock bzw. Stock Options gemäß § 87 Abs. 1 Nr. 10 BetrVG. Die genannte Norm betrifft ausweislich ihres Wortlauts Fragen der betrieblichen Lohngestaltung. Im konkreten Fall fehlt es indes am Bezug zur betrieblichen Lohngestaltung. Schließt der Arbeitnehmer eine Vereinbarung über die Gewährung von Aktienoptionen nicht mit seinem Arbeitgeber, sondern mit einem anderen Konzernunternehmen ab, so können Ansprüche aus dieser Vereinbarung grundsätzlich nur gegenüber dem vertragsschließenden Konzernunternehmen geltend gemacht werden und werden nicht Bestandteil des Arbeitsverhältnisses mit einer Tochtergesellschaft dieses Konzernunternehmens. Der Vertrag über die Gewährung von Aktienoptionen steht rechtlich selbstständig neben dem Vertrag des Arbeitnehmers mit der Tochtergesellschaft (BAG 16. Januar 2008 – 7 AZR 887/06 – Rn. 17 mwN). Nach diesen Grundsätzen liegt schon keine Entgeltleistung der Arbeitgeberin vor, sodass es bereits an einer Grundvoraussetzung für die Anwendbarkeit des § 87 Abs. 1 Nr. 10 BetrVG fehlt. In dieser Hinsicht folgt die erkennende Kammer den zutreffenden Ausführungen des Arbeitsgerichts (ebenso Annuß/Lembke BB 2003, 2230, 2231 mit der Auffassung, dass in Fällen „ausschließlicher Drittleistung" das Mitbestimmungsrecht nicht ausgelöst werde). Auch wenn ein etwaiger Zusammenhang zwischen der Gewährung der Aktienoptionen und Nachzugsaktien und dem Arbeitsverhältnis angenommen würde, änderte sich an dieser Wertung nichts. Denn die von einem Dritten im Hinblick auf das Arbeitsverhältnis erbrachten Leistungen stellen nach der zutreffenden Rechtsprechung des Bundesarbeitsgerichtes nur dann Arbeitsentgelt dar, wenn der Dritte sie nach der Abrede der Arbeitsvertragsparteien an Stelle oder neben dem zwischen ihnen vereinbarten Arbeitsentgelt erbringen soll (BAG 16. Januar 2008 – 7 AZR 887/06 – Rn. 16). Dies ist vorliegend nicht der Fall. Auch aus der Tatsache, dass ggf. Vorgesetzte im Zuweisungsverfahren mitwirken, ergibt sich keine andere Bewertung. Soweit die Vorgesetzten in anderen Konzerngesellschaften angestellt sind, fehlt es bereits am betrieblichen Bezug, denn bei einer anderen Gesellschaft wird es sich im Regelfall auch um einen anderen Betrieb handeln. Sollte dies nicht der Fall sein sowie für den Fall, dass die Vorgesetzten bei der Arbeitgeberin angestellt sein sollten, folgt aber auch hieraus nicht, dass ein Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 10 BetrVG bestünde. Dem Arbeitsgericht ist darin zu folgen, dass es sich auch bei diesen Vorgesetzten lediglich um „Erfüllungsgehilfen" der T. handelt und es vor diesem Hintergrund um eine mitbestimmungsfreie Mitwirkung hinsichtlich der Leistung eines Dritten geht. Schließlich scheidet das Mitbestimmungsrecht auch bereits deshalb aus, weil dem Betriebsrat überhaupt kein Gestaltungsspielraum verbleibt (hierzu sogleich auch unter b)). Die zwingenden Vorgaben der Konzernmutter bilden die Grenze der Mitbestimmung (so auch Otto/Mückl, DB 2009 1594, 1597). Da letztlich die Muttergesellschaft unstreitig – Gegenteiliges behauptet auch der Betriebsrat nicht – alleine und ohne Bindung an die Mitwirkung der Vorgesetzten über die Zuteilung von Deferred Stock und Stock Options entscheidet, verbleibt bei der Arbeitgeberin und damit auch für den Betriebsrat keine Möglichkeit der Gestaltung über § 87 Abs. 1 Nr. 10 BetrVG. Die Arbeitgeberin hat weder rechtlich noch tatsächlich einen Spielraum bei der Ausgestaltung der Einzelheiten des Aktienoptionsplans. Hat der Arbeitgeber aber bereits keinen Gestaltungsspielraum, kann der Betriebsrat schon aus tatsächlichen Gründen nicht mitbestimmen (so auch Lingemann/Diller/Mengel NZA 2000, 1191, 1200).

b) Auskunftsansprüche mit Blick auf ein etwaiges Beteiligungsrecht nach § 87 Abs. 1 Nr. 10 BetrVG schieden mit demselben Argument auch auf der zweiten Prüfungsstufe aus. Die

begehrten Auskünfte wären nicht zur Aufgabenwahrnehmung iSd. Rechtsprechung des Bundesarbeitsgerichtes erforderlich. Dem Betriebsrat verbleibt überhaupt kein Verhandlungsspielraum, weil die Entscheidung über das Ob und Wie der Gewährung von Deferred Stock und Stock Options allein von der Muttergesellschaft getroffen wird. Dem Betriebsrat fehlt es an Möglichkeiten, ein Beteiligungsrecht nach § 87 Abs. 1 Nr. 10 BetrVG anzubringen.

3. Ein Auskunftsanspruch des Betriebsrates ergibt sich aber aus § 80 Abs. 2 Satz 1 BetrVG iVm. § 80 Abs. 1 und § 75 Abs. 1 BetrVG.

a) Nach § 75 Abs. 1 BetrVG haben Arbeitgeber und Betriebsrat darüber zu wachen, dass alle im Betrieb tätigen Personen nach den Grundsätzen von Recht und Billigkeit behandelt werden, insbesondere, dass jede Benachteiligung von Personen aus Gründen ihrer Rasse oder wegen ihrer ethnischen Herkunft, ihrer Abstammung oder sonstigen Herkunft, ihrer Nationalität, ihrer Religion oder Weltanschauung, ihrer Behinderung, ihres Alters, ihrer politischen oder gewerkschaftlichen Betätigung oder Einstellung oder wegen ihres Geschlechts oder ihrer sexuellen Identität unterbleibt. Recht und Billigkeit verlangen insbesondere die Beachtung des Gleichbehandlungsgrundsatzes (Richardi BetrVG/Maschmann/ Richardi 15. Aufl. BetrVG § 75 Rn. 15). Die in der Vorschrift niedergelegten Pflichten sind für Arbeitgeber und Betriebsrat gesetzliche Pflichten iSd. Betriebsverfassungsgesetzes (Richardi aaO Rn. 50). Den Arbeitgeber trifft eine Reaktionspflicht, soweit Beschäftigte wegen eines in § 1 AGG genannten Grundes benachteiligt werden. Sie besteht gegenüber Beschäftigten, die gegen das Benachteiligungsverbot verstoßen, und gegenüber Dritten, durch die Beschäftigte bei der Ausübung ihrer Tätigkeit benachteiligt werden (§ 12 Abs. 3 und 4 AGG): Der Arbeitgeber hat die im Einzelfall geeigneten, erforderlichen und angemessenen Maßnahmen zur Unterbindung der Benachteiligung wie Abmahnung, Umsetzung, Versetzung oder Kündigung zu ergreifen bzw. die im Einzelfall geeigneten, erforderlichen und angemessenen Maßnahmen zum Schutz der Beschäftigten vorzunehmen (Richardi aaO. Rn. 12).

b) Nach diesen rechtlichen Maßstäben besteht im vorliegenden Fall eine Überwachungspflicht des Betriebsrates hinsichtlich der von der Muttergesellschaft gewährten Aktienoptionen und Nachzugsaktien und damit auch ein Aufgabenbezug, welcher gemäß § 80 Abs. 2 Satz 1 BetrVG zu einem Auskunftsanspruch führt.

aa) Ein Überwachungsrecht nach § 75 Abs. 1 Satz 1 BetrVG scheidet nicht schon deshalb aus, weil die amerikanische Muttergesellschaft aufgrund eines rechtlich selbstständigen Verpflichtungsgrundes die Vergütung gewährt. Anknüpfungspunkt für die Überwachungspflicht des Betriebsrats im Rahmen des § 75 BetrVG ist nicht die Vergütung als solche, sondern die Behandlung der im Betrieb tätigen Personen. Dabei ist nicht danach zu unterscheiden, von welcher Seite die im Raume stehende Maßnahme ausgeht. Soweit die Arbeitgeberin im Verhandlungstermin ausgeführt hat, dass es bei § 75 Abs. 1 BetrVG lediglich um arbeitgeberseitige Maßnahmen gehen könne, folgt das Gericht dem nicht. § 75 Abs. 1 BetrVG ist nicht derart eng zu verstehen und auszulegen.

(1) Maßgebend für das Verständnis und die Auslegung einer Norm ist der in der Norm zum Ausdruck gekommene objektivierte Wille des Gesetzgebers, wie er sich aus dem Wortlaut der Vorschrift und dem Sinnzusammenhang ergibt, in den die Regelung hineingestellt ist. Der Erfassung des objektiven Willens des Gesetzgebers dienen die anerkannten Methoden der Gesetzesauslegung aus dem Wortlaut der Norm, der Systematik, ihrem Sinn und Zweck sowie aus den Gesetzesmaterialien und der Entstehungsgeschichte (st. Rspr. des BAG, vgl. zuletzt 25. Mai 2016 – 5 AZR 135/16 – Rn. 28 mit Verweis auf BVerfG 19. März 2013 – 2 BvR 2628/10, 2 BvR 2883/10, 2 BvR 2155/11 – Rn. 66).

(2) Die Auffassung der Arbeitgeberin findet bereits im Wortlaut der Norm keine Stütze. Die Norm formuliert: „behandelt werden". Wer „behandelt", wird vom Gesetz offengelassen. Insofern spricht schon der Wortlaut dafür, dass § 75 Abs. 1 BetrVG nicht nur bei Maßnahmen des Arbeitgebers Anwendung findet.

(3) Auch die Systematik sowie Sinn und Zweck von § 75 Abs.1 BetrVG gebieten, ihn auch bei Maßnahmen Dritter zur Geltung zu bringen. Das Ziel der Norm besteht darin, die Einhaltung der Grundsätze von Recht und Billigkeit und insbesondere der Gleichbehandlung sicherzustellen (Fitting 28. Aufl. § 75 Rn. 1). Dies kann nur dadurch geschehen, dass jedwede diskriminierende Handlung, gleich welchen Ursprungs, von der Überwachungspflicht abgedeckt wird. Die verengende Auffassung der Arbeitgeberin würde beispielsweise den praktisch relevanten Bereich, dass Kunden der Arbeitgeberin ihre Arbeitnehmer entgegen den in § 75 Abs. 1 BetrVG genannten Grundsätzen behandeln, vollständig von der Überwachungspflicht des Betriebsrates ausnehmen. Die Drittbezogenheit von Überwachungspflichten ist dem Konzept des Diskriminierungsschutzes vielmehr immanent, so zB in Gestalt des § 12 Abs. 4 AGG. Danach hat der Arbeitgeber die im Einzelfall erforderlichen und angemessenen Maßnahmen zum Schutz der Beschäftigten zu ergreifen, wenn Beschäftigte bei der Ausübung ihrer Tätigkeit durch Dritte nach § 7 Abs. 1 AGG benachteiligt werden. Auch § 17 Abs. 3a KSchG kennt (wenngleich in anderem Zusammenhang), Auskunfts-, Beratungs- und Anzeigepflichten, wenn die Entscheidung über Entlassungen von einem Dritten, nämlich einem den Arbeitgeber beherrschenden Unternehmen getroffen wurde.

(4) Bestätigt wird dieses Auslegungsergebnis durch die Gesetzesmaterialien und die Entstehungsgeschichte. § 75 Abs. 1 BetrVG wurde durch Art. 3 Abs. 3 des Gesetzes zur Umsetzung europäischer Richtlinien zur Verwirklichung des Grundsatzes der Gleichbehandlung vom 14. August 2006 an die Terminologie des Allgemeinen Gleichbehandlungsgesetzes angepasst (BGBl. Jahrgang 2006, Teil I, 1897, 1908). Nach dem Willen des Gesetzgebers richten sich der Begriff der Benachteiligung und die Zulässigkeit einer unterschiedlichen Behandlung in § 75 Abs. 1 BetrVG nach den Bestimmungen des Allgemeinen Gleichbehandlungsgesetzes (BT-Drs. 16/1780, S. 56). Insofern ist eine Norm wie § 12 Abs. 4 AGG ohne weiteres zur Auslegung von § 75 Abs. 1 BetrVG heranzuziehen.

bb) Eine Auskunftserteilung (zur Reichweite sogleich unter cc)) ist auch zur Aufgabenwahrnehmung des Betriebsrates erforderlich, denn nur mit entsprechenden Informationen kann er seiner Überwachungspflicht nachkommen. Dass der Betriebsrat kein Mitspracherecht bei der Zuteilung von Deferred Stock und Stock Options hat, steht dem nicht entgegen, genauso wenig, dass ihm kein Verhandlungsspielraum über das Ob und Wie zusteht. Denn anders als bei § 87 Abs. 1 Nr. 10 BetrVG geht es bei § 75 Abs. 1 BetrVG nicht um ein Mitbestimmungsrecht. Bezugspunkt ist vielmehr die Aufgabe der Überwachung. Für diese ist es entgegen der Auffassung der Arbeitgeberin nicht unnütz,

dass Auskünfte erteilt werden. Insbesondere spielt es keine Rolle, dass der Betriebsrat aus den ihm zur Verfügung gestellten Informationen keine belastbaren Rechte oder dergleichen herleiten kann. Alleine die Tatsache, dass der Betriebsrat einen etwaigen Verstoß gegen die in § 75 Abs. 1 BetrVG aufgeführten Grundsätze benennen, ansprechen und ggf. auch dadurch auf eine Veränderung hinwirken kann, stellte eine sinnvolle und durch die Rechtsordnung gewünschte Reaktion dar. Genauso wie bei § 12 Abs. 4 AGG kann es bei einem festgestellten Verstoß durch Maßnahmen Dritter um die im Einzelfall geeigneten, erforderlichen und angemessenen Maßnahmen gehen. § 12 Abs. 4 AGG verlangt lediglich, dass der Arbeitgeber alles im Rahmen der Verhältnismäßigkeit Zumutbare unternimmt, um eine Benachteiligung für die Zukunft auszuschließen. Er genügt regelmäßig seiner Verpflichtung nach § 12 Abs. 4 AGG, wenn er Kunden oder Lieferanten auf den Verstoß gegen das Benachteiligungsverbot hinweist und zur Abhilfe auffordert (Bauer/Göpfert/Krieger AGG 3. Aufl. § 12 Rn. 12). Auch § 17 Abs. 1 AGG sieht vor, dass die einzelnen Akteure „im Rahmen ihrer Aufgaben und Handlungsmöglichkeiten" an der Verwirklichung des in § 1 AGG genannten Ziels mitwirken. Die Argumentation der Arbeitgeberin, dass der Betriebsrat aus den erlangten Informationen keine tatsächlichen Schlussfolgerungen ziehen kann, geht mit diesem veränderten Bezugspunkt – Überwachungspflicht statt Mitbestimmung – ins Leere.

cc) Die mit den Hauptanträgen geltend gemachten Auskünfte sind von ihrem Umfang – unabhängig von der zeitlichen Komponente – allerdings nicht erforderlich, um die Einhaltung der Grundsätze des § 75 Abs. 1 BetrVG zu überwachen.

(1) Die Erforderlichkeit einer Auskunft ist auch in inhaltlicher Hinsicht an der Aufgabe zu messen. Ein Anspruch auf Auskunft kann nicht über die Informationen hinausgehen, welche der Betriebsrat zur Aufgabenwahrnehmung benötigt. Die gesetzliche Aufgabe, die den Informationsanspruch begründet, begrenzt diesen auch in seiner Reichweite im konkreten Einzelfall (vgl. statt vieler Weber-GK BetrVG 10. Aufl. § 80 Rn. 59).

(2) Um die Einhaltung des Gleichbehandlungsgrundsatzes zu überprüfen, reicht es aus, wenn der Betriebsrat darüber Auskunft erhält, welchen Mitarbeitern in welchem Umfang Stock Options und/oder Deferred Stock gewährt werden. Nicht erforderlich ist es hingegen zu erfahren, wie zunächst der Vorschlag von T. lautete, inwieweit und mit welcher Begründung abweichende Vorschläge unterbreitet wurden und inwieweit diesen gefolgt wurde. Anhand der Information, welchen Mitarbeitern in welchem Umfang Deferred Stock bzw. Stock Options zugeteilt wurden, ist es dem Betriebsrat möglich, etwaige Verstöße gegen den Gleichbehandlungsgrundsatz zu benennen. So kann der Betriebsrat ersehen, gegenüber welchen Mitarbeitern eine Zuteilung erfolgte und welche Mitarbeiter hiervon ausgenommen wurden. Er kann zudem feststellen, wie viele Deferred Stock bzw. Stock Options einzelne Mitarbeiter erhalten haben und kann die einzelnen Zuteilungen in ein Verhältnis zueinander setzen. Gerade dadurch wird ihm die Überprüfung des Gleichbehandlungsgrundsatzes ermöglicht.

(3) Greifbare Anhaltspunkte dafür, dass die Arbeitgeberin eine „Regelverletzung" begeht, bedarf es, um die Erforderlichkeit der Auskunft zu bejahen, nicht (BAG 19. Februar 2008 – 1 ABR 84/06 – Rn. 25).

(4) In inhaltlicher Hinsicht war der Hilfsantrag des Betriebsrats leicht abzuändern. Statt gewährt „wurden", war gewährt „werden" in die Tenorierung aufzunehmen. Dies ergibt eine Auslegung des Antrags, der Auskünfte bezüglich der Zuteilung von Deferred Stock und Stock Options „ab dem Jahr 2016" begehrt.

c) Der Auskunftsanspruch in der Gestalt des Hilfsantrages scheitert auch nicht an tatsächlicher oder rechtlicher Unmöglichkeit gemäß § 275 Abs. 1 BGB bzw. auf Grund eines Leistungsverweigerungsrechts nach § 275 Abs. 2 BGB. Falls die Arbeitgeberin keine eigene Kenntnis hat, ist sie verpflichtet, sich die Informationen darüber zu beschaffen, welche Mitarbeiter in welchem Umfang Deferred Stock und/oder Stock Options gewährt bekommen.

aa) An sich ist die Arbeitgeberin im Rahmen des § 80 Abs. 2 Satz 1 BetrVG nur verpflichtet, die Informationen zu geben, über die sie selbst verfügt; sie muss sich grundsätzlich keine weiteren Informationen beschaffen (Richardi BetrVG/Thüsing 15. Aufl. BetrVG § 80 Rn 56). Dies gilt allerdings nicht, wenn sich aus § 75 Abs. 1 BetrVG auch für die Arbeitgeberin selbst, wie im vorliegenden Fall, eine Überwachungspflicht ergibt. Zur Frage der Vertrauensarbeit hat das Bundesarbeitsgericht entschieden, dass der Arbeitgeber auch dann zur Auskunft verpflichtet sei, wenn er über die entsprechenden Kenntnisse (im konkreten Fall zu Beginn und Ende der täglichen Arbeitszeit) bislang nicht verfüge (BAG 6. Mai 2003 – 1 ABR 13/02 – Rn. 63). Er habe seinen Betrieb so zu organisieren, dass er die Durchführung der geltenden Gesetze selbst gewährleisten könne (BAG aaO Rn. 65). Die benötigten Auskünfte seien zu deren Durchführung, anders als zusätzlich gewünschte Unterlagen, unverzichtbar, da die Überwachungsaufgabe ohne sie nicht erfüllt werden könne (BAG aaO Rn. 67). Unabhängig davon hat das Bundesarbeitsgericht im Rahmen eines Auskunftsanspruches nach § 5 Abs. 1 EBRG schon dann eine (subjektive) Unmöglichkeit verneint, wenn die Arbeitgeberin zur Auskunftserteilung in der Lage ist, weil sie sich der Mitwirkung Dritter bedienen kann, welche die notwendigen Kenntnisse besitzen (BAG 29. Juni 2004 – 1 ABR 32/99 – Rn. 33). Hieran ändere sich auch nichts dadurch, dass sich die Arbeitgeberin vergeblich um die begehrten Informationen bemüht habe. Der Arbeitgeberin stünden rechtliche Wege offen (BAG aaO Rn. 34). Falls sich im Anschluss herausstellen sollte, dass die Arbeitgeberin trotz Beschreitens des Rechtswegs nicht in der Lage sei, ihre Auskunftspflicht zu erfüllen, so wäre dies im Rahmen eines möglichen Vollstreckungsverfahrens zu ihren Gunsten zu berücksichtigen (BAG aaO Rn. 43).

Auch in der Kommentarliteratur wird vertreten, dass sich der Vertragsarbeitgeber ggf. die entsprechenden Daten auch über die Muttergesellschaft beschaffen muss (Weber-GK BetrVG 10. Aufl. § 80 Rn. 57; in diesem Sinne auch Fitting 28. Aufl. § 80 Rn. 56 und 59; DKKW-Buschmann 15. Aufl. § 80 Rn. 101; a.A. Richardi BetrVG/Thüsing 15. Aufl. BetrVG § 80 Rn. 64; ErfK/Kania 17. Aufl. BetrVG § 80 Rn. 23; vgl. in diesem Zusammenhang auch LAG Nürnberg 22. Januar 2002 – 6 TaBV 19/01 – Rn. 31, das hinsichtlich der Gewährung von Aktienoptionen einer ausländischen Muttergesellschaft entschieden hat, dass Unterlagen dem Arbeitgeber auch dann zur Verfügung stehen, wenn lediglich die Gesellschafter und nicht die Geschäftsführer hierüber verfügen).

bb) Dies zugrunde gelegt, kann der Betriebsrat in der konkreten Fallkonstellation verlangen, dass die Arbeitgeberin die aus dem Tenor ersichtlichen Informationen ggf. beschafft, sollte sie nicht bereits darüber verfügen. Das Bundesarbeitsgericht hat in seiner Entscheidung vom 6. Mai 2003 (1 ABR

13/02) mit überzeugenden Argumenten dargestellt, dass sich die Arbeitgeberin eines Auskunftsanspruches des Betriebsrats nicht alleine dadurch entledigen kann, dass sie auf die bislang nicht erfolgte Erhebung der begehrten Daten abstellt, soweit es um die Durchführung geltender Gesetze geht. Auch im vorliegenden Fall besteht für die Arbeitgeberin aus § 75 Abs. 1 BetrVG eine gesetzliche Überwachungspflicht (s.o.), die ebenso wie die damit korrespondierende Überwachungspflicht des Betriebsrats vollständig vereitelt würde, wenn ausschließlich auf das Vorhandensein der Daten abgestellt würde. Auch wenn die Arbeitgeberin im Unterschied zu dem vom Bundesarbeitsgericht entschiedenen Fall vom 6. Mai 2003 nicht selbst zur Datenerhebung in der Lage und auf die Mitwirkung Dritter angewiesen wäre, änderte sich am gefundenen Ergebnis nichts. Jedenfalls schlösse dies einen Auskunftsanspruch des Betriebsrats nicht aus, denn die Arbeitgeberin ist zunächst verpflichtet, sich die Daten über die Muttergesellschaft oder andere Konzernunternehmen zu beschaffen. Lediglich wenn mit Gewissheit anzunehmen wäre, dass eine Inanspruchnahme der erwähnten Unternehmen – auch auf dem Rechtsweg – erfolglos bliebe, läge eine Unmöglichkeit im Sinne des § 275 Abs. 1 BGB vor (BAG 29. Juni 2004 – 1 ABR 32/99 – Rn. 40). Dass sie den Rechtsweg zur Informationsbeschaffung beschritten hätte, behauptet allerdings nicht einmal die Arbeitgeberin selbst. Soweit sie meint, dass die Entscheidung des Bundesarbeitsgerichts vom 29. Juni 2004 nicht auf den vorliegenden Sachverhalt übertragbar wäre, weil sie lediglich das EBRG betroffen habe, kann dem nicht gefolgt werden. Zwar bestand in der erwähnten Entscheidung eine andere Anspruchsgrundlage hinsichtlich der begehrten Auskunft. Im konkreten Zusammenhang geht es aber nicht um die Anspruchsgrundlage, sondern um die Frage, ob eine Unmöglichkeit nach § 275 Abs. 1 BGB vorliegt. Diese Frage stellt sich unabhängig von der Anspruchsgrundlage, denn § 275 Abs. 1 BGB gilt für jeden – auch gesetzlichen – Anspruch (BAG 29. Juni 2004 – 1 ABR 32/99 – Rn. 30).

cc) Auch ein Leistungsverweigerungsrecht der Arbeitgeberin nach § 275 Abs. 2 BGB ist nicht zu erkennen. Die Informationsbeschaffung über die Muttergesellschaft ist ihr ohne weiteres zumutbar. In diesem Zusammenhang ist in den Blick zu nehmen, dass der geldwerte Vorteil aus der Ausübung der Stock Options bzw. der Deferred Stock steuerrechtlich Arbeitslohn darstellt (BAG 12. Februar 2003 – 10 AZR 299/02 – Rn. 59). Zwar führt dies nicht dazu, dass es sich um ein Entgelt seitens der Arbeitgeberin handeln würde (LAG München 12. Februar 2009 – 3 Sa 833/08 – Rn. 44). Gleichwohl folgt aus der steuerrechtlichen Behandlung als Arbeitslohn, dass entsprechende Zuteilungen auf Gehaltsmitteilungen aufzuführen sind. Dies stellt selbst die Arbeitgeberin nicht in Abrede; sie trägt vielmehr vor, dass die Gehaltsmitteilung die Anzahl der dem betreffenden Mitarbeiter ggf. von T. zugebilligten Optionen / Deferred Stock enthalte (Schriftsatz vom 31. Oktober 2013, Seite 9 oben). Ob die Arbeitgeberin über die Gehaltsmitteilungen verfügt, spielt hierbei keine Rolle. Dass es ihr unzumutbar wäre, Gehaltsmitteilungen ihrer eigenen Mitarbeiter zu beschaffen, liegt fern.

d) Das Bundesdatenschutzgesetz steht einer Weitergabe von Informationen an den Betriebsrat nicht entgegen. Das Bundesdatenschutzgesetz verdrängt das Betriebsverfassungsgesetz nicht. Gesetzliche Vorschriften wie § 80 Abs. 2 Satz 1 BetrVG, welche die Information des Betriebsrats und damit uU auch die Weitergabe von Daten vorschreiben, gehen dem Bundesdatenschutzgesetz vor (Weber-GK BetrVG § 80 Rn. 80 mwN).

Die Frage, inwieweit Auskunftsansprüche und damit zusammenhängend Beteiligungs- und Überwachungsrechte des Betriebsrates bei der Gewährung von Aktienoptionen und Nachzugsaktien durch eine ausländische Muttergesellschaft bestehen, hat grundsätzliche Bedeutung. Sie ist vom Bundesarbeitsgericht auch noch nicht entschieden. Vor diesem Hintergrund hat die Kammer die Rechtsbeschwerde zum Bundesarbeitsgericht zugelassen (§§ 92 Abs. 1, 72 Abs. 2 Satz 1 ArbGG).

Vorgabe zur Nutzung elektronischer Verfahren zwecks Datenübermittlung an den Staat

(**Oberverwaltungsgericht Münster**, Beschluss vom 22. Dezember 2016 – 4 B 1001/16 –)

1. **Die Verpflichtung von Betrieben und Unternehmen, die für eine Bundesstatistik zu erhebenden Daten (hier: Verdienststrukturerhebung) grundsätzlich mittels eines dafür zur Verfügung gestellten elektronischen Verfahrens zu übermitteln, ist verfassungsgemäß.**
2. **Ein trotz angemessener technischer Sicherheitsmaßnahmen verbleibendes Risiko unberechtigter Datenzugriffe durch Hacker-Angriffe muss der Betroffene hinnehmen.**

Aus den Gründen:

Die Beschwerde der Antragsteller ist unbegründet.

Das Verwaltungsgericht hat den sinngemäßen Antrag, die aufschiebende Wirkung der Klage 3 K 2927/15 (VG Minden) gegen die Bescheide des J. .O. aus Februar 2015, Mai 2015, vom 8.6.2015 und vom 5.10.2015 anzuordnen, zu Recht abgelehnt und zur Begründung im Wesentlichen ausgeführt: Der Antrag der Antragstellerin zu 2. sei mangels Antragsbefugnis unzulässig. Hinsichtlich der hier streitigen Auskunfts- und Übermittlungspflicht nach § 8 Abs. 1 des Gesetzes über die Statistik der Verdienste und Arbeitskosten (Verdienststatistikgesetz – VerdStatG) i.V.m. § 15 Abs. 1 des Gesetzes über die Statistik für Bundeszwecke (Bundesstatistikgesetz – BStatG) und § 11a Abs. 2 BStatG sei die Antragstellerin zu 2. nicht Inhaltsadressatin der Bescheide aus Februar 2015 und vom 5.10.2015 sowie der Schreiben aus Mai 2015 und vom 8.6.2015. Der Antrag des Antragstellers zu 1. sei wegen fehlenden Rechtsschutzbedürfnisses unzulässig, soweit er sich gegen die – tatsächlichen oder vermeintlichen – Bescheide aus Februar 2015, Mai 2015 und vom 8.6.2015 richte. Unter dem 5.10.2015 habe J. .O. eine neue Sachentscheidung getroffen und damit einen sog. Zweitbescheid erlassen, womit sich vorausgegangene Bescheide erledigt hätten. Im Übrigen sei der Antrag des Antragstellers zu 1. unbegründet. Der Bescheid vom 5.10.2016 erweise sich bei summarischer Prüfung als rechtmäßig. Der Antragsteller zu 1. sei als Inhaber der in die Verdienststrukturerhebung einbezogenen Antragstellerin zu 2. bzw. als mit deren Leitung Beauftragter gemäß § 8 Abs. 1 VerdStatG i.V.m. § 15 Abs. 1 BStatG auskunftspflichtig. Zur Datenübermittlung müsse er sich gemäß § 11a Abs. 2 Satz 1 BStatG des von der Antragsgegnerin zur Verfügung gestellten elektronischen Verfahrens bedienen. Sowohl die Auskunftspflicht als auch die Verpflichtung zur elektronischen Datenübermittlung stünden mit höherrangigem Recht, namentlich dem Recht auf informationelle Selbstbestimmung aus

Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in Einklang. Insbesondere sei ein etwaiges trotz Anwendung der zur Verfügung stehenden technischen Sicherungsmöglichkeiten verbleibendes Restrisiko eines Hacker-Angriffs auf gespeicherte oder übermittelte Daten im überwiegenden Interesse des Allgemeinwohls hinzunehmen.

Diese Einschätzung des Verwaltungsgerichts wird durch das Beschwerdevorbringen nicht durchgreifend in Frage gestellt.

Die von der Beschwerde unter Hinweis auf die Adressierung der streitgegenständlichen Schreiben an die Antragstellerin zu 2. geäußerten Zweifel am Fehlen ihrer Antragsbefugnis entsprechend § 42 Abs. 2 VwGO sind nicht berechtigt. Das Verwaltungsgericht hat zutreffend angenommen, dass Inhaltsadressat des Bescheides vom 5.10.2015 der Antragsteller zu 1. ist, nicht aber (auch) die Antragstellerin zu 2.

Allein auf diesen Bescheid kommt es an. Mit ihm hat – wovon das Verwaltungsgericht zu Recht ausgegangen ist und was auch die Beschwerde nicht in Zweifel zieht – J. .O. eine (neue) Sachentscheidung getroffen. Diese Entscheidung hätte als sog. Zweitbescheid die von den Antragstellern so bezeichneten „Bescheide“ aus Februar und Mai 2015 sowie vom 8.6.2015 mit erledigender Wirkung ersetzt, soweit es sich bei diesen Schreiben – was offen bleiben kann – um Verwaltungsakte im Sinne von §§ 42, 80 VwGO, 35 VwVfG gehandelt haben sollte. Insoweit ist der Antrag auf Anordnung der aufschiebenden Wirkung daher in jedem Fall nicht statthaft bzw. mangels Rechtsschutzbedürfnisses unzulässig.

Die Antragstellerin zu 2. ist nicht Inhaltsadressatin des Bescheides vom 5.10.2015. Dies ist allein der Antragsteller zu 1.

Inhaltsadressat eines Verwaltungsaktes ist derjenige, dem gegenüber die Einzelfallregelung getroffen wird, der sie mit anderen Worten zu beachten hat und daran gebunden ist. Etwaige Unklarheiten sind unter dem Gesichtspunkt des Bestimmtheitsgebotes (§ 37 Abs. 1 VwVfG NRW) unschädlich, sofern sie sich im Wege der Auslegung des Verwaltungsaktes beseitigen lassen. Dabei kommt es auf den objektiven Empfängerhorizont und mithin darauf an, wie der Betroffene nach den ihm bekannten Umständen den Verwaltungsakt unter Berücksichtigung von Treu und Glauben verstehen musste.

Vgl. BVerwG, Urteil vom 27.6.2012 – 9 C 7.11 –, BVerwGE 143, 222 = juris, Rn. 11; VGH Bad.-Württ., Urteil vom 21.4.2016 – 1 S 665/14 –, DÖV 2016, 697 (Leitsatz) = juris, Rn. 27; OVG NRW, Beschluss vom 13.11.2015 – 12 A 1946/14 –, juris, Rn. 8 f., jew. m.w.N.

Gemessen hieran richtet sich der formell an die „W.-Werkstätten GmbH & Co. KG z. H. des Geschäftsführers U.W1.“ adressierte Bescheid inhaltlich ausschließlich an den Antragsteller zu 1. Aus der Begründung des Bescheides geht hervor, dass der persönlich angesprochene („Sehr geehrter Herr W1. „) Antragsteller zu 1., der nach Aktenlage alleiniger Kommanditist sowie Geschäftsführer der persönlich haftenden Gesellschafterin der Antragstellerin zu 2. ist, „als Inhaber bzw. Leiter der o. a. Erhebungseinheit ... auskunftspflichtig“ sei, weil nach § 8 VerdStatG die Inhaber der in die Erhebung einbezogenen Erhebungseinheiten sowie die mit deren Leitung Beauftragten im Rahmen der ihnen übertragenen Aufgaben und Befugnisse zur Auskunft verpflichtet seien. Einen entsprechenden Hinweis enthielt bereits das Schreiben von J. .O. vom 8.6.2015. Und auch in der dem Schreiben von J. .O. aus Februar 2015 als Anlage beigefügten „Unterrichtung nach § 17 Bundestatistikgesetz“, auf die dieses Schreiben wegen der „Einzelheiten zur Auskunftspflicht“ ausdrücklich Bezug nahm, war auf die Auskunftspflicht der Inhaber bzw. Leiter der in die Verdienststrukturerhebung einbezogenen Erhebungseinheiten hingewiesen worden. Danach war für den Antragsteller zu 1. erkennbar, dass – nur – er zur Auskunftserteilung herangezogen werden sollte.

Das Verwaltungsgericht hat zutreffend angenommen, der Antragsteller zu 1. sei nach § 8 Abs. 1 Sätze 1 und 3 VerdStatG i.V.m. § 15 Abs. 1 BStatG auskunftspflichtig. Er sei Inhaber bzw. Leiter der Antragstellerin zu 2., die gemäß § 2 VerdStatG als Erhebungseinheit in die Erhebung der Struktur der Arbeitsverdienste im Jahr 2014 nach § 4 VerdStatG einbezogen sei. Gegen diese Einschätzung wendet sich die Beschwerde ebenso wenig wie gegen die gleichfalls zutreffende weitere Annahme des Verwaltungsgerichts, die für Zwecke wirtschaftspolitischer Planungsentscheidungen sowie zur Erfüllung von Berichtspflichten nach dem Recht der Europäischen Gemeinschaften dienende (vgl. § 1 VerdStatG) Auskunftspflicht im Rahmen der Verdienststrukturerhebung stehe mit höherrangigem Recht, namentlich dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, in Einklang. Insoweit nimmt der Senat gemäß § 122 Abs. 2 Satz 3 VwGO Bezug auf die Gründe der angefochtenen Entscheidung.

Vgl. zudem Nds. OVG, Beschluss vom 27.1.2015 – 11 ME 226/14 –, DVBl. 2015, 372 = juris, Rn. 9 ff. (zur Erhebung der Arbeitsverdienste nach § 3 VerdStatG); vgl. auch BVerwG, Urteil vom 20.12.2001 – 6 C 7.01 –, BVerwGE 115, 319 = juris, Rn. 17 ff. (zur Erhebung der Arbeitsverdienste und Arbeitszeiten nach dem Lohnstatistikgesetz).

Ohne Erfolg rügt die Beschwerde eine Verletzung des informationellen Selbstbestimmungsrechts durch die auf § 11a Abs. 2 Satz 1 BStatG gestützte Verpflichtung zur Datenübermittlung mittels der von J. .O. dafür zur Verfügung gestellten elektronischen Verfahren. Auch insoweit nimmt der Senat zunächst Bezug auf die zutreffenden Gründe der erstinstanzlichen Entscheidung. Die Einwände hiergegen greifen nicht durch.

Die Verpflichtung von Betrieben und Unternehmen nach § 1a Abs. 2 Satz 1 BStatG, die für eine Bundesstatistik zu erhebenden Daten grundsätzlich mittels eines dafür zur Verfügung gestellten elektronischen Verfahrens zu übermitteln, dient der Verwaltungsvereinfachung und mithin der administrativen Kosten- und Zeitersparnis.

Vgl. Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften, BT-Drs. 17/11473, S. 55 f.

Wie bereits das Verwaltungsgericht im Anschluss an den Bundesfinanzhof, vgl. Urteil vom 14.3.2012 – XI R 33/09 –, BFHE 236, 283 = juris, Rn. 31, m.w.N (zur elektronischen Abgabe von Umsatzsteuervoranmeldungen), zu Recht ausgeführt hat, handelt es sich bei der Gewährleistung einer effektiven, möglichst wirtschaftlichen und einfachen Verwaltung um einen gewichtigen öffentlichen Belang. Dieser wird durch die Verpflichtung zur elektronischen Datenübermittlung gefördert. Die jeweils zu übermittelnden statistischen Daten werden von den Auskunftspflichtigen elektronisch aufbereitet und können so nach Übermittlung an die Verwaltung von dieser im Rahmen der gesetzlichen Vorschriften ohne weiteres maschinell weiterverarbeitet werden. Dadurch wird der Antragsteller zu 1. im Rahmen der hier in Rede stehenden Verdienststrukturerhebung nicht unverhältnismäßig belastet. Das gilt auch unter Berücksichtigung des von der Beschwerde geltend gemachten Risikos unberechtigter Datenzugriffe durch Hacker-Angriffe. Zwar fordert der Verhältnismäßigkeitsgrundsatz die Gewährleistung eines dem Gewicht der jeweiligen Grundrechtsbeeinträchtigung angemessenen Maßes an Datensicherheit.

Vgl. BVerfG, Urteil vom 2.3.2010 – 1 BvR 256, 263, 586/08 –, BVerfGE 125, 260 = juris, Rn. 221 ff. (zu Art. 10 GG).

Es ist aber weder dargetan noch sonst ersichtlich, dass vorliegend ein im Hinblick auf Art und Umfang der in Rede stehenden Erhebungsmerkmale nach § 4 VerdStatG hinreichender Schutz vor unberechtigten Datenzugriffen Dritter nicht gewährleistet wäre. Die Datenübermittlung erfolgt mittels der von J. .O. dafür zur Verfügung gestellten Online-Meldeverfahren „IDEV" (Internet Datenerhebung im Verbund) und „.CORE" (Common Online Rawdata Entry) in verschlüsselter Form.

Vgl. https://erhebungsportal.estatistik.de/ Erhebungsportal (Infos für Melder/Schutz der Daten/Personenbezogene Daten und Datensicherheit).

Die Verwendung dem Stand der Technik entsprechender Verschlüsselungsverfahren bei der elektronischen Datenübermittlung ist nunmehr auch – die bereits bislang geübte Praxis festschreibend –, vgl. Entwurf eines Gesetzes zur Änderung des Bundesstatistikgesetzes und anderer Statistikgesetze, BT-Drs. 18/7561, S. 25, in § 11a Abs. 3 BStatG in der Fassung des Gesetzes vom 21.7.2016 (BGBl. I S. 1768) gesetzlich ausdrücklich angeordnet. Die Antragsgegnerin hat mitgeteilt, dass sie auch im Übrigen alle erforderlichen organisatorischen, personellen und technischen Maßnahmen nach den Standards des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) getroffen habe. Unter anderem seien die internen Server vom Internet abgeschirmt und stünden in einem gesondert gesicherten Bereich. Dem ist die Beschwerde nicht entgegengetreten.

Ein gegebenenfalls gleichwohl noch verbleibendes Risiko eines Hacker-Angriffs auf übermittelte oder gespeicherte Daten ist, wie schon das Verwaltungsgericht zutreffend erkannt hat, im überwiegenden Interesse des Gemeinwohls – konkret: der mit der elektronischen Datenverarbeitung bezweckten Verwaltungsvereinfachung – hinzunehmen.

Vgl. auch BFH, Urteil vom 14.3.2012 – XI R 33/09 –, BFHE 236, 283 = juris, Rn. 68 ff., und Beschluss vom 14.4.2015 – V B 158/14 –, BFH/NV 2015, 1115 = juris, Rn. 3 f. (zur elektronischen Abgabe von Umsatzsteuervoranmeldungen bzw. Steuererklärungen)

Aus dem Beschwerdevorbringen ergibt sich nicht, dass das Risiko eines unberechtigten Zugriffs auf die von dem Antragsteller zu 1. elektronisch zu übermittelnden Daten trotz der von J.O. ergriffenen Sicherheitsmaßnahmen unzumutbar hoch ist. Konkrete Sicherheitslücken, die etwaige Hacker-Angriffe auf die betreffenden Daten mit hinreichender Wahrscheinlichkeit erfolgreich erscheinen ließen, haben die Antragsteller nicht benannt. Die von ihnen vorgelegten Berichte über eine im Zuge zunehmenden Digitalisierung der öffentlichen Verwaltung anwachsende Bedrohung durch Hacker-Angriffe und Schadprogramme beschreiben lediglich ein mit der Nutzung moderner Datenverarbeitungssysteme unausweichlich verbundenes allgemeines Risiko, das den Betroffenen zumutbar ist, soweit – wie hier – geeignete Maßnahmen zur Gewährleistung eines nach den jeweiligen Umständen hinreichenden Maßes an Datensicherheit ergriffen worden sind. Soweit die Beschwerde konkret auf Berichte über einen Hacker-Angriff auf das Computer-System des Deutschen Bundestages im Jahr 2015 verweist, sind diese nicht geeignet, unzumutbar gesteigerte Sicherheitsrisiken der Datenverarbeitung (gerade) im Rahmen der Verdienststrukturerhebung zu belegen. Nichts anderes gilt für die ebenfalls vorgelegten Medienberichte über eine Cyber-Attacke auf Systeme der US-Regierung, bei der im Jahr 2015 personenbezogene Daten von mehr als 21 Mio. Mitarbeitern illegal abgegriffen worden sein sollen.

Dieser Beschluss ist gemäß § 152 Abs. 1 VwGO, § 68 Abs. 1 Satz 2 i.V.m. § 66 Abs. 3 Satz 3 GKG unanfechtbar.

Zum Auskunftsrecht bei geltend gemachter Lohngleichheit zwischen Frauen und Männern (Ls)

(**Arbeitsgericht Berlin**, Urteil vom 1. Februar 2017 – 56 Ca 5356/15 –)

Die Feststellung einer ungerechtfertigte Ungleichbehandlung einer Arbeitnehmerin in Bezug auf ihre Vergütung gegenüber der männlicher Kollegen setzt derzeit voraus, dass zu benennende Mitarbeiter vergleichbar sind. Das ist nicht der Fall, wenn diese zum Teil in einem anderen Rechtsverhältnis tätig sind oder – soweit sie in einem vergleichbaren Rechtsverhältnis stehen – über längere Beschäftigungszeiten verfügen.

(Nicht amtlicher Leitsatz)

Zum Auskunftsanspruch eines Insolvenzverwalters gegenüber dem Finanzamt des Schuldners

(**Verwaltungsgericht Lüneburg**, Urteil vom 1. März 2017 – 1 A 343/15 –)

1. **Ein Insolvenzverwalter hat gegen das Finanzamt außerhalb eines laufenden Steuerverfahrens keinen Anspruch auf Erteilung eines Steuerkontoauszugs des Insolvenzschuldners nach § 16 NDSG.**
2. **Die Regelung ist zwar anwendbar, aber in ihren Voraussetzungen vorliegend nicht erfüllt. Der Kläger ist nicht „Betroffener" i.S.d. § 16 Abs. 1 und 3 NDSG.**
3. **Für die Geltungmachung des Anspruchs ist der Verwaltungsgerichtsweg eröffnet.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Beteiligten streiten über die Erteilung eines Steuerkontoauszugs für das Konto eines Insolvenzschuldners an den Kläger als gerichtlich bestellten Insolvenzverwalter.

Der Kläger forderte den Beklagten mit Schreiben vom 19. April 2012 dazu auf, seine Forderungen bei ihm als Insolvenzverwalter anzumelden.

Der Beklagte meldete dem Kläger mit Schreiben vom 9. Mai 2012 für dieses Insolvenzverfahren Abgabenforderungen in Höhe von insgesamt 258.143,81 EUR und führte die Abgabenforderungen im Einzelnen in einer Anlage auf.

Mit Schreiben vom 18. Juni 2012 teilte der Kläger dem Beklagten mit, das Amtsgericht J. habe den angemeldeten Betrag in Höhe von 258.143,81 EUR festgestellt.

Mit Schreiben vom 21. Juli 2015 bat der Kläger den Beklagten um die Übersendung eines Auszugs aus dem Steuerkonto zu der Steuernummer K. oder allen weiteren Steuernummern, unter denen der Insolvenzschuldner in der Vergangenheit – gegebenenfalls auch vorübergehend – bei ihm geführt worden sei.

Mit Schreiben vom 23. Juli 2015 teilte der Beklagte dem Kläger mit, für die Übersendung eines Kontoauszugs sei sein Antragsschreiben nicht ausreichend. ..... Er – der Kläger – müsse sein berechtigtes Interesse, d.h. aus welchen Gründen er die Auskunft benötige, substantiiert darlegen. .....

Mit Schreiben vom 20. August 2015 legte der Kläger gegen dieses Ablehnungsschreiben Einspruch ein. Er nahm Bezug auf § 16 Abs. 1 und 3 NDSG.

Mit Einspruchsbescheid vom 21. August 2015 wies der Beklagte den Einspruch des Klägers als unbegründet zurück. Zur Begründung verwies er auf seinen „Bescheid vom 23. Juli 2015" und führte aus, der Hinweis auf § 16 Abs. 1 und 3 NDSG führe zu keiner anderen Ermessensentscheidung, da der Antrag keine weitere Begründung/Konkretisierung enthalte. ..... Die getroffene Entscheidung sei daher ermessensgerecht.

In der Rechtsbehelfsbelehrung heißt es u.a., gegen diese Entscheidung könne beim Niedersächsischen Finanzgericht Klage erhoben werden.....

Der Kläger ist der Ansicht, es handele sich um eine verwaltungsgerichtliche Streitigkeit.

Aus den Gründen:

Die Klage hat keinen Erfolg.

Der Verwaltungsrechtsweg ist eröffnet.

Gemäß § 40 Abs. 1 Satz 1 VwGO ist der Verwaltungsrechtsweg in allen öffentlich-rechtlichen Streitigkeiten nichtverfassungsrechtlicher Art gegeben, soweit die Streitigkeiten nicht durch Bundesgesetz einem anderen Gericht ausdrücklich zugewiesen sind.

Bei dem vorliegenden Rechtsstreit handelt es sich um eine öffentlich-rechtliche Streitigkeit nichtverfassungsrechtlicher Art. Der Kläger stützt seinen Anspruch auf einen Auszug aus dem Steuerkonto auf § 16 Abs. 1 und 3 NDSG. Das Niedersächsische Datenschutzgesetz verpflichtet gemäß § 2 Abs. 1 Satz 1 NDSG i.V.m. § 16 Abs. 1 und 3 NDSG nur Behörden als Träger hoheitlicher Gewalt. Diese Normen sind als Sonderrecht der öffentlichen Hand dem öffentlichen Recht zuzuordnen (so auch VG Stade, Beschl. v. 22.9.2016 – 1 A 2323/15 -, juris).

Eine abdrängende Sonderzuweisung, insbesondere zu den Finanzgerichten, liegt nicht vor. Gemäß § 33 Abs. 1 FGO ist der Finanzrechtsweg gegeben in öffentlich-rechtlichen Streitigkeiten über Abgabenangelegenheiten, soweit die Abgaben der Gesetzgebung des Bundes unterliegen und durch Bundesfinanzbehörden oder Landesfinanzbehörden verwaltet werden (Nr. 1), in öffentlich-rechtlichen Streitigkeiten über die Vollziehung von Verwaltungsakten in anderen als den in Nummer 1 bezeichneten Angelegenheiten, soweit die Verwaltungsakte durch Bundesfinanzbehörden oder Landesfinanzbehörden nach den Vorschriften der Abgabenordnung zu vollziehen sind (Nr. 2), in öffentlich-rechtlichen und berufsrechtlichen Streitigkeiten über Angelegenheiten, die durch den Ersten Teil, den Zweiten und den Sechsten Abschnitt des Zweiten Teils und den Ersten Abschnitt des Dritten Teils des Steuerberatungsgesetzes geregelt werden (Nr. 3) und in anderen als den in den Nummern 1 bis 3 bezeichneten öffentlich-rechtlichen Streitigkeiten, soweit für diese durch Bundesgesetz oder Landesgesetz der Finanzrechtsweg eröffnet ist (Nr. 4). Abgabenangelegenheiten im Sinne dieses Gesetzes sind alle mit der Verwaltung der Abgaben einschließlich der Abgabenvergütungen oder sonst mit der Anwendung der abgabenrechtlichen Vorschriften durch die Finanzbehörden zusammenhängenden Angelegenheiten einschließlich der Maßnahmen der Bundesfinanzbehörden zur Beachtung der Verbote und Beschränkungen für den Warenverkehr über die Grenze; den Abgabenangelegenheiten stehen die Angelegenheiten der Verwaltung der Finanzmonopole gleich (§ 33 Abs. 2 FGO).

Bei dem Antrag auf Erteilung eines Steuerkontoauszugs nach dem Niedersächsischen Datenschutzgesetz handelt es sich nicht um eine Abgabenangelegenheit im Sinne von § 33 Abs. 2 FGO. Mit den Regelungen in § 33 Abs. 1 und 2 FGO wird keine umfassende behördenbezogene Zuständigkeit der Finanzgerichte für die gesamte öffentlich-rechtliche Tätigkeit der Finanzbehörden geschaffen. Der Rechtsweg zu den Finanzgerichten ist nicht bereits deshalb eröffnet, weil die Steuerakten Vorgänge wiedergeben, über die in Anwendung abgabenrechtlicher Vorschriften entschieden worden ist. Die Zuordnung einer Streitigkeit, die die Auskunftserteilung eines Finanzamtes betrifft, bestimmt sich nicht nach dem Gegenstand der Auskunft, sondern nach der Rechtsnatur des erhobenen Anspruchs, wie sie sich aus dem tatsächlichen Vorbringen des Klägers ergibt. Für die Eröffnung des Finanzgerichtswegs muss die Angelegenheit gerade mit der Anwendung abgabenrechtlicher Vorschriften verknüpft und dadurch geprägt sein. Daran fehlt es hier. Der vom Kläger geltend gemachte Anspruch auf Auskunft nach § 16 Abs. 1 und 3 NDSG wurzelt nicht im Abgabenverhältnis, sondern ist bereichsübergreifend und folglich als außersteuerlicher Anspruch ausgestaltet. Er steht eigenständig neben Ansprüchen auf der Grundlage der Abgaben- und Insolvenzordnung und verwaltungsverfahrensrechtlichen Akteneinsichtsansprüchen (Nds. OVG, Beschl. v. 14.11.2016 – 11 OB 233/16 -, NordÖR 2017, S. 103 f. und NVwZ-RR 2017, S. 216).

Ist bei einem einheitlichen Streitgegenstand und rechtswegüberschreitender Anspruchsnormenkonkurrenz – wie sie hier mit Blick auf den geltend gemachten Anspruch auf Informationszugang nach dem Niedersächsischen Datenschutzgesetz und einen allgemeinen steuerverfahrensrechtlichen Anspruch auf Akteneinsicht nach der Abgabenordnung in Erwägung zu ziehen sind – für eine der Anspruchsgrundlagen der Rechtsweg zum Verwaltungsgericht gegeben, käme eine Verweisung an das Finanzgericht nur dann in Betracht, wenn die Voraussetzungen des Anspruchs, der im Verwaltungsrechtsweg zu verfolgen ist, aufgrund des vorgetragenen Sachverhaltes offensichtlich fehlen (vgl. BVerwG, Beschl. v. 4.3.2015 – 6 B 58/14 – und Vorlagebeschluss v. 15.10.2012 – 7 B 2/12 -, jew. juris). Der Anspruch nach § 16 Abs. 1 und 3 NDSG ist nicht von vornherein gemäß § 2 Abs. 6 NDSG ausgeschlossen und auch nicht offensichtlich unter keinen Umständen einschlägig. Zwar gehen nach § 2 Abs. 6 NDSG besondere Rechtsvorschriften über die Verarbeitung personenbezogener Daten den Bestimmungen des Niedersächsischen Datenschutzgesetzes vor. Ob § 2 Abs. 6 NDSG eine bereichsspezifische Ausnahme für Ansprüche eines Insolvenzverwalters auf Akteneinsicht und Auskunftserteilung hinsichtlich von Steuerdaten auf der Grundlage von Bestimmungen des Niedersächsischen Datenschutzgesetzes darstellt, ist jedoch nicht höchstrichterlich geklärt. Ob dem Kläger der streitgegenständliche Anspruch nach den Vorschriften des Niedersächsischen Datenschutzgesetzes zusteht, ist im Rahmen der materiellen Prüfung des Anspruchs im Hauptsacheverfahren und nicht bei der Bestimmung des zulässigen Rechtsweges zu klären (Nds. OVG, Beschl. v. 14.11.2016 – 11 OB 233/16 –, a.a.O.).

Die Klage ist zulässig.....

Die Klage ist nicht begründet.

Der Ablehnungsbescheid des Beklagten vom 23. Juli 2015 in der Gestalt des Einspruchsbescheids vom 21. August 2015 ist rechtmäßig. Der Kläger hat keinen Anspruch gegen den Beklagten auf Erteilung eines umfassenden Auszugs aus dem Steuerkonto für die Steuernummer K. Der Kläger hat auch keinen An-

spruch auf Verpflichtung des Beklagten, seinen Antrag auf Erteilung eines solchen Steuerkontoauszugs unter Beachtung der Rechtsauffassung des Gerichts neu zu bescheiden.

Auch wenn der Kläger seinen Anspruch auf § 16 Abs. 1 und 3 NDSG stützt und deshalb der Verwaltungsrechtsweg gegeben ist, entscheidet nach § 17 Abs. 2 Satz 1 GVG das Gericht des zulässigen Rechtswegs den Rechtsstreit unter allen in Betracht kommenden rechtlichen Gesichtspunkten. Bei einem gemischten Rechtsverhältnis, d.h. in dem Fall, in dem ein prozessualer Anspruch bei identischem Lebenssachverhalt gegebenenfalls auf mehrere materiell-rechtliche Anspruchsgrundlagen aus unterschiedlichen Rechtsgebieten gestützt werden kann, ist das zuerst angerufene Gericht insgesamt zuständig, sofern seine Zuständigkeit für zumindest einen Klagegrund gegeben ist (Nds. OVG, Beschl. v. 14.11.2016 – 11 OB 233/16 –, a.a.O.). Das erkennende Gericht hat vorliegend neben § 16 Abs. 1 und 3 NDSG auch rechtswegfremde mögliche Anspruchsgrundlagen nach der Abgaben- und Insolvenzordnung zu prüfen.

Der Kläger hat keinen Anspruch auf Erteilung eines umfassenden Auszugs aus dem Steuerkonto für die Steuernummer K. nach § 16 Abs. 1 und Abs. 3 NDSG.

Nach § 16 Abs. 1 Satz 1 NDSG ist Betroffenen von der Daten verarbeitenden Stelle auf Antrag Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Speicherung,
3. die Herkunft der Daten, die Empfänger von Übermittlungen, in den Fällen des § 6 auch die Auftragnehmer, sowie
4. in den Fällen des § 10a über die Art und Struktur der automatisierten Verarbeitung.

Gemäß § 16 Abs. 1 Satz 2 NDSG gilt dies nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind. Für gesperrte Daten, die nur deshalb noch gespeichert sind, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, gilt die Verpflichtung zur Auskunftserteilung nur, wenn Betroffene ein berechtigtes Interesse an der Erteilung der Auskunft über diese Daten glaubhaft machen (§ 16 Abs. 1 Satz 3 NDSG).

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft begehrt wird, näher bezeichnet werden (§ 16 Abs. 2 Satz 1 NDSG). Die Daten verarbeitende Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen (§ 16 Abs. 2 Satz 2 NDSG).

Sind die Daten in Akten gespeichert, so können Betroffene gemäß § 16 Abs. 3 NDSG Auskunft aus Akten oder Akteneinsicht verlangen, soweit sie Angaben machen, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen.

Diese Regelungen des Niedersächsischen Datenschutzgesetzes sind für die Speicherung von Steuerdaten durch den Beklagten als Landesbehörde gemäß § 2 Abs. 1 Satz 1 Nr. 1 NDSG anwendbar. Die Anwendung von § 16 Abs. 1 und 3 NDSG ist nicht durch besondere Rechtsvorschriften über die Verarbeitung personenbezogener Daten gemäß § 2 Abs. 6 NDSG ausgeschlossen. Die Vorschrift des § 2 Abs. 6 NDSG stellt klar, dass das Niedersächsische Datenschutzgesetz nur Grundlagencharakter hat und daher bereichsspezifische Datenschutzvorschriften vorgehen. Die Regelung des § 2 Abs. 6 NDSG gilt unmittelbar nur für landesrechtliche Regelungen. Im Verhältnis zum Bundesrecht ergibt sich ein Vorrang spezifischer bundesrechtlicher Regelungen bereits aus Art. 31 GG (vgl. Begründung des Entwurfs des Niedersächsischen Datenschutzgesetzes, LT-Drs. 12/3290, S. 33 f.).

Zutreffend hat der Beklagte zwar darauf hingewiesen, dass der Bundesgesetzgeber mit der Abgabenordnung von seiner Kompetenz gemäß Art. 108 Abs. 5 Satz 2 GG zur Schaffung eines von den Landesfinanzbehörden anzuwendenden abschließenden Verfahrensrechtes Gebrauch gemacht hat. Die Abgabenordnung kann gemäß Art. 31 GG landesrechtlich nicht geändert oder ergänzt werden.

Die Abgabenordnung enthält jedoch weder eine Regelung, die ein Akteneinsichtsrecht gewährt, noch eine Vorschrift, die Auskunft über und Akteneinsicht in steuerrechtliche Unterlagen verbietet. In der Abgabenordnung sind das Recht auf vorherige Anhörung (§ 91 Abs. 1 AO) und auf Mitteilung der Besteuerungsgrundlagen (§ 364 AO) geregelt. Eine Sperrwirkung für jegliche Zugangsrechte zu amtlichen Informationen der Finanzverwaltung wird daraus nicht hergeleitet. Anerkannt wird im steuerrechtlichen Verfahren ein (ungeschriebener) Anspruch auf ermessensfehlerfreie Entscheidung der zuständigen Finanzbehörde über einen Antrag auf Akteneinsicht, welcher die Darlegung entsprechender Gründe voraussetzt (vgl. Schoch, Informationsfreiheitsgesetz, Kommentar, 2. Aufl. 2016, § 1 Rn. 390 ff. m.w.N.; Winterfeld, NVwZ 2013, S. 815). Ermessensleitende Grundsätze finden sich im Schreiben des Bundesministers für Finanzen vom 17. Dezember 2008 (– IV A 3 – S 0030/08/10001, BGStBl. 2009, S. 6).

Der Beklagte ist der Ansicht, die Abgabenordnung enthalte eine Art „absichtsvolle Nichtregelung" für den Umgang mit den im Besteuerungsverfahren gespeicherten Daten. Die Nichtaufnahme einer Regelung zum Auskunfts-und Akteneinsichtsrecht des Steuerpflichtigen in der Abgabenordnung sei eine bewusste gesetzgeberische Entscheidung und damit ein absichtsvoller Regelungsverzicht, welcher eine umfassende Sperrwirkung entfalte. Der Gesetzgeber habe ein allgemeines Akteneinsichtsrecht im Steuerverwaltungsverfahren gerade zum Schutz Dritter und des Ermittlungsinteresses der Finanzbehörden sowie wegen des Verwaltungsaufwandes für nicht praktikabel gehalten. Dieser Ansicht folgt das Gericht nicht.

Dabei bestehen bereits ernsthafte Zweifel, ob der Verzicht auf die Regelung des Akteneinsichtsrechts in der Abgabenordnung absichtsvoll, d.h. vom Gesetzgeber (weiterhin) als bewusst und gewollt anzusehen ist. Vieles spricht dafür, dass die Abgabenordnung keine bereichsspezifische Ausschlussregelung (mehr) enthält (vgl. dazu OVG Hamburg, Beschl. v. 21.12.2011 – 5 So 111/11 –; OVG NRW, Urt. v. 15.6.2011 – 8 A 1150/10 –, jew. juris). Der Bundesgesetzgeber hatte wohl aus Praktikabilitätserwägungen Abstand davon genommen, Beteiligten eines steuerrechtlichen Verfahrens einen Anspruch auf Akteneinsicht in der Abgabenordnung nach dem Vorbild des § 29 VwVfG einzuräumen. Dafür spricht der Bericht und Antrag des Finanzausschusses vom 7. November 1975 (BT-Drs. 7/4292, S. 24 f.). Zu diesem Zeitpunkt hatte das Bundesverfassungsgericht noch nicht das informelle Selbstbestimmungsrecht entwickelt, denn dieses wurde vom Bundesverfassungsgericht erst im sogenannten Volkszählungsurteil 1983 als Grundrecht anerkannt (BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 –, BVerfGE 65, 1 ff.). Seitdem das Informationsfreiheitsgesetz des Bundes am 1. Januar 2006 in Kraft getreten ist, gilt der Grundsatz, dass die Gewährung von Zugang zu bundesbehördlichen Informationen die Regel und die Verwehrung des Zugangs die Ausnahme ist. Auch an die Informationsfreiheits-, Informationszugangs- und Datenschutzgesetze der einzelnen Bundesländer in der gegenwärtigen Form war in den 70er Jahren noch nicht zu denken. Ins-

besondere in Folge der EU-Richtlinie Nr. 95/46/EG hat sich eine grundlegend veränderte rechtliche Situation ergeben, die auch die Finanzverwaltung zu mehr Transparenz zwingt (vgl. Seer, in: Tipke/Kruse, AO/FGO, 146. Lief., Stand: Oktober 2016, § 91 AO Rn. 29; Winterfeld, NVwZ 2013, S. 815). Der pauschale Hinweis auf eine – angebliche – „abschließende Negativregelung" des Akteneinsichtsrechts in der Abgabenordnung, die nur zu einem Ermessensanspruch führt, hilft nicht weiter, denn dieser setzt voraus, was es zu ermitteln gilt: das heutige Verhältnis zwischen der Abgabenordnung und dem Niedersächsischen Datenschutzgesetz (so Schoch für das IFG, a.a.O., § 1 Rn. 392).

Es ist zu beachten, dass es sich bei den Informationsrechten nach dem Niedersächsischen Datenschutzgesetz und den Informationsfreiheitsgesetzen des Bundes und der Ländern um eigenständige Verwaltungsverfahren handelt (vgl. Schoch, a.a.O., § 1 Rn. 392; Winterfeld, NVwZ 2013, S. 816 unter Berufung auf OVG Schleswig-Holstein, Urt. v. 6.12.2012 – 4 LB 11/12 –). Die Versagung eines Anspruchs auf Akteneinsicht im Steuerverwaltungsverfahren führte de facto zu einer Ausnahme nur für den Bereich der Finanzverwaltung. Weder in § 2 Abs. 6 NDSG noch in § 1 Abs. 3 IFG des Bundes ist eine solche Bereichsausnahme für die Finanzverwaltung ausdrücklich vorgesehen. Stattdessen wird in den spezifischen Ausschlussgründen zum Informationszugang gemäß § 3 Nr. 1d und 1e IFG geradezu vorausgesetzt, dass das Informationsfreiheitsgesetz auch bezüglich der Finanzbehörden anwendbar ist, denn diese nennen ausdrücklich die „Finanzbehörden" bzw. „Angelegenheiten der externen Finanzkontrolle" (vgl. Schoch, a.a.O., § 1 Rn. 393). Es ist auch nicht ersichtlich, dass eine anderweitige Regelung gegenüber niedersächsischen Landesbehörden wie den niedersächsischen Finanzämtern erforderlich wäre. Dafür spricht auch die ratio legis. Wenn § 2 Abs. 7 NDSG und § 1 Abs. 3 IFG im Interesse der praktischen Wirksamkeit des Niedersächsischen Datenschutzgesetzes bzw. Informationsfreiheitsgesetzes des Bundes schon dem geschriebenen Akteneinsichtsrecht im (Niedersächsischen) Verwaltungsverfahrensgesetz keinen Vorrang einräumen, kann dies sinnvollerweise erst recht nicht bezüglich eines nur von der Rechtsprechung entwickelten Anspruchs auf fehlerfreie Ermessenentscheidung über das Akteneinsichtsbegehren nach der Abgabenordnung der Fall sein (vgl. Schoch, a.a.O., § 1 Rn. 393). Der Vorrang einer nicht existierenden Rechtsvorschrift ist weder in Art. 31 GG noch in § 2 Abs. 6 NDSG noch in § 1 Abs. 3 IFG normiert.

Eine abschließende Regelung folgt auch nicht aus dem in § 30 AO statuierten Steuergeheimnis. Die Berufung auf das Steuergeheimnis in § 30 AO geht schon deshalb fehl, weil es sich bei Geheimhaltungsvorschriften gerade nicht um Regelungen über den Zugang zu amtlichen Informationen handelt, sondern um Regelungen zu dessen Begrenzung (so auch Schoch, a.a.O., § 1 Rn. 392). Über einen Anspruch des Steuerpflichtigen, seines Vertreters oder eines Dritten gegenüber einer Finanzbehörde auf Mitteilung der über ihn gespeicherten Daten sagt diese Vorschrift nichts aus. Die Bestimmungen in § 30 AO mögen daher im Einzelfall dem Anspruch auf Informationszugang entgegenstehen, sie sind aber keine „besonderen Rechtsvorschriften über die Verarbeitung personenbezogener Daten". § 30 AO ist daher erst auf der Ebene der Ausschlusstatbestände zu berücksichtigen (vgl. OVG NRW, Urt. v. 15.6.2011 – 8 A 1150/10 –, juris).

Es kann vorliegend offen bleiben, ob im Hinblick auf die Informationszugangsgesetzgebung auf Bundesebene aus jüngerer Zeit noch von einer „absichtsvollen Nichtregelung" in Bezug auf den hier streitigen Informationszugangsanspruch die Rede sein kann. Jedenfalls käme einem „absichtsvollen Regelungsverzicht" der Abgabenordnung im vorliegenden Zusammenhang keine anspruchsverdrängende Wirkung zu.

Ein gegenüber dem Finanzamt geltend gemachter Informationsanspruch des Insolvenzverwalters, der gegebenenfalls anschließend einen Anfechtungsanspruch durchsetzen will, wird bereits vom Regelungsbereich der Abgabenordnung nicht erfasst. Der Gesetzgeber hat sich beim Erlass der Abgabenordnung nur mit der Frage befasst, ob der Beteiligte eines steuerrechtlichen Verfahrens nach dem Vorbild des § 29 VwVfG einen Anspruch auf Akteneinsicht haben soll (vgl. BT-Drs. 7/4292, S. 24 f.). Gegenstand der Überlegungen und der nachfolgenden Nichtregelung war demnach nur der Informationszugang im Rahmen des Besteuerungsverfahrens. Einen solchen auf ein laufendes Steuerverfahren bezogenen Anspruch als Beteiligter macht der Kläger nicht geltend. Denn er handelt nicht gemäß § 34 Abs. 3 und 1 AO in Erfüllung der steuerlichen Pflichten des Insolvenzschuldners und, um dessen Rechte zu wahren. Er ist vielmehr im Interesse der Gesamtheit der Gläubiger tätig, zu deren Gunsten Zahlungen des Insolvenzschuldners im Wege der Anfechtung zur Insolvenzmasse gezogen werden könnten; dabei handelt es sich um ein eigenständiges Rechtsverhältnis zwischen dem Kläger und dem Beklagten (BVerwG, Beschl. v. 14.5.2012 – 7 B 53/11 –, juris, mit Hinweis auf die Rechtsprechung des BFH). Darüber hinaus umfasst die Gesetzgebungskompetenz des Art. 108 Abs. 5 Satz 2 GG mit dem von den Landesfinanzbehörden anzuwendenden „Verfahren" der Steuerverwaltung selbst bei Beteiligten lediglich anhängige Steuerverwaltungsverfahren. Eine Sperrwirkung für Informationszugangsrechte auf anderer Grundlage als der Abgabenordnung kann deshalb für den Zeitraum nach Abschluss eines solchen Steuerverwaltungsverfahrens von vornherein nicht eintreten (OVG Schleswig-Holstein, Urt. v. 6.12.2012 – 4 LB 11/12 –, juris; dagegen Sydow, ZD 2013, S. 11 ff.). Informationsansprüche außerhalb eines konkreten Besteuerungsverfahrens können geltend gemacht werden (Seer, in: Tipke/Kruse, AO/FGO, 146. Lief., Stand: Oktober 2016, § 91 AO Rn. 29).

Die insolvenzrechtlichen bzw. auf das Insolvenzverfahren bezogenen Vorschriften über Auskunftsansprüche nach §§ 97, 101 InsO bzw. § 242 BGB, die die privatrechtlichen Rechtsverhältnisse im Insolvenzverfahren und Informationsansprüche der Betroffenen untereinander regeln, stehen dem Anspruchsbegehren des Klägers ebenfalls nicht vorrangig entgegen, da sie gerade nicht den Zugang zu amtlichen Informationen gegenüber Landesbehörden regeln (vgl. VG Stade, Beschl. v. 22.9.2016 – 1 A 2323/15 –, m.w.N.; OVG NRW, Urt. v. 24.11.2015 – 8 A 1032/14 – und Urt. v. 15.6.2011 – 8 A 1150/10 –; VG Schleswig-Holstein, Urt. v. 31.10.2014 – 8 A 1/14 , jew. juris).

Die Regelungen des § 16 Abs. 1 und 3 NDSG sind zwar anwendbar. Ihre Voraussetzungen sind indes nicht erfüllt.

§ 16 Abs. 1 NDSG sieht ein Auskunftsrecht und § 16 Abs. 3 NDSG ein Akteneinsichtsrecht nur vor, wenn „Betroffene" einen Antrag hinsichtlich der „zu ihrer Person gespeicherten Daten" stellen (§ 16 Abs. 1 Satz 1 Nr. 1 i.V.m. Abs. 3 NDSG). Der Kläger ist nicht „Betroffener" i.S.d. § 16 Abs. 1 und 3 NDSG.

Der Kläger hat nicht einen Antrag hinsichtlich der zu seiner eigenen Person gespeicherten Daten gestellt. Er hat beantragt, den Beklagten zu verpflichten, ihm einen umfassenden Auszug aus dem Steuerkonto für die Steuernummer K. zur Verfügung zu

stellen. Dieses Steuerkonto ist nicht das Steuerkonto des Klägers, sondern das Steuerkonto des Insolvenzschuldners. In diesem Steuerkonto sind keine Daten über den Kläger gespeichert.

Der Kläger hat auch nicht deshalb einen Anspruch auf Auskunft bzw. Akteneinsicht gegenüber dem Beklagten nach dem Niedersächsischen Datenschutzgesetz, weil das Amtsgericht Hamburg ihn mit Beschluss vom 4. April 2012 zum Insolvenzverwalter bestellt und der Kläger in dieser Funktion einen Antrag auf Erteilung eines Auszugs für das Steuerkonto des Insolvenzschuldners beantragt hat. Der Kläger hat insoweit nicht als Vertreter des insolvenzschuldners gehandelt. Denn – wie oben erläutert – handelt ein Insolvenzverwalter, der gegenüber dem Finanzamt einen Informationsanspruch geltend macht, um gegebenenfalls anschließend einen Anfechtungsanspruch durchzusetzen, nicht gemäß § 34 Abs. 3 und 1 AO, § 155 InsO in Erfüllung der steuerlichen Pflichten des Insolvenzschuldners und um dessen Rechte zu wahren. Er ist vielmehr im Interesse der Gesamtheit der Gläubiger tätig, zu deren Gunsten Zahlungen des Insolvenzschuldners im Wege der Anfechtung zur Insolvenzmasse gezogen werden könnten und diese die Insolvenzmasse stärken würden (BVerwG, Vorlagebeschl. v. 15.10.2012 – 7 B 2/12 – und Beschl. v. 14.5.2012 – 7 B 53/11 –, mit Hinweis auf die Rechtsprechung des BFH; OVG NRW, Urt. v. 24.11.2015 – 8 A 1032/14 –; VG Schleswig-Holstein, Urt. v. 31.10.2014 – 8 A 1/14 –, jew. juris). Das Niedersächsische Datenschutzgesetz sieht auch weder ein Sonderrecht auf Auskunft für Insolvenzverwalter noch einen Anspruch für jedermann vor. Im Gegensatz zu dem Informationsfreiheitsgesetz des Bundes und den Informationszugangsgesetzen anderer Bundesländer, nach denen „jeder" grundsätzlich ein umfassendes Auskunftsrecht hat, ist das Niedersächsische Datenschutzgesetz als Betroffenenrecht ausgestaltet. Systematisch zutreffend findet sich die Regelung des § 16 NDSG im Dritten Abschnitt des Niedersächsischen Datenschutzgesetzes mit der Überschrift „Rechte der Betroffenen". Ein Informationsfreiheitsgesetz ist in Niedersachsen bisher nicht geschaffen worden.

Der Kläger hat keinen Anspruch auf Erteilung des Steuerkontoauszugs nach dem Informationsfreiheitgesetz des Bundes. Der Bundesgesetzgeber hat zwar mit dem bundesrechtlichen Informationsfreiheitsgesetz für den Bürger ein umfassendes, voraussetzungsloses Akteneinsicht geschaffen. Jede natürliche oder juristische Person hat grundsätzlich ein unbedingtes Recht auf freien Zugang zu den Informationen, über die eine öffentliche Stelle verfügt. Eingeschränkt werden kann dieses nicht durch fiskalisch dominierte Umstände, sondern nur durch bestimmte, gesetzlich vorgeschriebene, ausnahmsweise vorliegende Versagungsgründe. Der Informationsanspruch besteht gemäß § 1 Abs. 1 Satz 1 IFG indes nur gegenüber Behörden des Bundes. Bei dem Beklagten handelt es sich um eine Landesbehörde, auf die § 1 Abs. 1 Satz 1 IFG keine Anwendung findet. Ein entsprechendes Informationsfreiheitsgesetz ist in Niedersachsen – im Gegensatz zu den meisten Bundesländern – bisher nicht geschaffen worden. In Ländern ohne Informationsfreiheitsgesetz greift das Informationsfreiheitsgesetz des Bundes nicht etwa „lückenschließend" ein (Schoch, NVwZ 2017, S. 97 f.). Die daraus resultierenden Ungleichheiten sind durch das föderale Gefüge der Bundesrepublik Deutschland bedingt.

Der Kläger hat keinen Anspruch auf Erteilung des geltend gemachten Steuerauszugs nach der Abgabenordnung. Wie oben ausgeführt, enthält die Abgabenordnung keine Regelung, die ein Auskunfts- bzw. Akteneinsichtsrecht gewährt. Anerkannt wird im steuerrechtlichen Verfahren nur ein (ungeschriebener) Anspruch auf ermessensfehlerfreie Entscheidung der zuständigen Finanzbehörde über einen Antrag auf Akteneinsicht, weil diese nicht durch Vorschriften gehindert ist, in Einzelfällen Akteneinsicht zu gewähren (BFH, Urt. v. 19.3.2013 – II R 17/11 – und Urt. v. 23.2.2010 – VII R 19/09 – sowie Beschluss v. 4.6.2003 – VII B 138/01 –; Schoch, Informationsfreiheitsgesetz, Kommentar, 2. Aufl. 2016, § 1 Rn. 390 ff. m.w.N.; Seer, in: Tipke/Lang, Steuerrecht, 22. Aufl. 2015, § 21 Rn 10; Winterfeld, NVwZ 2013, S. 815). Ermessensleitende Grundsätze finden sich im Schreiben des Bundesministers für Finanzen vom 17. Dezember 2008 (– IV A 3 – S 0030/08/10001, BGStBl. 2009, S. 6). Dieses befasst sich als verwaltungsinterne Vorgabe zur gleichmäßigen Anwendung von steuerrechtlichen Normen mit dem rechtlichen Zusammenhang des finanzgerichtlich entwickelten Anspruchs eines Beteiligten i.S.v. §§ 78, 359 AO im Besteuerungsverfahren auf Ermessensentscheidung über Akteneinsicht im laufenden Verfahren. Nach Nr. 1 dieses Schreibens ist Beteiligten (§§ 78, 359 AO) auf Antrag Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen, wenn sie ein berechtigtes Interesse darlegen und keine Gründe für eine Auskunftsverweigerung vorliegen. Ein berechtigtes Interesse ist nach Nr. 3 des Schreibens namentlich nicht gegeben, wenn die Auskunft dazu dienen kann, zivilrechtliche Ansprüche gegen den Bund oder ein Land durchzusetzen und Bund oder Land zivilrechtlich nicht verpflichtet sind, Auskunft zu erteilen (z.B. Amtshaftungssachen, Insolvenzanfechtung).

Der Bundesfinanzhof geht davon aus, dass auch dem Insolvenzverwalter das Recht zusteht, dass das Finanzamt über seinen im Besteuerungsverfahren gestellten Antrag auf Akteneinsicht oder Erteilung eines Steuerkontoauszugs nach pflichtgemäßem Ermessen entscheidet (BFH, Urt. v. 19.3.2013 – II R 17/11 -, juris). Begehre ein Insolvenzverwalter Auskunft über steuerliche Verhältnisse des Insolvenzschuldners, habe das Finanzamt im Rahmen der ihm obliegenden Ermessensabwägung das Interesse des Insolvenzverwalters an der Auskunft und den steuerrechtlichen Charakter dieser Auskunft zu berücksichtigen. Dazu habe der Insolvenzverwalter substantiiert darzulegen, aus welchen Gründen er die Auskunft begehre und dass die Auskunft auf dem Steuerrechtsverhältnis beruhe. Es reiche insoweit nicht aus, dass ein Insolvenzverwalter eine Auskunft im Hinblick auf die ordnungsgemäße Bearbeitung des Insolvenzverfahrens beantrage. Denn für das Finanzamt müsse erkennbar sein, dass ein berechtigtes Interesse an der Auskunft vorliege und diese im Steuerrechtsverhältnis und nicht in einem sonstigen Verhältnis (schuldrechtlicher oder verwaltungsrechtlicher Art) wurzele. Habe der Insolvenzverwalter in ausreichender Weise dargelegt, dass er Auskunft in Form eines Kontoauszugs für den Insolvenzschuldner zur Erfüllung steuerlicher Pflichten oder zur Prüfung der vom Finanzamt angemeldeten Forderungen benötige, könne das Finanzamt den Kontoauszug erteilen. Fehle jedoch eine solche Darlegung, könne das Finanzamt schon aus diesem Grunde die Erteilung eines Kontoauszugs ablehnen (BFH, Urt. v. 19.3.2013 – II R 17/11 –, juris). Ob der Auskunftsanspruch des Insolvenzverwalters dabei per se ausgeschlossen ist, wenn der Insolvenzverwalter Informationen nur im Hinblick auf eine Insolvenzanfechtung benötigt, kann vorliegend dahinstehen. Denn der Kläger hat gegenüber dem Beklagten keinerlei berechtigtes Interesse an dem Zugang zu den begehrten Informationen dargelegt und sich insbesondere nicht auf eine mögliche Insolvenzanfechtung berufen. Gründe sind weder seinem

Antragsschreiben vom 21. Juli 2015 noch seinem Einspruchsschreiben vom 20. August 2015 zu entnehmen. War dem Beklagten das konkrete Informationsinteresse des Klägers nicht bekannt, konnte er es auch nicht gegen Geheimhaltungsinteressen, Praktikabilitätsgesichtspunkte etc. abwägen. Er konnte ein Interesse des Klägers folglich nicht bei seiner Ermessensentscheidung berücksichtigen und insbesondere nicht von einer Ermessensreduzierung auf Null ausgehen, die zu einem Anspruch des Klägers auf Erteilung des Steuerkontoauszugs geführt hätte.

Auch aus insolvenzrechtlichen Vorschriften kann der Kläger den begehrten Informationszugang nicht beanspruchen. Die Insolvenzordnung sieht einen Auskunftsanspruch des Insolvenzverwalters gegen Gläubiger, die im Wege der Insolvenzanfechtung in Anspruch genommen werden sollen, nicht vor. §§ 20, 97, 101 InsO regeln die Auskunfts- und Mitwirkungspflichten des Insolvenzschuldners bzw. seiner Organe und Angestellten gegenüber dem Insolvenzgericht, dem Insolvenzverwalter, dem Gläubigerausschuss und auf Anordnung des Gerichts der Gläubigerversammlung. §§ 20, 97, 101 InsO sagen zur Auskunftspflicht der Insolvenzgläubiger gegenüber dem Insolvenzverwalter nichts aus. Sie regeln jedenfalls in diesem Verhältnis den Zugang zu amtlichen Informationen ersichtlich nicht. Vielmehr sind die über §§ 20, 97, 101 InsO verfügbaren Informationen typischerweise nichtamtliche Aufzeichnungen von Privatpersonen (vgl. BVerwG, Beschl. v. 20.05.2010 – 7 B 28.10 –; BGH, Urt. v. 13.8.2009 – IX ZR 58/06 –; OVG NRW, Urt. v. 24.11.2015 – 8 A 1032/14 – und Urt. v. 15.6.2011 – 8 A 1150/10 –; OVG Sachsen-Anhalt, Urt. v. 23.4.2014 – 3 L 319/13 –; VG Stade, Beschl. v. 22.9.2016 – 1 A 2323/15 –, jew. juris).

Für den Kläger kann sich auch nicht aus dem Grundsatz von Treu und Glauben (§ 242 BGB) ein entsprechender Auskunfts- und Akteneinsichtsanspruch gegen den Beklagten ergeben. Die Pflicht, Treu und Glauben zu genügen (§ 242 BGB), erstreckt sich, auf einem allgemeinen Rechtsgedanken beruhend, auch auf das öffentliche Recht (vgl. BVerwG, Urt. v. 22.1.1993 – 8 C 46/91 –, juris, m.w.N.). Sie ist dementsprechend auch im Steuerrecht als allgemeiner Rechtsgrundsatz uneingeschränkt anerkannt (BFH, Urt. v. 8.2.1996 – V R 54/94 –). Treu und Glauben gebieten, dem Anspruchsberechtigten einen Auskunftsanspruch zuzubilligen, wenn die zwischen den Beteiligten bestehenden Rechtsbeziehungen es mit sich bringen, dass der Anspruchsberechtigte in entschuldbarer Weise über das Bestehen oder den Umfang seines Rechts im Ungewissen ist, und wenn der Verpflichtete in der Lage ist, unschwer die zur Beseitigung dieser Ungewissheit erforderliche Auskunft zu erteilen (BGH, Urt. v. 6.2.2007 – X ZR 117/04 –, juris). Voraussetzung ist demnach, dass zwischen dem Kläger als Insolvenzverwalter und dem Beklagten als Finanzamt eine rechtliche Sonderverbindung besteht, in deren Rahmen der Kläger zur Wahrung seiner Rechte auf die Auskunft angewiesen ist. Eine solche Sonderverbindung besteht nicht. Wie bereits ausgeführt, handelt der Kläger, wenn er einen Auszug für das Steuerkonto des Insolvenzschuldners beantragt, nicht gemäß § 34 Abs. 3 und 1 AO, § 155 InsO in Erfüllung der steuerlichen Pflichten des Insolvenzschuldners und um dessen Rechte zu wahren. Er ist vielmehr im Interesse der Gesamtheit der Gläubiger tätig, zu deren Gunsten Zahlungen des Insolvenzschuldners im Wege der Anfechtung zur Insolvenzmasse gezogen werden könnten, die die Insolvenzmasse stärken würden (BVerwG, Vorlagebeschl. v. 15.10.2012 – 7 B 2/12 – und Beschl. v. 14.5.2012 – 7 B 53/11 –, mit Hinweis auf die Rechtsprechung des BFH; OVG NRW, Urt. v. 24.11.2015 – 8 A 1032/14 –; VG Schleswig-Holstein, Urt. v. 31.10.2014 – 8 A 1/14 –, jew. juris). Der Bundesgerichtshof macht einen Auskunftsanspruch des Insolvenzverwalters gegen Gläubiger des Insolvenzschuldners wegen möglicher Anfechtungsansprüche in ständiger Rechtsprechung davon abhängig, dass ein Anfechtungsanspruch dem Grunde nach besteht und es nur noch um die nähere Bestimmung von Art und Umfang des Anspruchs geht. Solange ein Rückgewährschuldverhältnis nicht feststeht, hat sich der Insolvenzverwalter wegen aller benötigten Auskünfte an den Vollstreckungsschuldner gemäß §§ 97, 101 InsO zu halten. Im vorliegenden Fall ist diese Voraussetzung nicht gegeben. Der Kläger vermutet wohl anfechtbare Rechtshandlungen. Gegenüber Personen/Behörden, die lediglich im Verdacht stehen, sie könnten etwas vom Insolvenzschuldner in anfechtbarer Weise erworben haben, besteht nach der Rechtsprechung des Bundesgerichtshof jedoch kein Anspruch auf Auskunft nach § 242 BGB (BGH, Urt. v. 13.8.2009 – IX ZR 58/06 –, juris, m.w.N.). Nach diesen Grundsätzen müsste der Kläger als Insolvenzverwalter seinen insolvenzrechtlichen Auskunftsanspruch zunächst gegenüber dem Insolvenzschuldner nach § 97 InsO geltend machen.

Das Gericht lässt die Berufung wegen grundsätzlicher Bedeutung der Rechtssache gemäß § 124 a Abs. 1 i.V.m. § 124 Abs. 2 Nr. 3 VwGO zu. Das Niedersächsische Oberverwaltungsgericht hat in seinem Beschluss vom 14. November 2016 (11 OB 233/16) ausgeführt, dass die Frage, ob § 2 Abs. 6 NDSG eine bereichsspezifische Ausnahme für Ansprüche eines Insolvenzverwalters auf Akteneinsicht und Auskunftserteilung hinsichtlich von Steuerdaten auf der Grundlage von Bestimmungen des Niedersächsischen Datenschutzgesetzes darstellt, höchstrichterlich nicht geklärt sei. Sollte das Niedersächsische Oberverwaltungsgericht die Auffassung des erkennenden Gerichts bestätigen und die Anwendbarkeit des § 16 Abs. 1 und 3 NDSG bejahen, bedarf es darüber hinaus der grundsätzlichen Klärung, ob ein Insolvenzverwalter, der die Erteilung eines Auszugs für das Steuerkonto des Insolvenzschuldners begehrt, Betroffener im Sinne des § 16 Abs. 1 und 3 NDSG ist.

Berichte, Informationen, Sonstiges

Gesetz zur Änderung des Bundesdatenschutzgesetzes

Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz)

Der Bundestag hat am 09.03.2017 mit dem Videoüberwachungsverbesserungsgesetz die nachstehende Ergänzung des § 6b BDSG beschlossen. Der Bundesrat hat am 31.03.2017 zugestimmt.

Änderung des Bundesdatenschutzgesetzes

§ 6b des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. IS. 66), das zuletzt durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162) geändert worden ist, wird wie folgt geändert:

1. Dem Absatz 1 wird folgender Satz angefügt:

   „Bei der Videoüberwachung von

   1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder

   2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

   gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse."

2. Nach Absatz 3 Satz 1 wird folgender Satz eingefügt: „Absatz 1 Satz 2 gilt entsprechend."

Aus der Gesetzesbegründung (BT-Drs – 18/10941)

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Ziel des Gesetzesentwurfes ist es, die Sicherheit bei öffentlich zugänglichen großflächigen Anlagen (z.B. Einkaufszentren) sowie bei Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs, der in Privatrechtsform betrieben wird, zu erhöhen und Anschläge wie in Ansbach und München im Sommer 2016 zu verhindern. Die Zulässigkeit der Beobachtung mit optisch-elektronischen Einrichtungen (Videoüberwachung) richtet sich nach § 6b BDSG. Die Einrichtung solcher Anlagen durch die Betreiber wird durch die Datenschutzaufsichtsbehörden der Länder überprüft, die einer Videoüberwachung in solchen Anlagen eher ablehnend gegenüber stehen. Angesichts der jüngsten Vorfälle sollten Sicherheitsbelange stärker von den Betreibern von öffentlich zugänglichen großflächigen Anlagen sowie Einrichtungen und Fahrzeugen des öffentlichen Schienen-, Schiffs- und Busverkehrs in die durchzuführende Abwägungsentscheidung einbezogen und von den Datenschutzaufsichtsbehörden bei ihrer Überprüfungsentscheidung entsprechend berücksichtigt werden. Der Einsatz optisch-elektronischer Sicherheitstechnologie in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Schienen-, Schiffs- und Busverkehr kann präventiv dazu beitragen, dieSicherheit der Bevölkerung zu erhöhen, indem potentielle Täter etwa bei der Erkundung von Örtlichkeiten im Vorfeld oder unmittelbar vor einer Tatbegehung erkannt und diese vereitelt werden kann. Darüber hinaus erleichtert eine verstärkte Videoüberwachung die Ermittlungstätigkeit von Polizei und Staatsanwaltschaft erheblich, wenn Videoaufzeichnungen auf der Grundlage polizeirechtlicher Befugnisnormen oder allgemeiner Übermittlungstatbestände zur Verfolgung von Straftaten weitergegeben werden.

II. Wesentlicher Inhalt des Entwurfs

Der Gesetzentwurf enthält eine normative Gewichtungsvorgabe für die weiterhin zu treffende Abwägungsentscheidung bei der Entscheidung über den Einsatz von optisch-elektronischen Einrichtungen nach § 6b Absatz 1 Bundesdatenschutzgesetz bei öffentlich zugänglichen großflächigen Anlagen sowie Einrichtungen und Fahrzeugen des öffentlichen Schienen-, Schiffs- und Busverkehrs, die von nicht-öffentlichen Stellen betrieben werden.

III. Alternativen

Keine.

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes ergibt sich aus Artikel 73 Absatz 1 Nummer 6a, Artikel 74 Absatz 1 Nummer 21 und Artikel 74 Absatz 1 Nummer 23 des Grundgesetzes (GG), sowie Artikel 74 Absatz 1 Nummer 11 und Artikel 74 Absatz 1 Nummer 22 GG. Nach Artikel 72 Absatz 2 GG steht dem Bund die Gesetzgebungskompetenz in den beiden zuletzt genannten Fällen unter anderem dann zu, wenn und soweit eine bundesgesetzliche Regelung zur Wahrung der Rechtseinheit im gesamtstaatlichen Interesse erforderlich ist. Eine solche bundesgesetzliche Regelung ist hier notwendig, um einer Rechtszersplitterung entgegenzuwirken.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union vereinbar.

VI. Gesetzesfolgen

Erfüllungsaufwand

Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein zusätzlicher Erfüllungsaufwand.

Wirtschaft

Aufgrund einer voraussichtlich steigenden Anzahl von zulässigen Videokameras erhöhen sich die Bürokratiekosten aus der Informationspflicht zur Kenntlichmachung und Kennzeichnung einer Videoüberwachung nach § 6b Absatz 2 Bundesdatenschutzgesetz (ID-IP 2006100413180112). In WebSKM ist eine jährliche Fallzahl von 32.800 Fällen ausgewiesen. Es ist allerdings zu berücksichtigen, dass sich hiervon ein Großteil (rund 17.200 Fälle) auf Einrichtungen bezieht, die durch das vorliegende Gesetz nicht tangiert sind, weil diese Einrichtungen u.a. zu klein sind oder bereits eine Videoüberwachung installiert haben. Bei den übrigen 15.600 Fällen wird durch die gesetzliche Änderung eine Steigerung der zulässigen Videokameras um 20 Prozent angenommen, womit sich eine Fallzahl von rund 3.100 ergibt. Der zusätzliche Erfüllungsaufwand für die Wirtschaft beträgt rund 141.900 Euro pro Jahr, der sich aus Personalkosten in Höhe von rund 48.900 Euro (3.100 Fallzahl x 20 Minuten x 47,30/60 Lohnsatz) und aus Anschaffungskosten in Höhe von 93.000 Euro (3.100 Fallzahl x 30 Euro) zusammensetzt.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Bundesdatenschutzgesetzes)

Zu Nummer 1 (§ 6b Absatz 1 Satz 2)

Zum Schutz von Leben, Gesundheit oder Freiheit von Personen in Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs und öffentlich zugänglichen großflächigen Anlagen soll der Einsatz von optisch-elektronischer Sicherheitstechnologie in höherem Maße als bisher möglich sein und dadurch die Sicherheit der Bevölkerung insgesamt erhöht werden.

Öffentlich zugängliche großflächige Anlagen sind bauliche Anlagen, die nach dem erkennbaren Willen des Betreibers von jedermann betreten oder genutzt werden können und von ihrer Größe her geeignet sind, eine größere Anzahl von Menschen aufzunehmen. Insbesondere kommen hierbei Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren und Parkräume in Betracht, die einen entsprechenden Publikumsverkehr aufweisen. Hierzu gehören auch Flächen, die eine gleichzeitige Anwesenheit vieler Menschen bei Veranstaltungen ermöglichen, und ganz oder teilweise aus baulichen Anlagen bestehen und daher auch besonderen baurechtlichen Bestimmungen der Länder und der Baunutzungsverordnung unterliegen.

Die Beurteilung der Zulässigkeit einer Videoüberwachung unterliegt bei Einrichtungen und Fahrzeugen des Schienen-, Schiffs- und Busverkehrs nur dann dem § 6b BDSG, wenn der Verkehrsbetrieb nicht öffentlich-rechtlich betrieben wird. Zu den öffentlich zugänglichen großflächigen Einrichtungen des Schienen-, Schiffs- und Busverkehrs gehören beispielsweise Busfernbahnhöfe.

Die Regelung in Absatz 1 Satz 2 legt normativ fest, dass der Schutz von Leben, Gesundheit oder Freiheit als besonders wichtiges Interesse in solch hochfrequentierten Räumen gilt. Damit können der Schutz und die Erhöhung der Sicherheit von Personen, die sich in solchen Einrichtungen aufhalten, ein berechtigtes Interesse der Betreiber darstellen. Zugleich werden mit der Formulierung des „besonders wichtigen Interesses“ in Absatz 1 Satz 2 diese Belange besonders hervorgehoben. Sie können von den Betreibern von solchen hochfrequentierten Anlagen dementsprechend in die Abwägungsentscheidung nach § 6b Absatz 1 Satz 1 Nummer 3 BDSG über den Einsatz einer Videoüberwachung einbezogen und neben ihren zivilrechtlichen Verpflichtungen (z.B. Verkehrssicherungspflicht) verstärkt beachtet werden. Dabei gibt es keine Verpflichtung des Betreibers eine Videoüberwachung einzusetzen. Soweit der Betreiber eine Videoüberwachung einsetzen möchte und die Schutzgüter Leben, Gesundheit oder Freiheit in solchen Anlagen betroffen sein können, wird durch die Formulierung „gilt als...ein besonders wichtiges Interesse“ die Abwägungsentscheidung zugunsten der Zulässigkeit des Einsatzes einer Videoüberwachungsmaßnahme geprägt.

Insofern können die Betreiber solcher Anlagen, Einrichtungen und Fahrzeuge in ihrem eigenen Interesse einen Beitrag zur Sicherheit der aufhältigen Personen leisten, der auch im öffentlichen Interesse liegt.

Damit stehen der Polizei und Staatsanwaltschaft verstärkt effektive Übersichts-, Aufklärungs- und Ermittlungsmöglichkeiten zur Verfügung, gerade wenn es darum geht, unmittelbar reagieren zu können. Die bestehenden polizeirechtlichen Rechtsgrundlagen, die einen Zugriff auf die von nicht-öffentlichen Stellen erhobenen Videoaufzeichnungen ermöglichen (z.B. § 21 Absatz 3 Satz 2 und § 47 Bundespolizeigesetz bzw. die entsprechenden Vorschriften der Strafprozessordnung), bleiben durch die (Neu-)Regelung unberührt. Entsprechendes gilt, soweit die Videoüberwachung in anderen Gesetzen spezieller geregelt ist (z.B. § 27 Bundespolizeigesetz).

Die aus dem grundgesetzlich abgesicherten Recht auf informationelle Selbstbestimmung herrührende Interessenabwägung nach § 6b Absatz 1 Satz 1 BDSG bleibt weiterhin notwendig. Die Abwägung hinsichtlich der Zulässigkeit von Videoüberwachungsanlagen ist nicht pauschal, sondern für jede Teilanlage in diesen öffentlich zugänglichen großflächigen Anlagen oder Einrichtungen und Fahrzeugen des öffentlichen Schienen-, Schiffs- und Busverkehrs, gesondert vorzunehmen.

Zu Nummer 2 (§ 6b Absatz 3)

Es handelt sich um eine Klarstellung. Bei der Verarbeitung und Nutzung der nach Absatz 1 Satz 1 Nummer 3 erho-

benen personenbezogenen Daten sollen dieselben Gewichtungsmaßstäbe des Absatzes 1 Satz 2 für die Abwägungsentscheidung gelten. Aus dem Beitrag, den private Betreiber für sicherheitsrelevante Belange leisten, folgt, dass die Gefahrenabwehr und Strafverfolgung im Grundsatz mit vom Erhebungszweck umfasst sein können. Diese Ausgangslage ist bei der Frage der Zulässigkeit der Übermittlung der Daten an Strafverfolgungsbehörden nach den einschlägigen datenschutzrechtlichen Vorschriften zu berücksichtigen.

Zu Artikel 2 (Inkrafttreten)

Das Inkrafttreten wird auf den frühestmöglichen Zeitpunkt gelegt.

Bitkom unterstützt Deklaration für Meinungsfreiheit

Breites Bündnis lehnt Gesetzentwurf gegen Hasskriminalität im Netz ab

Eine breite Allianz von Wirtschaftsverbänden, netzpolitischen Vereinen, Bürgerrechtsorganisationen und Rechtsexperten hat sich in einer gemeinsamen Erklärung gegen das geplante Netzwerkdurchsetzungsgesetz (NetzDG) gewandt, mit dem die Bundesregierung gegen Hassrede im Internet vorgehen will. In einer gemeinsamen „Deklaration für die Meinungsfreiheit" warnen die Unterzeichner vor „katastrophalen Folgen", sollte das NetzDG vom Bundestag verabschiedet werden. So zwinge die Androhung hoher Bußgelder in Verbindung mit allzu kurzen Reaktionsfristen die Plattformbetreiber, sich im Zweifel zu Lasten der Meinungsfreiheit und für die Löschung oder Sperrung von Inhalten zu entscheiden. Dies werde nicht nur jene typischen stupiden Hassreden betreffen, auf die das Gesetz abzielt. Ebenso könnten Meinungsäußerungen von Bürgerrechtlem und Veröffentlichungen von etablierten Medien in sozialen Netzwerken sowie von Vertretern der politischen Parteien von diesen Zwangslöschungen betroffen sein. Viele dieser Inhalte würden womöglich bei sorgfältiger Prüfung durch das grundgesetzlich garantierte Recht auf Meinungsfreiheit gedeckt sein. Die Politik sollte sich angesichts dieser breiten Kritik besinnen und das Gesetz in dieser Form nicht beschließen. Man müsse verstärkt gegen Hassrede und andere Straftaten im Netz vorgehen, aber nicht auf Kosten der Grundrechte und rechtsstaatlicher Verfahren."

Die Unterzeichner fordern im Kampf gegen „absichtliche Falschmeldungen, Hassrede und menschenfeindliche Hetze" eine „Kooperation von Staat, Zivilgesellschaft und der Anbieter". Ziel müsse eine „gesamtgesellschaftliche Lösung" sein, durch die „strafwürdiges Verhalten konsequent verfolgt" sowie „Gegenrede und Medienkompetenz gestärkt werden".

(Bitkom, Pressemitteilung vom 11.04.2017)

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen „abweichendes Verhalten" erkannt werden soll.[1]

Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.

Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwachungstechniken. Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen oder -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungs-

1 Siehe auch Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz".

vorgänge. Aufgrund des deutlich intensiveren Grundrechtseingriffs, der durch Videotechnik mit erweiterter Auswertung einhergeht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von KFZ-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von KFZ-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

Der europäische Gesetzgeber hat die enormen Risiken dieser Technik für die Privatsphäre erkannt und die Verarbeitung biometrischer Daten zur Identifizierung sowohl in der ab Mai 2018 wirksamen Datenschutz-Grundverordnung als auch in der bis Mai 2018 umzusetzenden Datenschutz-Richtlinie im Bereich Justiz und Inneres nur unter entsprechend engen Voraussetzungen für zulässig erachtet. Wird über den Einsatz dieser Technik nachgedacht, muss der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben, und es müssen angemessene und spezifische Regelungen zum Schutz der Grundrechte und -freiheiten der Betroffenen vorgesehen werden. Hierzu gehören u. a. eine normenklare Regelung für die Verwendung von Templates, z.B. von Personen im Fahndungsbestand, für den Anlass zum Abgleich des Templates mit den aufgenommenen Gesichtern sowie zum Verfahren zur Zulassung von technischen Systemen für den Einsatz.

Etwaige gesetzliche Regelungen müssten die vorgenannten verfassungs- und europarechtlichen Bedingungen beinhalten und den mit dieser Technik verbundenen erheblichen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger angemessen Rechnung tragen!

(Die Landesbeauftragte für den Datenschutz Niedersachsen)

Literaturhinweise

Philipp Byers, **Mitarbeiterkontrollen**, Beck-Verlag, München, 2016, 196 S., 49,00 €

Auch Mitarbeiter können ein Risikofaktor für den Betrieb sein.

Kontrollen am Arbeitsplatz sind daher, wenn auch in unterschiedlichen Umfang und ausgerichtet an dem Gefährdungspotential, unverzichtbar. Compliance, d.h. die Einhaltung der für das Unternehmen geltenden äußeren und inneren Vorgaben, bedeutet auch, deren Einhaltung unter Beachtung datenschutzrechtlicher Vorgaben sicherzustellen. Arbeitsrecht und Datenschutz sind in kompatiblen Einklang zu bringen. Dazu werden die nachstehenden Fallbereiche ausführlich erörtert:

- Überwachung betrieblicher Kommunikationsmittel
- Zeiterfassungs- und Zugangskontrollsysteme
- Videokontrollen
- Tor- und Taschenkontrollen
- Ortung von Mitarbeitern
- Gesundheits- und Eignungsuntersuchungen
- Kontrolle von Social-Media-Aktivitäten
- Background-Checks
- Terrorlisten
- Überwachung des Betriebsrats

Aufgezeigt werden die dabei bestehenden Mitbestimmungsrechte und die Folgen des Überschreitens der Kontrollbefugnisse. Zahlreiche Mustervereinbarungen und zusammenfassende „Praktische Hinweise" geben der Praxis Hilfestellung.

(Schriftleitung)

Utz Schliesky/Sönke E. Schulz/Friedrecht Gottberg/Florian Kuhlmann, **Demokratie im digitalen Zeitalter – DIVSI-Perspektiven,** hrsg. vom Deutschen Institut für Vertrauen und Sicherheit im Internet, Bd. 5, Nomos Verlag, Baden-Baden, 2016, 138 S., 36,00 €

Die Entscheidung von Wahlen durch digital verbreitete sog. Fake-News und die unverblümte Verbreitung solcher Informationen auch durch öffentliche Stellen stellt die Demokratie im digitalen Zeitalter vor ein Problem von manchen anderen. Die Schrift, die den Untertitel „Das Grundgesetz im digitalen Zeitalter" hat, versucht diesen nachzugehen. Sie enthält neben einem Leitwort von Roman Herzog Beiträge der vier genannten Autoren. Schliesky widmet sich dem Demokratieprinzip des Grundgesetzes; Schulz befasst sich mit Wahlen und Abstimmungen im digitalen Zeitalter, Kuhlmann geht der Rolle der Abgeordneten im digitalen Zeitalter nach, und Gottberg untersucht die diesbezügliche Rolle des Parlaments. Fasst man das Ergebnis zusammen, so können zwei Sätze aus den Schlusswort von Schulz zitiert werden: „Gerade die fehlende Ergebnisverantwortung und -sicherung sind es aber, die innovativen Partizipations-, Kommunikations- und Kollaborationsformen – zum Teil zu Recht – zum Vorwurf gemacht werden. Entwicklungen der vergangenen Jahre, in denen es Partikular- oder Individualinteressen gelungen ist – auch unter Rückgriff auf neue Technologien – Einfluss auf Politik und Gesetzgebung zu erhalten, zeigen dies. Bei aller Offenheit des demokratischen Prozesses (für Online-Partizipation, Mitwirkung über Twitter und andere Dienste, die elektronische Stimmabgabe, die Bereitschaft, Schwarmintelligenz anzuerkennen und als Ergänzung zur repräsentativen Demokratie zu sehen) muss die Gemeinwohlorientierung – und das Gemeinwohlethos – allen staatlichen Handelns gesichert bleiben." Aber auch gegenüber digitalen Äußerung des „Volkes" gilt: „Res publica ist Herrschaft für das Volk, nicht notwendigerweise durch das Volk." Der prinzipielle Unterschied zwischen dem wahren Willen des Volkes und der guten Sache des Volkes bleibt bestehen."

(Schriftleitung)

Matthias Damm, **Der Zugang zu staatlichen Geodaten als Element der Daseinsvorsorge**, Schriftenreihe der Deutschen Universität für Verwaltungswissenschaften Speyer, Band 232, Duncker & Humblot, Berlin, 2017, 455 S., 89,90 €

Das Recht digitaler Geodaten ist ein junges Phänomen, dessen Praxisrelevanz durch Panoramadienste, Navigationssysteme, Scoring und räumliche Vernetzung stetig zunimmt. Der Zugang zu und die Nutzung von raumbezogenen Daten ist aus dem modernen Leben nicht mehr wegzudenken; ihre Zurverfügungstellung bildet ein Element moderner Daseinsvorsorge. Die Arbeit leuchtet den völker-, unions- und verfassungsrechtlichen Hintergrund des Geodatenrechts aus und entwickelt ein Verständnis des Geodatenrechts als Querschnittsmaterie des Informations(verwaltungs)rechts, des Rechts geistigen Eigentums und des Datenschutzrechts. Dabei ist die rechtliche Dimension nur durch die Nutzung von Hilfswissenschaften der Jurisprudenz zu begreifen: Die Informationstheorie beschreibt den Gegenstand, das verwaltungswissenschaftliche Konzept des geoGovernment als Teil des eGovernment (und seit 2012 auch des Open Government) beschreibt die Einbindung in den Verwaltungsaufbau. Die ökonomische Analyse des Rechts hilft, die verschiedenen Konzepte von Verteilungsgerechtigkeit, welche hinter den unterschiedlichen Bundes- und Landesnormen stehen, zu begreifen und zu bewerten.

(Redaktion)

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.

Culik, Nicolai/Döpke, Christian, **Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data Anwendungen,** ZD 2015, S. 226
Der Beitrag analysiert, inwieweit der Zweckbindungsgrundsatz nach der DS-GVO noch als „scharfes Schwert" gegen einen unkontrollierten Einsatz von Big Data Anwendungen ist und kommt zu dem Ergebnis, dass viele Ausnahmen bestehen, insbesondere im Hinblick darauf, wie konkret der ursprüngliche Zweck festzulegen ist. Der DS-GVO gelinge nur bedingt die intendierte Annäherung an die digitale Realität und die Schaffung von klaren, zukunftsweisenden Regelungen für die Anwendungen von Big Data.

Hofmann, Johanna M./Johannes Paul C, **DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs,** ZD 2017, S. 221
Die nach Unionsrecht autonome und einheitliche Auslegung der DS-GVO führt zu dem Ergebnis, dass die Verordnung auf einen relativen Personenbezug abstellt. Da sich absolute Anonymität kaum noch herstellen lässt, sei ein relatives Element, abhängig von der Art der Anonymisierung und den Möglichkeiten des Verarbeiters, wie es § 3 Abs. 6 BDSG vorsieht, bei der Feststellung, ob Daten Personenbezug haben, unerlässlich.

Martini, Mario/Wenzel, Michael, **„Gelbe Karte" von der Aufsichtsbehörde: Die Verwarnung als datenschutzrechtliches Sanktionshybrid,** PinG 2017, S. 92
Der Beitrag untersucht inwieweit einem Umsetzungsdefizit mit der neuen Sanktionsform der Verwarnung wirksam begegnet werden kann.

Müller, Daniel, **Cloud Computing,** DuD 2017, S.371
Der Beitrag zeigt auf, dass der strafrechtliche Schutz der Datenvertraulichkeit vor potenziellen Insiderangriffen bislang nur unzureichend ist. Insoweit werfen vor allem Tathandlungen durch Administratoren der Cloudanbieter und der Cloudnutzer ungeklärte Rechtsfragen auf. Problematisch sei ferner, dass die Vorschriften ein erhebliches Vollzugsdefizit aufweisen und keine effektive Präventivwirkung entfalten.

Nolde, Malaika, **Sanktionen nach DSGVO und BDSG-neu: Wem droht was warum?,** PinG 2017, S. 114
Der Beitrag zeigt hinsichtlich der vorgesehenen ordnungs- und strafrechtlichen Sanktionen eine Reihe offener Fragen auf, mit denen sich die Unternehmen auseinanderzusetzen haben.

Pohl, Dirk, **Durchsetzungsdefizite der DSGVO?,** PinG 2017, S. 85
Nur basierend auf einem verständlichen Rechtsrahmen kann eine einheitliche Anwendung und effektive Durchsetzung der DS-GVO erfolgen. Wirksame Durchsetzungsmechanismen können jedoch bestehende materiell-rechtliche Schwächen bis zu einem gewissen Grad kompensieren.

Schwichtenberg, Simon, **„Doppeltes Netz" im Datenschutz? – Die Rolle der Verbraucherverbände unter der DS-GVO,** PinG 2017, S. 10
Bereits durch die Reform des UKlaG wurden den Verbraucherverbänden Kompetenzen bei der Durchsetzung datenschutzrechtlicher Vorgaben übertragen. Der Autor kommt zu dem Ergebnis, dass sich durch die DS-GVO die Rolle der Verbraucherverbände insoweit nicht grundlegend ändert.

Wolff, Heinrich Amadeus, **Verhaltensregelungen nach Art. 40 DS-GVO auf dem Prüfstand,** ZD 2017, S. 151
Die Datenschutzgrundverordnung hat die sog. Verhaltensregelungen als Instrument der Selbstregulierung übernommen ohne die Gründe, die bisher zu einer praktischen Bedeutungslosigkeit führten, wirklich zu beseitigen, wobei „ein Lichtblick" die Möglichkeit der Erklärung der allgemeinen Gültigkeit gem. Art. 40 Abs. 9 DS-GVO sei.

Aus den Anfängen der Emojis

Digitale Höhlenschrift

WhatsApp ohne Emojis sind für viele undenkbar. Sie können in Chats längere Begriffe ersetzen, um die Schrift zu ergänzen und Gefühle zu zeigen. Dass die Zeichen keine definierte Bedeutung haben, kann zu Verwirrung führen. Wer von seinem Partner eine Nachricht ohne, oder mit zu wenig, oder mit den falschen Küssen - nämlich ohne Herz - bekommt, der ist vielleicht verwirrt. Kuss vergessen, sauer, nachlässig oder auf dem Absprung? Was soll das alberne Winken bedeuten, wo sonst ein Kuss kommt? Heißt die von vorne gesehene Faust „Check“, also Zuspruch oder dass Gewalt droht?

Bildschrift ist keine Erfindung der Digitalisierung. Schon Hieroglyphen bestanden aus Bildern. Man konnte mit dieser vollständigen Schrift Mengen, Fakten und Gefühle präzise ausdrücken. Das geht mit Emojis, die ähnlich komplex sind wie steinzeitliche Höhlenmalereien nicht. Sie bereichern aber unsere Schrift um Bilder, die über Sprachgrenzen hinweg Gefühle zeigen. Es macht die Schriftsprache aber auch ärmer und phantasieloser, wenn man statt einem Liebesbrief nur noch Herzen schickt. Manchmal sollte man auf Emojis verzichten. Bei Facebook den Tod eines Menschen mit einem weinenden Smiley zu kommentieren, kann an Verniedlichung von Trauer empfunden werden. Wie macht man es denn richtig?

Wer sich über passende Emojis informieren will, der kann das auf der Internetseite Emojipedia. Dort werden verschiedene Deutungen erklärt. Die gefalteten Hände lassen danach vier Deutungen zu beten, „High Five“ oder im japanischen Kulturraum „Bitte“ oder „Danke“. Das Lachen mit Schweißtropfen ist der glückliche Schweiß-Emoji, der nach dem Training eingesetzt wird. Hochgehaltene Hände sind das „Arms in the Air Emoji“ und bedeuten Party. Das verrückte Emoji – knipsendes Auge mit ausgestreckter Zunge bedeutet „Ich bin gerade verrückt drauf, richtig crazy.“ Wichtig ist das Emoji mit den vor dem Gesicht verschränkten Armen. Es bedeutet „Nein, auf gar keinen Fall!“

DS-GVO: Wissen aus erster Hand.

Die neue Datenschutz-Grundverordnung (DS-GVO)

führt erstmals unmittelbar geltendes europäisches Datenschutzrecht für Unternehmen, Privatpersonen und die öffentliche Verwaltung ein. **Bei Nicht-Beachtung drohen Unternehmen, aber auch Vorständen und dem sonstigen Management erhebliche finanzielle Risiken und Bußgelder von bis zu 20 Mio EUR oder 4 % des globalen Konzernumsatzes des Unternehmens.** Dies zwingt zu einer weitgehenden Neuausrichtung der bisherigen Datenschutzkonzepte und zu einem grundlegenden rechtlichen Umdenken. Neu geregelt werden u.a.

- Recht auf Löschung (»Vergessenwerden«)
- Gestärkte Befugnisse der unabhängigen Aufsichtsbehörden
- Geldbußen
- Verbandsklagen
- Umgang mit Datenpannen
- Verzeichnis von Verarbeitungstätigkeiten
- Auftragsverarbeitung und Sicherheit der Verarbeitung
- Datenübermittlungen in Drittstaaten.

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.

Unverzichtbar

für interne und externe Datenschutzbeauftragte von Unternehmen und Behörden, Geschäftsführer europäisch ausgerichteter Unternehmen, Mitarbeitern in Rechtsabteilungen und Personalabteilungen, Marketingfachleute, Rechtsanwälte, Richter und Rechtswissenschaftler.

Ehmann/Selmayr
Datenschutz-Grundverordnung
2017. XXXVI, 1243 Seiten.
In Leinen € 139,–
ISBN 978-3-406-70215-0
Neu im Mai 2017

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

C.H.BECK

Datenschutz neu geregelt.

Haftungsrisiken vermeiden und jetzt handeln

Kühling/Buchner
DS-GVO
2017. XVI, 1169 Seiten.
In Leinen € 159,–
ISBN 978-3-406-70212-9
Neu im März 2017

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

Die neue DS-GVO

wird nach einer zweijährigen Übergangsfrist im Mai 2018 geltendes Recht. Sie behandelt den europaweit einheitlichen Schutz von Daten. Zugleich will sie den freien Datenverkehr in der Europäischen Union gewährleisten.

Der neue Kommentar

ist auf die Bedürfnisse von Praxis und Wissenschaft gleichermaßen zugeschnitten. Dogmatisch fundiert, aber stets auch den Rechtsanwender im Blick werden die Normen der Datenschutz-Grundverordnung und ihre Auswirkungen auf das nationale Recht stringent und mit Blick auf das Wesentliche dargestellt. Der zunehmenden Vernetzung und Digitalisierung der Wirtschaft wird dabei besonders Rechnung getragen. Für eine schnelle und verlässliche Orientierung sorgt ein hochkarätiges Herausgeber- und Autorenteam, bestehend aus Experten aus Praxis, Wissenschaft und Aufsichtsbehörden.

Eine wertvolle Hilfe für

Unternehmensjuristen, Rechtsanwälte, Richter, Datenschutzbeauftragte, Behördenmitarbeiter und Wissenschaftler.

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 167062

C.H.BECK