ISSN 0178-8930

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

1/2017

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
Februar 2017
Seiten 1–50

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

33. Jahrgang 2017
Heft 1
Seiten 1–50

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Beilagenhinweis GDD-Mitteilungen 1/2017; 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 1
Seiten 1–50

RDV
Recht der Datenverarbeitung

33. Jahrgang · Februar 2017 · Seiten 1–50

Editorial

Heimliche Überwachung von Beschäftigten – Regelungsbedarf im BDSG-neu

§ 32 Abs. 1 Satz 2 BDSG soll in § 26 Abs. 1 Satz 2 BDSG-neu fortgeführt werden (vgl. zum DS-AnpUG in diesem Heft S. 25). Danach soll der Arbeitgeber unter Beachtung des Verhältnismäßigkeitsgrundsatzes zur Überwachung von straftatverdächtigten Beschäftigten berechtigt bleiben. Ohne dass der Gesetzeswortlaut es deutlich macht, erfolgen entsprechende Überwachungsmaßnahmen – z.B. eine Videoinstellation oder die Beauftragung eines Detektivs – logischerweise hinter dem Rücken des Betroffenen. Die Heimlichkeit der Maßnahme ist vorgegeben. Der Erlaubnistatbestand setzt einen konkreten Straftatsverdacht voraus. Ob diese Vorschrift auch anzuwenden ist, wenn die Datenerhebung zur Aufklärung von Vertragspflichtverletzungen oder Ordnungswidrigkeiten erfolgen soll – mithin von Verhaltensweisen außerhalb des strafbaren Bereichs –, ist umstritten. In der Literatur wird teilweise auch eine entsprechende Anwendung des § 32 Abs. 1 Satz 2 BDSG, teilweise eine Anwendung von § 32 Abs. 1 Satz 1 BDSG befürwortet. Andere, wie nunmehr auch das LAG Baden Württemberg (in diesem Heft S. 37) sehen § 32 Abs. 1 S. 2 BDSG als eine abschließende Regelung an. Nach dieser Auffassung erlaubt § 32 Abs. 1 S. 2 BDSG aufgrund des eindeutigen Wortlauts eine heimliche Überwachung allein zur Aufdeckung von Straftaten. § 32 Abs. 1 Satz 1 BDSG erfasse demgegenüber nur solche Maßnahmen, die nicht gezielt auf die Entdeckung konkret Verdächtiger gerichtet sind und daher zwecks ihres Abschreckungseffekts offen zu erfolgen haben. Daraus folge, dass eine zielgerichtete verdeckte Aufklärung schwerer Vertragspflichtverletzungen und Ordnungswidrigkeiten im Beschäftigungsverhältnis datenschutzrechtlich de lege lata unzulässig sei. Das Gericht überlässt die endgültige Entscheidung dem BAG. Zu berücksichtigen haben wird das BAG dabei seine Entscheidung vom 21.04.2012 (RDV 2012, 297), in der es dem Arbeitgeber eine dem Wortlaut des § 9b Abs. 2 BDSG entgegenstehende heimliche Videoüberwachung als ultima ratio sowohl für den Fall des Verdachts einer Straftat als auch einer sonstigen schweren Verfehlung erlaubt und damit dem Gesetzgeber untersagt, dem Arbeitgeber eine diesbezügliche Kontrollbefugnis zu verweigern. Gleichermaßen hatte es auch einen Detektiveinsatz zwecks Überprüfung eines konkreten Verdachts unerlaubter Konkurrenztätigkeit als berechtigt angesehen und den Arbeitnehmer zur Erstattung der Detektivkosten verpflichtet (U.v. 28.10.2010, RDV 2011, 87), wobei der zu entschiedene Fall sich jedoch vor Inkrafttreten des § 32 BDSG abspielte.

Es sollte jedoch nicht dem BAG überlassen bleiben eine verfassungs- und DS-GVO-widrige Regelung durch entsprechende Interpretation zu korrigieren. Vielmehr bietet es sich zwingend an, diese Korrektur im Rahmen des § 24 Abs. 1 BDSG-neu vorzunehmen, wie es auch eine Reihe von Stellungnahmen zu dem Entwurf des DS-AnpUG anregen. Der DAV (Stellungnahme 84/16 zum DS-AnpUG: https://www.juris.de/jportal/portal/page/homerl.psml?nid=jnachr-JUNA16...) und der DIHK (http://www.dihk.de/themenfelder/recht-steuern/rechtspolitik/nationale-...) fordern dies u.a. deshalb zutreffend, weil nach Art. 6 lit. c oder Art. 6 lit. f DS-GVO eine derartige Datenverarbeitung zulässig wäre. Da schwerwiegende Pflichtverletzungen von Arbeitnehmern zu einer fristlosen Kündigung führen können, müssen diese bei Verdacht auch aufgeklärt werden dürfen.

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
06.03.2017	Dokumentation, Meldepflichten und IT-Sicherheitsmanagement nach DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
06.03.2017	Dokumentation, Meldepflichten und IT-Sicherheitsmanagement nach DS-GVO (2)	Berlin	GDD e.V. und DATAKONTEXT
07.03.2017	Auftragsverarbeitung nach DS-GVO – Grundlagen für den Übergang vom BDSG zur DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
07.03.2017	Auftragsverarbeitung nach DS-GVO – Grundlagen für den Übergang vom BDSG zur DS-GVO (3)	Berlin	GDD e.V. und DATAKONTEXT
14.03.2017	ISO 27001 und Datenschutz	Berlin	GDD e.V. und DATAKONTEXT
15.03.2017	Grundlagen der Auftragsverarbeitung (AV)	Köln	GDD e.V. und DATAKONTEXT
21.03.2017	IT-Sicherheit für Datenschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
22.03.2017	Einsatz mobiler Endgeräte: Datenschutz und IT-Sicherheit	Frankfurt/M.	GDD e.V. und DATAKONTEXT
23.03.2017	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Frankfurt/M.	GDD e.V. und DATAKONTEXT
23.03.2017	Fachtagung zur Datenschutz-Grundverordnung	Berlin	GDD e.V. und DATAKONTEXT
27.03.2017	Die Wahrnehmung der Überwachungsaufgaben des DSB gemäß DS-GVO (4)	Berlin	GDD e.V. und DATAKONTEXT
28.03.2017	Der Umsetzungsplan vom BDSG zur DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
28.03.2017	Der Umsetzungsplan vom BDSG zur DS-GVO (2)	Berlin	GDD e.V. und DATAKONTEXT
29.–30.03.2017	Intensiv-Workshop Bundesdatenschutzgesetz (BDSG) – aktuell datenschutzkonform handeln	Köln	GDD e.V. und DATAKONTEXT
03.–04.04.2017	Datenschutz Kompakt	Köln	GDD e.V. und DATAKONTEXT
03.–05.04.2017	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Köln	GDD e.V. und DATAKONTEXT
04.–06.04.2017	Das SAP-System für Datenschutzbeauftragte	Düsseldorf	GDD e.V. und DATAKONTEXT
10.04.2017	Datenschutz-Schwachstellen und die erheblichen Bußgeld-risiken nach der DS-GVO vermeiden	Köln	GDD e.V. und DATAKONTEXT
25.04.2017	SAP-Funktionen für den Datenschutz	Köln	GDD e.V. und DATAKONTEXT
24.–25.04.2017	Datenschutz-Management – Teil 3	Köln	GDD e.V. und DATAKONTEXT
25.04.2017	Ausgewählte Themen zur Implementierung der DS-GVO in die Unternehmensorganisation (5)	Berlin	GDD e.V. und DATAKONTEXT
27.04.2017	Datenschutz und Strafrecht – Beschäftigten- und Kundendaten in internen Ermittlungsverfahren und Strafverfolgungsmaß-nahmen	Köln	GDD e.V. und DATAKONTEXT
27.04.2017	Fachtagung zur Datenschutz-Grundverordnung	Frankfurt/M.	GDD e.V. und DATAKONTEXT
04.05.2017	Fachtagung zur Datenschutz-Grundverordnung	München	GDD e.V. und DATAKONTEXT

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

Aufsätze

Univ.-Prof. Dr. Jürgen Taeger

Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018

Die hoch komplexen Regelungen des nationalen allgemeinen Datenschutzrechts werden von der EU-Datenschutzgrundverordnung (DS-GVO) ab dem 25. Mai 2018 abgelöst. Die 2009 in das Bundesdatenschutzgesetz aufgenommenen Vorschriften zu den Voraussetzungen der Übermittlung personenbezogener Daten an Wirtschaftsauskunfteien (§ 28a BDSG), zur Berechnung eines Wahrscheinlichkeitswertes über die künftige Erfüllung von Leistungspflichten (Scoring, § 28b BDSG) sowie zu den erweiterten Auskunftspflichten der Auskunfteien (§ 34 Abs. 2 und 4 BDSG) finden sich in der DS-GVO nicht ausdrücklich wieder. Zwangsläufig stellt sich die Frage, auf Grund welcher Erlaubnisnorm und mit welchem Regelungsinhalt das Scoring durch Wirtschaftsauskunfteien künftig zulässig sein wird.

I. Verbot der automatisierten Entscheidung im Einzelfall gemäß Art. 22 Abs. 1 DS-GVO ab 25. Mai 2018

Ab dem 25. Mai 2018 wird die EU-DS-GVO mit Anwendungsvorrang auch vor dem BDSG gelten (Art. 288 AEUV). Das BDSG wird in der jetzt geltenden Fassung nicht mehr anzuwenden sein. Bis dahin soll ein Anpassungs- oder Überleitungsgesetz als Artikelgesetz, das mit Art. 1 ein neues Bundesdatenschutzgesetz (BDSG neu) einführt, verabschiedet werden. Es soll die bis dahin vorzunehmenden *Regelungsaufträge* umsetzen und die aufgrund von Öffnungsklauseln bestehenden *Regelungsoptionen* wahrnehmen. Das Anpassungsgesetz darf dabei kein gegenüber der Datenschutzgrundverordnung höheres Schutzniveau zu bestimmten, in der DS-GVO enthaltenen Regelungen enthalten, soweit eine Öffnungsklausel dies nicht ausdrücklich vorsieht (Art. 6 Abs. 2 und 3 DS-GVO).

Vor diesem Hintergrund stellt sich die Frage der Auslegung und Anwendung des Art. 22 DS-GVO. Die Norm enthält in seinem Absatz 1 ein Recht der Betroffenen, „nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt." Die Vorschrift enthält damit ausdrücklich ein Verbot der *automatisierten Einzelentscheidung*. Es ist nach dem Wortlaut als ein „Recht" des Betroffenen ausgestaltet, der bei Zuwiderhandlung einen Unterlassungsanspruch gegenüber dem Verantwortlichen (Art. 4 Ziff. 7 DS-GVO) hat. Im Art. 22 Abs. 2 DS-GVO werden Ausnahmen normiert, bei denen dieses Recht nicht greift.

II. Anknüpfung an das Verbot der ausschließlich auf automatisierter Verarbeitung personenbezogener Daten gestützten Entscheidung gem. § 6a BDSG

Die Vorschrift des Art. 22 DS-GVO knüpft an Art. 15 EG-Datenschutzrichtlinie an, der mit § 6a BDSG umgesetzt wurde. Nach § 6a BDSG dürfen „Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, … nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen". Die starke Orientierung des Wortlauts an Art. 15 EG-DSRl bzw. § 6a BDSG wird in dieser Hinsicht kaum zu Problemen bei der Anwendung der Vorschrift im Fall automatisierter Entscheidungen im Einzelfall führen.

Mit dem Texteinschub „einschließlich Profiling" sowohl in der Normüberschrift des Art. 22 DS-GVO als auch im Normtext stellt sich die Frage nach dem Regelungsinhalt dieses Zusatzes. Es ist unklar, was den Verordnungsgeber veranlasst haben mag, das ‚Profiling' als eine Beispielanwendung der automatisierten Verarbeitung in dieser Weise hervorzuheben, weil das Profiling ausschließlich in einen Kontext mit der automatisierten Entscheidung im Einzelfall gebracht wurde. Nach der Definition in Art. 4 Ziff. 4 DS-GVO ist unter Profiling „jede Art der automatisierten Verarbeitung personenbezogener Daten [zu verstehen], die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässig-

keit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen." Damit fällt das Scoring, insbesondere das Kreditscoring, unter den Begriff des Profiling[1].

Diese Definition bezieht sich generell auf jedes Profiling, wie man es auch vom Direktmarketing oder vom Kreditscoring kennt und geht damit über die in Art. 22 DS-GVO geregelte Anwendung bei einer (automatisierten) Entscheidungsfindung hinaus. Ansonsten kommt der Verordnungsgeber auf das Profiling nur noch im Zusammenhang mit der Regelung der Betroffenenrechte zurück. So muss der Verantwortliche im Fall eines jeden Profiling die Informationspflicht bei einer Erhebung von personenbezogenen Daten bei der betroffenen Person für Zwecke der automatisierten Entscheidungsfindung [Art. 13 Abs. 2 lit. f) DS-GVO] und bei der Erhebung zum gleichen Zweck bei einer anderen Person oder auf andere Weise (Art. 14 Abs. 2 lit. g) DS-GVO) sowie dem Auskunftsanspruch des Betroffenen (Art. 15 Abs. 1 lit. h) DS-GVO) beachten.

Außerdem findet sich in der Datenschutzgrundverordnung in Art. 21 Abs. 1 Satz 1 DS-GVO ein Widerspruchsrecht, wenn die Datenverarbeitung – einschließlich eines Profiling – auf Art. 6 Abs. 1 lit. f) DS-GVO gestützt wird. Nach diesem Erlaubnistatbestand darf eine Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erfolgen, wenn sie erforderlich ist. Im Falle eines Widerspruchs muss der Verantwortliche gem. Art. 21 Abs. 1 S. 2 DS-GVO nachweisen, dass zwingende schutzwürdige Gründe vorliegen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Und schließlich hat der Betroffene ein Recht, im Fall der personalisierten Werbung dem Profiling zu widersprechen, wenn dieses mit der Direktwerbung in Verbindung steht (Art. 21 Abs. 2 DS-GVO).

Schließlich ist der Verantwortliche, der ein Profiling für Zwecke der automatisierten Entscheidungsfindung gem. Art. 22 Abs. 1 und 2 DS-GVO vornimmt, zu einer Datenschutzfolgenabschätzung gem. Art. 35 Abs. 3 lit. a DS-GVO verpflichtet. Art. 47 Abs. 2 lit. e DS-GVO sieht vor, dass in den Fällen, in denen sich der Verantwortliche bei einer Verarbeitung in einem Drittstaat auf verbindliche interne Datenschutzvorschriften als geeigneter Garantie gem. Art. 46 Abs. 1 DS-GVO stützen will, auch die beim Profiling zu beachtenden Rechte des Betroffenen mit berücksichtigt (Art. 48 Abs. 2 lit. e) DS-GVO).

Das alles zeigt, dass das Profiling als solches nicht ausdrücklich Gegenstand einer Verbots- bzw. Erlaubnisnorm der DS-GVO ist, sondern nur als eine Verarbeitungsform bei der automatisierten Entscheidungsfindung nach Art. 22 DS-GVO Erwähnung findet. Scoring ist ansonsten nur Gegenstand von Regelungen über Anforderungen an die Datenverarbeitung oder über Rechte der Betroffenen. Es findet sich in der DS-GVO kein spezifischer Erlaubnistatbestand für das Scoring über den Anwendungsfall der automatisierten Entscheidungsfindung (internes Scoring) hinaus.

Hieraus folgt die Anschlussfrage, ob sich die bisher in § 28b BDSG geregelten Anforderungen an das ‚Scoring', dem ein Profiling im Sinne des Art. 4 Ziff. 4 DS-GVO zu Grunde liegt,

a) aus einer entsprechend auszulegenden allgemeinen Erlaubnisnorm in Art. 6 Abs. 1 lit. b, e oder f DS-GVO oder gar aus einer weit zu interpretierenden Anwendung des Art. 22 DS-GVO wiederfinden,
b) anderenfalls aufgrund einer Öffnungsklausel in einem Anpassungsgesetz datenschutzrechtlich vom nationalen Gesetzgeber geregelt werden dürfen, oder, wenn dies nicht der Fall ist,
c) Gegenstand einer künftigen nationalen *verbraucherrechtlichen* Regulierung sein könnten.

III. Regulierung des Scoring de lege lata in § 28b BDSG aus datenschutz- und verbraucherschutzrechtlichen Motiven

Vor einer Auseinandersetzung mit den vorgenannten Fragen ist an die Bedeutung der Wahrscheinlichkeitsberechnung für die betroffenen Verbraucher und für solche Unternehmen, die kreditorische Risiken eingehen, zu erinnern und auf das hohe Datenschutzniveau der derzeitigen Regulierung des Scoring hinzuweisen. Der deutsche Gesetzgeber regelte mit der sog. BDSG-Novelle I von 2009 nach einer längeren kontroversen Diskussion über das Kreditscoring durch Wirtschaftsauskunfteien die Voraussetzungen für eine Übermittlung personenbezogener Daten an Wirtschaftsauskunfteien in § 28a BDSG, die Anforderungen an ein datenschutzkonformes Scoring in § 28b BDSG und die Auskunftsrechte über Wahrscheinlichkeitswerte und ihre Berechnung in § 34 Abs. 2 und 4 BDSG[2].

Damit brachte der Gesetzgeber zum Ausdruck, dass die Berechnung von auf der Grundlage wissenschaftlicher Verfahren gebildeter Wahrscheinlichkeitswerte bezüglich eines bestimmten zukünftigen Verhaltens, namentlich die Erfüllung vertraglicher Leistungspflichten, zur Risikoabschätzung grundsätzlich zulässig ist. Diese spezifische Regulierung stellte Rechtssicherheit beim Scoring her. Es wurden Rahmenbedingungen geschaffen, die sowohl die Wirtschaft vor Kreditausfällen schützen, als auch unzulässige Eingriffe in die Persönlichkeitsrechte der Betroffenen verhindern.

Vor Abschluss von Darlehensverträgen oder von Verträgen mit Finanzierungshilfen prüfen Unternehmen wie Kreditinstitute, Handels- und Telekommunikationsunternehmen in der Regel die Bonität ihrer künftigen Kunden[3]. Auch die Rechtsprechung[4] und die Literatur[5] erkennen an, dass die

1 Ebenso Moos/Rothkegel, ZD 2016, 561 (567).

2 Vgl. Taeger, Datenübermittlung an Auskunfteien und das Scoring, in: Taeger/Rose (Hrsg.) Rechtliche Rahmenbedingungen für das Scoring in Deutschland und in weiteren ausgewählten Staaten, K&R Beihefter 4/2014, S. 2.

3 Siehe Taeger, ebenda, und Born, ZD 2015, 66.

4 EuGH, NJW 2014, 1941; EuGH, ZD 2015, 175 ; EuGH, DuD 2007, 136 = EuZW 2006, 753 m. Anm. Stappert/Esser-Wellie; BGH, NJW 2011, 2204, Rn. 21; KG Berlin, ZD 2013, 189.

5 Piltz/Holländer, ZRP 2008, 143 (144); Hofmann, NJW 2010, 1782; Schröder/Lang/Lerbs/Radev, Ökonomische Bedeutung und Funktionsweise von Credit Scoring, in: Schröder/Taeger (Hrsg.), Scoring im Fokus: Ökonomische Bedeutung und rechtliche Rahmenbedingungen im internationalen Vergleich, 2014, S. 8.

Prüfung der Kreditwürdigkeit von Kunden aus volks- und betriebswirtschaftlichen Erwägungen unabdingbar ist.

Nach § 505a Abs. 1 BGB haben Darlehensgeber vor dem Abschluss eines Verbraucherdarlehensvertrags sogar die verbraucherschützende Pflicht, die Kreditwürdigkeit des Darlehensnehmers zu prüfen[6]. Der Darlehensgeber darf nach Absatz 2 den Verbraucherdarlehensvertrag nur abschließen, wenn sich aus der Kreditwürdigkeitsprüfung ergibt, dass bei einem Allgemein-Verbraucherdarlehensvertrag keine erheblichen Zweifel daran bestehen, dass der Darlehensnehmer seinen aus dem Darlehensvertrag folgenden Verpflichtungen vertragsgemäß nachkommen wird. Zur Erfüllung der Überprüfungspflicht können die Darlehensgeber Auskünfte beim Betroffenen einholen oder sich einen Score mit einer statistischen Aussage über die Kreditwürdigkeit von einer Wirtschaftsauskunftei übermitteln lassen (§ 505b BGB). Das Scoring durch Wirtschaftsauskunfteien wird vom Gesetzgeber hiermit ausdrücklich als eine Möglichkeit angesehen, die Pflicht zur Prüfung der Kreditwürdigkeit zu erfüllen. § 505b Abs. 5 BGB betont ausdrücklich, dass dadurch die Bestimmungen zum Schutz personenbezogener Daten, also insbesondere §§ 28a und 28b BDSG, unberührt bleiben. Das unterstreicht die Brisanz der Frage, was an hohem datenschutzrechtlichem Standard bleibt, wenn aufgrund des Anwendungsvorrangs der DS-GVO diese speziellen strengen Datenschutzregelungen zum Scoring und zur Übermittlung der in die Wahrscheinlichkeitsberechnung einfließenden Daten 2018 wegfielen.

Ähnlich wie §§ 505a, 505b BGB enthält auch § 18a Abs. 1 Satz 1 KWG, mit dem die Verbraucherkredit-RL umgesetzt wurde, eine verbraucherschützende Pflicht von Kreditinstituten, vor Abschluss eines Verbraucherdarlehensvertrags die Kreditwürdigkeit des Darlehensnehmers zu prüfen. Das Kreditinstitut darf nach Absatz 2 den Verbraucherdarlehensvertrag nur abschließen, wenn aus der Kreditwürdigkeitsprüfung hervorgeht, dass bei einem Allgemein-Verbraucherdarlehensvertrag keine erheblichen Zweifel an der Kreditwürdigkeit bestehen. Absatz 3 sieht vor, dass Grundlage für die Kreditwürdigkeitsprüfung „Auskünfte des Darlehensnehmers und erforderlichenfalls Auskünfte von Stellen sein [können], die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zwecke der Übermittlung erheben, speichern, verändern oder nutzen". Nach § 18a Abs. 9 KWG bleiben die Vorschriften zum Schutz personenbezogener Daten unberührt.

Zudem verweist die aufsichtsrechtliche Regelung des § 10 Abs. 2 KWG darauf, dass die Anforderungen an die Eigenkapitalausstattung von Kreditinstituten eine Berechnung von Adressausfallrisiken erforderlich machen können, wobei die zu erhebenden und zu berücksichtigenden Daten von Auskunfteien stammen können.

Danach ist erkennbar, dass aus Gründen des Verbraucherschutzes und der Vermeidung von Ausfallrisiken für solche Unternehmen, die kreditorische Risiken eingehen, die Berechnung von Wahrscheinlichkeitswerten über die Erfüllung von Leistungspflichten, also das Scoring, unverzichtbar ist. Das hilft diesen Unternehmen, der Volkswirtschaft und letztlich den Kunden, die von niedrigen Preisen aufgrund der Vermeidung von Zahlungsausfällen profitieren[7].

Mit der Erlaubnis zum Scoring korrespondiert seit 2009 mit den genannten §§ 28a, 28b und 34 Abs. 2 BDSG ein sehr weitgehender Schutz der Persönlichkeitsrechte der vom Scoring Betroffenen. Es ist nachvollziehbar, dass der Wunsch besteht, dieses Niveau auch über Mai 2018 hinaus zu erhalten und keine ‚Liberalisierung der Wahrscheinlichkeitsberechnung' beispielsweise zugunsten der auf Big Data-Analysen spezialisierten FinTech-Unternehmen zuzulassen, denen der deutsche Markt aufgrund des hohen Datenschutzniveaus (noch) versperrt ist.

IV. Verbot des Scoring als Anwendungsbeispiel des Profiling gemäß Art. 22 Abs. 1 DS-GVO mit Vorbehalt der Erlaubnis nach Art. 22 Abs. 2 DS-GVO

Es wird in der Literatur erwogen, Art. 22 DS-GVO nicht nur auf die automatisierte Entscheidungsfindung anzuwenden, sondern auch auf das der Entscheidung vorgelagerte und nicht unmittelbar zu einer automatisierten *Entscheidung* führende (externe) Scoring. Anlass für eine derartige Überlegung könnte Erwägungsgrund 71 geben. Dort heißt es in Absatz 1 Satz 2, dass „zu einer derartigen [automatisierten] Verarbeitung auch das „Profiling" [zählt], das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt".

Weiter heißt es im Erwägungsgrund 71 in dem an § 28b BDSG erinnernden Absatz 2: „Um unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten, sollte der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und

6 Dazu Buck-Heeb, NJW 2016, 2065.

7 Vgl. dazu Taeger, Datenschutz bei Direktmarketing und Bonitätsprüfung, in: Brunner/Seeger/Turturica (Hrsg.), Fremdfinanzierung von Gebrauchsgütern, 2010, S. 53.

mit denen verhindert wird, dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu Maßnahmen kommt, die eine solche Wirkung haben. Automatisierte Entscheidungsfindung und Profiling auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollten nur unter bestimmten Bedingungen erlaubt sein."

Dies interpretiert *Piltz* so, dass Erwägungsgrund 71 deutlich mache, „dass nicht unbedingt erst eine finale Entscheidung vorliegen muss, sondern bereits ‚eine Maßnahme' ausreichen kann"[8], um Art. 22 Abs. 1 und 2 DS-GVO als Erlaubnistatbestand auch für das externe Scoring heranzuziehen.

Härting ist der Ansicht, dass bereits „die Datenanalyse, die beim ‚Profiling' vorgenommen wird, als eine ‚automatisierte Entscheidung im Einzelfall [anzusehen ist], auf die Art. 22 DSGVO anzuwenden ist"[9], und führt aus, dass in Verbindung mit dem Erwägungsgrund 71 „Art. 22 DS-GVO … somit beispielsweise auf das Scoring (‚Online-Kreditantrag') … anwendbar" ist. Das ist so für das externe Scoring sicher nicht richtig. An anderer Stelle[10] weist *Härting* allerdings selbst darauf hin, dass der nationale Gesetzgeber eine dem § 28b BDSG entsprechende Vorschrift erst noch schaffen müsse, wozu dieser aufgrund der Öffnungsklausel, die er in Art. 22 Abs. 2 lit b DS-GVO sieht, befugt sei.

Tatsächlich erhellt Erwägungsgrund 71 also nicht, dass er bei der Auslegung des Art. 22 DS-GVO dahingehend zu berücksichtigen wäre, dass auch das nicht zu einer automatisierten Entscheidung führende Scoring von der Erlaubnisnorm des Art. 22 Abs. 2 i.V.m Abs. 1 DS-GVO mit umfasst ist. Aus dem Gesamtzusammenhang ergibt sich eher, dass sich die Erlaubnis eines Scorings aus Art. 6 DS-GVO ergibt und der Verantwortliche diese im Erwägungsgrund 71 formulierten Grundsätze bei seiner nach Art. 6 DS-GVO vorzunehmenden Abwägung zu berücksichtigen hat. Im Übrigen mag ErwG 71 auch Anknüpfungspunkt für die Ausarbeitung von Leitlinien des nach Art. 68 Abs. 1 DS-GVO einzurichtenden Europäischen Datenschutzausschusses sein. Dieser hat gem. Art. 70 Abs. 1 lit. f DS-GVO auch die Aufgabe, Leitlinien, Empfehlungen und bewährte Verfahren zur näheren Bestimmung der Kriterien und Bedingungen für die auf Profiling beruhenden Entscheidungen gemäß Art. 22 Abs. 2 DS-GVO bereitzustellen. Erwägungsgrund 72 formuliert diese Empfehlung ausdrücklich.

Weil durch die Vornahme einer Wahrscheinlichkeitsberechnung allein noch niemand einer „Entscheidung unterworfen" wird, führt das externe Scoring durch die Auskunftei, die den Entscheidern einen die Entscheidung nicht vorwegnehmenden Wahrscheinlichkeitswert liefert, nicht zu einer automatisierten Einzelfallentscheidung. Der zu übermittelnde Score fließt erst beim Empfänger in dessen (ggf. automatisierten) Entscheidungsfindungsprozess ein.

Das räumten auch die Berichterstatter im LIBE-Ausschuss des EU-Parlaments *Albrecht* und *Lotzo* ein, die bestätigen, dass der EU-Gesetzgeber für ‚Profiling' (noch) keine eigenständige Rechtsgrundlage beschließen wollte, die über den Kontext mit der automatisierten Entscheidungsfindung hinausgeht, sondern dass primär ein „Anknüpfungspunkt" für die nachfolgenden Debatten über dieses wichtige Zukunftsthema geschaffen werden sollte[11].

Festgehalten werden kann folglich, dass von Art. 22 DS-GVO nur das sogenannte *interne* Scoring, bei dem der Darlehensgeber eine Wahrscheinlichkeitsberechnung selbst mit eigenen Daten durchführt, in die ein Score einer Wirtschaftsauskunftei eingeflossen sein mag, erfasst wird. Nur muss diese Berechnung auch unmittelbar zu einer Entscheidung geführt haben, die dem Betroffenen gegenüber eine rechtliche Wirkung entfaltet oder ihn in ähnlicher Weise erheblich beeinträchtigt. Eine die Entscheidung nur vorbereitende Berechnung eines Scores ist deshalb nach ganz herrschender Ansicht nicht von der Regelung des Art. 22 DS-GVO erfasst[12].

Aus Art. 22 Abs. 1 DS-GVO lässt sich also ein mit Ausnahmen versehenes Verbot des Scoring nicht ableiten, wenn dieses nicht – wie bei einem internen Scoring – automatisiert zu einer Entscheidung führt[13]. Eine andere Auslegung würde Art. 22 DS-GVO zu sehr strapazieren und wäre nicht europarechtskonform.

Danach wäre die Rechtmäßigkeit des Kreditscoring allein anhand der §§ 5 ff., insbesondere des Art. 6 Abs. 1 lit. f DS-GVO zu bestimmen, wenn nicht der bundesdeutsche Gesetzgeber eine Öffnungsklausel zur Regulierung des Scoring nutzen könnte. Während einerseits vertreten wird, dass sich eine solche Öffnungsklausel für die Beibehaltung einer den §§ 28a, 28b, 34 Abs. 2 und 4 BDSG entsprechenden Regelung nicht finden lasse und dies dem Willen des europäischen Gesetzgebers, hierfür keine speziellen Anforderungen zu formulieren, entspräche[14], werden in der Literatur verschiedene Denkmodelle durchgespielt, nach denen sich eine spezifische nationale Regelung rechtfertigen ließe.

V. Art. 22 Abs. 2 lit. b DS-GVO als Öffnungsklausel zur Regelung des Scoring in einem nationalen Anpassungsgesetz

Es wird als erwägenswert angesehen, in Art. 22 Abs. 2 lit. b DS-GVO eine Öffnungsklausel zu sehen, die es dem nationalen Gesetzgeber, beispielsweise eines deutschen Anpas-

8 Piltz, K&R 2016, S. 629 (635). Bei Gola/Jaspers/Müthlein/Schwartmann, Datenschutz-Grundverordnung im Überblick, 2016, heißt es: „In der DS-GVO werden in Art. 22 die bisherigen Themen zu automatisierten Einzelentscheidungen (§ 6a BDSG) und zum Scoring (§ 28b BDSG) gemeinsam behandelt."

9 Datenschutzgrundverordnung, 2016, Rn. 610, 617.

10 Datenschutzgrundverordnung, 2016, Rn. 641.

11 Albrecht/Lotzo, Das neue Datenschutzrecht der EU, 2016, S. 60.

12 Vgl. auch Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016.

13 Ebenso Kühling et al., Die Datenschutzgrundverordnung und das nationale Recht, 2016, S. 440 ff.

14 Moos/Rothkegel, ZD 2016, S. 561 (568); Pahl/Pauly-Martini, DS-GVO, 2016, Art. 22 Rn. 24.

sungsgesetzes, ermöglicht, das Profiling und damit auch das Scoring im Sinne des § 28b BDSG zu erhalten. *Härting* hat darauf aufmerksam gemacht[15]. Wenn von der Öffnungsklausel des Art. 22 Abs. 2 lit. b DS-GVO die Berechnung eines Wahrscheinlichkeitswertes adressiert ist, könnte auch das Scoring inkludiert sein[16]. Danach dürfe das Scoring durch das Recht eines Mitgliedstaates zugelassen sein oder werden, wenn diese Rechtsvorschriften geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten. Weil diese Bedingungen gerade durch den § 28b BDSG geregelt wurden, könne auch § 28b BDSG in ein Anpassungsgesetz aufgenommen werden. Auch *Richter* ist der Auffassung, dass § 28b BDSG „über die Öffnungsklausel des Art. 22 Abs. 2 lit. b DS-GVO weiter Anwendung finden" könne[17].

Kamlah[18] weist dagegen zutreffend darauf hin, dass sich diese Öffnungsklausel lediglich auf die [automatisierte] Entscheidungsfindung nach Abs. 1 und nicht auf die davon losgelöste Regelung des Scoring bezieht. Auch *Kühling* et al.[19] sehen in der Öffnungsklausel des Art. 22 Abs. 2 lit. b DS-GVO lediglich eine Option der Mitgliedstaaten, „vom Verbot einer *automatisierten Generierung von Einzelentscheidungen* Ausnahmen vorzusehen, wenn geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorgesehen sind". Danach ist eher zu verneinen, dass sich aus Art. 22 Abs. 2 lit. b DS-GVO eine Öffnungsklausel ergibt, die es dem nationalen Gesetzgeber ermöglicht, den hohen Datenschutzstandard des das Scoring regelnden § 28b BDSG in ein Anpassungsgesetz zu überführen.

VI. Art. 6 Abs. 1 lit. f DS-GVO als Öffnungsklausel zur Regelung des Scoring in einem nationalen Anpassungsgesetz

Kühling et al.[20] prüfen, ob sich nicht aus Art. 6 Abs. 1 lit. f DS-GVO ein Regelungsspielraum ergeben könnte. Sie lehnen dies jedoch mit dem Hinweis darauf ab, dass der Art. 6 Abs. 1 lit. f DS-GVO anders als Art. 6 Abs. 1 lit. c und lit. e DS-GVO keine Möglichkeit vorsieht, dass man „spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung beibehalten oder einführen" könne. *Martini*[21] stellt entsprechend lapidar fest, dass generell „für § 28b BDSG grds. kein nationaler Handlungsspielraum mehr verbleibt".

VII. Art. 6 Abs. 4 i.V.m. Art. 23 Abs. 1 DS-GVO als Öffnungsklausel zur Regelung des Scoring in einem nationalen Anpassungsgesetz

Das Bundesministerium des Innern (BMI) hatte am 5.8.2016 einen ersten (inoffiziellen) Referentenentwurf für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) vorgelegt. Mit dem nach diesem Entwurf geplanten Gesetz sollten die sich aus der DS-GVO ergebenden Regelungspflichten und Regelungsoptionen aufgegriffen werden. Art. 1 DSAnpUG-EU sah ein ‚Allgemeines Bundesdatenschutzgesetz (ABDSG)" vor. § 39 ABDSG-E enthielt eine Vorschrift zum Scoring, die die wesentlichen Regelungen des § 28b BDSG aufrechterhält. Auch eine dem § 28a BDSG entsprechende Vorschrift zur Übermittlung von Daten an Wirtschaftsauskunfteien wurde mit § 38 ABDSG-E aufgenommen. Die Gesetzesbegründung nannte eine in der Diskussion bis dahin – soweit ersichtlich – noch nicht erwähnte Öffnungsklausel, aus der sich die Befugnis des deutschen Gesetzgebers zur Regelung des Scoring ergeben soll. Danach folge eine „mitgliedstaatliche Regelungsbefugnis … aus der Zusammenschau der Artikel 6 Absatz 4 und Artikel 23 Absatz 1 Verordnung (EU) 2016/679." Dafür sei Voraussetzung, „dass die nationale Vorschrift eine „in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt". Art. 23 Abs. 1 lit. e DS-GVO nenne hierzu den „Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses". Die Rechtsprechung des *BGH*[22] habe anerkannt, dass „die Erteilung von Bonitätsauskünften für das Funktionieren der Wirtschaft von erheblicher Bedeutung ist". Verbraucher würden dadurch vor Überschuldung geschützt, was sowohl im Interesse der Verbraucher als auch der Wirtschaft liegen würde.

Der Entwurf hob hervor, dass „die Ermittlung der Kreditwürdigkeit und die Erteilung von Bonitätsauskünften … das Fundament des deutschen Kreditwesens und damit auch der Funktionsfähigkeit der Wirtschaft" bilden würden. Das erforderliche wichtige Ziel von allgemeinem öffentlichem Interesse sei damit gegeben.

Damit greift die Begründung Erwägungen auf, die bereits im Gesetzgebungsverfahren zur Einführung des § 509 BGB a.F. (heute: § 505a BGB) angestellt wurden und nach denen eine Pflicht zur Prüfung der Kreditwürdigkeit im öffentlichen Interesse bestehe.[23] Bei der Umsetzung der Verbraucherkreditrichtlinie[24] wurde wiederholt, dass die geforderte Kreditwürdigkeitsprüfung neben dem Schutz des individuellen Verbrauchers auch dem öffentlichen Interesse diene.

In einer öffentlich gemachten Stellungnahme vom 31.8.2016[25] begrüßte das Bundesministerium der Justiz und für Verbraucherschutz (BMJV), dass das „BMI die in §§ 28a,

15 Härting, Datenschutzgrundverordnung, 2016, Rn. 641.

16 Siehe auch Taeger, ZRP 2016, S. 72 (74 f.).

17 Roßnagel-Richter (Hrsg.), Europäische Datenschutz-Grundverordnung, 2016, § 4 Rn. 116. Siehe auch Voßhoff, BT-Ausschuss Digitale Agenda, Drs. 18(24)93, S. 5.

18 Plath-Kamlah, BDSG/DS-GVO, Rn. 9 zu Art. 22 DS-GVO.

19 Die Datenschutzgrundverordnung und das nationale Recht, 2016, S. 441 f.

20 Die Datenschutzgrundverordnung und das nationale Recht, 2016, S. 441 f.

21 Pahl/Pauly-Martini, DS-GVO, 2016, Art. 22 Rn. 24.

22 NJW 2011, 2204.

23 BT-Drs. 16/11643, S. 95 f.

24 Gesetz zur Umsetzung der Wohnimmobilienkreditrichtlinie v. 11.3.2016, BGBl. I S. 396.

25 Https://netzpolitik.org/wp-upload/2016/09/BMJV_Stellungnahme_DSAnpUG_ EU.pdf.

28b BDSG enthaltenen Regelungen fortführen möchte“. Bei diesen Regelungen handele es sich allerdings „nicht um originär datenschutzrechtliche, sondern Regelungen des wirtschaftlichen Verbraucherschutzes“. § 28b BDSG bezwecke mit seinen qualitativen Anforderungen an das Scoring, „Diskriminierungseffekte und daraus resultierende wirtschaftliche Nachteile für die Verbraucherinnen und Verbraucher zu vermeiden“. Die Stellungnahme widerspricht auch der Annahme einer sich aus Art. 23 Abs. 1 lit e DS-GVO ergebenden Öffnungsklausel zur Regelung des Scoring, weil die Tätigkeit von Auskunfteien nicht im „allgemeinen öffentlichen Interesse“ liege.

Trotz der Verneinung einer Öffnungsklausel setzt sich die Stellungnahme des BMJV inhaltlich mit § 39 ABDSG-E auseinander und unterbreitet Änderungsvorschläge. Es wird im BMJV offenbar nicht ausgeschlossen, dass § 39 ABDSG-E – aufgrund welcher Öffnungsklausel auch immer – das Gesetzgebungsverfahren erfolgreich passieren könnte.

Auf der Linie des BMJV liegen auch *Ehrig/Glatzner*[26], die die Vorschriften im BDSG zur Datenübermittlung an Auskunfteien sowie zum Scoring im Kern ihres Regelungsinhalts nicht als Datenschutzregelungen, sondern als solche des Verbraucherschutzes ansehen, die den Verbraucher vor wirtschaftlichen Nachteilen und Diskriminierung schützen sollen. Sie schlagen deshalb vor, die Vorschriften zum Scoring in andere Gesetze aus dem Zivil-, Vertrags- und Versicherungsrecht oder dem Kreditwesengesetz zu überführen. Auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit *Voßhoff* empfiehlt in ihrer Stellungnahme zum Referentenentwurf[27], von einer Regelung in einem ABDSG abzusehen. Wörtlich heißt es: „Im Ergebnis erscheint die vorgeschlagene partielle Übernahme der §§ 28a, 28b BDSG nicht als Ideallösung. BfDI hält es für notwendig, angesichts der sehr fragwürdigen Regelungsbefugnis und der inhaltlichen Defizite entweder auf spezifische Regelungen derzeit zu verzichten oder eine datenschutzrechtlich zufriedenstellende Lösung unter Berücksichtigung der Erfahrungen der Aufsichtsbehörden zu finden.“

Inzwischen liegt mit Datum vom 23.11.2016 ein überarbeiteter Referentenentwurf vor[28], zu dem die Verbände bis zum 7.12.2016 Stellung nehmen konnten. Ziel ist, den Entwurf im Januar 2017 vom Bundeskabinett beschließen zu lassen und danach zeitnah zu verabschieden. Im Anschluss daran sollen die weiteren bereichsspezifischen Datenschutzvorschriften angepasst werden, um rechtzeitig vor Mai 2018 die Anpassung an die DS-GVO abgeschlossen zu haben. Dieser nun nicht mehr als ‚ABDSG‘ sondern wie bisher als BDSG (neu) bezeichnete Entwurf zeigt sich von der Kritik an der Aufnahme einer den §§ 28a, 28b, 34 BDSG entsprechenden Regelung und an der Legitimation durch die erwähnte Öffnungsklausel unbeeindruckt und verfolgt die Regulierung des Scoring in einem nationalen Anpassungsgesetz mit den nun in den §§ 27, 28 BDSG-E zu findenden Vorschriften weiter. Die Gesetzesbegründung sieht die mitgliedstaatliche Regelungsbefugnis in einer Zusammenschau der Art. 6 Abs. 4 und Art. 23 Abs. 1 DS-GVO. Die Aufnahme der §§ 27, 28 BDSG-E regele die Datenverarbeitung beim Scoring, das dem Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses eines Mitgliedstaats diene.

VIII. Schlussfolgerungen und Perspektiven

Gelangt dieser Referentenentwurf so in das Kabinett, müssen in der weiteren Beratung allerdings handwerkliche und inhaltliche Korrekturen erfolgen. So sollte es in § 27 Abs. 2 BDSG-E wegen der Verlagerung des Zahlungsverkehrsrechts vom Kreditwesengesetz (KWG) in das Zahlungsdiensteaufsichtsgesetz (ZAG) nicht mehr „Kreditinstitute“ sondern „Kreditinstitute, Finanzdienstleistungsunternehmen und Zahlungsinstitute“ heißen. Außerdem läuft in § 27 Abs. 2 BDSG-E der Verweis auf § 1 Abs. 1 S. 2 Nr. 9 KWG leer, so dass als Tatbestandsmerkmal statt „betreffend ein Bankgeschäft nach § 1 Absatz 1 Satz 2 Nummer 2, 8 oder Nummer 9 des Kreditwesengesetzes“ besser „betreffend ein Geschäft mit finanziellem Ausfallrisiko“ formuliert werden sollte.

Zumindest in der Gesetzesbegründung, besser im Normtext selbst, sollte wie bei der BDSG-Novelle I von 2009 darauf hingewiesen werden, dass diese Regelung nicht abschließend ist, sondern die genannten Finanzdienstleistungsunternehmen auf der Grundlage einer Einwilligung, die nach der DS-GVO nur unter höheren Anforderungen wirksam ist, auch andere Daten übermitteln können. Außerdem gehen nicht nur Finanzdienstleister kreditorische Risiken ein, sondern auch andere in Vorleistung tretende Branchen. Es empfiehlt sich daher, auch andere Unternehmen wie beispielsweise Telekommunikationsunternehmen, Versicherungen und Handelsunternehmen aufzunehmen, denen Datenübermittlungen auf der Grundlage von Einwilligungen erlaubt werden müssen. Daher sollte in § 27 Abs. 1 BDSG-E klarstellend auch das Wort ‚nur‘ gestrichen werden (Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist *nur* zulässig, soweit…“).

§ 27 Abs. 2 Satz 3 BDSG-E kann keinen Bestand mehr haben, weil es in § 35 Abs. 2 Zahlungskontengesetz (ZKG)[29] heißt, dass ein Verpflichteter berechtigt ist, vor Abschluss eines Basiskontovertrags nachzuprüfen, ob der Berechtigte bereits Inhaber eines Zahlungskontos ist, und dass der Verpflichtete sich dabei auch an eine Stelle wenden darf, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit herangezogen werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder ändert. Dementsprechend ist das Verbot der Übermittlung in § 27 Abs. 2 S. 3 BDSG-E zu streichen, weil die Auskunfteien ansonsten der von § 35 ZKG geforderten Verpflichtung nicht nachkommen könnten.

26 PinG 2016, S. 211 (214).

27 Stellungnahme der BfDI vom 31.08.2016 zum Entwurf eines Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU-DSAnpUG-EU, https://netzpolitik.org//wp-upload/2016/09/BfDI_Stellungnahme_DSAnpUG_EU.pdf.

28 Https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/12/161123_BDSG-neu-RefE_-2.-Ressortab-Verbaende-Laender.pdf.

29 ZKG v. 11.04.2016 (BGBl. I S. 720).

§ 27 Abs. 2 S. 4 BDSG-E sollte so formuliert werden, dass die Anfragen nicht für die Bildung eines Scorewertes verwendet, aber vom Angefragten für die Dokumentation der Anfrage gespeichert werden dürfen.

Ob die herangezogene Öffnungsklausel auch eine spezielle Pflicht zur Löschung legitimiert (§ 27 Abs. 4 BDSG-E), ist sehr fraglich. Die DS-GVO kennt solche Löschfristen nicht mehr und sieht auch nicht vor, dass die Mitgliedstaaten solche einführen dürfen. Die großen Wirtschaftsauskunfteien haben darauf reagiert und in einem Code of Conduct die Löschungsfristen des § 35 BDSG übernommen, um sich entsprechend selbstverpflichtend daran zu binden.

IX. Ausblick

Die sehr divergenten Auslegungen des Art. 22 DS-GVO in Verbindung mit Erwägungsgrund 71 und die Suche nach einer Öffnungsklausel offenbaren zweierlei:

1. *Politik und Wissenschaft sind sich einig in dem Ziel, auch unter der Geltung der DS-GVO das Kredit-Scoring an die Rechtssicherheit bietenden datenschutz- und verbraucherrechtlichen Voraussetzungen zu knüpfen, wie sie derzeit noch in § 28b BDSG in Verbindung mit den §§ 28a und 34 BDSG bestehen.*
2. *Die verschiedenen Interpretationen des Art. 22 DS-GVO und die unterschiedlichen Auslegungen der DS-GVO zur Begründung einer Öffnungsklausel stellen dem europäischen Gesetzgeber ein schlechtes Zeugnis aus, weil er es nicht vermochte, eine rechtssichere einheitliche europäische Regulierung des Scoring vorzunehmen. Die Definition des Profiling in Art. 4 Nr. 4 DS-GVO und die Formulierung von Erwartungen in Erwägungsgrund 71 finden jedenfalls keinen Anknüpfungspunkt in Art. 22 DS-GVO, soweit durch Profiling bzw. Scoring keine automatisierte Entscheidung im Einzelfall erfolgt.*

Die weitere Rechtsentwicklung ist kaum abschätzbar. Folgende Alternativen sind denkbar:

1. *Das Scoring wird in einem nationalen Anpassungsgesetz nicht geregelt, so dass als Erlaubnistatbestand der Art. 6 Abs. 1 lit. f DS-GVO heranzuziehen ist, wobei bei der vorzunehmenden Abwägung Erwägungsgrund 71 zu berücksichtigen wäre. Der Europäische Datenschutzausschuss könnte auf dieser Grundlage konkretisierende Leitlinien formulieren, die EU-weit zu berücksichtigen wären. Für dieses Szenario spräche, dass dem Ziel der Harmonisierung Rechnung getragen würde, allerdings zu Lasten des in Deutschland erreichten hohen Niveaus an Rechtssicherheit sowie des Daten- und Verbraucherschutzes und des Schutzes der kreditgebenden Wirtschaft.*
2. *Der nationale Gesetzgeber könnte – wie perspektivisch auch die übrigen EU-Mitglieder – die Anforderungen an die Übermittlung von personenbezogenen Daten an Wirtschaftsauskunfteien und an das Scoring außerhalb des Datenschutzrechts in einem verbraucherschützenden Gesetz aufnehmen. Eine solche Lösung ist unsicher, käme spät und könnte zu Konflikten bei der Auslegung des Art. 6 Abs. 1 lit. f DS-GVO führen.*
3. *Das Scoring wird im BDSG neu geregelt, wie es im Referentenentwurf mit den §§ 27, 28 BDSG-E vorgesehen ist. Eine Öffnungsklausel ergibt sich nach der Begründung des Entwurfs aus der Zusammenschau der Art. 6 Abs. 4 und Art. 23 Abs. 1 der DS-GVO.*

Bei einer Abwägung der möglichen Szenarien erscheint das letztgenannte den richtigen Weg zu weisen, obwohl das Ziel der Vollharmonisierung bezüglich des Scoring dann aktuell nicht zu erreichen wäre. Aber die Vollharmonisierung hat der zu Kompromissen gezwungene Europäische Gesetzgeber schon bei Beschluss der DS-GVO aufgegeben, als er Öffnungsklauseln in großer Zahl schaffen musste.

Univ.-Prof. Dr. Jürgen Taeger
ist Direktor des Instituts für Rechtswissenschaften an der Carl von Ossietzky Universität Oldenburg. Er hat dort den Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht sowie Rechtsinformatik inne und leitet den berufsbegleitenden weiterbildenden Studiengang ‚Informationsrecht LL.M.'. Er ist Vorsitzender der Deutschen Stiftung für Recht und Informatik (DSRI).

Carolyn Eichler

Zulässigkeit der Tätigkeit von Auskunfteien nach der DS-GVO*

Bei Auskunfteien handelt es sich um ein etabliertes Geschäftsmodell nach der derzeitigen Rechtslage. In vielen Vorschriften des Bundesdatenschutzgesetzes (BDSG) werden Auskunfteien explizit erwähnt. Die einzelnen Datenverarbeitungsschritte sind in den §§ 28a ff. BDSG ausdifferenziert geregelt. Die Europäische Datenschutz-Grundverordnung (DS-GVO) dagegen erwähnt das Geschäftsmodell nicht[1], sondern arbeitet mit Generalklauseln. Diese werfen viele Fragen auf. Der folgende Beitrag soll daher einen ersten Überblick über die Zulässigkeit der Tätigkeit von Kreditauskunfteien unter der DS-GVO bieten.

I. Rechtslage unter dem BDSG

Unter Auskunfteien werden im Allgemeinen Unternehmen verstanden, die unabhängig vom Vorliegen einer konkreten Anfrage geschäftsmäßig bonitätsrelevante Daten über Unternehmen oder Privatpersonen sammeln, um sie bei Bedarf Geschäftspartnern für die Beurteilung der Kreditwürdigkeit der Betroffenen gegen Entgelt zugänglich zu machen.[2] Ihnen wird aufgrund des anonymer werdenden Geschäftsverkehrs eine zentrale Funktion zum Schutz potentieller Kreditgeber vor zahlungsunfähigen oder -unwilligen Schuldnern zugesprochen.[3] Das BDSG sieht ausdrückliche Regelungen für das Geschäftsmodell der Auskunfteien vor.[4] Eine zentrale Norm stellt § 29 BDSG dar. Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung ist zulässig, insbesondere wenn es der Tätigkeit von Auskunfteien oder dem Adresshandel dient, sofern die Erlaubnistatbestände des § 29 Abs. 1 BDSG[5] erfüllt sind. Die Zulässigkeit von Datenübermittlungen durch Auskunfteien richtet sich nach § 29 Abs. 2 BDSG.

Unter den in § 28a Abs. 1 BDSG genannten Voraussetzungen ist die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien zulässig. Gem. § 28a Abs. 2 BDSG dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft an Auskunfteien übermitteln. § 28a Abs. 3 BDSG statuiert eine Nachberichtspflicht sowohl an als auch durch die Auskunftei.

Scoring ist eines der Kernprodukte von Auskunfteien[6] neben dem Eigenscoring etwa durch Kreditinstitute selbst. Im Rahmen der BDSG-Novelle 2009 wurde mit § 28b BDSG eine explizite Regelung für die Erhebung und Verwendung von Wahrscheinlichkeitswerten geschaffen.

Die §§ 33-35 BDSG enthalten auskunfteispezifische Betroffenenrechte. So besteht nach § 33 Abs. 1 Satz 2 BDSG eine spezielle Regelung der Benachrichtigungspflicht für Auskunfteien. § 34 BDSG sieht in Abs. 1 Satz 3 und Abs. 3 auskunfteispezifische Auskunftspflichten vor. § 34 Abs. 4 BDSG betrifft ausdifferenzierte Auskunftspflichten zu Scorewerten. Außerdem bestehen nach § 35 Abs. 2 Satz 2 Nr. 4 BDSG für Auskunfteien spezielle Prüf- und Löschpflichten.

II. Rechtslage unter der DS-GVO

Die DS-GVO sieht ein nicht annähernd so detailliertes Regelungssystem zu Auskunfteien vor. Dass Auskunfteien in der DS-GVO nicht erwähnt werden, bedeutet aber wohl nicht, dass das Geschäftsmodell von vornherein unzulässig sein soll. Vielmehr sieht die DS-GVO generell keine branchenspezifischen Regelungen vor. Im Folgenden sollen die Zulässigkeit von Bonitätsabfragen und Scoring sowie Informations- und Auskunftspflichten von Auskunfteien betrachtet werden.

1. Bonitätsabfragen

1.1 Rechtsgrundlage für die Abfragen durch Vertragspartner der Auskunfteien

Unternehmen führen vorvertragliche Bonitätsprüfungen beispielsweise durch, wenn sie mit einem Vertragsabschluss ein kreditorisches Risiko eingehen. Aber auch zur Prüfung der Erfolgsaussichten von Vollstreckungsmaßnahmen werden Bonitätsdaten bei Auskunfteien abgefragt. Bisher kam als Rechtsgrundlage für Abfragen § 28 Abs. 1 Satz 1 Nr. 2 BDSG[7] in Betracht. Künftig wird Art. 6 Abs. 1 lit. f) DS-GVO zu prüfen sein. Grundsätzlich kommt bei vorvertraglichen Bonitätsprüfungen zwar auch Art. 6 Abs. 1 lit. b) DS-GVO als Rechtsgrundlage in Betracht.[8] Dies kann jedoch höchstens Fällen vorbehalten sein, in denen Bonitätsprüfungen zur Zweckbestimmung des Vertrages oder des vorvertraglichen Verhältnisses gehören, wie etwa bei Abschluss eines Kreditvertrages.

Grundsätzlich ist somit für Bonitätsabfragen bei Auskunfteien eine Interessenabwägung nach Art. 6 Abs. 1 lit. f)

* Aufsatz zum Vortrag im Rahmen des 35. RDV-Forums am 16.11.2016 in Köln.

1 Gola, in: Gola, DS-GVO Einl. Rn. 39.

2 Ehmann, in: Simitis, BDSG § 29 Rn. 83 f.

3 BT-Drs. 16/10529, S. 9.

4 Daneben erwähnt auch § 38 Abs. 1 Nr. 2 Gewerbeordnung Auskunfteien.

5 Buchner, in: BeckOK DatenSR, BDSG § 29 Rn. 49.

6 Schulz, in: Gola, DS-GVO Art. 6 Rn.133.

7 Zur Auslegung des § 28 BDSG: Gola/Schomerus/Körffer/Klug, BDSG § 28 Rn. 19.

8 Schulz, in: Gola, DS-GVO Art. 6 Rn. 37.

DS-GVO durchzuführen. Die Abfrage muss zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich sein und die Interessen der betroffenen Person dürfen nicht überwiegen. Gem. Erwägungsgrund 47 der DS-GVO sind hierbei die vernünftigen Erwartungen der betroffenen Person, die auf der Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Ein berechtigtes Interesse kann vorliegen, wenn die betroffene Person ein Kunde des Verantwortlichen ist. Bei der Abwägung soll geprüft werden, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftiger Weise absehen kann, dass möglicherweise eine Verarbeitung zu diesem Zweck erfolgen wird. Konkrete Anhaltspunkte[9] dafür, dass ein der Verarbeitung entgegenstehendes schutzwürdiges Interesse besteht, werden gerade nicht gefordert. Ob jedes wirtschaftliche Interesse, wie etwa die Steigerung der Kundenzufriedenheit[10], Bonitätsabfragen rechtfertigen kann, ist fraglich. Dies wäre für betroffene Personen vernünftiger Weise jedenfalls nicht absehbar. Das Interesse, kreditorische Risiken vor Abschluss eines entsprechenden Vertrages mit Hilfe von Bonitätsinformationen einzuschätzen, ist dagegen berechtigt i.S.v. Art. 6 Abs. 1 lit. f) DS-GVO.

1.2 Rechtsgrundlage für die Übermittlung durch Auskunfteien

Bisher kam als Rechtsgrundlage für die Übermittlung von Bonitätsdaten durch Auskunfteien § 29 Abs. 2 BDSG in Betracht. Zukünftig wird wie bei den Abfragen durch die Vertragspartner auch Art. 6 Abs. 1 lit. f) DS-GVO zu prüfen sein.[11] Es ist also im Rahmen einer Interessenabwägung zu prüfen, ob eine Erforderlichkeit zur Wahrung berechtigter Interessen eines Dritten besteht und Interessen der betroffenen Person überwiegen. Gem. Erwägungsgrund 47 sind die vernünftigen Erwartungen der betroffenen Person zu berücksichtigen. Fraglich ist, ob die kontextfremde Erteilung von Auskünften den vernünftigen Erwartungen der betroffenen Person entspricht. So dürften betroffene Personen etwa davon ausgehen, dass Informationen zu Mietforderungen nur in diesem Kontext Aussagekraft erlangen und daher ausschließlich auf entsprechende Anfragen bei Abschluss eines Mietvertrages beauskunftet werden. Hierfür spricht auch, dass die Begleichung von Forderungen mit existenziellen Auswirkungen wie Mietschulden eine höhere Priorität bei Schuldnern erhalten wird als beispielsweise das Begleichen der Telefonrechnung. Die derzeit existierenden branchenübergreifenden Auskunfteisysteme, die etwa Forderungen aus Telekommunikationsverträgen auch auf Anfragen von Vermietern beauskunften, könnten somit auf der Grundlage des Art. 6 Abs. 1 lit. f) DS-GVO nicht zu rechtfertigen sein.

Es besteht keine Regelung dazu, wie der Nachweis des berechtigten Interesses gegenüber der Auskunftei zu führen ist. Verantwortliche müssen allerdings gem. Art. 5 Abs. 2 DS-GVO die Rechtmäßigkeit der Verarbeitungen nachweisen können. Eine Privilegierung in Form eines Stichprobenverfahrens für automatisierte Abrufverfahren wie bisher in § 29 Abs. 2 Satz 4 und 5 BDSG enthält die DS-GVO nicht. Soll auch zukünftig in den Massenverfahren der Auskunfteien auf den Nachweis eines berechtigten Interesses durch den Abfragenden in jedem Einzelfall verzichtet werden, müssen entsprechend kompensierende technische und organisatorische Schutzmaßnahmen eingerichtet werden. Dazu zählt insbesondere die Beschränkung auf einen potentiell berechtigten Empfängerkreis, die geeignete Dokumentation der glaubhaft dargelegten Abfragegründe, die stichprobenartige Überprüfung[12] der Berechtigung der Abfragen in einem angemessenen Umfang und der Ausschluss von Verantwortlichen von dem vereinfachten Verfahren, die ohne berechtigtes Interesse Abfragen getätigt haben. Die Dokumentation dieser Maßnahmen dient auch dem Nachweis gegenüber der Aufsichtsbehörde.

2. Scoring

Mit der BDSG-Novelle 2009 wurde eine ausdrückliche Regelung zu Scoring in § 28b BDSG geschaffen.[13] Die Regelung betrifft die Errechnung eines Wahrscheinlichkeitswertes für ein bestimmtes zukünftiges Verhalten zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen. Die DS-GVO enthält in Art. 4 Nr. 4 eine Definition zu Profiling. Darunter soll jede Art der automatisierten Datenverarbeitung zur Analyse und Vorhersage persönlicher Aspekte zu verstehen sein, was auch auf die bekannten Scoringverfahren zutrifft. Art. 4 Nr. 4 DS-GVO stellt aber keine Rechtsgrundlage für entsprechende Datenverarbeitungen dar. Auch Art. 22 DS-GVO enthält keinen Erlaubnistatbestand[14], sondern sieht vergleichbar mit dem bisherigen § 6a BDSG[15] Rahmenbedingungen für automatisierte Entscheidungen einschließlich Profiling vor.

2.1 Rechtsgrundlage für Scoreberechnungen

Eine mögliche Rechtsgrundlage für Scoringverfahren stellt Art. 6 Abs. 1 lit. f) DS-GVO dar. Es ist eine eigenständige Interessenabwägung durchzuführen, welche unabhängig von der Prüfung der Zulässigkeit der Verarbeitung der Datengrundlage zu erfolgen hat. Die zulässige Speicherung von Daten impliziert noch nicht deren zulässige Verwendung für Scoringzwecke. So kann etwa das Speichern der Voranschrift einer Person für eine Auskunftei zu Identifizierungszwecken zulässig sein. Das heißt jedoch nicht, dass das Datum zulässigerweise in ein Bonitätsscoring einbezogen werden darf.[16]

9 A.A. Schulz, in: Gola, DS-GVO Art. 6 Rn. 138.

10 Schulz, in: Gola, DS-GVO Art. 6 Rn. 135.

11 Zum Fehlen einer den §§ 28 und 29 BDSG vergleichbaren Differenzierung zwischen Datenverarbeitungen für eigene Geschäftszwecke und solchen, die geschäftsmäßig zum Zwecke der Übermittlung erfolgen: Schulz, in: Gola, DS-GVO Art. 6 Rn. 59.

12 Schulz, in: Gola, DS-GVO Art. 6 Rn. 136.

13 Zu der Frage, ob die Vorschriften im BDSG zum Scoring erhalten bleiben können: Taeger, ZRP 2016, 72.

14 Schulz, in: Gola, DS-GVO Art. 22 Rn. 3.

15 Martini, in: Paal/Pauly, DS-GVO Art. 22 Rn. 42.

16 Schulz, in: Gola, DS-GVO Art. 6 Rn. 132.

2.2 Maßnahmen zur Gewährleistung einer fairen und transparenten Verarbeitung

Gem. Erwägungsgrund 71 ist insbesondere eine faire und transparente Verarbeitung zu gewährleisten. Entsprechend muss die Informationsqualität in Hinblick auf den Einsatz von Scoreverfahren in der Zukunft generell verbessert werden. Vielen Verbraucherinnen und Verbrauchern sind die Berechnungsverfahren unbekannt.[17] Der Grundsatz der Transparenz bezieht sich gem. Erwägungsgrund 58 allerdings auch auf Informationen für die Öffentlichkeit.

Wie bereits unter § 28b Nr. 1 BDSG sind nur geeignete mathematische und statistische Verfahren für das Scoring einzusetzen. Des Weiteren sind technische und organisatorische Maßnahmen zu treffen, um insbesondere das Risiko von Fehlern zu minimieren.[18] Die Berechnungsverfahren, die Zuverlässigkeit ihrer Datenquellen sowie die Aussagekraft der Ergebnisse sind demnach ständig zu überwachen. Voraussetzung hierfür ist, dass die Verfahren beherrschbar und kontrollierbar sind.

Neu ist zudem die Regelung besonderer Datenschutzmaßnahmen[19] für automatisierte Entscheidungen bei Vertragsbeziehungen und aufgrund einer Einwilligung in Art. 22 Abs. 3 DS-GVO. Es besteht das Recht auf Eingreifen durch eine Person, Darlegung des eigenen Standpunktes und Anfechtung der Entscheidung. Gem. Erwägungsgrund 71 hat als logische Voraussetzung für die Wahrnehmung dieser Rechte eine spezifische Unterrichtung der betroffenen Person zu erfolgen. Diese Maßnahmen zur Wahrung der Interessen der betroffenen Personen sind auch nicht deshalb unbeachtlich, weil Auskunfteien in der Regel nicht selbst rechtswirksame oder ähnliche Entscheidungen gegenüber den betroffenen Personen treffen. Die Schutzmaßnahmen sind jedenfalls zu gewährleisten, wenn an der Vorbereitung entsprechender Entscheidungen mitgewirkt wird. Für die Kriterien und Bedingungen der auf Profiling basierenden Entscheidungen wird der Europäische Datenschutzausschuss gem. Art. 70 Abs. 1 S. 2 lit. f) DS-GVO Leitlinien, Empfehlungen und bewährte Verfahren bereitstellen.

3. Betroffenenrechte

3.1 Informationspflichten der Auskunfteien

Da Auskunfteien eine Fremderhebung vornehmen, sind die Informationspflichten des Art. 14 zu beachten.[20] Gem. Art. 12 Abs. 1 DS-GVO sind die Informationen in präziser, transparenter, verständlicher, leicht zugänglicher Form sowie in klarer und einfacher Sprache[21] bereitzustellen. Die aktuell verwendeten Informationsschreiben nach § 33 BDSG sind anzupassen.[22] Die Informationen können gem. Art. 12 Abs. 1 DS-GVO auch in elektronischer Form erteilt werden. Gem. Art. 12 Abs. 7 DS-GVO dürfen Bildsymbole[23] verwendet werden, um einen aussagekräftigen Überblick über die Verarbeitung zu vermitteln.

Hinsichtlich des Zeitpunkts der Informationserteilung haben Auskunfteien Art. 14 Abs. 3 lit. c) DS-GVO zu beachten. Die Informationen nach Art. 14 Abs. 1 und 2 DS-GVO sind spätestens zum Zeitpunkt der ersten Offenlegung an einen Empfänger zu erteilen. Ausnahmen von der Informationspflicht sind in Art. 14 Abs. 5 DS-GVO geregelt. Ein unverhältnismäßiger Aufwand[24] gem. Art. 14 Abs. 5 lit. b) DS-GVO kann in der Regel für Auskunfteien nicht angenommen werden. Denn das Geschäftsmodell besteht gerade in der geschäftsmäßigen Datenverarbeitung und verlangt aufgrund der Fremderhebung eine nur restriktive Einschränkung der Transparenzmaßnahmen. Soll die Informationspflicht von Dritten erfüllt werden, um sich auf den Ausnahmetatbestand des Art. 14 Abs. 5 lit. a) DS-GVO zu berufen, trägt der Verantwortliche das Risiko.[25] Der Bußgeldtatbestand des Art. 83 Abs. 5 lit. b) DS-GVO spricht für eine besonders sorgfältige Erfüllung der Informationspflichten sowie der übrigen Betroffenenrechte.

3.2 Auskunftsrechte

Das Auskunftsrecht der betroffenen Person ist nun in Art. 15 DS-GVO geregelt. Neu ist eine Fristenregelung in Art. 12 Abs. 3 DS-GVO. Danach muss unverzüglich, in jedem Fall innerhalb eines Monats, auf den Auskunftsantrag reagiert werden. Eine Verlängerung der Frist ist in komplexen Fällen zwar möglich. Selbst dann ist die betroffene Person aber innerhalb eines Monats über die Gründe der Verzögerung zu unterrichten. Generell haben Verantwortliche somit ein geeignetes Verfahren einzurichten, um Anträge innerhalb der vorgegebenen Fristen bearbeiten zu können. Dies betrifft gem. Art. 12 Abs. 4 DS-GVO auch Fälle, in denen der Verantwortliche gar nicht tätig werden will. Für Auskunfteien stellen diese Vorgaben eine gesteigerte Herausforderung dar, da sie erfahrungsgemäß in größerem Umfang von Auskunftsersuchen betroffen sind. Auskünfte sind dabei gem. Art. 12 Abs. 5 DS-GVO grundsätzlich unentgeltlich zu erteilen. Neu ist eine Regelung zu „offenkundig unbegründeten oder exzessiven Anträgen“, wobei den Verantwortlichen diesbezüglich eine Nachweispflicht trifft. Gem. Erwägungsgrund 63 soll das Auskunftsrecht in angemessenen Abständen wahrgenommen werden können, was für einen Fortbestand der mindestens einmal jährlich kostenlos erteilten Auskunft[26] spricht.

Schwierigkeiten können für eine Auskunftei bestehen, die Auskunft auf elektronischem Weg zuverlässig an den Berechtigten[27] zu erteilen. Dieser Weg soll gem. Art. 12 Abs. 3 Satz 4 DS-GVO „nach Möglichkeit“ genutzt werden, wenn

17 Https://www.bundesregierung.de/Content/DE/Artikel/2015/05/2015-05-06-scoring-transparenz-verbraucher.html.

18 Erwägungsgrund 71.

19 Martini, in: Paal/Pauly, DS-GVO Art. 22 Rn. 39.

20 Schulz, in: Gola, DS-GVO Art. 6 Rn. 133.

21 Paal, in: Paal/Pauly, DS-GVO Art. 12 Rn. 33.

22 Franck, in: Gola, DS-GVO Art. 12 Rn.12.

23 Zu Vorschlägen des Parlamentsentwurfs der DS-GVO, die sich im Abstimmungsprozess nicht durchsetzen konnten: Franck, in: Gola, DS-GVO Art. 12 Rn. 47.

24 Franck, in: Gola, DS-GVO Art. 14 Rn. 23.

25 Piltz, K&R 2016, 629, 630.

26 Bisher § 34 Abs. 8 BDSG.

27 Piltz, K&R 2016, 629.

auch der Antrag elektronisch gestellt wurde. Kann aber etwa eine E-Mailadresse, unter der ein Auskunftsanspruch geltend gemacht wurde, nicht sicher als diejenige der berechtigten Person verifiziert werden, sollte eine Auskunft postalisch an die im Datenbestand der Auskunftei gespeicherte Anschrift gesendet werden. Gleiches gilt für den Kopieherausgabeanspruch gem. Art. 15 Abs. 3 DS-GVO. Im Übrigen kann der Verantwortliche bei Zweifeln an der Identität der auskunftsersuchenden Person gem. Art. 12 Abs. 6 DS-GVO zur Identifizierung erforderliche Informationen zusätzlich anfordern.

Inhaltlich umfasst der Anspruch gem. Art. 15 Abs. 1 DS-GVO die Auskunft, ob personenbezogene Daten zur betroffenen Person verarbeitet werden und wenn ja, welche. In diesem Fall sind zusätzlich die katalogartig aufgezählten Informationen zu erteilen. Neu sind hier die Information über die geplante Speicherdauer oder die Kriterien für deren Festlegung sowie die Information über Betroffenenrechte, insbesondere das Beschwerderecht bei der Aufsichtsbehörde. Zum Bestehen automatisierter Entscheidungsfindungen einschließlich Profiling sind aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen zu erteilen. Dies ist keinesfalls ein Weniger gegenüber der bisherigen Auskunftsregelung des § 34 Abs. 4 BDSG. Vielmehr spricht der Transparenzgrundsatz gem. Art. 5 Abs. 1 lit. a) DS-GVO für eine weite Auslegung des Art. 15 Abs. 1 lit. h) DS-GVO, die von Geschäftsgeheimnissen[28] der Auskunftei beschränkt werden kann.

III. Fazit

Auskunfteien verlieren ein ausdifferenziertes Regelungssystem im BDSG. Die Prozesse sind hinsichtlich der Vereinbarkeit mit der DS-GVO zu überprüfen. Insbesondere im Bereich der Betroffenenrechte sind Anpassungen vorzunehmen, um etwa Fristenregelungen und inhaltlich ausgeweiteten Transparenzansprüchen gerecht zu werden.

Carolyn Eichler
ist Referentin bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit. Der Beitrag gibt die persönliche Auffassung der Autorin wieder.

28 Vgl. Erwägungsgrund 63.

Maria Christina Rost

Bußgeld im digitalen Zeitalter – was bringt die DS-GVO?

Datenschutz als Damoklesschwert der Haftung und der finanziellen Belastung. Drastische Bußgelderhöhungen, mehr Bußgeldtatbestände, unbestimmte Bußgeldtatbestände, neue erhöhte Anforderungen an ein Datenschutz-Compliance, leichtere Begründung der Verantwortlichkeit eines Unternehmens, auch wenn der „Täter" nicht feststellbar ist. Ist das schlichtweg der unvorhersehbare Horror oder kann ich als Unternehmen präventiv vorsorgen?

A. Allgemeine Bedingungen für die Verhängung von Geldbußen nach Art. 83 DS-GVO

Die europäische Datenschutzreform steht im Zeichen des digitalen Zeitalters. Daten sind zu einer Ware geworden, die tagtäglich an finanzieller Bedeutung gewinnt. Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen[1]. Dem europäischen digitalen Binnenmarkt steht das Recht auf informationelle Selbstbestimmung und das Bedürfnis eines unionsweiten wirksamen Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten als Gegenspieler gegenüber. Die Grundverordnung verfolgt den Zweck, der Harmonisierung der Vorschriften zum Schutz der Grundrecht und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten[2]. Dazu gehört auch, dass die konsequente Durchsetzung der DS-GVO sichergestellt wird. Art. 58 Abs. 2 DS-GVO sieht hierfür eine Reihe an Abhilfebefugnissen vor. Eine der zehn Maßnahmen ist es, eine Geldbuße gemäß Art. 83 DS-GVO zu verhängen,

1 Vgl. Erwägungsgrund 6 DS-GVO.
2 S. Erwägungsgründe 3, 9 DS-GVO.

zusätzlich zu oder anstelle von den in Art. 58 Abs. 2 lit. a)-h) und j) DS-GVO genannten Maßnahmen.

I. Ausgangslage in Deutschland

Deutschland gehört zu den Mitgliedsstaaten in der Europäischen Union, in denen „administrative sanction" Tradition hat. Gemäß § 1 Abs. 1 OWiG ist die Ordnungswidrigkeit eine mit Geldbuße bedrohte, tatbestandsmäßige, rechtswidrige und vorwerfbare Handlung. Von ihr zu unterscheiden ist die Straftat, die eine mit Geld- und oder Freiheitsstrafe bedrohte Handlung ist. Im Gegensatz zur Kriminalstrafe fehlt der Geldbuße ein Unwerturteil und der Ernst staatlichen Strafens[3]. Die Geldbuße ist in erster Linie darauf gerichtet, eine bestimmte Ordnung durchzusetzen, die Geldbuße ist eine ernste Pflichtenmahnung des Betroffenen[4].

Die mit Geldbußen sanktionierten Verstöße gegen das Bundesdatenschutzgesetz (BDSG) sind derzeit in § 43 Abs. 1 und 2 BDSG geregelt. § 43 Abs. 1 BDSG enthält Tatbestände, die gemäß § 43 Abs. 3 S. 1, 1. Halbsatz BDSG mit einem Bußgeld von bis zu 50.000 EUR geahndet werden können. In § 43 Abs. 2 BDSG werden schwere Verstöße aufgeführt, für die gemäß § 43 Abs. 3 S. 1, 2. Halbsatz BDSG ein Bußgeld von bis zu 300.000 EUR verhängt werden kann.

Das geltende Verfahren kann gegen natürliche Personen, natürliche und juristische Personen im gemeinsamen Verfahren oder gegen die natürliche Person und die juristische Person als Nebenbeteiligte in getrennten Verfahren geführt werden. Das Ordnungswidrigkeitenverfahren ist im Gesetz über Ordnungswidrigkeiten (OWiG) geregelt und wird durch die in Bezug genommenen Vorschriften der StPO, GVG und JGG über § 46 Abs. 1 OWiG ergänzt.

Die Einhaltung des BDSG wird zum einen durch die Verhängung von Bußgeldern und zum anderen durch die Anordnungs- und Untersagungsrechte der Aufsichtsbehörde gemäß § 38 Abs. 5 BDSG gewährleistet.

II. Die neuen Vorschriften zum Bußgeldverfahren im Überblick

Die DS-GVO[5] löst die Richtlinie 95/46/EG ab. Während die Richtlinie in nationales Recht umzusetzen war, findet die DS-GVO als Verordnung ab dem 25. Mai 2018 direkt Anwendung. Für den nationalen Gesetzgeber verbleibt wenig Umsetzungsspielraum, so beispielsweise im Rahmen der in der Verordnung an verschiedenen Stellen vorzufindenden Öffnungsklauseln[6]. Öffnungsklauseln mit Bezug auf das Bußgeldverfahren finden sich in Art. 58 Abs. 6, Art. 83 Abs. 7 und 8 sowie in Art. 84 DS-GVO.

Zentrale Normen im Zusammenhang mit dem Bußgeldverfahren sind Art. 58 Abs. 2, Art. 70 lit. k, Art. 83, Art. 84 DS-GVO und erläuternd die Erwägungsgründe 148, 149, 150, 151 und 152.[7]

III. Zuständige Aufsichtsbehörde

Die heute für die Umsetzung des BDSG zuständigen Aufsichtsbehörden sind die für die Durchsetzung der DS-GVO zuständigen Behörden von morgen. Nach Art. 55 Abs. 1 DS-GVO ist jede Aufsichtsbehörde für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaates zuständig.

Folgende Aufgaben werden der Aufsichtsbehörde durch die DS-GVO übertragen:

- Durchsetzung der Verordnung (Art. 57 Abs. 1 lit. a DS-GVO),
- Sensibilisieren der Verantwortlichen und Auftragsverarbeiter für die ihnen aus dieser Verarbeitung entstehenden Pflichten (Art. 57 abs. 1 lit. d),
- Führen interner Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Art. 58 Abs. 2 DS-GVO ergriffene Maßnahmen (Art. 57 Abs. 1 lit. u DS-GVO).

Zu den Aufgaben kommen die Befugnisse aus Art. 58 DS-GVO. Die Aufsichtsbehörde hat Untersuchungsbefugnisse (Art. 58 Abs. 1 DS-GVO), sie hat Abhilfebefugnisse (Art. 58 Abs. 2 DS-GVO) und Genehmigungsbefugnisse (Art. 58 Abs. 3 DS-GVO).

Die Abhilfebefugnisse in Art. 58 Abs. 2 DS-GVO enthalten einen Strauß an 10 Maßnahmen, die der Aufsichtsbehörde bei der Umsetzung ihrer Aufgaben dienlich sein sollen:

- einen Verantwortlichen oder den Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen[8],
- einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen die DS-GVO verstoßen hat[9],
- den Verantwortlichen oder den Auftragsverarbeiter anweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach der DS-GVO zustehenden Rechte zu entsprechen[10],
- den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen[11],
- den Verarbeiter anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen[12],

3 Vgl. Wieser, Gesetz über Ordnungswidrigkeiten, § 1 Rz. 5.

4 S. BVerfG, Beschluss v. 16.07.1969, Az. 2 BvL2/69; BVerfGE 27, 18.

5 Informativ zu DS-GVO Piltz, K&R 2016, 557; ders., K&R 2016, 629; ders. K&R 2016, 709; ders., K&R 2016, 777; Gola, RDV 2013, 1; Dieterich, ZD 2016, 260; Ashkar, DuD 2015, 796; Faust/Spittka/Wybitul, ZD 2016, 120; Thode, CR 2016, 714.

6 Zu den Öffnungsklauseln: Benecke/Wagner DVBl. 2016, 600; zur DS-GVO und den Öffnungsklauseln: Piltz K&R 2016, 557; ders., K&R 2016, 629; ders., K&R 2016, 709; ders., K&R 2016, 777.

7 Das wird ergänzt durch die Vorschriften zu Zusammenarbeit und Kohärenz in Art. 60 bis 66 DS-GVO.

8 S. Art. 58 Abs. 2 lit. a DS-GVO.

9 S. Art. 58 Abs. 2 lit. b DS-GVO.

10 S. Art. 58 Abs. 2 lit. c DS-GVO.

11 S. Art. 58 Abs. 2 lit. d DS-GVO.

12 S. Art. 58 Abs. 2 lit. e DS-GVO.

- eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen[13],
- die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen[14],
- eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden[15],
- eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls[16],
- die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen[17].

In welchem Verhältnis die Geldbuße zu den anderen Maßnahmen zu sehen ist, gibt die Grundverordnung in Art. 83 Abs. 2 Satz 1 DS-GVO und Erwägungsgrund 148 Satz 1 DS-GVO vor. Geldbußen sollen, im Interesse einer konsequenteren Durchsetzung der Vorschriften, je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Art. 58 Abs. 2 Buchstaben a bis h und i DS-GVO verhängt werden. Dem Verordnungsgeber ist wohl ein redaktionelles Versehen unterlaufen, es dürfte der Buchstabe j statt dem Buchstaben i gemeint gewesen sein.

IV. Adressat des Bußgeldverfahrens

Bußgelder wegen Verstößen gegen die DS-GVO können sowohl gegen Unternehmen als auch gegen „Personen, bei denen es sich nicht um ein Unternehmen handelt“[18] verhängt werden. Dem Bußgeldverfahren liegt nicht der datenschutzrechtliche Unternehmensbegriff gemäß Art. 4 Nr. 18 DS-GVO zugrunde, sondern der weiter zu verstehenden kartellrechtliche Unternehmensbegriff im Sinne der Art. 101 und 102 Vertrages über die Arbeitsweise der Europäischen Union (AEUV). Dies ist gerade im Zusammenhang mit der Bußgeldzumessung von besonderer Relevanz.

V. Die Bußgeldtatbestände

Die neuen, mit Bußgeldern sanktionierten Tatbestände sind in Art. 83 Abs. 4, 5 und 6 DS-GVO geregelt. Teilt man die Tatbestände nach Ihrem Bußgeldrahmen auf, ergeben sich zwei Gruppen.

Die erste Gruppe sind die Tatbestände in Art. 83 Abs. 4 DS-GVO. Ihre Verletzung kann mit einem Bußgeld bis zu 10 Mio. Euro sanktioniert werden. Der Höchstbetrag von 10 Mio. Euro kann überschritten werden, wenn ein Unternehmen im letzten Geschäftsjahr einen weltweiten Umsatz erzielt hat, von dem 2 % höher sind als der Höchstbetrag von 10 Mio. Euro.

Die zweite Gruppe sind die Bußgeldtatbestände nach Art. 83 Abs. 5 und 6 DS-GVO. Ihre Verletzung kann mit einem Bußgeld von bis zu 20 Mio. Euro geahndet werden bzw. mit Bußgeldern bis zu 4 % des weltweiten Jahresumsatzes eine Unternehmens.

Art. 83 Abs. 4 und 5 DS-GVO sanktionieren Verpflichtungen, die sich aus der DS-GVO ergeben. Art. 83 Abs. 6 DS-GVO sanktioniert die Verstöße, die eine Missachtung einer Anweisung der Aufsichtsbehörde aus Artikel 58 Abs. 2 DS-GVO darstellen.

Die in Art. 83 DS-GVO normierten Tatbestände reichen deutlich weiter als die bisherigen Bußgeldtatbestände nach § 43 BDSG. Hinzu kommt, dass sie sehr unbestimmt sind – ein europäisches Phänomen, das Wieser bereits für den Bereich des europäisierten Lebensmittelhygienerecht im Zusammenhang mit den Ausfüllungstatbeständen bemängelt hat[19]. Der in Artikel 103 Abs. 2 GG enthaltene verfassungsrechtliche Bestimmtheitsgrundsatz enthält die Verpflichtung des Gesetzgebers, die Voraussetzungen der Strafbarkeit so konkret zu umschreiben, dass Tragweite und Anwendungsbereich der Straf- und Ordnungswidrigkeitentatbestände zu erkennen sind und sich durch Auslegung ermitteln lassen[20]. In der Unbestimmtheit der Tatbestände liegen aus Unternehmenssicht erhebliche Haftungsrisiken. [21]

1. Art. 83 Abs. 4 DS-GVO

Sanktioniert werden nach Art. 83 Abs. 4 lit. a DS-GVO Verstöße gegen die Pflichten der Verantwortlichen[22] und der Auftragsverarbeiter[23] gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43 DS-GVO. Art. 83 Abs. 4 lit. b DS-GVO sanktioniert Verstöße gegen die Pflichten der Zertifizierungsstelle gem. Art. 42 und 43 DS-GVO[24]. Nach Art. 83 Abs. 4 lit. c DS-GVO werden Verstöße gegen die Pflichten der Überwachungsstelle gemäß Artikel 41 Abs. 4 DS-GVO geahndet.

13 S. Art. 58 Abs. 2 lit. f DS-GVO.

14 S. Art. 58 Abs. 2 lit. g DS-GVO.

15 S. Art. 58 Abs. 2 lit. h DS-GVO.

16 S. Art. 58 Abs. 2 lit. i DS-GVO.

17 S. Art. 58 Abs. 2 lit. j DS-GVO.

18 Erwägungsgrund 150 DS-GVO.

19 S. dazu Wieser OWiG § 3 Rn 4.4.

20 Vgl. BVerfG (ständige Rechtsprechung) Beschluss v. 23.10.1985, Az. 1 BvR 1053/82, BVerfGE 71, 108.

21 S. Faust/Spittka/Wybitul, ZD 2016, 120.

22 Verantwortlicher i.S.v. Artikel 4 Zif. 7 DS-GVO = eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten vorgesehen werden.

23 Auftragsverarbeiter i.S.v. Art. 4 Zif. 8 DS-GVO = eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

24 Hier wird eine Abgrenzung zu Art. 83 Abs. 4 lit. a DS-GVO erforderlich werden.

2. Art. 83 Abs. 5 DS-GVO

Verstöße gegen die in Art. 83 Abs. 5 aufgelisteten Pflichten werden als schwere Verstöße eingestuft. Ihr Bußgeldrahmen reicht bis zu 20 Mio. Euro. Hierunter fallen Verstöße gegen die Grundsätze der Verarbeitung einschließlich der Bedingungen für die Einwilligung gemäß den Artikeln 5, 6,7 und 9 DS-GVO[25]. Verstöße gegen die Rechte der betroffenen Personen gemäß Artikel 12 bis 22 DS-GVO[26], Verstöße gegen die Pflichten im Rahmen der Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49 DS-GVO[27], die Nichtbefolgung aller Pflichten gemäß den Rechtsvorschriften der Mitgliedsstaaten, die im Rahmen des Kapitels IX der DS-GVO erlassen wurden[28], sowie die Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Abs. 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Abs. 1 DS-GVO[29].

3. Art. 83 Abs. 6 DS-GVO

Zu guter Letzt können nach Art. 83 Abs. 6 DS-GVO bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 2 DS-GVO Bußgelder in Höhe von bis zu 20 Mio. Euro festgesetzt werden. Art. 83 Abs. 6 DS-GVO ist eine sogenannte Blankettvorschrift[30]. Die Vorschrift bezieht sich auf eine von der Aufsichtsbehörde erlassene Maßnahme, einen Verwaltungsakt. Für die Sanktionierung bedeutet das, dass der Verwaltungsakt für den Adressaten zur Tatzeit verbindlich ist. Der Verwaltungsakt muss also entweder nach Ablauf der einmonatigen Widerspruchsfrist (§ 70 VwGO) bzw. nach Ablauf der Klagefrist (§ 74 Abs. 1 VwGO) bestandskräftig geworden sein oder, wenn kein Widerspruchverfahren vorgesehen ist, von Gesetzes wegen sofort (§ 80 Abs. 1 Satz 1 Nr. 3 VwGO) bzw. aufgrund der Anordnung der sofortigen Vollziehung durch die Behörde im Einzelfall (§ 80 Abs. 2 Satz 1 Nr. 4 VwGO) vollziehbar sein[31].

Die Zuwiderhandlung gegen ein durch den Verwaltungsakt angeordnetes Tun, Dulden oder Unterlassen ist daher grundsätzlich nicht schon mit Erlass der behördlichen Entscheidung bußgeldbewehrt, sondern erst dann, wenn der Verwaltungsakt für den Betroffene verbindlich ist. Die Ahndung eines Ungehorsams setzt voraus, dass der Betroffene den Vollzug der gegen ihn gerichteten Verfügungen ohne die Möglichkeit hemmender Rechtsbehelfe zunächst einmal hinnehmen muss[32].

Soweit die Behörde den Adressaten zur Mitwirkung auffordert, reicht es nicht aus, die fristgemäße Erfüllung von Mitwirkungspflichten durch dienstliches Schreiben ohne Zustellung, Begründung und Rechtsbehelfsbelehrung anzudrohen. Das ist kein vollziehbarer Verwaltungsakt, außer das behördliche Verlangen ist von Gesetzes wegen sofort vollziehbar[33]. Schlechthin falsch ist laut Wieser[34] der Hinweis, der Mitwirkungspflichtige begehe eine Ordnungswidrigkeit, wenn er dieses Schreiben nicht beantworte.

Damit sanktioniert die DS-GVO sowohl in Art. 83 Abs. 5 e als auch Art. 83 Abs. 6 DS-GVO Verstöße gegen Maßnahmen aus Abhilfebefugnissen gemäß Art. 58 Abs. 2 DS-GVO. Dies ist auf den ersten Blick strukturell unlogisch, aber anscheinend vom Verordnungsgeber gewollt.

B. Die Geldbuße nach DS-GVO und ihre Zumessung

Bei Unternehmen sollen Verstöße gegen die DS-GVO im Falle eines Verstoßes mit „starken Sanktionen" geahndet werden, richtig teuer werden und wehtun[35]. Daher sieht die Verordnung auch vor, dass in datenschutzrechtlichen Bußgeldverfahren gegen Unternehmen die Aufsichtsbehörden Bußgelder von bis zu 10 Mio. Euro und im Fall der Tatbestände in Art. 83 Abs. 5 und 6 DS-GVO bis zu 20 Mio. bzw. von bis zu 2% bzw. 4 % des weltweiten Umsatzes des Vorjahres verhängen können.

1. Der Funktionale Unternehmensbegriff

Eine wichtige Neuerung ist die Einführung des aus dem Kartellrecht entstammenden weiten Unternehmensbegriffs nach Art. 101 und 102 AEUV[36]. Die DS-GVO verwendet somit zwei unterschiedliche Unternehmensbegriffe an. Den datenschutzrechtlichen nach Art. 4 Nr. 18 DS-GVO und den kartellrechtlichen nach Art. 101, 102 AEUV.

a) Der Begriff

Der Unternehmensbegriff nach Art. 101 und 102 AEUV ist ein weiter Unternehmensbegriff.

Der sogenannte „funktionale Unternehmensbegriff" ist in jahrelanger Entscheidungspraxis der Kommission und des EuGH im Kartellrecht geprägt worden[37].

b) Die „wirtschaftliche Einheit"

Unternehmen ist demnach „jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung"[38]. Entscheidend ist nicht

25 S. Art. 3 Abs. 5 lit. a DS-GVO.

26 S. Art. 83 Abs. 5 lit. b DS-GVO.

27 S. Art. 83 Abs. 5 lit. c DS-GVO.

28 S. Art. 83 Abs. 5 lit. d DS-GVO.

29 S. Art. 83 Abs. 5 lit. e DS-GVO.

30 S. Wieser, OWiG § 1 Ziff. 2.2.2 (Stand: 28.10.2016).

31 S. dazu Wieser, OWiG § 1 Ziff. 2.2.2.1 (Stand: 28.10.2016)

32 OLG Hamm, Beschluss v. 12.04.2012, Az. 3 RBs 426/11, NZS 2012, 713, OLG Bamberg, Beschluss v. 04.12.2007, Az. 2 Ss OWi 1265/07, DAR 2008, 99.

33 Vgl. § 84 Abs. 1 AufenthG.

34 Wieser, OWiG § 1 Ziff. 2.2.2.1.

35 LIBE-Ausschuss des Europäischen Parlaments, EU-Datenschutzgrundverordnung: Stand der Dinge – 10 wichtige Punkte v. 11.06.2015, S. 2.

36 S. Erwägungsgrund 150, Satz 3 DS-GVO.

37 Dazu vertiefend Faust/Spittka/Wybitul, ZD 2016, 120; zum Kartellrecht: Mansdörfer/Timmerbeil, EuZW 2011, 214; Koenig/Engelmann, EuZW, 2004, 682; Schindler, KommJur 2011, 126.

38 Ständige Rechtsprechung des EuGH seit EuGH Höfner und Elsner/Macroton, C-41/90 – Slg. 1993, I-1979, 2016, R. 21; SAT Fluggesellschaft/Eurocontrol, C-364/92, Slg. 1994, I-43; Albany, C-67/696 – Slg. 1999, 5751,5886, Rn. 77; Pavlov, C-180 bis 184/98 – Slg. 2000, 6451, 6520, Rn. 74; Glöckner, C-475/99 – Slg. 2001, I-8099, 8145, Rn. 19; AOK Bundesverband, C-264, 206, 254 u 355/01 – Slg. 2004, 2493, 2542.

wer tätig ist, sondern die aktive Teilnahme am Wirtschaftsleben durch das Anbieten oder u.U. auch Nachfragen von Gütern oder Dienstleistungen auf einem bestimmten Markt[39].

Mutter- und Tochtergesellschaft sind dann eine „wirtschaftliche Einheit" und können gemeinsam für ein Fehlverhalten des Tochterunternehmens sanktioniert werden, wenn die Muttergesellschaft auf die Tochtergesellschaft aus wirtschaftlichen, organisatorischen oder rechtlichen Gründen einen bestimmenden Einfluss ausübt[40]. Dann sind sie ein einziges Unternehmen. Eine weitere Konsequenz der wirtschaftlichen Einheit ist es, dass es genügt, wenn eine natürliche Person für das Unternehmen handelt. Der EuGH geht für den kartellrechtlichen Bereich davon aus, dass ein Verhalten dem Unternehmen zuzurechnen ist, ohne dass eine konkret handelnde Person überhaupt benannt werden muss. Erfasst sind daher nicht nur wie bisher die gesetzlichen Vertreter oder Leitungspersonen (§ 30 Abs. 1 OWiG), sondern sämtliche Bedienstete oder auch Beauftragte außerhalb des Unternehmens oder der Unternehmensvereinigung.[41] Eine Kenntnis der Inhaber oder Geschäftsführer des Unternehmens von der konkreten Handlung oder eine Verletzung der Aufsichtspflicht (bisher für § 130 OWiG notwendig) ist für die Zuordnung der Verantwortlichkeit nicht erforderlich.

c) Was bedeutet das für den Datenschutz

Der Transfer des „funktionalen Unternehmensbegriff" in den Bereich des Datenschutzrechts zeigt zugleich, dass der Verordnungsgeber dem Handel mit Daten eine ähnlich gelagerte Bedeutung im Wirtschaftshandel zumisst wie den Kartellen. Die Daten sind Ware von wachsender Bedeutung in einem aufstrebenden digitalen und digitalisierten Binnenmarkt in einer fortschreitenden Globalisierung der digitalen Welt.[42]

2. Bußgeldzumessung

Für die Bußgeldzumessung bei Verstößen gegen die DS-GVO sind die Vorschriften Art. 83 Abs. 1 und 2 DS-GVO relevant. Hintergrundinformationen ergeben sich aus Erwägungsgründen 148 und 150 Satz 2,3,4. Sofern das EDPB[43] gemäß Art. 70 lit. k DS-GVO Leitlinien erlässt, nehmen diese ebenfalls Einfluss auf die Bußgeldzumessung. Die Grundverordnung fordert, dass es für die Verhängung von Sanktionen einschließlich Geldbußen angemessene Verfahrensgarantien geben soll, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtschutz und ein faires Verfahren, entsprechen[44].

a) Art. 83 Abs. 1 DS-GVO

Art. 83 Abs. 1 DS-GVO gibt an die Aufsichtsbehörde den Auftrag, sicherzustellen, dass die Verhängung von Geldbußen gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

Wenn Geldbußen Personen auferlegt werden, bei denen es sich nicht um Unternehmen handelt, soll die Aufsichtsbehörde bei der Erwägung des angemessenen Betrages für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen[45].

Ob das Auslassen von Art. 83 Abs. 4 DS-GVO in der Benennung der Tatbestände in Art. 83 Abs. 1 DS-GVO beabsichtigt war oder ob es sich um ein redaktionelles Versehen handelt, ist noch abzuklären. Es spricht viel für ein redaktionelles Versehen.

b) Art. 83 Abs. 2 DS-GVO

Nach Art. 83 Abs. 2 S. 1 DS-GVO können Geldbußen je nach den Umständen des Einzelfalls zusätzlich oder anstelle von Maßnahmen nach Artikel 58 Abs. 2 lit. a bis h und j[46] verhängt werden.

Die DS-GVO gibt der Aufsichtsbehörde für ihre Entscheidung Kriterien an die Hand. Diese sind bei der Entscheidung über das „ob" und die „Höhe" durch die Aufsichtsbehörde zu berücksichtigen. Geregelt sind sie in Art. 83 Abs. 2 S. 2 lit. a bis k DS-GVO. Diese Kriterien eröffnen den Betroffenen im Bußgeldverfahren zugleich im Umkehrschluss einen Hinweis darauf, was im Rahmen des Krisenmanagement im Falle des Verstoßes als Unternehmen unternommen werden kann, um eine Geldbuße abzuwenden oder eine Geldbuße zu reduzieren – allerdings immer mit dem Risiko, dass keine Gewähr dafür besteht, in dem jeweiligen Einzelfall die gewünschte Wirkung zu erzielen.

Im Einzelnen empfiehlt es sich für den Betroffenen, die nachfolgend vorgestellten Kriterien zu kennen und möglichst Präventions- und Verteidigungsstrategien daran auszurichten.

aa) Art. 83 Abs. 2 S.2 lit a DS-GVO

Die Aufsichtsbehörde hat Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens ihrer Entscheidung zugrunde zu legen.

39 EuGH- Kommission/Italien – 118/85 – Slg. 1987, 2599, Rn. 7; Diego Cali Figli, C-343/95 – Slg. 1997, I-1547, Rn. 16; Schröter, in: von der Groeben/Schwarze/Hatje, AEUV, 7. Auflage vor Art. 101-105, Rn. 67 ff. m.w.N.

40 Hierzu Schröter, in: von der Groeben/Schwarze/Hatje, AEUV, 7. Auflage vor Art. 101-105, Rn. 51 ff. m.w.N., EuGH, Urteil v. 20.01.2011 – Genaral Quimka, C-90/09 – Slg. 2011, I-0001, Rn. 85, 89.

41 S. EuGH – Musique Diffusion française, Urteil v. 07.06.1983, 100-103/80 – Slg. 1983, 1825, Rn. 97; Tokai Carbon, T-236/01- Slg. 2004, 1181, Rn. 278; Protimonopolný úrad Slovenskej republiky, C-68/12, Rn. 25-28; Faust/Spittka/Wybitul, ZD 2016, 120 (121).

42 Hierzu Albrecht, Finger weg von unseren Daten! Wie wir entmündigt und ausgenommen werden, München 2014.

43 EDPB = European Data Protection Board.

44 S. Erwägungsgrund 149 Satz 4 DS-GVO.

45 Vgl. Erwägungsgrund 150, Satz 4 DS-GVO.

46 Zwar steht in Artikel 83 Abs. 2 S. 1 DS-GVO „i", aber allein schon das Wort „und" davor spricht dafür, dass eigentlich „j" gemeint war, zumal es sich bei „i" um die Abhilfemaßnahme Geldbuße handelt.

bb) Art. 83 Abs. 2 S.2 lit b DS-GVO

Bei der Bußgeldzumessung spielt außerdem eine Rolle, ob die Tat vorsätzlich oder fahrlässig begangen wurde.

cc) Art. 83 Abs. 2 S.2 lit c DS-GVO

Berücksichtigt werden jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens. Dem Verantwortlichen oder Auftragsverarbeiter sollte es daher ein Anliegen sein, Maßnahmen zu ergreifen und sie zu dokumentieren.

dd) Art. 83 Abs. 2 S.2 lit d DS-GVO

In die Beurteilung fließt außerdem der Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 DS-GVO getroffenen technischen und organisatorischen Maßnahmen ein.

ee) Art. 83 Abs. 2 S.2 lit e DS-GVO

Für die Entscheidung über das „ob" und das „wie" sind auch etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters zu berücksichtigen.

ff) Art. 83 Abs. 2 S.2 lit f DS-GVO

Für den Betroffenen rechnet es sich, mit der Aufsichtsbehörde von sich aus zusammenzuarbeiten. In die Bußgeldzumessung fließt der Umfang der Zusammenarbeit mit der Aufsichtsbehörde ein, der aufgewandt wurde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern. Um einen Anhaltspunkt dafür zu erhalten, was an dieser Stelle sachdienlich wäre, kann man u.a. im Kartellrecht im Zusammenhang mit der dortigen Bonusregelung spieken[47]. Dort gibt es mittlerweile eine umfangreiche Rechtsprechung zu den verschärfenden und mildernden Faktoren.

So ist zum Beispiel von der kartellrechtlichen Rechtsprechung als Begründung für eine nur geringe Bußgeldermäßigung anerkannt worden: der allgemeine Charakter der vorgelegten Informationen und Beweismittel[48], die Unvollständigkeit der vorgelegten Informationen[49], Unternehmen bagatellisiert zugleich die Dauer der Zuwiderhandlung und seine dabei gespielte Rolle[50], und mit Vorbehalten verbundene Eingeständnisse oder mehrdeutige Erklärungen[51].

Diese Rechtsprechung bezieht sich zwar auf das kartellrechtliche Ordnungswidrigkeitenverfahren, gibt aber dennoch erste Orientierungspunkte für das datenschutzrechtliche Ordnungswidrigkeitenverfahren.

gg) Art. 83 Abs. 2 S.2 lit g DS-GVO

Für die Bewertung des Einzelfalls spielt es zudem eine Rolle, welche Kategorien personenbezogener Daten von dem Verstoß betroffen sind.

hh) Art. 83 Abs. 2 S.2 lit h DS-GVO

Die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat, werden ebenfalls berücksichtigt.

ii) Art. 83 Abs. 2 S.2 lit i DS-GVO

Relevant für die Beurteilung des Einzelfalls ist die Einhaltung der nach Artikel 58 Absatz 2 DS-GVO früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden. Mit anderen Worten: Hat die Aufsichtsbehörde hier bereits andere Maßnahmen angeordnet und wurden diese nicht eingehalten, wird dies voraussichtlich erschwerend Berücksichtigung in der Entscheidung der Aufsichtsbehörde finden.

jj) Art. 83 Abs. 2 S.2 lit j DS-GVO

Die Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 DS-GVO und von genehmigten Zertifizierungsverfahren nach Artikel 42 DS-GVO fließt ebenfalls in die Bußgeldzumessung mit ein. Dadurch wird die Durchführung solcher Maßnahmen für Unternehmen an Attraktivität gewinnen.

kk) Art. 83 Abs. 2 S.2 lit k DS-GVO

Außerdem fließen in die Bewertung jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall ein, wie z.B. unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

c) Deckelung nach Art. 83 Abs. 3 DS-GVO

Die Verordnung sieht eine Deckelung der Bußgeldhöhe für den Bußgeldgesamtbetrag im Falle von Tateinheit vor. In Art. 83 Abs. 3 DS-GVO ist geregelt, dass wenn ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung verstößt, der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß übersteigt.

3. Leitlinien zur Bußgeldfestsetzung

Um die einheitliche Anwendung der Verordnung sicherzustellen, nimmt der Europäische Datenschutzausschusses[52]

47 M.w.N. Winterstein/Ceyssens/Wessely, in: Groeben/Schwarze/Hatje, AEUV, 7. Auflage, nach Art, 101, Rn. 46 ff. und vor allem Rn. 86 ff.

48 EuG BASF u.a./Kommission, T-101/05 u.a. – Slg. 2007, II-04949, Rn. 103,106.

49 EuG BASF u.a./Kommission, T-101/05 u.a. – Slg. 2007, II-04949, Rn. 116,127.

50 EuG – ABB/Kommission, T-31/99 – Slg. 2002, II-01881, Rn. 243.

51 EuG – Bolloré u.a./Kommission, T-109/02 u.a. – Slg. 2007, II-00947, Rn. 717.

52 Europäischer Datenschutzausschuss = EDAS bzw. European Data Protection Board = EDPB.

(Art. 68 DS-GVO) Aufgaben wahr, die ihm ausdrücklich in Art. 70 DS-GVO zugeschrieben sind. In diesem Zusammenhang ist der EDAS gemäß Art. 70 lit. k DS-GVO[53] mit der Ausarbeitung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Artikel 58 Absätze 1, 2 und 3 DS-GVO und die Festsetzung von Geldbußen gemäß Artikel 83 DS-GVO beauftragt.

Die Cooperation Subgroup, eine Unterarbeitsgruppe der Artikel-29 Gruppe, hat den Auftrag erhalten, in Vorbereitung auf den 25. Mai 2018 unter anderem Leitlinien für die Bebußung[54] auszuarbeiten. Aufgrund der vielen anderen Fragestellungen wurde das Thema aber nach ersten Anläufen und Entwürfen vorerst zurückgestellt.

Leitlinien für die Bebußung sind im Zusammenhang mit Geldbußen nicht neu, und vor allem nicht in Deutschland. Das Bundeskartellamt hat Bußgeldleitlinien für das Kartellordnungswidrigkeitenverfahren. In den Leitlinien für die Bußgeldzumessung in Kartellordnungswidrigkeitenverfahren (Bußgeldleitlinien) ist festgelegt, wie das Bundeskartellamt schwerwiegende Kartellrechtsverstöße ahndet und welche Kriterien für die Bußgeldzumessung herangezogen werden.[55] Die letzte Fassung wurde am 23. Juni 2013 bekannt gemacht.[56]

Anstoß für die Entwicklung gab die Europäisierung des Kartellrechts. In Ausübung seines Ermessens legt das Bundeskartellamt gemäß § 81 Abs. 7 GWB mit den Leitlinien für die Bußgeldzumessung in Kartellordnungswidrigkeitenverfahren fest, wie es bei der Bemessung des ahndenden Teils der Geldbuße für sog. schwere Kartellordnungswidrigkeiten gegenüber Unternehmen und Unternehmensvereinigungen vorgehen wird.[57]

Dieses Modell der Incentive-Setzung oder auch „the stick and the carrot" genannt findet seine gedankliche Grundlage in den U.S. Federal Sentencing Guidelines („Guidelines"). Im November 1999 hat der US-amerikanische Kongress die „Guidelines" verabschiedet und eine dramatische Auswirkung auf das unternehmerische Amerika erreicht.[58]

Inwieweit die „Anlehnung" an das Kartellrecht auch ein Indiz für die zukünftige datenschutzrechtliche Bußgeldpraxis ist, wird sich in der Umsetzungsphase herauskristallisieren. Die Hinweise in der Verordnung sprechen dafür.

4. Kohärenzverfahren

Das Kohärenzverfahren kann auch genutzt werden, um eine kohärente Anwendung von Geldbußen zu fördern[59].

5. Verzeichnisse

Die Aufsichtsbehörden müssen gemäß Art. 57 Abs. 1 lit u DS-GVO interne Verzeichnisse über Verstöße gegen dies Verordnung und gemäß Artikel 58 Abs. 2 ergriffene Maßnahmen führen. Der EDAS kann nach Art. 70 Abs. 1 lit. y DS-GVO ein öffentlich zugänglich elektronisches Register der Beschlüsse der Aufsichtsbehörden und Gerichte in Bezug auf Fragen führen, die im Rahmen des Kohärenzverfahrens behandelt wurden. Im Zusammenhang mit dem Hinweis[60], dass das Kohärenzverfahren auch dazu genutzt werden kann, um einen kohärente Anwendung von Geldbußen zu fördern, kann das dazu führen, dass Bußgeldentscheidungen in diesem Register veröffentlicht werden.

C. Das OWi-Verfahren im DSAnpUG-EG

Das Bundesinnenministerium arbeitet aktuell[61] am „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680" (Datenschutz-Anpassung- und -Umsetzungsgesetz EU – DSAnpUG-EU). Der erste Entwurf kam im August 2016 heraus. Der zweite Entwurf wurde mit Stand 23.11.2016/09:18 in die Länder- und Verbändebeteiligung gegeben. Im Dezember 2016 arbeitete das Bundesinnenministerium am 3. Entwurf. Der Gesetzesentwurf soll im Januar 2017 ins Bundeskabinett. Die Vorschriften, die das Bußgeldverfahren betreffen, sind §§ 39 und 40 DSAnpUG-EU.

Mit dem neuen § 39 Abs. 1 DSAnpUG-EU wird das Gesetz über Ordnungswidrigkeiten (OWiG) auch auf Verstöße nach Artikel 83 Abs. 4 bis 6 der DS-GVO erstreckt[62]. Gemäß § 39 Abs. 1 Satz 2 finden §§ 9,17,30,36 und 130 OWiG keine Anwendung. Die Anwendung der §§ 9, 30 und 130 OWiG ist ausgeschlossen, da die DS-GVO hinsichtlich der Frage der Zurechnung von Handlungen abschließend ist. § 17 des Gesetzes über Ordnungswidrigkeiten kommt nicht zur Anwendung, da die DS-GVO auch die Bußgeldhöhe abschließend regelt. §§ 35 und 36 OWiG werden nicht angewendet, da sich bereits aus Artikel 83 DS-GVO ergibt, dass die Aufsichtsbehörden für die Verhängung von Geldbußen zuständig sind. Die Verordnung selbst regelt das Straf- und Buß-

53 Lit. k hebt sich dadurch von den anderen Aufgaben ab, dass es sich um einen Absatz handelt, die sich an die Aufsichtsbehörden wendet. Daher ist die Einstiegsformulierung auch anders. Die Leitlinien werden ausgearbeitet, während z.B. die Leitlinien zu lit. f „bereitgestellt" werden.

54 Guidelines for the imposition of administrative fines; Berichterstatter sind Großbritannien und Norwegen.

55 Https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Leitlinien/Bekanntmachung%20-%20Bu%C3%9Fgeldleitlinien-Juni%202013.html (Stand: 16.12.2016).

56 Leitlinien BKartA v. 23. Juni 2013: http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Leitlinien/Bekanntmachung%20-%20Bu%C3%9Fgeldleitlinien-Juni%202013.html?nn=3591418.

57 Bundeskartellamt, Leitlinien für die Bußgeldzumessung in Kartellordnungswidrigkeiten (Stand. 25. Juni 2013), S. 2.

58 "Cartel Criminalization in Ireland and Europe: Can the United States Model of Criminal Antitrust enforcement be successfully transferred to Ireland and Europe?", Rede von Caroly Galbreath auf dem ABA International Section 2007 Fall Meeting am 1. Oktober 2007 in Dublin, http://sti.strata3test.com/sites/default/files/2207-10-01%20Galbreath%20ABA_0.pdf (Stand: 16.12.2016); "Cartel Settlements in the U.S. and E.U: Similarities, Differences & Remaining Questions", Rede Ann O´Brien, 13th Annual EU Competition Law and Policy Workshop, am 06.06.2008 in Florence, Italy, https://www.justice.gov/atr/file/519681/download; Izraeli/Schwartz, What can we learn from the U.S. Federal sentencing Guidelines for Organizational Ethics? Journal of Business Ethics 17 (9-10), S. 1045-1055 (1998).

59 Vgl. Erwägungsgrund 150, Satz 5.

60 Erwägungsgrund 150 Satz 5 DS-GVO.

61 Stand: Dezember 2016.

62 Begründung Entwurf DSAnpUG-EU (Stand: 23.11.2016 09:18 Uhr), S. 104.

geldverfahren nicht. An den bisherigen Grundzügen des datenschutzrechtlichen Bußgeld- und Strafverfahren wird festgehalten, da insbesondere Artikel 83 Absatz 8 DS-GVO ausdrücklich fordert, dass die Mitgliedstaaten angemessene Verfahrensgarantien vorsehen. § 39 Absatz 2 Satz 1 DSAnpUG-EU regelt, dass die Vorschriften des OWiG und der allgemeinen Gesetze über das Strafverfahren grundsätzlich Anwendung finden.[63] Gemäß § 39 Abs. 2 Satz 2 DSAnpUG-EU finden §§ 56 bis 58, 87, 99, 100 OWiG keine Anwendung. Die Anwendung der §§ 56 bis 58 OWiG ist ausgeschlossen, da die Verwarnung[64] bereits in Art. 58 Abs. 2 lit b DS-GVO geregelt ist. Indem die §§ 87, 88, 99, 100 für nicht anwendbar erklärt werden, ist die Anwendung einzelner Vorschriften zu Geldbußen gegen juristische Personen und zu Nebenfolgen sowie zur Vollstreckung[65] von Bußgeldentscheidungen ausgeschlossen. In § 39 Abs. 2 Satz 3 DSAnpUG-EU ist ob der hohen Bußgeldbeträge, die die DS-GVO ermöglicht, in Anlehnung an § 23 Nr. 1 Gerichtsverfassungsgesetz (GVG) die Zuständigkeit des Landgerichts vorgesehen, wenn der Betrag einer Geldbuße die Summe von fünftausend Euro übersteigt. Indem Absatz 2 Satz 4 bestimmt, dass die Staatsanwaltschaft im Zwischenverfahren das Verfahren nur mit Zustimmung der Aufsichtsbehörde einstellen kann, die den Bußgeldbescheid erlassen hat, wird der Bedeutung der Geldbußen in der DS-GVO und der Unabhängigkeit der Datenschutzaufsicht Rechnung getragen.[66] In § 40 DSAnpUG-EU werden weitere Vorschriften für die Verhängung von Geldbußen geregelt.

D. Ausblick auf die Umsetzungsphase

Im derzeitigen Stadium der Umsetzung der DS-GVO sind noch viele Fragen offen, und zwar solche, die zur Definition der unbestimmten Begriffe in den Bußgeldtatbeständen in Art. 83 Abs. 4, 5 und 6 DS-GVO grundlegend sind. Es gibt Verfahrensfragen die noch zu klären sind. Der nationale Gesetzgeber ist auf Bundes- und Landesebene gefordert, sich den Öffnungsklauseln und ihrer Auskleidung zu widmen – eine aus unternehmerischer Sicht bisweilen sicher unbefriedigende Situation. Aber schon heute ist klar, dass Datenschutz in Compliance und die Implementierung von Strategien für den Notfall, dem Datenschutzverstoß, an Bedeutung immens zugenommen haben. Bis zum 25. Mai 2018 wird sich noch einiges tun und ist noch einiges zu tun.

Was können die Unternehmen tun? Faust/Spittka/Wybitul empfehlen ein Datenschutz-Management-System.[67] Es macht sicherlich Sinn, dort zu schauen, wo bereits mit Leitlinien gearbeitet wird, und sich anhand der Rechtsprechung einen Überblick zu verschaffen. Denn es ist unwahrscheinlich, dass das Rad neu erfunden wird. Höchstens wird modifiziert und den speziellen Begebenheiten angepasst.

Im Bereich der Kartellrechtsverstöße und der Korruptionsprävention wurde über das Potential des Whistleblowings diskutiert. Vielleicht wäre dies auch ein Tool im Bereich Datenschutz. Erste Überlegungen, noch zur Datenschutzrichtlinie, hat Forst in einem Aufsatz[68] dazu niedergelegt.

Maria Christina Rost
ist Referentin in der Bußgeldstelle und persönliche Referentin des Hessischen Datenschutzbeauftragten. Vor ihrer Tätigkeit beim HDSB war sie in der Kanzlei des Hessischen Landtags, im Ministerium für Schule und Weiterbildung NRW und als Rechtsanwältin tätig.

63 Begründung Entwurf DSAnpUG-EU (Stand: 23.11.2016 09:18 Uhr), S. 104.

64 Hier wird noch zu diskutieren sein, ob die Verwarnung in der DS-GVO mit der Verwarnung nach OWiG tatsächlich gleichwertig ist.

65 Ob der Ausschluss der besonderen Verfahrensvorschriften über die Vollstreckung erforderlich war, erscheint fraglich. Es wäre zumindest unschädlich gewesen, diese Vorschriften vorerst stehen zu lassen.

66 Dazu Entwurf DSAnpUG-EU (Stand: 23.11.2016 09:18 Uhr), S. 104 f.

67 Faust/Spittka/Wybitul ZD 2016, S. 120, 125.

68 Forst, RDV 2013, 122.

Kurzbeiträge

Informationenspflichten gegenüber Bewerbern nach der DS-GVO

Dr. Niels Lepperhoff, Düsseldorf*

Unternehmen sind gesetzlich verpflichtet, Personen, deren Daten sie erheben oder empfangen, über die Verarbeitung dieser Daten zu informieren. Diese Pflicht ergibt sich aus dem BDSG nach § 4 Abs. 3 und § 33 Abs. und demnächst nach der DS-GVO aus Art. 13 und 14, wobei die Informationspflichten nach der DS-GVO erheblich umfangreicher sind. Unterschieden wird danach, ob die Informationen beim Bewerber erhoben werden oder – mit oder ohne sein Wissen – bei anderen Stellen.

Die Ausgestaltung der Informationspflicht ist hinsichtlich Zeitpunkt (siehe Abschnitt 2), Form (siehe Abschnitt 3) und Inhalt (siehe Abschnitt 4) gesetzlich detailliert geregelt. Es gibt nur wenige Ausnahmen (siehe Abschnitt 5). Sobald personenbezogene Daten für neue Zwecke verarbeitet werden, lebt die Informationspflicht wieder auf (siehe Abschnitt 6). Eine korrekte Umsetzung bedarf einiger Vorarbeiten (siehe Abschnitt 1). Fehlerhafte, verspätete, unverständliche, unvollständige, fehlende oder anderweitig nicht gesetzeskonforme Informationen können Bußgelder nach sich ziehen (siehe Abschnitt 7).

1. Direkte und indirekte Erhebung

Um die Informationspflicht auszulösen, müssen personenbezogene Daten „erhoben“ werden. Werden Daten im rechtlichen Sinne nicht „erhoben“, besteht auch keine Informationspflicht. Da nicht jede Form des Erlangens, d.h. der technischen Erhebung, auch rechtlich eine „Erhebung“ darstellt, lohnt sich eine nähere Beschäftigung mit dem Begriff „Erheben“.

Von einer „Erhebung“ im rechtlichen Sinn wird gesprochen, wenn sich das Unternehmen Daten aktiv beschafft. Füllt bspw. ein Bewerber einen Bewerberfragebogen aus, so erfragt das Unternehmen von ihm Daten. Es liegt eine Erhebung vor. Anders verhält es sich, wenn beispielsweise ein Bewerber im Aufzug ungefragt von seinen Hobbys erzählt, dann handelt es sich um eine aufgedrängte Information. Das „Sich beschaffen“-Wollen durch das Unternehmen fehlt. Wenn im nachfolgenden Vorstellungsgespräch Fragen zu den im Aufzug erwähnten Hobbys gestellt werden, liegt jedoch wieder eine Erhebung vor.

Auf die Art und Weise der Erhebung kommt es nicht an, d.h. es reicht, dass für die betroffene Person erkennbar ist, welche Daten von ihr verlangt werden. Eine Bewerbung auf eine Stellenanzeige hin ist regelmäßig eine Erhebung, eine unverlangt erhaltene Initiativbewerbung dagegen erst dann, wenn sie wie eine Bewerbung gesichtet wird. Wird sie ungelesen zurückgesandt, liegt keine Erhebung vor.

Werden Daten bei der betroffenen Person erhoben, spricht man von einer Direkterhebung. Eine indirekte Erhebung liegt vor, wenn die Daten nicht bei der betroffenen Person erhoben werden. Beispiele für indirekte Erhebungen sind

- Gespräche mit früheren Arbeitgebern,
- Bonitätsprüfung und
- Sicherheitsüberprüfungen.

Auch die Abfrage des Xing- oder Facebook-Profils eines Bewerbers kann unter die indirekte Erhebung fallen, sofern der Bewerber in seiner Bewerbung nicht explizit auf sein Profil verweist.

2. Zeitpunkt

Der vorgeschriebene Zeitpunkt der Information unterscheidet sich zwischen Direkterhebung und indirekter Erhebung.

2.1 Direkterhebung

Die Information muss „zum Zeitpunkt der Erhebung“ erfolgen. Bei einer Datenerhebung mittels eines (elektronischen) Formulars ist der Zeitpunkt einfach bestimmbar. Sobald das Formular auf dem Bildschirm angezeigt wird, beginnt die Erhebung, die mit dem Absenden des Formulars abgeschlossen ist. Die Information kann bspw. als Erläuterung oder im Rahmen einer Einleitung ins Formular integriert werden.

Als Faustregel mag gelten, dass der Zeitpunkt der Erhebung beendet ist, sobald die Daten beim Unternehmen eingetroffen sind oder Mitarbeiter sie zur Kenntnis nehmen könnten. Bei E-Mail-Bewerbungen ist die Erhebung mit Zugang zum E-Mail-Postfach des Empfängers abgeschlossen. Die Informationspflicht ließe sich bspw. durch eine entsprechend automatisch erzeugte E-Mail – analog einer Eingangsbestätigung – umsetzen. Eine solche Gestaltung bietet sich insbesondere bei E-Mail-Adressen an, die ausschließlich für Bewerbungen gedacht sind, z.B. „karriere@unternehmen.de“.

* Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (einem Gemeinschaftsunternehmen des BvD e.V und der GDD e.V.). Er verfügt über langjährige Erfahrung als externer Datenschutzbeauftragter und berät sowohl deutsche als auch internationale Unternehmen. Daneben lehrt er im Rahmen eines Lehrauftrags im Masterstudiengang „Medienrecht und Medienwirtschaft“ an der Technischen Hochschule Köln.

Bei E-Mails, die an ein allgemeines Postfach gerichtet sind, bspw. „info@unternehmen.de“, endet die Erhebung mit einer Sichtung durch einen Mitarbeiter, der dabei den Zweck identifiziert. E-Mails an allgemeine Postfächer dienen üblicherweise zahlreichen Zwecken wie z.B. Angebotsanfragen, Beschwerden, Werbung, Initiativbewerbungen oder Rückfragen. Die Informationspflicht kann durch einen manuellen Versand der Informationen unmittelbar nach Zweckfeststellung durch einen Mitarbeiter umgesetzt werden. Dabei ist darauf zu achten, dass die versendeten Informationen zu dem Zweck der E-Mail passen, d.h. eine Information für Bewerber beispielsweise nicht auf eine Angebotsanfrage hin versendet wird.

2.2 Indirekte Erhebung

Lässt sich der Erhebungszeitpunkt bei einer direkten Erhebung relativ eindeutig bestimmen, so liegt dieser bei einer indirekten Erhebung regelmäßig in der Vergangenheit. Der „Datenlieferant“ hat die Daten in der Vergangenheit erhoben, die das Unternehmen heute erhält. Deshalb räumt die DS-GVO bei indirekten Erhebungen eine Frist zur Information ein.

Die betroffene Person ist innerhalb einer angemessenen Frist nach Erhalt der Daten, die einen Monat nicht überschreiten darf, zu informieren.[1] „Angemessen“ bedeutet in der Praxis so schnell wie möglich. Werden die bei der indirekten Erhebung erlangten Daten für die Kommunikation mit der Person, z.B. dem Bewerber, verwendet, muss die Person auch früher – nämlich spätestens bei der ersten Kommunikation – informiert werden (Art. 14 Abs. 3 lit. c). Sollen die erhobenen Daten anderen Unternehmen, z.B. innerhalb eines Konzerns, übermittelt werden, so muss die Person spätestens *vor* der Übermittlung informiert werden.[2]

Funktionspostfächer, die von verschiedenen Unternehmen innerhalb eines Konzerns gelesen oder automatisch an diese weitergeleitet werden, stellen im Regelfall eine Übermittlung dar. Je nach technischer Umsetzung schrumpft der Zeitraum zwischen Eingang der Initiativbewerbung und ihrer Übermittlung auf wenige Millisekunden. Wenn solche Funktionspostfächer eindeutigen Zwecken, wie Bewerbungen, dienen, ließe sich die Information beim E-Mail-Eingang automatisiert versenden. Auch wenn die Zwecke nicht feststehen oder zu verschieden sind, wie bei dem Beispiel info@unternehmen.de, müsste die Information trotzdem automatisiert *vor der* Übermittlung erfolgen. Dieses bedeutet u. U. eine sehr umfangreiche Information, deren Länge sie wieder unverständlich und damit unzulässig macht.

Solche gemeinsam genutzten Funktionspostfächer können auch eine gemeinsame Verantwortung verschiedener Unternehmen begründen (Art. 26 DS-GVO). Eine solche „gemeinsame Verantwortung“ zieht zusätzlich rechtliche Pflichten nach sich, zu denen auch eine erweiterte Informationspflicht gehört. Um diese zusätzlichen Pflichten und die skizzierten Risiken zu vermeiden, bietet es sich an, die Funktionspostfächer statt konzernweit („karriere@konzern.de“) unternehmensspezifisch (karriere@deutsche-tochter.de“) zu gestalten.

3. Form und Sprache

Das Unternehmen darf die Form der Information wählen. Zur Auswahl stehen die Schriftform, d.h. auf Papier, oder eine anderen Form, d.h. im Regelfall elektronische Optionen. Eine mündliche Information ist nur auf explizites Verlangen der betroffenen Person zulässig (Art. 12 Abs. 1 DS GVO) Angesichts der Informationsfülle (siehe Abschnitt 4) sowie der problematischen Nachweisbarkeit der Vollständigkeit ist eine mündliche Information nicht empfehlenswert. Die Wahlfreiheit hat den Vorteil, dass die Informationen in dem gleichen Medium erfolgen können, in dem auch die Daten erhoben werden, bspw. als Merkblatt, das zusammen mit einem Papierfragebogen ausgehändigt wird.

Die Information muss in „leicht zugänglicher Form“ dargeboten werden, d.h. die betroffene Person, z.B. der Bewerber oder Mitarbeiter, muss auf sie aufmerksam gemacht werden. Ein „Verstecken“ in anderen Texten wird tendenziell unzulässig sein. Das Gleiche gilt für eine leseunfreundliche Gestaltung, wie z.B. eine Schrift in Größe 8-Punkt oder eine fehlende Absatzstrukturierung.

Eine größere Herausforderung liegt in der Sprache, denn die Darstellung muss in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache erfolgen (Art. 12 Abs. 1 DS-GVO). Da die Information vom Leser verstanden werden soll, sollten sich die Sprache und die Darstellung nach dessen Sprachkenntnissen und Verständnismöglichkeiten richten.

Es empfiehlt sich, die Sprache, bspw. Deutsch oder Englisch, für jeden Mitarbeiter zu wählen, in der auch die für ihn gültigen Arbeitsanweisungen und vergleichbare Dokumente verfasst sind. Für Bewerber kann analog verfahren werden. Für multinationale Unternehmen bedeutet dies, dass die Informationen in verschiedenen Sprachen dargeboten werden müssen. Struktur und Inhalt lassen sich zentral festgelegen und steuern.

Neben der Sprache entscheidet auch die Formulierung über die Verständlichkeit. Soll sich bspw. die Information an Bewerber sowohl auf Schülerpraktika als auch auf Positionen in der Rechtsabteilung beziehen – was zulässig wäre –, ist eine Orientierung an den Schülern empfehlenswert. Eine verständliche Gestaltung lässt sich z.B. durch eine gemeinsame Gestaltung mit der Zielgruppe, Azubis, Lagerarbeiter, Sachbearbeiter usw., oder durch einen Test durch die betroffenen Personen erreichen.

Bildsymbole („Icons“) dürfen im Prinzip verwendet werden.[3] Elektronische Icons müssen in maschinenlesbarer Form vorliegen, die eine automatische Auswertung erlaubt (Art. 12 Abs. 7 DS-GVO). Die EU-Kommission ist ermächtigt, diese Icons zu standardisieren. Entsprechende standardisierte Icons liegen aktuell nicht vor, so dass auf die Verwendung von Icons verzichtet werden sollte. Unternehmen müssen nachweisen können, dass die Darbietung der Information den gesetzlichen Vorgaben der DS-GVO genügt.

1 Art. 14 Abs. 3 Lit. a DS-GVO.

2 Art. 14 Abs. 3 Lit. c DS-GVO.

3 Art. 12 Abs. 7 DS GVO.

4. Inhalt

Da sich die Inhalte der Informationspflicht nur unwesentlich zwischen Direkterhebung und indirekter Erhebung unterscheiden, bietet sich eine kombinierte Information an. Tabelle 1 listet die darzubietenden Informationen auf. Die Kreuze in der zweiten und dritten Spalte zeigen an, dass die entsprechende Angabe jeweils bei einer Direkterhebung oder einer indirekten Erhebung zu machen ist.

Die Angabe der Zwecke setzt eine gründliche Recherche im Unternehmen voraus. Das Beispiel des Mitarbeiters Herrn Maus illustriert die Problemstellung. Die Daten von Herrn Maus werden zur Erfüllung des Arbeitsvertrags verarbeitet, d.h. für die Entgeltabrechnung, Leistungsbeurteilung, Beförderung usw. Herr Maus bedient eine Fräsmaschine. Seine Urlaubs- und Krankheitszeiten werden für die Schichtplanung benötigt. Er zeichnet die Laufkarten der einzelnen Arbeitsaufträge für die Qualitätssicherung ab. Seine Daten zu Alter und Qualifikation werden für die mittelfristige Personalplanung ausgewertet. Eine Auswertung von Fehlzeiten soll „Blaumacher" entdecken helfen. Die Produktentwicklung nutzt seine Bearbeitungszeiten einzelner Werkstücke

Inhalt	Direkterhebung	Indirekte Erhebung
Firmierung des Unternehmens	X	X
Kontaktdaten des Unternehmens	X	X
Name und Kontaktdaten des Vertreters (nur bei Unternehmen ohne Niederlassung/Sitz in der EU)	X	X
Name und Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden)	X	X
Alle Zwecke der Datenverarbeitung	X	X
Nennung der gesetzlichen Legitimation, die Daten zu verarbeiten	X	X
Bei Interessensabwägungen nach Art. 6 Abs. 1 Lit. f DS-GVO: – Berechtigte Interessen des Unternehmens oder Dritter und – Hinweis auf Widerspruchsrecht gegen die Interessensabwägung im Einzelfall	X	X
Empfänger der Daten	X	X
Bei Transfer außerhalb des EWRs: – Existenz oder Fehlen einer Angemessenheitsentscheidung der EU-Kommission und – Verwendete Standardverträge oder Binding Corporate Rules inkl. Angabe, wie eine Kopie erhalten werden kann, und – bei Interessensabwägungen ohne angemessene Schutzmaßnahmen (Angemessenheitsentscheidung, EU-Standardverträge, Binding Corporate Rules): Tatsache des Drittstaatentransfers und die legitimen Interessen des Unternehmens	X	X
Speicherfrist oder Kriterien, um die Frist zu bestimmen	X	X
Hinweis auf die Rechte auf Auskunft, Berichtigung, Löschung, Beschränkung, Widerspruch, Datenportabilität	X	X
Bei Einwilligungen: Widerrufsmöglichkeit	X	X
Hinweis auf das Beschwerderecht gegenüber der Datenschutzaufsichtsbehörde	X	X
Datenquellen		X
Angabe, ob die Datenquelle öffentlich zugänglich ist		X
Ob die Angabe der Daten eine gesetzliche oder vertragliche Pflicht ist oder notwendig, einen Vertrag zu schließen	X	
Ob die Angabe der Daten verpflichtend ist oder nicht und was die Konsequenzen bei Nichtangabe sind	X	
Bei automatischen Entscheidungen nach Art. 22 Abs. 1, 4 DS-GVO: – Existenz des Entscheidungsmechanismus und – aussagekräftige Darstellung der Entscheidungslogik und – Bedeutung und Konsequenzen für den Bewerber	X	X
Widerspruchsrecht gegen Direktmarketingmaßnahmen	X	X

Tabelle 1: Übersicht über die Inhalte der Informationspflicht[4].

4 Zusammengestellt aus Art. 13, 14, 21 Abs. 4 DS-GVO.

zur Produktoptimierung hinsichtlich kürzerer Herstellungszeiten. Die Liste der Zwecke ist in keiner Weise vollständig. Sie umfasst folgende unterschiedliche Zwecke:

- Erfüllung des Arbeitsvertrags,
- Schichtplanung,
- Qualitätssicherung,
- Personalplanung,
- Auswertung von Fehlzeiten und
- Produktentwicklung.

Die Angabe „Speicherfrist oder Kriterien, um die Frist zu bestimmen" verlangt regelmäßig eine komplexe Umsetzung. Die Speicherfrist gibt an, wie lange die Daten im Unternehmen vorhanden sein werden. Eventuell bestehende gesetzliche Aufbewahrungsfristen sind einzurechnen. Die Speicherfrist bezieht sich nicht auf eine konkrete Anwendung, sondern umfasst alle Anwendungen, Speichermedien und auch das Back-up des Unternehmens. E-Mails oder Dateien auf dem Fileserver sind ebenfalls zu berücksichtigen.

Da personenbezogene Daten zwingend unaufgefordert und unverzüglich zu löschen sind, sobald ihre Zwecke entfallen sind, d.h. sie nicht mehr für konkret benennbare Zwecke benötigt werden, bestimmen die Zwecke die Speicherfrist maßgeblich. Mitarbeiterdaten werden, wie oben dargestellt, für zahlreiche Zwecke verarbeitet. Jedoch sind pro Zweck meistens nur wenige Daten betroffen. Die Stammdaten werden mindestens während der Dauer des Arbeitsverhältnisses benötigt. Eine E-Mail mit Rückfragen zur Gehaltsabrechnung braucht bspw. – wenn überhaupt – nur wenige Tage gespeichert zu werden. Deshalb ist eine Betrachtung und Darstellung der Speicherfrist auf Datenfeldebene unumgänglich. Eine Darstellung im Rahmen der Information muss also die Zwecke und die betroffenen Datenfelder einbeziehen.

Unzulässige Darstellungen wären bspw.:

- „im Rahmen der gesetzlichen Fristen",
- „nach Ablauf der gesetzlichen Aufbewahrungsfristen",
- „wenn die Zwecke entfallen sind" und
- „nach zehn Jahren" ohne Nennung des Fristbeginns.

Zulässige Darstellungen könnten bspw. sein:

- „Daten für die Entgeltzahlung: 6 Jahre nach Ausscheiden" oder
- „Angaben auf Laufkarten: bis zum 23.05.2017".

Sollte bis dato keine Datenlöschung stattfinden, ist jetzt die Zeit gekommen umzudenken. Auch nach bisherigem Recht besteht die gesetzliche Löschpflicht, d.h. die Löschpflicht ist keine Neuerung. Neu sind das gestiegene Entdeckungsrisiko und die maximale Bußgeldhöhe (siehe Abschnitt 7). Wer nicht löscht, muss entweder bei der Angabe der Speicherfrist falsche Angaben machen oder ehrlicherweise schreiben „nie". Im ersten Fall wissen mindestens die mit der entsprechenden Datenverarbeitung betrauten Mitarbeiter, dass die Angaben falsch sind. Diese könnten eine Anzeige bei der Datenschutzaufsichtsbehörde einreichen. Im letzten Fall muss ein Mitarbeiter das Informationsschreiben nur einer Aufsichtsbehörde vorlegen, die damit bereits den Nachweis des Gesetzverstoßes „schwarz auf weiß" vorliegen hätte. Die Informationsschreiben müssen zwingend auf die Beschwerderechte hinweisen – auch bei unzufriedenen Mitarbeitern.

5. Ausnahmen

Bei der Direkterhebung kann von einer Information abgesehen werden, wenn die betroffene Person, bspw. der Bewerber oder Mitarbeiter, bereits über die Informationen verfügt.[5] Er muss dazu über alle Informationen vollständig verfügen. Verfügt er über einen Teil der Informationen, muss er mindestens über die ihm unbekannten Angaben unterrichtet werden. Aus Praktikabilitätsgründen bietet sich eine einheitliche und standardisierte Information ohne Rücksicht auf den Informationsstand an. Ein Blick in die Liste von Tabelle 1 zeigt, dass im Regelfall ein Mitarbeiter oder Bewerber bspw. keine Kenntnis über die Speicherfrist der Daten oder alle Zwecke hat, so dass die Informationspflicht auflebt.

Auf eine Information bei indirekten Erhebungen kann verzichtet werden, wenn[6]

- die betroffene Person alle Informationen hat (wie auch schon bei der Direkterhebung),
- das Informieren unmöglich oder unverhältnismäßig aufwendig ist,
- die Erhebung oder auch die Weitergabe der Daten explizit gesetzlich vorgeschrieben ist oder
- in Fällen, in denen die Daten unter ein Berufsgeheimnis fallen.

Die Ausnahmen „unverhältnismäßiger Aufwand" oder Unmöglichkeit dürften bei Bewerbern oder Mitarbeitern höchstens in besonderen Konstellationen zutreffen. Der Abgleich mit EU-Terrorlisten käme als Ausnahme in Betracht, da die EG-Verordnung Nr. 881/2002 diesen vorschreibt. Rechtsanwälte sind Berufsgeheimnisträger, weshalb ein Anwalt über den Empfang personenbezogener Daten nicht informieren muss. Ein Unternehmen hingegen sollte generell Anwälte als mögliche Datenempfänger nennen, da gerade arbeitsrechtliche Auseinandersetzungen immer wieder vorkommen.

6. Informationspflichten bei neuen Zwecken

Sobald Daten für andere Zwecke als die, für die sie erhoben wurden, verarbeitet werden sollen, lebt die Informationspflicht wieder auf.[7] Ob die Daten ursprünglich direkt oder indirekt erhoben wurden, ist dabei unerheblich. Beispiele für neue Zwecke sind:

5 Art. 13 Abs. 4 DS-GVO.

6 Art. 14 Abs. 5 DS-GVO: Eine gemeinsame Verantwortung kann bspw. dann vorliegen, wenn eine Bewerbung von unterschiedlichen Konzerngesellschaften im eigenen Interesse verarbeitet wird.

7 Art. 13 Abs. 3 und Art. 14 Abs. 4 DS-GVO.

- Auswertung von Stellenbörsen nach Bewerberqualität,
- Messung der durchschnittlichen Dauer des Bewerbungsprozesses,
- nachträgliche Aufnahme in einen Bewerbungsprozess oder
- Nutzung von Mitarbeiterdaten für Zufriedenheitsumfragen.

Ein häufiges „Nachschieben" von neuen Zwecken führt schnell zu Irritationen und Misstrauen. Deshalb lohnt es sich, bei der Zusammenstellung der Zwecke nicht nur den Status quo zu betrachten, sondern auch einen Blick in die (nahe) Zukunft zu werfen. Welche Zwecke kommen in den nächsten 12 Monaten dazu? Das Aufzählen aller denkbaren Zwecke ist jedoch nicht empfehlenswert, da ein Verstoß gegen das Gebot zur Transparenz droht.[8] Die betroffene Person soll sich ein Bild über die tatsächliche Datenverarbeitung machen können.

7. Folgen bei einem Verstoß

Ein Verstoß gegen die Informationspflichten ist bußgeldbewehrt. Unvollständige, verspätete, unrichtige, unverständliche, unleserliche und fehlende Informationen zählen zu den Verstößen. Das Unternehmen muss zudem nachweisen, dass es die Informationspflicht korrekt erfüllt. Misslingt der Nachweis, liegt ein Verstoß gegen die Nachweispflicht vor. Deshalb empfiehlt es sich, die Umsetzung der Informationspflicht zu dokumentieren.

Verstöße gegen die Informationspflicht oder die Nachweispflicht können mit einem Bußgeld von bis zu 20 Mio. Euro oder – sofern höher – 4 Prozent des weltweiten Jahresumsatzes bestraft werden. Das gleiche Bußgeld droht ebenfalls bei unterlassener Datenlöschung.

8 Art. 5 Abs. 1 Lit. a DS-GVO.

Einige Aspekte der DS-GVO, des DS-AnpUG und des Beschäftigtendatenschutzes

Prof. Peter Gola, Königswinter*

Redaktioneller Hinweis: Das DS-AnpUG wurde vom Bundeskabinett am 01.02.2017, d.h. dem Tage der Drucklegung dieses Heftes in einer gegenüber der hiesigen Darstellung teilweise erweiterten Fassung in das Gesetzgebungsverfahren eingebracht. Die hier erörterten Aspekte gelten auch für den überarbeiteten Gesetzestext.

1. Vorbemerkung

Ein sich zu dieser Zeit noch in der Ressortabstimmung befindliche Entwurf des EU-DS-AnpUG,[1] dessen Artikel 1 ein ab dem 25.5.2018 geltendes BDSG-neu enthält, wurde vom BMI am 23.11.2016 den Verbänden etc. zur kurzfristigen Stellungnahme zugeleitet. Die Stellungnahmen sind – wie nicht anders zu erwarten war – unterschiedlich ausgefallen. Während einerseits praxisgerechte Verbesserungen, die u.a. in der „Wiederbelebung" von BDSG-Recht bestehen, begrüßt wurden,[2] sehen andere den Datenschutzstandard in Deutschland gefährdet.

Zutreffend ist die Kritik aber in zwei Aspekten. Das Gesetz erscheint aufgrund der gleichzeitigen Umsetzung von Datenschutz-Grundverordnung und JI-Richtlinie[3] strukturell unübersichtlich und für den Rechtsanwender schwer verständlich. Zusätzliche Verwirrung wird dadurch erzeugt, dass die Möglichkeit, Teile der Verordnung, „soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen" (ErwG 8), zu wiederholen, in extensiver und keineswegs zur Verständlichkeit beitragender Weise genutzt wird.

Weitgehend einheitlich ist die Kritik auch darin, dass mit der Zusammenführung der DS-GVO und des alten Bundesdatenschutzgesetzes neue Auslegungs- und Anwendungsfragen entstehen,[4] die unter Umständen zu langwierigen

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

1 Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DS-AnpUG-EU).

2 Https://www.gdd.de/downloads/gdd.stellungnahme.

3 Die parallel mit der DS-GVO verabschiedete Richtlinien „Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. L 119 vom 4. Mai 2016, S. 89 ff.), sollen umgesetzt werden, soweit die Mitgliedstaaten nach Artikel 63 der Richtlinie verpflichtet sind, bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu erlassen, die erforderlich sind, um dieser Richtlinie nachzukommen.

4 Vgl. z.B. Stellungnahme eco-Verband der Intenetwirtschaft e.V. https://www.eco.de/wp-content/blogs.dir/20161207_eco_stn_dsanpg-eu_fin.

Rechtsstreitigkeiten führen können. Die Wirtschaft soll mit einem neuen Bundesdatenschutzgesetz zwar gestärkt werden, gleichzeitig werde aber mit ggf. den Gestaltungsraum des nationalen Gesetzgebers überschreitenden Regelungen auch ein massives Risiko geschaffen. Nach dem Eindruck *Wybituls*[5] wird auf Kosten der Rechtssicherheit die Strategie, möglichst viel im BDSG-neu zu regeln und im Zweifel den EuGH entscheiden zu lassen, ob es mit der Datenschutz-Grundverordnung vereinbar ist.

2. Die Fortschreibung des § 32 BDSG im BDSG-neu

Fraglich ist, ob diese Aussage auch für die Absicht des BMI zutrifft, § 32 BDSG, als bisherige Minimal-Regelung des Beschäftigtendatenschutzes, in § 24 BDSG-neu als eine in Artikel 88 Abs. 1 DS-GVO gestattete „spezifizierende" nationale Regelung zur Datenverarbeitung im Beschäftigungskontext ausdrücklich[6] fortgelten zu lassen.

Inhaltlicher Erläuterungen bedarf § 24 BDSG-neu nicht, da er geltendes Recht wiedergibt. Seine Absätze 1 bis 3 entsprechen § 32 BDSG-alt. Absatz 4 übernimmt weitgehend die bisher in § 3 Abs. 11 BDSG-alt enthaltene Begriffsbestimmung des Beschäftigten.

Ergänzende Regelungswünsche hat das BMAS eingebracht. Diese wurden um ein 01.02.2017 verabschiedeten Text berichtigt.

Ergänzender Regelungsentwurf des BMAS:

a) Einwilligung

Die Einwilligung in die Datenverarbeitung im Beschäftigungskontext unterliegt besonderen Anforderungen. Sie muss grundsätzlich schriftlich erteilt werden, und der Arbeitgeber hat den Beschäftigten über den Zweck der Datenverarbeitung und über dessen Widerrufsrecht in Textform aufzuklären. Außerdem ist die Einwilligung nur wirksam, wenn der Beschäftigte diese freiwillig erklärt. Freiwilligkeit soll nach der vorgeschlagenen Regelung nur dann gegeben sein, wenn die Umstände des Einzelfalls, einschließlich des im Beschäftigungsverhältnis bestehenden Abhängigkeitsverhältnisses, berücksichtigt werden. Das Vorliegen rechtlicher oder wirtschaftlicher Vorteile für den Beschäftigten oder gleichgelagerte Interessen bei Beschäftigtem und Arbeitgeber geben Hinweise auf den Maßstab für die Beurteilung der Frage, ob im konkreten Anwendungsfall von Freiwilligkeit ausgegangen werden kann.

b) Kollektivvereinbarungen

Durch die Einfügung eines eigenständigen Absatzes soll klargestellt werden, dass die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses auch auf Grundlage von Kollektivvereinbarungen (Tarifverträge, Betriebs- und Dienstvereinbarungen) zulässig ist. Dabei ist Artikel 88 Absatz 2 DS-GVO zu beachten.

c) Weitere Regelungen

Des Weiteren soll der Beschäftigtenbegriff auch Leiharbeitnehmer im Verhältnis zum Entleiher erfassen. Diese Regelung sowie ein eigenständiger Absatz zu der Verarbeitung besonderer Kategorien personenbezogener Daten von Beschäftigten soll in § 24 BDSG-neu integriert werden.

Das Vorhaben, § 32 BDSG fortzuschreiben, entspricht Vorschlägen der Literatur[7], die darauf verweist, dass § 32 nach der Gesetzesbegründung das Ziel hatte, die bisherige Rechtsprechung des BAG gesetzlich abzusichern und dass diese Absicherung beibehalten werden sollte.[8] Rechtssicherheit werde erreicht, da von der Rechtsprechung in allen Phasen des Beschäftigungsverhältnisses für die dem Arbeitgeber zugestandenen Informationen Kriterien gesetzt wurden.[9] Damit enthalte die Norm gemeinsam mit der dazu ergangenen Rechtsprechung einen funktionierenden und austarierten Regelungsrahmen, der den Anforderungen des Art. 88 DS-GVO genüge.[10]

Keineswegs übersehen wurde dabei, dass § 32 BDSG-alt/§ 24 BDSG-neu Zulässigkeitsregelungen nur für zwei Fälle der Beschäftigtendatenverarbeitung aufstellen. Zum einen werden Datenverarbeitungserlaubnisse erteilt für Verarbeitungen, die erforderlich sind im Rahmen der Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses. Zum anderen werden restriktive Vorgaben für die Überwachung eines der Begehung von Straftaten Verdächtigten gemacht, wobei diese Bestimmung als Spezialfall einer im Rahmen der Durchführung des Beschäftigungsverhältnisses stattfindenden Datenverarbeitung zu verstehen ist.[11]

Konkret heißt dies: Präzisiert und damit verdrängt wird durch § 24 BDSG-neu ausschließlich Art. 6 Abs. 1 lit. b DS-GVO, der zum einen darauf abstellt, dass die Verarbeitung zur Erfüllung eines zwischen dem Verantwortlichen, sprich dem Arbeitgeber und der betroffenen Person, sprich dem Beschäftigten, bestehenden Arbeitsvertrages erforderlich ist, wobei die Bestimmung abweichend vom reinen Wortlaut dahingehend zu verstehen ist, dass sämtliche ein bestehendes Vertragsverhältnis betreffende Verarbeitungen, d.h. alle für den Abschluss, die Durchführung, die Änderung und die Beendigung[12] der Vertragsbeziehung erforderlichen, ge-

5 Wybitul. https://www.udldigital.de/kritik-am-datenschutz-gesetzentwurf/.

6 Von der auch ohne ausdrückliche Regelung weiteren Anwendung des § 32 BDSG und der dazu ergangenen Rechtsprechung nach dem 25.5.2018 geht Maier/Ossoinig, in: Roßnagel (Hrsg.), § 4 Rn. 44 aus.

7 Gola/Pötters/Thüsing, RDV 2016, 57; Kühling/Martini, EuZW 2016, 298; Wybitul, EU-Datenschutzgrundverordnung im Unternehmen, 2016, Rn. 310; so wohl auch Wedde, Datenschutz-Grundverordnung, 2016, 30.

8 BT-Drucks. 16/13657, 35.

9 Maier/Ossoinig, in: Roßnagel (Hrsg.),Europäische Datenschutz-Grundverordnung, § 4 Rn. 44.

10 Wybitul/Sörup/Pötters, ZD 2015, 559 (561).

11 Gola/Schomerus, BDSG § 32 Rn. 39 ff; Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn.1197 ff.

12 Härting, Datenschutz-Grundverordnung, Rn. 420 zählt die Beendigung" noch zur Erfüllung.

meint sind.[13] Zum anderen gestattet Art. 6 Abs. 1 lit. b DS-GVO Verarbeitungen, die im Rahmen der Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen. Die vorvertraglichen Beziehungen zwischen Arbeitgeber und Bewerber, die im Arbeitsrecht im sog. Anbahnungsverhältnis[14] bestehen, fallen unter den genannten Tatbestand.[15] Maßgebend ist in beiden Zulässigkeitsalternativen die Erforderlichkeit der jeweiligen Datenverarbeitung, deren Kriterien nach der DS-RL bzw. dem BDSG und der DS-GVO die gleichen sind.[16] Maßgebend ist ggf. auch hier eine unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes vorzunehmende Interessenabwägung. Käme es nicht zur Verabschiedung des § 24 BDSG-neu, bliebe auch im Rahmen des Art. 6 Abs. 1 lit. b DS-GVO Ausgangspunkt der Zulässigkeitsbetrachtung der auf deutschem Arbeitsrecht beruhende Vertrag, der auch unter der Norm des Art. 6 Abs. 1 lit. b DS-GVO mit seinen Rechten und Pflichten und den für deren Erfüllung erforderlichen Verarbeitungen nicht anders interpretiert werden kann als nach § 32 Abs. 1 S. 1 BDSG bzw. § 24 BDSG-neu. Gleichwohl kann § 24 BDSG-neu als ein diesen Aspekt verdeutlichende Norm hilfreich sein. Mit der Übernahme des § 32 Abs. 1 BDSG in das BDSG-neu bleibt die Bindungswirkung an die BAG-Rechtsprechung beibehalten[17] und die Befugnis des Arbeitgebers zur Überwachung von der Begehung einer Straftat verdächtigten Beschäftigten präzise geregelt.

Die sonstigen Zulässigkeitsregelungen des Art. 6 DS-GVO und der Spezialregelungen für sensible Daten in Art. 9 DS-GVO oder Straftatsdaten in Art. 10 DS-GVO werden durch § 24 BDSG-neu nicht tangiert. Sollen Personaldaten für andere Zwecke, d.h. für sog. beschäftigungsfremde Zwecke, verarbeitet werden, gibt die Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO den Zulässigkeitsrahmen.[18] Gleiches gilt für Art. 22 DS-GVO mit dem Verbot automatisierter Einzelentscheidungen.

Abweichend von dem Geltungsbereich der Verordnung (Art. 2 Abs. 1 DS-GVO) soll § 24 Abs. 1 BDSG-neu – so wie es bisher § 32 Abs. 2 BDSG vorsieht – auch gelten bei nicht automatisierter oder dateistrukturierter Verarbeitung der Beschäftigtendaten (§ 24 Abs. 2 BDSG-neu).[19]

3. Die Kritik

Gegenüber dieser „ausschnittsweisen" Regelung des Beschäftigtendatenschutzes werden nun zunehmend Bedenken geltend gemacht. Nachgefragt wird – weitgehend ohne dies im Detail zu belegen – zum einen, ob die bloße Übernahme des § 32 BDSG den Anforderungen des Art. 88 DS-GVO an bereichsspezifische Vorschriften des Beschäftigtendatenschutzes entspricht, etwa in Bezug auf die dort geforderte Transparenz, Vorhersehbarkeit und Grundrechtegarantie.[20] Gem. Art. 88 Abs. 2 DS-GVO soll eine nationale Regelung zur Verarbeitung von personenbezogenen Daten im Beschäftigungskontext „angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz" umfassen. Davon findet sich zumindest im Wortlaut des Referentenentwurfs nichts.

Zum anderen wird die Ausdehnung der Norm auf „manuelle" Verarbeitungen von einigen Stimmen der Literatur im Hinblick auf das damit beabsichtigte Abweichen vom Schutzniveau der DS-GVO „nach oben" hinterfragt. Indem z.B. auch rein tatsächliche Handlungen erfasst werden,[21] handele es sich nicht mehr um eine dem nationalen Gesetzgeber allein erlaubte „spezifischere" Regelung. Nicht gestattet sei ein Abweichen von der Verordnung sowohl „nach unten" als auch „nach oben".[22] § 24 BDSG-neu sei bezüglich der Ausdehnung seines Anwendungsbereichs nichtig.[23] Andere Stimmen bejahen dagegen die Möglichkeit über die Anforderungen der DS-GVO hinauszugehen.[24] Art. 88 Abs. 1 DS-GVO verbiete allein ein Absenken des Datenschutzniveaus der Verordnung.[25]

4. Berechtigung der Kritik

4.1 Wahrung der berechtigten Interessen und der Grundrechte der betroffenen Person

Art. 24 BDSG-neu will, dass die bisher von der Rechtsprechung des BAG entwickelten Kriterien des Beschäftigtendatenschutzes Bestand haben. Beispiele bieten die beiden jüngsten sich mit einer Mitarbeiterkontrolle befassenden Entscheidungen,[26] die als Teil eines „neuen Datenschutzes", mit dem das Bundesarbeitsgericht u.a. mehr Klarheit bei der Anwendung des § 32 BDSG schaffe, bewertet wurden.[27] Wenngleich das Bundesarbeitsgericht die Lösung der Fälle nicht unter systematisch richtiger Anwendung des § 32

13 Vgl. Gola, in: Gola (Hrsg.), DS-GVO, Art. 6 Rn. 23 f.

14 Vgl. zum Begriff Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn. 611 ff.

15 Gola, in: Gola (Hrsg.), DS-GVO, Art. 6 Rn. 27.

16 Schulz, in: Gola (Hrsg.), DS-GVO, Art. 6 Rn. 34 ff.

17 Wybitul/Pötters, RDV 2016, 10 (14).

18 Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn. 402 ff.

19 Zu den diesbezüglichen Abgrenzungsfragen bei „geordneten" Akten: Gola, in: Gola (Hrsg.), DS-GVO, Art. 4 Rn. 42 ff.; Spelge, DuD 2016, 777 (779).

20 Weichert, http://www.netzwerk-datenschutzexpertise.de/sites/default/files/dvd_dse_bdsg_041216fin.pdf; wohl trotz der Bestätigung der Zweifel positiv: Kort, ZD 2016, 555 (556).

21 Gola, ZBVR-online, 17/2014, 33.

22 Kort, DB 2016, 711 (714).

23 Spelge, DuD 2016, 775 (777).

24 Pauly, in: Paal/Pauly, DS-GVO, Art. 88 Rn. 18; Kort, DB 2016, 771 (714); Wybitul, ZD 2016, 203 (206).

25 Pauly, in: Paal/Pauly, DS-GVO, Art. 88 Rn. 4; so wohl auch Pötters in Gola (Hrsg.), DS-GVO Art. 88 Rn. 20.

26 BAG, RDV 2014, 103 = NZA 2014, 143 (Spindkontrolle); BAG, RDV 2014, 272 = NZA 2014, 551 (Torkontrolle).

27 Brink/Wybitul, ZD 2014, 225; Wybitul, NZA 2014, 225.

BDSG, sondern unter Heranziehung anderer Normen findet, weist es jedoch gleichzeitig darauf hin, dass „die gesetzlichen Anforderungen an eine zulässige Datenverarbeitung im BDSG den Schutz des Rechts auf informationelle Selbstbestimmung konkretisieren und aktualisieren".[28] Das Ergebnis der Entscheidungen, d.h. die Bewertung der Rechtmäßigkeit bzw. Unrechtmäßigkeit der Kontrollmaßnahmen, leitet es zwar aus § 75 Abs. 2 Satz 1 BetrVG bzw. Art. 2 Abs. 1 GG ab, wobei es jedoch die hierbei aufgestellten Prinzipien für allgemeingültig, d.h. zu dem auch bei einer Anwendung des § 32 BDSG geltenden Maßstab, erklärt. Demgemäß heißt es hinsichtlich der Bewertung der heimlichen Durchsuchung eines Mitarbeiterspinds: „Für die Überprüfung der Verhältnismäßigkeit der Durchsuchung des Spinds ergeben sich aus § 32 Abs. 1 S. 2 BDSG gegenüber einer unmittelbar an Art. 2 Abs. 1 GG orientierten Überprüfung der Rechtmäßigkeit des Eingriffs in das Persönlichkeitsrecht des Klägers keine anderen Vorgaben" bzw. zur Rechtmäßigkeit der Betriebsvereinbarung einer Torkontrolle: „Wenn die in einer die Zulässigkeitsregelungen des BDSG verdrängenden Betriebsvereinbarung geregelten Kontrollmaßnahmen einer datenschutz-rechtlichen Kontrolle am Maßstab des § 75 Abs. 2 BetrVG standhalten, sind sie auch mit dem BDSG vereinbar." Damit gewährleistet das BAG die in Art. 88 Abs. 3 DS-GVO geforderten „zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person angemessenen" persönlichkeitsrechtlichen Garantien.[29]

4.2 Transparenz

Nichts gesagt ist in § 24 Abs. 1 S. 2 BDSG-neu zur regelmäßig geheim durchgeführten Überwachung eines potentiellen Straftäters. Sofern die Überwachung im Anwendungsbereich der Verordnung (Art. 2 Abs. 1) stattfindet, greift Art. 14 DS-GVO. Anderenfalls, also z.B. bei der Spindkontrolle[30] oder der Beobachtung durch einen Detektiv[31] oder der Anhörung vor einer Verdachtskündigung[32] gilt wieder der vom BAG den Betroffenen gewährten Persönlichkeitsschutz.

4.3 Der Anwendungsbereich

Die Verordnung gestattet dem nationalen Gesetzgeber für den Beschäftigtendatenschutz, „spezifischere" Regelungen zu schaffen, d.h. solche die nicht nur die die allgemeinen Grundsätze der Verordnung präzisieren, sondern ggf. darüber hinausgehen.[33] Mit § 24 BDSG-neu wird eine eigenständige Norm geschaffen, wie sie für den Beschäftigtendatenschutz auch anderweitig und über den Anwendungsbereich der DS-GVO hinausgehend seit langem bestehen. Bei dem Beschäftigungsdatenschutz handelt es sich um eine Querschnittsmaterie aus Daten- und Arbeitsrecht, wobei die Verordnung die arbeitsrechtlichen Regelungsbefugnisse nicht einschränken kann.[34] Nicht kann davon ausgegangen werden, dass die Regelungen zum Personalaktenrecht in § 83 BetrVG oder die diesbezüglichen Vorschriften des öffentlichen Dienstes nunmehr hinfällig sind. Festzuhalten ist damit mit den bereits genannten Stimmen, dass Art. 88 DS-GVO eine Ausdehnung des Beschäftigtendatenschutzes auf jegliche Art der Datenverarbeitung, d.h. also eine Regelung des Datenschutzes „nach oben", nicht untersagt.

5. Die Meldepflicht

Keine eindeutige Auffassung ist auch aus Art. 88 Abs. 3 DS-GVO oder in der Literatur[35] erkennbar, welche Folge die Missachtung der angeordneten Meldung von nationalen Beschäftigtendatenschutznormen hätte, d.h. ob, wenn keine Meldung vorhandener Normen fristgemäß bei der Kommission erfolgt, die nationale Kompetenz zur Regelung des Beschäftigtendatenschutzes entfällt bzw. nicht gemeldete Normen ihre Geltung verlieren. Des Weiteren bedarf es der Interpretation der Norm dahingehend, ob die Meldepflicht nur nach dem 25.5.2016 erlassene Regelungen betrifft.[36] Die Frage kann hier jedoch dahinstehen, wenn § 24 BDSG-neu erlassen wird. Demgemäß ist die Norm in jedem Falle meldepflichtig. Gleichzeitig ist davon auszugehen, dass die Mitgliedstaaten, die innerhalb der Mitteilungsfrist keine Aktivitäten insoweit gemeldet haben, ihre Rechtssetzungskompetenz verlieren.[37] Ob die gegenteilige Ansicht zutrifft, nach der Art. 88 Abs. 3 DS-GVO nur eine Mitteilungs- und keine Ausschlußfrist ist,[38] wird jedenfalls letztendlich der EuGH[39] zu entscheiden haben, wobei man es hierauf nicht ankommen lassen sollte. Die unsichere Rechtslage spricht dafür, zumindest § 24 BDSG-neu als Grundnormen des Beschäftigungsdatenschutzes zu melden.[40]

28 So BAG RDV 2014, 103 = NZA 2014, 143.

29 Maier/Ossoinig, in: Roßnagel (Hrsg.), Europäische Datenschutz-Grundverordnung, § 4 Rn. 44 ff.

30 BAG, RDV 2014, 103 = NZA 2014, 143.

31 BAG, NZA 2015, 994.

32 BAG, RDV 2014, 328 sowie BAG, NZA 2015, 741.

33 Düwell/Brink, NZA 2016, 665 (666).

34 Körner, NZA 2016, 1383.

35 Ohne Aussage hierzu Stamer/Kuhnke, in: Plath (Hrsg.), DS-GVO, Art. 88 Rn. 11, Pauly, in: Paal/Pauly (Hrsg.), DS-GVO Art. 88 Rn. 16.

36 Zutreffend sind wohl alle nach und vor der Verabschiedung der Verordnung am 25.05.2018 geschaffenen Normen zu melden; vgl. Gola/Pötters/Thüsing, RDV 2016, 57; Pötters, in: Gola (Hrsg.), DS-GVO Art. 88 Rn. 16.

37 Ausführlich dazu Gola/Pötters/Thüsing, RDV 2016, 57.

38 Maier/Ossoinig, in: Roßnagel (Hrsg.),Europäische Datenschutz-Grundverordnung, § 4 Rn. 33; Körner, NZA 2016, 1383 (1386).

39 Körner, NZA 2016, 1383 (1386) verweist auf die vom EuGH (NZA 2015, 423) vorgenommene Einordnung als reine Meldepflicht hinsichtlich der Beurteilung einer ähnlichen Regelung in der Leiharbeitsrichtlinie.

40 Spelge, DuD 2016, 775 (781).

Rechtsprechung

Unzulässigkeit allgemeiner und unterschiedsloser Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten

(**Europäischer Gerichtshof**, Urteil vom 21. Dezember 2016 – C-203/15 und C-698/15 –)

1. **Art. 15 Abs. 1 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) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.**

2. **Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.**

Sachverhalt:

Die Vorabentscheidungsersuchen betreffen die Auslegung von Art. 15 Abs. 1 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) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

Zu den Vorlagefragen

Zur ersten Frage in der Rechtssache C-203/15

62 Mit der ersten Frage in der Rechtssache C-203/15 möchte der Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm) wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung wie der im Ausgangsverfahren streitigen entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.

63 Diese Frage geht u.a. darauf zurück, dass die Richtlinie 2006/24, die mit der im Ausgangsverfahren in Rede stehenden nationalen Regelung umgesetzt werden sollte, mit dem Urteil Digital Rights für ungültig erklärt wurde, die Parteien aber uneins sind über die Tragweite dieses Urteils und seine Auswirkungen auf die nationale Regelung, die für die Vorratsspeicherung von Verkehrs- und Standortdaten sowie für den Zugang der nationalen Behörden zu diesen Daten gilt.

64 Zunächst ist zu prüfen, ob eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende in den Anwendungsbereich des Unionsrechts fällt.

Zum Geltungsbereich der Richtlinie 2002/58

65 Die Mitgliedstaaten, die beim Gerichtshof schriftliche Erklärungen eingereicht haben, vertreten unterschiedliche Standpunkte zu der Frage, ob und inwieweit nationale Regelungen über die Vorratsspeicherung von Verkehrs- und Standortdaten sowie den Zugang der nationalen Behörden zu diesen Daten für Zwecke der Kriminalitätsbekämpfung in den Geltungsbereich der Richtlinie 2002/58 fallen. Während namentlich die belgische, die dänische, die deutsche und die estnische Regierung, Irland und die niederländische Regierung sich dafür ausgesprochen haben, diese Frage zu bejahen, hat die tschechische Regierung vorgeschlagen, sie zu verneinen, weil alleiniger Zweck dieser Regelungen die Kriminalitätsbekämpfung sei. Die Regierung des Vereinigten Königreichs macht geltend, dass in den Geltungsbereich dieser Richtlinie nur Regelungen über die Vorratsdatenspeicherung fielen, nicht aber Regelungen über den Zugang zu den gespeicherten Daten durch die nationalen Strafverfolgungsbehörden.

66 Die Kommission schließlich hat zwar in ihren schriftlichen Erklärungen, die sie beim Gerichtshof in der Rechtssache C-203/15 eingereicht hat, die Ansicht vertreten, dass die im Ausgangsverfahren streitige nationale Regelung in den Geltungsbereich der Richtlinie 2002/58 falle. In ihren schriftlichen Erklärungen in der Rechtssache C-698/15 hingegen hat sie vorgetragen, dass nur nationale Vorschriften über die Vorratsspeicherung von Daten, nicht aber solche über den Zugang der nationalen Behörden zu diesen Daten in den Geltungsbereich der Richtlinie fielen. Diese letztgenannten Vorschriften müssten gleichwohl berücksichtigt werden, um zu beurteilen, ob eine nationale Regelung über die Vorratsdatenspeicherung durch Betreiber elektronischer Kommunikations-

dienste einen unverhältnismäßigen Eingriff in die durch die Art. 7 und 8 der Charta gewährleisteten Grundrechte darstelle.

67 Insoweit ist darauf hinzuweisen, dass für die Bestimmung der Reichweite des Geltungsbereichs der Richtlinie 2002/58 insbesondere deren Systematik zu berücksichtigen ist.

68 Die Richtlinie 2002/58 sieht nach ihrem Art. 1 Abs. 1 u.a. die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation zu gewährleisten.

69 Art. 1 Abs. 3 dieser Richtlinie schließt von ihrem Geltungsbereich die „Tätigkeiten des Staates" in den dort genannten Bereichen aus, d.h. namentlich die Tätigkeiten des Staates im strafrechtlichen Bereich sowie Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates, einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt (vgl. entsprechend, zu Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46, Urteile vom 6. November 2003, Lindqvist, C-101/01, EU:C:2003:596, Rn. 43, sowie vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 41).

70 Nach Art. 3 der Richtlinie 2002/58 gilt diese für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen (im Folgenden: elektronische Kommunikationsdienste). Folglich ist davon auszugehen, dass diese Richtlinie die Tätigkeiten der Betreiber solcher Dienste regelt.

71 Nach Art. 15 Abs. 1 der Richtlinie 2002/58 können die Mitgliedstaaten unter den angegebenen Voraussetzungen „Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken". Art. 15 Abs. 1 Satz 2 der Richtlinie nennt als Beispiel für Vorschriften, die so von den Mitgliedstaaten erlassen werden können, Vorschriften, die „vorsehen, dass Daten ... aufbewahrt werden".

72 Zwar beziehen sich die Rechtsvorschriften, um die es in Art. 15 Abs. 1 der Richtlinie 2002/58 geht, auf spezifische Tätigkeiten der Staaten oder der staatlichen Stellen, die mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun haben (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 51). Zudem decken sich die Zweckbestimmungen, denen die Rechtsvorschriften nach dieser Bestimmung entsprechen müssen – Schutz der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit sowie Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen –, im Wesentlichen mit den Zielen, die mit den in Art. 1 Abs. 3 der Richtlinie genannten Tätigkeiten verfolgt werden.

73 In Anbetracht der Systematik der Richtlinie 2002/58 erlauben jedoch die in der vorstehenden Randnummer dieses Urteils genannten Gesichtspunkte nicht den Schluss, dass die Rechtsvorschriften im Sinne des Art. 15 Abs. 1 dieser Richtlinie von deren Geltungsbereich ausgeschlossen sind, da dieser Bestimmung damit jede praktische Wirksamkeit genommen würde. Art. 15 Abs. 1 der Richtlinie 2002/58 setzt nämlich zwangsläufig voraus, dass die dort genannten nationalen Vorschriften, wie Vorschriften über die Aufbewahrung von Daten für Zwecke der Kriminalitätsbekämpfung, in den Geltungsbereich der Richtlinie fallen, da diese Richtlinie die Mitgliedstaaten zum Erlass solcher Vorschriften ausdrücklich nur dann ermächtigt, wenn die darin vorgesehenen Voraussetzungen eingehalten werden.

74 Außerdem regeln die in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Rechtsvorschriften – zu den in dieser Bestimmung genannten Zwecken – die Tätigkeit der Betreiber elektronischer Kommunikationsdienste. Demnach ist Art. 15 Abs. 1 in Verbindung mit Art. 3 der Richtlinie 2002/58 dahin auszulegen, dass diese Rechtsvorschriften in den Geltungsbereich dieser Richtlinie fallen.

75 In ihren Geltungsbereich fällt insbesondere eine Rechtsvorschrift wie die im Ausgangsverfahren in Rede stehende, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, die Verkehrs- und Standortdaten auf Vorrat zu speichern, da damit zwangsläufig eine Verarbeitung personenbezogener Daten durch die Betreiber verbunden ist.

76 Ebenfalls in ihren Geltungsbereich fällt eine Rechtsvorschrift, die, wie im Ausgangsverfahren, den Zugang der nationalen Behörden zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten betrifft.

77 Der in Art. 5 Abs. 1 der Richtlinie 2002/58 garantierte Schutz der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Verkehrsdaten gilt nämlich für Maßnahmen sämtlicher anderer Personen als der Nutzer, unabhängig davon, ob es sich um private Personen oder Einrichtungen oder um staatliche Einrichtungen handelt. Wie ihr 21. Erwägungsgrund bestätigt, soll die Richtlinie 2002/58 jeden unerlaubten Zugang zu Nachrichten einschließlich zu „mit ihnen verbundenen Daten" verhindern, um die Vertraulichkeit elektronischer Kommunikationen zu schützen.

78 Daher betrifft eine Rechtsvorschrift, mit der ein Mitgliedstaat den Betreibern elektronischer Kommunikationsdienste auf der Grundlage von Art. 15 Abs. 1 der Richtlinie 2002/58 zu den in dieser Bestimmung genannten Zwecken vorschreibt, den nationalen Behörden unter in der betreffenden Rechtsvorschrift vorgesehenen Voraussetzungen den Zugang zu den von ihnen gespeicherten Daten zu gewähren, die Verarbeitung personenbezogener Daten durch die Betreiber, und eine solche Verarbeitung fällt in den Geltungsbereich dieser Richtlinie.

79 Grundsätzlich setzt eine nationale Regelung über die Vorratsdatenspeicherung, da diese allein zu dem Zweck erfolgt, die Daten gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, zwangsläufig voraus, dass es Bestimmungen über den Zugang dieser Behörden zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten gibt.

80 Diese Auslegung wird durch Art. 15 Abs. 1b der Richtlinie 2002/58 gestützt, wonach die Betreiber nach den gemäß Art. 15 Abs. 1 der Richtlinie eingeführten nationalen Vorschriften interne Verfahren zur Beantwortung von Anfragen über den Zugang zu den personenbezogenen Daten der Nutzer einrichten.

81 Nach alledem fällt eine nationale Regelung, wie sie in den Ausgangsverfahren der Rechtssachen C-203/15 und C-698/15 in Rede steht, in den Geltungsbereich der Richtlinie 2002/58.

Zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 im Hinblick auf die Art. 7, 8 und 11 sowie Art. 52 Abs. 1 der Charta

82 Nach Art. 1 Abs. 2 der Richtlinie 2002/58 stellen ihre Bestimmungen eine „Detaillierung und Ergänzung" der Richtlinie 95/46 dar. Wie in ihrem zweiten Erwägungsgrund zum Ausdruck gebracht wird, soll mit der Richtlinie 2002/58 gewährleistet werden, dass die in den Art. 7 und 8 der Charta niedergelegten Rechte uneingeschränkt geachtet werden. Insoweit ergibt sich aus der Begründung des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den

Schutz der Privatsphäre in der elektronischen Kommunikation (KOM[2000] 385 endgültig), aus dem die Richtlinie 2002/58 hervorgegangen ist, dass der Unionsgesetzgeber beabsichtigte, „sicher[zu]stellen, dass für alle elektronischen Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie weiterhin ein hochgradiger Schutz personenbezogener Daten und der Privatsphäre gewährleistet bleibt".

83 Zu diesem Zweck enthält die Richtlinie 2002/58 spezielle Vorschriften, die – wie sich u.a. aus ihren Erwägungsgründen 6 und 7 ergibt – die Nutzer elektronischer Kommunikationsdienste vor den sich aus den neuen Technologien und den zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung von Daten ergebenden Risiken für personenbezogene Daten und die Privatsphäre schützen sollen.

84 Insbesondere sieht Art. 5 Abs. 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch ihre innerstaatlichen Vorschriften sicherzustellen haben.

85 Der mit der Richtlinie 2002/58 eingeführte Grundsatz der Vertraulichkeit von Kommunikationen bedeutet u.a., dass – wie aus Art. 5 Abs. 1 Satz 2 der Richtlinie hervorgeht – es jeder anderen Person als dem Nutzer grundsätzlich untersagt ist, ohne dessen Einwilligung mit elektronischen Kommunikationen verbundene Verkehrsdaten zu speichern. Ausgenommen sind lediglich die gemäß Art. 15 Abs. 1 dieser Richtlinie gesetzlich dazu ermächtigten Personen sowie die für die Weiterleitung einer Nachricht erforderliche technische Speicherung (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 47).

86 Wie die Erwägungsgründe 22 und 26 der Richtlinie 2002/58 bestätigen, dürfen Verkehrsdaten nach Art. 6 der Richtlinie nur zur Gebührenabrechnung für die Dienste, zu deren Vermarktung und zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu erforderlichen Zeitraums verarbeitet und gespeichert werden (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 47 und 48). Was speziell die Gebührenabrechnung für die Dienste betrifft, ist diese Verarbeitung nur bis zum Ende des Zeitraums zulässig, in dem die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann. Danach sind die verarbeiteten und gespeicherten Daten zu löschen oder zu anonymisieren. Andere Standortdaten als Verkehrsdaten dürfen nach Art. 9 Abs. 1 der Richtlinie 2002/58 nur unter bestimmten Voraussetzungen und nur dann verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben.

87 Die Tragweite der Bestimmungen der Art. 5, 6 und 9 Abs. 1 der Richtlinie 2002/58, die die Vertraulichkeit von Kommunikationen und der damit verbundenen Daten gewährleisten und Missbrauchsrisiken verringern sollen, beurteilt sich außerdem unter Berücksichtigung des 30. Erwägungsgrundes der Richtlinie, wonach „[d]ie Systeme für die Bereitstellung elektronischer Kommunikationsnetze und -dienste … so konzipiert werden [sollten], dass so wenig personenbezogene Daten wie möglich benötigt werden".

88 Zwar erlaubt Art. 15 Abs. 1 der Richtlinie 2002/58 den Mitgliedstaaten, Ausnahmen von der in Art. 5 Abs. 1 der Richtlinie aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten und den entsprechenden, u.a. in den Art. 6 und 9 der Richtlinie genannten Pflichten vorzusehen (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 50).

89 Gleichwohl ist Art. 15 Abs. 1 der Richtlinie 2002/58, da er den Mitgliedstaaten erlaubt, die Tragweite der grundsätzlichen Verpflichtung, die Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Verkehrsdaten zu gewährleisten, einzuschränken, nach der ständigen Rechtsprechung des Gerichtshofs eng auszulegen (vgl. entsprechend Urteil vom 22. November 2012, Probst, C-119/12, EU:C:2012:748, Rn. 23). Eine solche Bestimmung vermag es daher nicht zu rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Verpflichtung und insbesondere von dem in Art. 5 der Richtlinie 2002/58 vorgesehenen Verbot, diese Daten zu speichern, zur Regel wird, soll die letztgenannte Vorschrift nicht weitgehend ausgehöhlt werden.

90 Insoweit ist darauf hinzuweisen, dass Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vorsieht, dass die in dieser Bestimmung genannten Rechtsvorschriften, die vom Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweichen, „die nationale Sicherheit (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen" zum Ziel haben müssen oder einen der anderen Zwecke verfolgen müssen, die in Art. 13 Abs. 1 der Richtlinie 95/46, auf den Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 verweist, genannt sind (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 53). Hierbei handelt es sich um eine abschließende Aufzählung der Zwecke, wie aus Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58 hervorgeht, wonach die Rechtsvorschriften aus den in Art. 15 Abs. 1 Satz 1 dieser Richtlinie „aufgeführten Gründen" gerechtfertigt sein müssen. Die Mitgliedstaaten dürfen demnach solche Vorschriften nicht zu anderen als den in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 aufgezählten Zwecken erlassen.

91 Außerdem müssen nach Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58 „[a]lle in [Art. 15 Abs. 1 dieser Richtlinie] genannten Maßnahmen … den allgemeinen Grundsätzen des [Unions]rechts einschließlich den in Artikel 6 Absätze 1 und 2 [EU] niedergelegten Grundsätzen entsprechen", zu denen die allgemeinen Grundsätze und die Grundrechte gehören, die nunmehr durch die Charta gewährleistet werden. Art. 15 Abs. 1 der Richtlinie 2002/58 muss somit im Licht der von der Charta garantierten Grundrechte ausgelegt werden (vgl. entsprechend, zur Richtlinie 95/46, Urteile vom 20. Mai 2003, Österreichischer Rundfunk u.a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 68, vom 13. Mai 2014, Google Spain und Google, C-131/12, EU:C:2014:317, Rn. 68, sowie vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 38).

92 In diesem Zusammenhang ist hervorzuheben, dass die den Betreibern elektronischer Kommunikationsdienste durch eine nationale Regelung, wie sie im Ausgangsverfahren in Rede steht, auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um diese gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die nicht nur die Einhaltung der in den Vorlagefragen ausdrücklich erwähnten Art. 7 und 8 der Charta, sondern auch die Einhaltung der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung betreffen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 25 und 70).

93 Folglich muss die Bedeutung sowohl des in Art. 7 der Charta gewährleisteten Grundrechts auf Achtung des Privatlebens als auch des in Art. 8 der Charta gewährleisteten Grundrechts auf Schutz personenbezogener Daten, wie sie sich aus der Rechtsprechung des Gerichtshofs ergibt (vgl. in diesem Sinne Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 39 und die dort angeführte Rechtsprechung), bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 berücksichtigt werden. Das Gleiche gilt in Anbetracht der besonderen Bedeutung, die der Freiheit der Mei-

nungsäußerung in jeder demokratischen Gesellschaft zukommt, für das Recht auf freie Meinungsäußerung. Dieses in Art. 11 der Charta gewährleistete Grundrecht stellt eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft dar, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet (vgl. in diesem Sinne Urteile vom 12. Juni 2003, Schmidberger, C-112/00, EU:C:2003:333, Rn. 79, und vom 6. September 2011, Patriciello, C-163/10, EU:C:2011:543, Rn. 31).

94 Insoweit ist darauf hinzuweisen, dass nach Art. 52 Abs. 1 der Charta jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und Wesensgehalt dieser Rechte und Freiheiten achten muss. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen der Ausübung dieser Rechte und Freiheiten nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (Urteil vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 50).

95 Was den letztgenannten Gesichtspunkt betrifft, sieht Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten eine Vorschrift erlassen können, die von dem Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweicht, sofern dies in Anbetracht der dort genannten Zwecke „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ ist. Im elften Erwägungsgrund dieser Richtlinie wird klargestellt, dass eine derartige Maßnahme in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss. Was speziell die Vorratsspeicherung von Daten betrifft, verlangt Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58, dass diese nur „während einer begrenzten Zeit“ und „aus den“ in Art. 15 Abs. 1 Satz 1 der Richtlinie aufgeführten Gründen erfolgen darf.

96 Dass der Grundsatz der Verhältnismäßigkeit zu beachten ist, ergibt sich ebenfalls aus der ständigen Rechtsprechung des Gerichtshofs, wonach der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken (Urteile vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 56, vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 77, Digital Rights, Rn. 52, sowie vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 92).

97 Hinsichtlich der Frage, ob eine nationale Regelung wie die in der Rechtssache C-203/15 in Rede stehende diesen Voraussetzungen genügt, ist festzustellen, dass sie eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht und die Betreiber elektronischer Kommunikationsdienste verpflichtet, diese Daten systematisch und kontinuierlich auf Vorrat zu speichern, und zwar ausnahmslos. Wie aus der Vorlageentscheidung hervorgeht, entsprechen die von dieser Regelung erfassten Datenkategorien im Wesentlichen denen, deren Vorratsspeicherung nach der Richtlinie 2006/24 vorgesehen war.

98 Die Daten, die somit von den Betreibern elektronischer Kommunikationsdienste auf Vorrat zu speichern sind, ermöglichen die Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie die Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte. Zu diesen Daten gehören Name und Anschrift des Teilnehmers oder registrierten Benutzers, die Rufnummer des anrufenden und des angerufenen Anschlusses sowie bei Internetdiensten eine IP-Adresse. Aus diesen Daten geht insbesondere hervor, mit welcher Person ein Teilnehmer oder registrierter Benutzer auf welchem Weg kommuniziert hat, wie lange die Kommunikation gedauert hat und von welchem Ort aus sie stattfand. Ferner ist ihnen zu entnehmen, wie häufig der Teilnehmer oder registrierte Benutzer in einem bestimmten Zeitraum mit bestimmten Personen kommuniziert hat (vgl. entsprechend, in Bezug auf die Richtlinie 2006/24, Urteil Digital Rights, Rn. 26).

99 Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 27). Diese Daten ermöglichen insbesondere – wie der Generalanwalt in den Nrn. 253, 254 und 257 bis 259 seiner Schlussanträge ausgeführt hat – die Erstellung des Profils der betroffenen Personen, das im Hinblick auf das Recht auf Achtung der Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikationen selbst.

100 Der mit einer solchen Regelung verbundene Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte ist von großem Ausmaß und als besonders schwerwiegend anzusehen. Der Umstand, dass die Vorratsspeicherung der Daten vorgenommen wird, ohne dass die Nutzer der elektronischen Kommunikationsdienste darüber informiert werden, ist geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 37).

101 Auch wenn eine solche Regelung nicht die Vorratsspeicherung des Inhalts einer Kommunikation erlaubt und folglich nicht den Wesensgehalt der vorgenannten Grundrechte antastet (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 39), könnte die Vorratsspeicherung der Verkehrs- und Standortdaten jedoch Auswirkungen auf die Nutzung der elektronischen Kommunikationsmittel und infolgedessen auf die Ausübung der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung durch die Nutzer dieser Mittel haben (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 28).

102 In Anbetracht der Schwere des Eingriffs in die betreffenden Grundrechte durch eine nationale Regelung, die für Zwecke der Kriminalitätsbekämpfung die Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, vermag allein die Bekämpfung der schweren Kriminalität eine solche Maßnahme zu rechtfertigen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 60).

103 Zudem kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 51).

104 Eine solche Regelung hat zum einen in Anbetracht ihrer in Rn. 97 des vorliegenden Urteils beschriebenen charakteristischen Merkmale zur Folge, dass die Vorratsspeicherung der Verkehrs- und Standortdaten die Regel ist, obwohl nach dem mit der Richtlinie

2002/58 geschaffenen System die Vorratsspeicherung von Daten die Ausnahme zu sein hat.

105 Zum anderen sieht eine nationale Regelung wie die im Ausgangsverfahren, die sich allgemein auf alle Teilnehmer und registrierten Nutzer erstreckt und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor. Sie betrifft pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keine Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 57 und 58).

106 Eine solche Regelung verlangt keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 59).

107 Eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt.

108 Hingegen untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist.

109 Um den in der vorstehenden Randnummer des vorliegenden Urteils genannten Erfordernissen zu genügen, muss die betreffende nationale Regelung erstens klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 54 und die dort angeführte Rechtsprechung).

110 Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterscheiden, doch muss die Vorratsspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen.

111 Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden.

112 In Anbetracht all dessen ist auf die erste Frage in der Rechtssache C-203/15 zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.

Zur zweiten Frage in der Rechtssache C-203/15 und zur ersten Frage in der Rechtssache C-698/15

113 Vorab ist darauf hinzuweisen, dass der Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm) die zweite Frage in der Rechtssache C-203/15 nur für den Fall gestellt hat, dass die erste Frage in dieser Rechtssache verneint wird. Diese zweite Frage ist jedoch unabhängig davon, ob eine Vorratsspeicherung von Daten in dem in den Rn. 108 bis 111 des vorliegenden Urteils in Betracht gezogenen Sinne allgemein oder gezielt erfolgt. Daher sind die zweite Frage in der Rechtssache C-203/15 und die erste Frage in der Rechtssache C-698/15, die unabhängig vom Umfang der den Betreibern elektronischer Kommunikationsdienste auferlegten Pflicht zur Vorratsspeicherung von Daten gestellt ist, gemeinsam zu beantworten.

114 Mit der zweiten Frage in der Rechtssache C-203/15 und der ersten Frage in der Rechtssache C-698/15 möchten die vorlegenden Gerichte wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten, zum Gegenstand hat, ohne diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne ihn einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne das Erfordernis vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.

115 Hinsichtlich der Zwecke, die eine vom Grundsatz der Vertraulichkeit elektronischer Kommunikationen abweichende nationale Regelung rechtfertigen können, ist darauf hinzuweisen, dass, da die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie

2002/58 genannten Zwecke – wie in den Rn. 90 und 102 des vorliegenden Urteils festgestellt – abschließend ist, der Zugang zu den auf Vorrat gespeicherten Daten tatsächlich strikt einem dieser Zwecke dienen muss. Da außerdem der mit der Regelung verfolgte Zweck im Verhältnis zur Schwere des mit dem Zugang einhergehenden Eingriffs in die Grundrechte stehen muss, vermag folglich im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur die Bekämpfung schwerer Straftaten einen solchen Zugang zu den auf Vorrat gespeicherten Daten zu rechtfertigen.

116 Was die Einhaltung des Grundsatzes der Verhältnismäßigkeit anbelangt, muss eine nationale Regelung über die Voraussetzungen, unter denen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den auf Vorrat gespeicherten Daten zu gewähren haben, nach den in den Rn. 95 und 96 des vorliegenden Urteils getroffenen Feststellungen sicherstellen, dass ein solcher Zugang nur innerhalb der Schranken des absolut Notwendigen stattfindet.

117 Da zudem die in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Rechtsvorschriften nach dem elften Erwägungsgrund der Richtlinie „angemessenen Garantien … entsprechen" müssen, muss eine solche Rechtsvorschrift – wie sich aus der in Rn. 109 des vorliegenden Urteils angeführten Rechtsprechung ergibt – klare und präzise Regeln aufstellen, in denen angegeben ist, unter welchen Umständen und unter welchen Voraussetzungen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den Daten zu gewähren haben. Außerdem muss eine derartige Vorschrift im innerstaatlichen Recht verbindlich sein.

118 Es ist zwar Sache des nationalen Rechts, die Voraussetzungen festzulegen, unter denen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden den Zugang zu den auf Vorrat gespeicherten Daten gewähren müssen, damit gewährleistet ist, dass dieser Zugang auf das absolut Notwendige beschränkt ist. Die betreffende nationale Regelung darf sich jedoch nicht darauf beschränken, dass der Zugang einem der in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Zwecke zu entsprechen hat, auch wenn es sich dabei um die Bekämpfung schwerer Straftaten handelt. Denn eine solche nationale Regelung muss auch die materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten festlegen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 61).

119 Infolgedessen, und weil ein allgemeiner Zugang zu allen auf Vorrat gespeicherten Daten unabhängig davon, ob irgendein – zumindest mittelbarer – Zusammenhang mit dem verfolgten Ziel besteht, nicht als auf das absolut Notwendige beschränkt angesehen werden kann, muss sich die betreffende nationale Regelung bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den Daten von Teilnehmern oder registrierten Nutzern zu gewähren ist, auf objektive Kriterien stützen. Insoweit darf im Zusammenhang mit dem Zweck der Bekämpfung von Straftaten Zugang grundsätzlich nur zu den Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein (vgl. entsprechend Urteil des Europäischen Gerichtshofs für Menschenrechte vom 4. Dezember 2015, Zakharov/Russland, CE:ECHR:2015:1204JUD004714306, Rn. 260). Allerdings könnte in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, der Zugang zu Daten anderer Personen ebenfalls gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten.

120 Damit in der Praxis die vollständige Einhaltung dieser Voraussetzungen gewährleistet ist, ist es unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und deren Entscheidung auf einen mit Gründen versehenen Antrag ergeht, der von den zuständigen nationalen Behörden u.a. im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellt wird (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 62; vgl. auch entsprechend, zu Art. 8 EMRK, Urteil des Europäischen Gerichtshofs für Menschenrechte vom 12. Januar 2016, Szabó und Vissy/Ungarn CE:ECHR:2016:0112JUD003713814, Rn. 77 und 80).

121 Außerdem ist es wichtig, dass die zuständigen nationalen Behörden, denen Zugang zu den auf Vorrat gespeicherten Daten gewährt worden ist, die betroffenen Personen im Rahmen der einschlägigen nationalen Verfahren davon in Kenntnis setzen, sobald die Mitteilung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann. Diese Information ist nämlich der Sache nach erforderlich, damit die betroffenen Personen u.a. das Recht auf Einlegung eines Rechtsbehelfs ausüben können, das in Art. 15 Abs. 2 der Richtlinie 2002/58 in Verbindung mit Art. 22 der Richtlinie 95/46 für den Fall einer Verletzung ihrer Rechte ausdrücklich vorgesehen ist (vgl. entsprechend Urteile vom 7. Mai 2009, Rijkeboer, C-553/07, EU:C:2009:293, Rn. 52, sowie vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 95).

122 Bezüglich der Vorschriften zur Sicherheit und zum Schutz der von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten ist festzustellen, dass Art. 15 Abs. 1 der Richtlinie 2002/58 den Mitgliedstaaten nicht erlaubt, von Art. 4 Abs. 1 und Art. 4 Abs. 1a der Richtlinie abzuweichen. Nach diesen Bestimmungen haben die Betreiber geeignete technische und organisatorische Maßnahmen zu ergreifen, um zu gewährleisten, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang geschützt sind. Unter Berücksichtigung der Menge an gespeicherten Daten, ihres sensiblen Charakters und der Gefahr eines unberechtigten Zugangs zu ihnen müssen die Betreiber elektronischer Kommunikationsdienste, um die Unversehrtheit und Vertraulichkeit der Daten in vollem Umfang zu sichern, durch geeignete technische und organisatorische Maßnahmen ein besonders hohes Schutz- und Sicherheitsniveau gewährleisten. Die nationale Regelung muss insbesondere vorsehen, dass die Daten im Unionsgebiet zu speichern und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten sind (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 66 bis 68).

123 Jedenfalls müssen die Mitgliedstaaten gewährleisten, dass die Einhaltung des Schutzniveaus, das das Unionsrecht im Rahmen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten garantiert, durch eine unabhängige Stelle überwacht wird, da eine solche Überwachung in Art. 8 Abs. 3 der Charta ausdrücklich gefordert wird und nach ständiger Rechtsprechung des Gerichtshofs ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten ist. Anderenfalls würde den Personen, deren personenbezogene Daten gespeichert wurden, das durch Art. 8 Abs. 1 und 3 der Charta garantierte Recht vorenthalten, sich zum Schutz ihrer Daten mit einer Eingabe an die nationalen Kontrollstellen zu wenden (vgl. in diesem Sinne Urteile Digital Rights, Rn. 68, und vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 41 und 58).

124 Es ist Sache der vorlegenden Gerichte, zu prüfen, ob und inwieweit die in den Ausgangsverfahren in Rede stehenden nationalen Regelungen die sich aus Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta ergebenden Erfordernisse beachten, wie sie in den Rn. 115 bis 123 des vorliegenden Urteils ausdrücklich benannt sind, sowohl was den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten als auch was den Schutz dieser Daten und das Sicherheitsniveau betrifft.

125 Aufgrund all dessen ist auf die zweite Frage in der Rechtssache C-203/15 und die erste Frage in der Rechtssache C-698/15 zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.

Zur zweiten Frage in der Rechtssache C-698/15

126 Mit der zweiten Frage in der Rechtssache C-698/15 möchte der Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen]) wissen, ob der Gerichtshof im Urteil Digital Rights die Art. 7 und 8 der Charta in einem Sinne ausgelegt hat, der über den hinausgeht, der Art. 8 EMRK vom Europäischen Gerichtshof für Menschenrechte gegeben wurde.

127 Zunächst ist darauf hinzuweisen, dass die in der EMRK anerkannten Grundrechte zwar, wie Art. 6 Abs. 3 EUV bestätigt, als allgemeine Grundsätze Teil des Unionsrechts sind, die EMRK jedoch, solange die Union ihr nicht beigetreten ist, kein Rechtsinstrument darstellt, das förmlich in die Unionsrechtsordnung übernommen wurde (vgl. in diesem Sinne Urteil vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 45 und die dort angeführte Rechtsprechung).

128 Daher ist die Richtlinie 2002/58, um die es vorliegend geht, einzig und allein anhand der durch die Charta garantierten Grundrechte auszulegen (vgl. in diesem Sinne Urteil vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 46 und die dort angeführte Rechtsprechung).

129 Außerdem heißt es in den Erläuterungen zu Art. 52 der Charta, dass mit ihrem Art. 52 Abs. 3 die notwendige Kohärenz zwischen der Charta und der EMRK geschaffen werden soll, „ohne dass dadurch die Eigenständigkeit des Unionsrechts und des Gerichtshofs der Europäischen Union berührt wird“ (vgl. in diesem Sinne Urteil vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 47). Insbesondere steht, wie aus Art. 52 Abs. 3 Satz 2 der Charta hervorgeht, Art. 52 Abs. 3 Satz 1 der Charta dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt als die EMRK. Zudem betrifft Art. 8 der Charta ein anderes als das in ihrem Art. 7 verankerte Grundrecht, für das es in der EMRK keine Entsprechung gibt.

130 Nach ständiger Rechtsprechung des Gerichtshofs liegt die Rechtfertigung für ein Vorabentscheidungsersuchen jedoch nicht in der Abgabe von Gutachten zu allgemeinen oder hypothetischen Fragen, sondern darin, dass das Ersuchen für die tatsächliche Entscheidung eines Rechtsstreits über das Unionsrecht erforderlich ist (vgl. in diesem Sinne Urteile vom 24. April 2012, Kamberaj, C-571/10, EU:C:2012:233, Rn. 41, vom 26. Februar 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, Rn. 42, sowie vom 27. Februar 2014, Pohotovos', C-470/12, EU:C:2014:101, Rn. 29).

131 Im vorliegenden Fall ist in Anbetracht der insbesondere in den Rn. 128 und 129 des vorliegenden Urteils enthaltenen Erwägungen die Frage, ob der in den Art. 7 und 8 der Charta verliehene Schutz über den in Art. 8 EMRK garantierten hinausgeht, nicht geeignet, die Auslegung der Richtlinie 2002/58 im Licht der Charta, um die es in der Rechtssache C-698/15 im Ausgangsverfahren geht, zu beeinflussen.

URTEIL VOM 21.12.2016 – VERBUNDENE RECHTSSACHEN C-203/15 UND C-698/15

I – 46

132 Es ist somit nicht ersichtlich, dass die Antwort auf die zweite Frage in der Rechtssache C-698/15 Hinweise zur Auslegung des Unionsrechts liefern könnte, die für die Entscheidung des betreffenden Rechtsstreits im Hinblick auf das Unionsrecht erforderlich sind.

133 Folglich ist die zweite Frage in der Rechtssache C-698/15 unzulässig.

Bei der Anordnung der stichprobenartigen Durchsuchung von Strafgefangenen muss eine Abweichung im Einzelfall möglich sein (Ls)

(**Bundesverfassungsgericht**, Beschluss vom 5. November 2016 – 2 BvR 6/16 –)

Eine vor der Vorführung zu Besuch stichprobenartig bei jedem fünften Gefangenen mit der Entkleidung und der Untersuchung körperlicher Öffnungen verbundene Durchsuchung verletzt das allgemeine Persönlichkeitsrecht des Strafgefangenen, wenn keine Abweichungen im Einzelfall zugelassen sind und daher dem Verhältnismäßigkeitsgrundsatz nicht ausreichend Rechnung getragen ist.

(Nicht amtlicher Leitsatz)

Keine regelmäßige Pflicht zur Teilnahme an einem Personalgespräch während der Arbeitsunfähigkeit (Ls)

(**Bundesarbeitsgericht**, Urteil vom 2. November 2016 – 10 AZR 596/15 –)

1. **Ein durch Arbeitsunfähigkeit infolge Krankheit an seiner Arbeitsleistung verhinderter Arbeitnehmer ist regelmäßig nicht verpflichtet, auf Anweisung des Arbeitgebers im Betrieb zu erscheinen, um dort an einem Gespräch zur Klärung der weiteren Beschäftigungsmöglichkeit teilzunehmen.**

2. **Eine wegen des Nichterscheinens erteilte Abmahnung ist aus der Personalakte zu entfernen.**

(Nicht amtliche Leitsätze)

Nachweispflichten bei krankheitsbedingter Arbeitsunfähigkeit – Zuständigkeit des Gesamtbetriebsrats

(**Bundesarbeitsgericht** Beschluss vom 23. August 2016, 1 ABR 43/14 –)

1. **Will der Arbeitgeber die Vorlage von ärztlichen Bescheinigungen über das Bestehen einer Arbeitsunfähigkeit abweichend von § 5 Abs. 1 S. 2 EFZG für alle Arbeitnehmer zu einem früheren Zeitpunkt regeln, so hat der Betriebsrat nach § 87 Abs. 1 Nr. 1 BetrVG sowohl über das „Ob" als auch das „Wie" mitzubestimmen.**

2. **Das Mitbestimmungsrecht steht originär den jeweiligen örtlichen Betriebsräten und nicht dem Gesamtbetriebsrat zu. Allein das Interesse an einer unternehmenseinheitlichen Regelung begründet keine Zuständigkeit.**

(Nicht amtliche Leitzsätze)

Sachverhalt:

A. Die Beteiligten streiten über die Zuständigkeit des Gesamtbetriebsrats zur Regelung von Nachweispflichten bei krankheitsbedingter Arbeitsunfähigkeit.

Die Arbeitgeberin ist ein Unternehmen der Logistikbranche. In ihren bundesweit 72 Betrieben sind etwa 15.000 Arbeitnehmer beschäftigt. Beteiligter zu 2. ist der für ihren Betrieb in D gebildete Betriebsrat. Dieser sowie weitere 29 Betriebsräte haben den zu 3. beteiligten Gesamtbetriebsrat errichtet. Mit diesem vereinbarte die Arbeitgeberin am 22. Januar 2008 eine „Gesamtbetriebsvereinbarung über eine Allgemeine Arbeitsordnung" (GBV AO). Deren Geltungsbereich erstreckt sich auf alle Betriebe mit einem Betriebsrat. § 9 GBV AO (idF vom 19. Juni 2013) legt Nachweispflichten im Krankheitsfall wie folgt fest:

„§ 9 Vorübergehende Nichtleistung der Arbeit

(3) Grundsätzlich hat jeder erkrankte Mitarbeiter für jeden vollen Arbeitstag, d.h. ab dem ersten vollen Krankheitstag, eine ärztliche Bescheinigung über die Arbeitsunfähigkeit sowie deren voraussichtliche Dauer vorzulegen. Die Bescheinigung muss spätestens am dritten Krankheitstag beim Arbeitgeber vorliegen und ist an die zuständige Personalabteilung oder den unmittelbaren Vorgesetzten bzw. bei dessen Verhinderung an den vom Arbeitgeber zu benennenden Stellvertreter zu adressieren.

(4) Dauert die Arbeitsunfähigkeit länger als in der vorgelegten ärztlichen Bescheinigung angegeben, so ist unverzüglich eine neue ärztliche Bescheinigung vorzulegen".

Der zu 2. beteiligte Betriebsrat bestritt die Zuständigkeit des Gesamtbetriebsrats für diese Regelungen und machte geltend, das Mitbestimmungsrecht stehe den örtlichen Betriebsräten zu.

Er meint, ihm stehe originär ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG zu, ob und wie von der gesetzlichen Vorgabe des § 5 Abs. 1 Satz 2 EFZG regelhaft abgewichen werden soll. Ein zwingendes Bedürfnis für eine betriebsübergreifende Regelung bestehe nicht.

Aus den Gründen:

1. Nach § 87 Abs. 1 Nr. 1 BetrVG hat der Betriebsrat mitzubestimmen bei Fragen der Ordnung des Betriebes und des Verhaltens der Arbeitnehmer im Betrieb. Verlangt der Arbeitgeber von Arbeitnehmern unabhängig von einer Arbeitsleistung in einer bestimmten Form und innerhalb einer bestimmten Frist den Nachweis jeglicher Arbeitsunfähigkeit, betrifft dieses regelhafte Verlangen nach der Rechtsprechung des Senats grundsätzlich das betriebliche Ordnungsverhalten (BAG 25. Januar 2000 – 1 ABR 3/99 – zu B I 2 a bb der Gründe, BAGE 93, 276). Hierfür eröffnet § 5 Abs. 1 Satz 3 EFZG dem Arbeitgeber einen Regelungsspielraum. Diese Vorschrift billigt ihm die Befugnis zu, die Vorlage einer ärztlichen Bescheinigung abweichend von § 5 Abs. 1 Satz 1 und Satz 2 EFZG vor dem vierten Krankheitstag zu verlangen. An der Ausgestaltung des Regelungsspielraums zum „Ob" und zum „Wie" der Nachweispflicht des § 5 Abs. 1 EFZG hat der Betriebsrat mitzubestimmen.

2. Entgegen der Auffassung der Arbeitgeberin wird diese Rechtsprechung durch die Entscheidung des Fünften Senats vom 14. November 2012 nicht in Frage gestellt. Danach steht es im freien Ermessen eines Arbeitgebers, ob er in einem Einzelfall von einem Arbeitnehmer abweichend von § 5 Abs. 1 Satz 2 und Satz 3 EFZG die Vorlage einer Arbeitsunfähigkeitsbescheinigung verlangt (BAG 14. November 2012 – 5 AZR 886/11 – Rn. 14, BAGE 143, 315). Stellt er aber wie vorliegend eine Regel auf, die für alle Arbeitnehmer Geltung beanspruchen soll, schafft er einen kollektiven Sachverhalt, den der Betriebsrat mitzubestimmen hat.

3. Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG bei Regelungen über Nachweispflichten bei Arbeitsunfähigkeit infolge Krankheit steht originär den örtlichen Betriebsräten und nicht dem Gesamtbetriebsrat zu.

a) Die Ausübung der Mitbestimmungsrechte nach dem Betriebsverfassungsgesetz obliegt grundsätzlich dem von den Arbeitnehmern unmittelbar gewählten Betriebsrat. Dem Gesamtbetriebsrat sind nach § 50 Abs. 1 Satz 1 BetrVG nur solche Angelegenheiten zugewiesen, die das Gesamtunternehmen oder mehrere Betriebe betreffen und für die ein zwingendes Erfordernis für eine betriebsübergreifende Regelung besteht. Ein solches kann sich aus technischen oder rechtlichen Gründen ergeben. Davon ist etwa auszugehen, wenn der Arbeitgeber im Bereich der freiwilligen Mitbestimmung zu einer Maßnahme oder Leistung nur betriebsübergreifend bereit ist. Kann er über deren „Ob" mitbestimmungsfrei entscheiden, so kann er ebenso mitbestimmungsfrei darüber befinden, ob eine solche Maßnahme oder Leistung überbetrieblich erfolgen soll. Entscheidet er sich dazu, begründet das eine Zuständigkeit des Gesamtbetriebsrats. Unterliegt aber bereits das „Ob" der Maßnahme oder Leistung der Mitbestimmung, vermögen weder Zweckmäßigkeitserwägungen noch der bloße Wunsch des Arbeitgebers nach einer betriebsübergreifenden Regelung eine Zuständigkeit des Gesamtbetriebsrats herbeizuführen.

b) Nach diesen Grundsätzen war der Gesamtbetriebsrat nicht originär zuständig. Entgegen der Auffassung der Arbeitgeberin war diese nicht frei darin, von der durch § 5 Abs. 1 Satz 3 EFZG eröffneten Befugnis gegenüber allen Arbeitnehmern Gebrauch zu machen. Vielmehr unterliegt bereits diese Entscheidung der zwingenden Mitbestimmung. Der Arbeitgeberin war demnach die Wahl desjenigen betriebsverfassungsrechtlichen Gremiums verwehrt, mit dem eine die Arbeitnehmer normativ bindende

Regelung geschaffen werden sollte. Dabei bedarf es keiner Entscheidung, ob der örtliche Betriebsrat im Wege eines Initiativrechts eine solche Regelung verlangen könnte. Initiativ wurde allein die Arbeitgeberin. Die örtlichen Betriebsräte haben kein entsprechendes Regelungsverlangen gestellt.

Auch das von der Arbeitgeberin bekundete Interesse an einheitlichen Arbeitsbedingungen für alle Mitarbeiter begründet keine Zuständigkeit des Gesamtbetriebsrats. Hierbei handelt es sich um eine reine Zweckmäßigkeitserwägung. Sie ist bei der Prüfung der gesetzlichen Zuständigkeit eines Gesamtbetriebsrats unbeachtlich.

c) Die Arbeitgeberin kann sich zur Begründung einer originären Zuständigkeit des Gesamtbetriebsrats nicht auf den Beschluss des Senats vom 21. Juli 2009 stützen. Danach unterliegt die Entscheidung des Arbeitgebers, an welchem Ort er eine Beschwerdestelle iSd. § 13 AGG einrichtet, nicht der Mitbestimmung des Betriebsrats nach § 87 Abs. 1 Nr. 1 BetrVG. Die örtliche Festlegung gestaltet nicht das betriebliche Zusammenleben und Zusammenwirken der Arbeitnehmer, sondern bezieht sich darauf, welche Stelle oder Person für den Arbeitgeber berechtigt und verpflichtet ist, die Beschwerden der Arbeitnehmer entgegenzunehmen. Dies betrifft – anders als in der vorliegenden Fallgestaltung – die mitbestimmungsfreie Organisation des Arbeitgebers (BAG 21. Juli 2009 – 1 ABR 42/08 – Rn. 22 ff., BAGE 131, 225).

d) Ohne Erfolg ist der Hinweis der Rechtsbeschwerde auf § 50 Abs. 1 Satz 1 Halbs. 2 BetrVG. Die danach bestehende Zuständigkeit des Gesamtbetriebsrats auch für Betriebe ohne Betriebsrat setzt dessen originäre Zuständigkeit für die zu regelnde Angelegenheit voraus, vermag eine solche aber nicht zu begründen (vgl. BAG 9. Dezember 2009 – 7 ABR 46/08 – Rn. 23 mwN, BAGE 132, 357). Unabhängig davon erfasst die GBV AO nach ihrem § 2 keine betriebsratslosen Betriebe. Ihr Geltungsanspruch erstreckt sich nur auf Betriebe, in denen ein Betriebsrat gebildet ist.

Informationsfreiheitsgesetz gibt keinen Zugang zu Mitarbeitertelefonlisten von Jobcentern (Ls)

(**Bundesverwaltungsgericht**, Urteile vom 20. Oktober 2016 – 7 C 20.15; 7 C 23.15; 7 C 27.15; M 7 C 28.15 –)

1. **Ein Anspruch nach dem Informationsfreiheitsgesetz besteht nach dem Ausschlussgrund des § 3 Nr. 2 IFG nicht, wenn das Bekanntwerden der Information die öffentliche Sicherheit gefährden kann. Zum Schutzgut der öffentlichen Sicherheit gehört auch die Funktionsfähigkeit und die effektive Aufgabenerledigung staatlicher Einrichtungen. Beeinträchtigungen der zügigen Aufgabenerfüllung können bei unmittelbarer telefonischer Kontaktaufnahme mit den Bediensteten eines Jobcenters eintreten.**

2. **Dem Anspruch auf Übermittlung der Telefonlisten ohne vorherige Einwilligung der betroffenen Bediensteten steht zudem § 5 Abs. 1 Satz 1 IFG entgegen. Danach darf ohne eine solche Einwilligung Zugang zu personenbezogenen Daten nur gewährt werden, soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt. Bei den dienstlichen Telefonnummern handelt es sich um personenbezogene Daten, die vom Schutzbereich des Grundrechts auf informationelle Selbstbestimmung erfasst werden. § 5 Abs. 1 Satz 1 IFG liegt daher ein relativer Vorrang des Datenschutzes vor dem Informationsinteresse zugrunde.**

(Nicht amtliche Leitzsätze)

Beweisverwertungsverbot bei unzulässigem Detektiveinsatz bei Verdacht von Wettbewerbsverstößen

(**Landesarbeitsgericht Baden-Württemberg** Urteil vom 20. Juli 2016 – 4 Sa 61/15 –)

1. **Eine konkrete und zielgerichtete Datenerhebung durch einen Detektiv wegen des Verdachts einer konkreten Vertragspflichtverletzung unterfällt nicht §§ 32 Abs. 1 Satz 1 BDSG, sondern bedarf des Vorliegens der Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG.**

2. **Der Verdacht eines Wettbewerbsverstoßes stellt in der Regel keinen Verdacht einer Straftat dar und kann deshalb eine Datenerhebung gem. § 32 Abs. 1 Satz 2 BDSG nicht rechtfertigen.**

Sachverhalt:

Die Parteien streiten in der Berufungsinstanz (nur) noch über die Wirksamkeit einer arbeitgeberseitigen außerordentlichen, hilfsweise ordentlichen Kündigung, sowie auf die Widerklage der Beklagten über Rückzahlung geleisteter Entgeltfortzahlung für den Krankheitsfall, über den Ersatz von Detektivkosten sowie über einen Auskunftsanspruch betreffend Wettbewerbshandlungen.

Der am 00.00.1961 geborene Kläger ist bei der Beklagten beschäftigt seit 04. Dezember 1978 als Mitarbeiter im Stanzformenbau.

Die Beklagte stellt Stanzwerkzeuge und Stanzformen her. Sie beschäftigt in ihrem Betrieb in H. ca. 395 Mitarbeiter. Ein Betriebsrat ist in diesem Betrieb nicht gebildet.

Die Beklagte kündigte das Arbeitsverhältnis mit dem Kläger mit Schreiben vom 28. Januar 2015 ordentlich zum 31. August 2015 und mit Schreiben vom 27. April 2015 ordentlich zum 30. November 2015 aus krankheitsbedingten Gründen. Gegen diese Kündigungen erhob der Kläger am 06. Februar 2015 und 06. Mai 2015 Kündigungsschutzklagen. Die Beklagte erklärte im Laufe des Verfahrens mit Schriftsatz vom 03. September 2015, aus diesen Kündigungen keine Rechte mehr gegenüber dem Kläger herzuleiten, diese Kündigungen werden „zurückgenommen".

Die Beklagte kündigte das Arbeitsverhältnis erneut mit Schreiben vom 11. Juni 2015, dem Kläger zugegangen am 11. Juni 2015, außerordentlich und fristlos, hilfsweise ordentlich zum 31. Januar

2016. Gegen diese Kündigung richtet sich die vorliegend noch streitige Kündigungsschutzklage, die als Klageerweiterungsantrag am 24. Juni 2015 in das Verfahren eingeführt wurde.

Die Beklagte stützt die Kündigung auf den Verdacht wettbewerbswidriger Konkurrenztätigkeiten des Klägers für die Firma seiner Söhne sowie auf den Verdacht des Erschleichens von Arbeitsunfähigkeitsbescheinigungen. Wegen dieses Verdachts wurde der Kläger mit Schreiben vom 08. Juni 2015 (Bl. 97-99 d. ArbG-Akte) angehört. Der Kläger beantwortete dieses Schreiben nicht.

Dem liegt folgender Sachverhalt zugrunde:

Die drei Söhne des Klägers gründeten eine Firma M. S. GmbH (nachfolgend: M.), welche am 05. November 2013 in das Handelsregister eingetragen wurde und deren Geschäftsführer der Sohn des Klägers, Herr G. A., ist. Dieses Unternehmen wurde unter der Wohnanschrift des Klägers angemeldet, verlagerte seinen Geschäftsbetrieb jedoch bald an eine Betriebsstätte in N. Gegenstand dieses Unternehmens ist der Stanzformenbau. Insbesondere im Bereich des Stanzformenbaus für den Akzidenzdruck (Wellpappe, Etiketten, Faltschachteln ua.) sind die Geschäftsbereiche identisch mit einem entsprechenden Teil des Geschäftsgegenstands der Beklagten. Auf die Internetauftritte beider Firmen (Bl. 188-194 d. LAG-Akte) wird Bezug genommen.

Die Firma M. schrieb an einen Kunden der Beklagten eine E-Mail, von der der Geschäftsführer der Beklagten am 29. Mai 2015 Kenntnis erhielt. Darin heißt es:

„hätten Sie interesse an Stanzformen, Bandstahlwerkzeuge, Ausbrechwerkzeugen, Rilma ect. wir sind in N. bei H., wir verkaufen unsere Produkte sehr kosten günstig bei gleich Qualität wie man eine Stafo so kennt, da wir unsere Werkzeuge in einem Familienunternehmen fertigen können wir einige Kosten sparen und unsere Kunden da entgegenkommen, deswegen haben wir einige große vorteile gegenüber meine Konkurrenten.

Mein Vater M. A. montiert seit 38 Jahren, unglaublich was er alles so hinbekommt, ich selber der Sohn von 3 Brüder, G. A., 33 Jahre bin Feinwerkmeister HWK und weis was Sache ist um das zu beurteilen.

Also wenn Sie interesse haben würde ich Sie herzlich begrüßen, wenn Sie schon mit allem zufrieden sind, never change the running systeme! dann möchte ich nicht unverschämt sein und verbleibe.

Mit freundlichen Grüßen."

Der Kläger war schon im Jahr 2014 mehrfach als arbeitsunfähig krankgeschrieben. Seit 20 Januar 2015 ist der Kläger durchgehend arbeitsunfähig krankgeschrieben. Die Beklagte leistete in 2015 noch Entgeltfortzahlung vom 20. Januar 2015 bis 02. März 2015. Wegen der geleisteten Entgeltfortzahlung seit Februar 2014 und im Jahr 2015 wird auf die Aufstellung der Beklagten verwiesen. Inzwischen ist der Kläger beim Krankengeldbezug ausgesteuert.

Der Kläger bestritt, in der Firma seiner Söhne gearbeitet zu haben. Er sei auch arbeitsunfähig krank gewesen. Er leide unter anderem an Hepatitis C und an Entzündungen innerer Organe. [...]

Die Beklagte hielt die außerordentliche Kündigung für gerechtfertigt.

Sie behauptete, sie habe unmittelbar nach Kenntniserlangung von der Gründung der M. mit dem Kläger am 06. November 2013 ein Personalgespräch geführt, bei welchem dem Kläger eindringlich mitgeteilt wurde, dass er in diesem Betrieb nicht konkurrierend tätig sein dürfe. Dies sei dem Kläger im Übrigen – unstreitig – auch bereits mit Schreiben vom 29. Oktober 2013 (Bl. 161 d. ArbG-Akte) mitgeteilt worden.

Die Beklagte habe das Privatfahrzeug des Klägers am 19. Februar 2014 während der Arbeitsunfähigkeit des Klägers auf dem Firmengelände der M. gesehen. Sie habe daraufhin ein Detektivbüro beauftragt, welches erkundet habe, dass das Fahrzeug auch am 24. Februar und 27. Februar 2014 und vom 25. bis 27. Juni 2014 während einer Arbeitsunfähigkeit des Klägers und am 03. März und 13. März 2014 während eines Erholungsurlaubs des Klägers, zu dem der Kläger angegeben habe, in der Türkei zu sein, auf dem Gelände der M. gestanden habe.

Nach Kenntnisnahme der E-Mail der M. am 29. Mai 2015 habe sie erneut ein Detektivbüro eingeschaltet, welches am 02. Juni 2015 bei der Firma M. angerufen habe. Der Detektiv habe namens einer Firma a. GmbH eine Stanzform beim Sohn des Klägers T. A. bestellt, welche am 03. Juni 2015 durch einen vermeintlichen Fahrer der a. GmbH hätte abgeholt werden sollen. Ein anderer Detektiv habe sich am 03. Juni 2015 zur Firma M. begeben und sich als Fahrer der a. GmbH ausgegeben. Der Detektiv habe um 9:39 Uhr festgestellt, dass der Kläger sich am Montagetisch befunden habe und an zwei Stanzformen gearbeitet habe. Eine Stunde später sei der Kläger noch immer am Montagetisch tätig gewesen. Der Kläger habe den Detektiv sogar noch durch den Betrieb geführt, die Maschinen erklärt und mitgeteilt, dass es sich um einen Familienbetrieb handele. Nachdem einer der Söhne, der zwischenzeitlich die Computerzeichnung für die Stanzform angefertigt habe, aus dem Büro gekommen sei, habe sich der Kläger zur Fertigungsmaschine begeben und die Stanzform hergestellt. Dies habe bis ca. 12:20 Uhr gedauert.

Die Beklagte behauptete, bei den vom Kläger für die Firma M. erbrachten Tätigkeiten habe es sich um exakt dieselben Tätigkeiten gehandelt, die der Kläger auch bei der Beklagten zu verrichten gehabt hätte. Der Kläger hätte deshalb unerlaubt Wettbewerb betrieben. Außerdem stehe für die Beklagte aus diesem Verhalten fest, dass der Kläger seine Arbeitsunfähigkeit nur vorgetäuscht habe.

Die Beklagte vertrat die Auffassung, durch die festgestellten unerlaubten Wettbewerbshandlungen des Klägers seien auch die Beweiswerte aller Arbeitsunfähigkeitsbescheinigungen seit Februar 2014 erschüttert. Sie begehrte daher die Rückzahlung sämtlicher seit Februar 2014 erbrachten Entgeltfortzahlungsleistungen.

Sie meinte, der Kläger schulde im Rahmen des Schadenersatzes auch Ersatz der Detektivkosten für die Einsätze in 2014 und den Einsatz im Juni 2015.

Außerdem schulde ihr der Kläger wegen der wettbewerbswidrigen Handlungen Schadenersatz nach § 61 HGB, wofür ihr im Rahmen einer Stufenklage auf der ersten Stufe ein Auskunftsanspruch zustehe.

Aus den Gründen:

Das Arbeitsverhältnis zwischen den Parteien wurde nicht durch die außerordentliche Kündigung der Beklagten vom 11. Juni 2015 aufgelöst. Die Kündigung ist nicht gemäß § 626 Abs. 1 BGB gerechtfertigt.

1. Das Arbeitsgericht hat zu Recht festgestellt, dass die Kündigung nicht gemäß § 7 KSchG als wirksam gilt.

2. Gemäß § 626 Abs. 1 BGB kann ein Arbeitsverhältnis aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, aufgrund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses bis zum Ablauf der Kündigungsfrist nicht zugemutet werden kann. Dafür ist zunächst zu prüfen, ob der Sachverhalt ohne seine besonderen Umstände „an sich", das heißt 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. Ein wich-

tiger Grund im Sinne von § 626 Abs. 1 BGB ist also nur gegeben, wenn das Ergebnis dieser Gesamtwürdigung die Feststellung der Unzumutbarkeit einer Weiterbeschäftigung des Arbeitnehmers auch nur bis zum Ablauf der Kündigungsfrist ist (BAG 9. Juni 2011 – 2 AZR 381/10; BAG 10. Juni 2010 – 2 AZR 541/09).

Auch der Verdacht einer schwerwiegenden Pflichtverletzung kann einen wichtigen Grund im Sinne von § 626 Abs. 1 BGB bilden. Ein solcher Verdacht stellt gegenüber dem Vorwurf, der Arbeitnehmer habe die Tat begangen, einen eigenständigen Kündigungsgrund dar. Eine auf ihn gestützte Kündigung kann gerechtfertigt sein, wenn sich der Verdacht auf objektive Tatsachen gründet, die Verdachtsmomente geeignet sind, das für die Fortsetzung des Arbeitsverhältnisses erforderliche Vertrauen zu zerstören, und der Arbeitgeber alle zumutbaren Anstrengungen zur Aufklärung des Sachverhalts unternommen, insbesondere dem Arbeitnehmer Gelegenheit zur Stellungnahme gegeben hat. Der Verdacht muss auf konkrete – vom Kündigenden darzulegende und ggf. zu beweisende – Tatsachen gestützt sein. Der Verdacht muss ferner dringend sein. Es muss eine große Wahrscheinlichkeit dafür bestehen, dass er in der Sache zutrifft. Die Umstände, die ihn begründen, dürfen nach allgemeiner Lebenserfahrung nicht ebenso gut durch ein Geschehen zu erklären sein, das eine außerordentliche Kündigung nicht zu rechtfertigen möchte. Bloße, auf mehr oder wenige haltbare Vermutungen gestützte Verdächtigungen reichen dementsprechend zur Rechtfertigung eines dringenden Tatverdachts nicht aus (BAG 20. Juni 2013 – 2 AZR 546/12).

3. Ein Arbeitnehmer, der während des bestehenden Arbeitsverhältnisses Konkurrenztätigkeiten entfaltet, verstößt gegen seine Pflicht zur Rücksichtnahme auf die Interessen des Arbeitgebers aus § 241 Abs. 2 BGB. Es handelt sich in der Regel um eine erhebliche Pflichtverletzung. Sie ist „an sich" geeignet, eine außerordentliche Kündigung zu rechtfertigen. Während des rechtlichen Bestehens eines Arbeitsverhältnisses ist einem Arbeitnehmer grundsätzlich jede Konkurrenztätigkeit zum Nachteil seines Arbeitgebers untersagt. Die für Handlungsgehilfen geltende Regelung des § 60 Abs. 1 HGB normiert einen allgemeinen Rechtsgedanken. Der Arbeitgeber soll vor Wettbewerbshandlungen seines Arbeitnehmers geschützt werden. Der Arbeitnehmer darf im Marktbereich seines Arbeitgebers Dienste und Leistungen nicht Dritten anbieten. Dem Arbeitgeber soll dieser Bereich uneingeschränkt und ohne die Gefahr einer nachteiligen Beeinflussung durch den Arbeitnehmer offenstehen. Dem Arbeitnehmer ist aufgrund des Wettbewerbsverbots nicht nur eine Konkurrenztätigkeit im eigenen Namen und Interesse untersagt. Ihm ist ebenso wenig gestattet, einen Wettbewerber des Arbeitgebers zu unterstützen (BAG 23. Oktober 2014 – 2 AZR 644/13).

4. Ebenso kann es einen wichtigen Grund im Sinne von § 626 BGB zur fristlosen Kündigung darstellen, wenn der Arbeitnehmer unter Vorlage eines Attests der Arbeit fern bleibt und sich Entgeltfortzahlungen gewähren lässt, obwohl es sich in Wahrheit nur um eine vorgetäuschte Krankheit handelt. Der Arbeitnehmer begeht hierbei regelmäßig einen vollendeten Betrug. Denn durch Vorlage der Arbeitsunfähigkeitsbescheinigung hat er den Arbeitgeber unter Vortäuschung falscher Tatsachen dazu veranlasst, ihm unberechtigterweise Entgeltfortzahlung zu gewähren (BAG 26. August 1993 – 2 AZR 154/93).

5. Es kann vorliegend aber kein dringender Verdacht einer unerlaubten Konkurrenztätigkeit oder eines Erschleichens von Entgeltfortzahlung festgestellt werden. Insbesondere den von der Beklagten behauptetermaßen über die Beobachtungen des Detektives gewonnenen Erkenntnissen darf nicht über eine Beweiserhebung nachgegangen werden. Die Beklagte hat die von ihr vorgetragenen Beweismittel gegen den Kläger nämlich rechtswidrig unter Verstoß gegen § 32 BDSG erlangt. Diese dürfen deshalb nicht verwertet werden.

a) Die Zivilprozessordnung kennt zwar für rechtswidrig erlangte Informationen und Beweismittel kein – ausdrückliches – prozessuales Verwendungs- bzw. Verwertungsverbot. Aus § 286 ZPO iVm. Art. 103 Abs. 1 GG folgt im Gegenteil die grundsätzliche Verpflichtung der Gerichte, den von den Parteien vorgetragenen Sachverhalt und die von ihnen angebotenen Beweise zu berücksichtigen. Dementsprechend bedarf es für die Annahme eines Beweisverwertungsverbots, das zugleich die Erhebung der angebotenen Beweise hindern soll, einer besonderen Legitimation in Gestalt einer gesetzlichen Grundlage. In gerichtlichen Verfahren tritt jedoch der Richter den Verfahrensbeteiligten in Ausübung staatlicher Hoheitsgewalt gegenüber. Er ist daher nach Art. 1 Abs. 3 GG bei der Urteilsfindung an die insoweit maßgeblichen Grundrechte gebunden und zu einer rechtsstaatlichen Verfahrensgestaltung verpflichtet. Dabei können sich auch aus materiellen Grundrechten wie Art. 2 Abs. 1 GG Anforderungen an das gerichtliche Verfahren ergeben, wenn es um die Offenbarung und Verwertung von persönlichen Daten geht, die grundrechtlich vor der Kenntnis durch Dritte geschützt sind. Das Gericht hat deshalb zu prüfen, ob die Verwertung von heimlich beschafften persönlichen Daten und Erkenntnissen, die sich aus diesen Daten ergeben, mit dem allgemeinen Persönlichkeitsrechts des Betroffenen vereinbar ist. Dieses Recht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen des Einzelnen Rechnung. Es gewährleistet die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Diesem Schutz dient auch Art. 8 Abs. 1 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK). Die gesetzlichen Anforderungen an eine zulässige Datenverarbeitung im BDSG konkretisieren und aktualisieren den Schutz auf informationelle Selbstbestimmung und regeln, in welchem Umfang im Anwendungsbereich des Gesetzes Eingriffe in dieses zulässig sind. Dies stellt § 1 BDSG ausdrücklich klar. Liegt keine Einwilligung des Betroffenen vor, ist die Datenverarbeitung nach dem Gesamtkonzept des BDSG nur zulässig, wenn eine verfassungsgemäße Rechtsvorschrift diese erlaubt. Fehlt es an der danach erforderlichen Ermächtigungsgrundlage oder liegen deren Voraussetzungen nicht vor, ist die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten verboten. Dieser das deutsche Datenschutzrecht prägende Grundsatz ist in § 4 Abs. 1 BDSG kodifiziert (BAG 20. Juni 2013 – 2 AZR 546/12; BAG 21. November 2013 – 2 AZR 797/11).

b) Die Beurteilung der Rechtmäßigkeit der Datenerhebung und letztlich auch der prozessualen Verwertbarkeit hat demnach an § 32 BDSG zu erfolgen. Es ist zu prüfen, ob ein rechtswidriger Eingriff in das Persönlichkeitsrecht vorliegt.

Gem. der Bestimmung des § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt

werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach dessen Begründung für seine Durchführung oder Beendigung erforderlich ist. Nach Abs. 1 Satz 2 der Regelung dürfen zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten am Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind (BAG 20. Juni 2013 – 2 AZR 546/12).

Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben wie persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Erheben ist das Beschaffen von Daten über den Betroffenen, § 3 Abs. 3 BDSG (BAG 19. Februar 2015 – 8 AZR 1007/13).

c) Dies zugrundegelegt ist festzustellen, dass die Überwachung des Klägers durch einen Detektiv eine Datenerhebung im Sinne von § 32 Abs. 1 BDSG darstellte, zumal der Anwendungsbereich gem. § 32 Abs. 2 BDSG auch für nicht automatisierte Datenerhebungen eröffnet ist (BAG 19. Februar 2015 – 8 AZR 1007/13 –; BAG 20. Juni 2013 – 2 AZR 546/12).

d) Die Datenerhebung durch Detektivermittlungen war aber keine, die unter den Anwendungsbereich des § 32 Abs. 1 Satz 1 BDSG fiel.

aa) Zwar können „zur Durchführung des Arbeitsverhältnisses" Daten erhoben werden, die der Arbeitgeber zur Erfüllung seiner Pflichten aber auch zur Wahrnehmung seiner Rechte gegenüber dem Arbeitnehmer vernünftigerweise benötigt. Gestattet sind demnach auch Maßnahmen zur Kontrolle, ob der Arbeitnehmer den geschuldeten Pflichten nachkommt (Gola/Schomerus BDSG § 32 Rn. 16). Unter § 32 Abs. 1 Satz 1 BDSG fallen aber nur solche Maßnahmen, die nicht auf die Entdeckung konkret Verdächtiger gerichtet sind. Soll einem konkreten Verdacht zielgerichtet nachgegangen werden, muss diese Maßnahme den Anforderungen des § 32 Abs. 1 Satz 2 BDSG genügen (Gola/Schomerus, BDSG 12. Aufl. § 32 Rn. 40, 41).

bb) Vorliegend ließe sich zwar argumentieren, die Beobachtungen durch den Detektiv hätten der Überprüfung der Einhaltung von Vertragspflichten gem. § 60 HGB gedient. Die Beobachtungen erfolgten jedoch gewollt und zielgerichtet nur gegen den Kläger wegen eines bereits bestehenden konkreten Verdachts. Die Maßnahme musste somit den Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG genügen.

e) Die Datenerhebung erfolgte aber auch nicht aufgrund tatsächlicher Anhaltspunkte, die den Verdacht einer im Beschäftigungsverhältnis begangenen Straftat begründen im Sinne von § 32 Abs. 1 Satz 2 BDSG.

aa) Das Erschleichen von Arbeitsunfähigkeitsbescheinigungen, ohne tatsächlich krank zu sein, kann zwar eine Straftat sein. In Betracht kommt ein Straftatbestand des Betrugs gem. § 263 Abs. 1 BGB. Dies aber nur dann, wenn der Arbeitgeber aufgrund einer Täuschungshandlung eine Vermögensverfügung in Form von Entgeltfortzahlung getroffen hätte. Vorliegend war der Kläger aber bereits seit 20.01.2015 durchgehend als arbeitsunfähig krankgeschrieben. Der Entgeltfortzahlungszeitraum endete bereits am 02. März 2015. Im Juni 2015 bezog der Kläger schon lange Krankengeld. Ein Detektiveinsatz im Juni 2015 konnte somit nicht mehr auf einen Verdacht einer strafbaren Handlung gründen.

Denkbar wäre zwar, dass der Kläger im Juni 2015 durch Vortäuschen einer Arbeitsunfähigkeit einen strafbaren Betrug zu Lasten der Krankenkasse begangen haben könnte, indem diese zu einer Krankengeldzahlung veranlasst wurde. Jedoch würde es sich hierbei um keine Straftat „im Beschäftigungsverhältnis" mehr handeln.

bb) Auch der Verdacht einer unerlaubten Konkurrenztätigkeit kann die Datenerhebung durch den Detektiveinsatz nicht rechtfertigen. Denn ein solches Handeln ist zwar grob vertragswidrig, aber jedenfalls im Regelfall, wenn nicht zugleich zB Geschäfts- und Betriebsgeheimnisse verraten werden (§ 17 UWG), nicht strafbar.

Soweit das Bundesarbeitsgericht in seiner Entscheidung vom 28. Oktober 2010 (BAG 28. Oktober 2010 – 8 AZR 547/09) die Erstattungspflicht von Detektivkosten zur Aufdeckung von Konkurrenztätigkeit grundsätzlich bejaht hat, ohne die Frage der Verwertbarkeit der so gewonnen Erkenntnis überhaupt zu problematisieren, so lag dies ersichtlich daran, dass der Fall einen Sachverhalt betraf, der vor Inkrafttreten des § 32 BDSG in der heutigen Fassung spielte.

cc) Die Beklagtenseite kann sich nicht darauf berufen, dass eine Beweiserhebung durch einen Detektiveinsatz auch in solchen Fällen möglich sein müsse, in denen zwar keine Strafbarkeit, wohl aber eine schwere Vertragspflichtverletzung vorliege. Diese Frage wurde von der Rechtsprechung zwar noch offen gelassen (BGH 26. September 2013 – VII ZR 227/12), ist jedoch angesichts des eindeutigen Wortlauts des § 32 Abs. 1 Satz 2 BDSG zu verneinen (Wedde, in: Däubler/Klebe/Wedde/Weichert BDSG 4. Aufl. § 32 Rn. 125; Gola/Schomerus, BDSG 12. Aufl. § 32 Rn. 41). Das mag für die Beklagte zwar unbefriedigend sein. Es ist jedoch ausschließlich dem Gesetzgeber vorbehalten, Gesetze zu ändern und korrigierend einzugreifen.

6. Ein dringender Tatverdacht einer Vertragswidrigkeit ergibt sich auch nicht aus anderen Umständen außerhalb der Wahrnehmung des Detektivs.

a) Allein aus der Tatsache, dass das Fahrzeug des Klägers während der Arbeitsunfähigkeitszeiten gelegentlich auf dem Firmengelände der M. gesichtet wurde, lässt nicht mit einer großen Wahrscheinlichkeit auf Arbeitstätigkeiten oder ein Erschleichen der Arbeitsunfähigkeit rückschließen. Es handelt sich um das Familienfahrzeug, welches auch von anderen Familienmitgliedern gefahren wird.

b) Auch aus der der Beklagten am 29. Mai 2015 bekannt gewordenen E-Mail der M. kann nicht auf einen dringenden Tatverdacht geschlossen werden.

In der E-Mail wurden zwar die Kenntnisse des Klägers gelobt, unter Hinweis, dass dieser seit 38 Jahren montiere und es unglaublich sei, was dieser so hinbekomme. Dass der Kläger für die M. tätig sei, wird jedoch nicht ausdrücklich beschrieben. Zwar spricht einige Wahrscheinlichkeit dafür, dass wenn die Firma M. auf diese Weise mit dem Kläger warb, sie damit zum Ausdruck bringen wollte, dass der Kläger auch für sie arbeite. Notwendig ist dieser Rückschluss aber nicht. Möglicherweise wollte Herr G. A. auch bloß die Bekanntheit des Klägers für Werbungszwecke ausnutzen und gegenüber dem Kunden zum Ausdruck bringen, aus welch „gutem Stall" er und seine Brüder kommen. Die Beklagte hat zu Recht erkannt, dass ein konkreter dringender Verdacht erst bestehen kann, wenn der Kläger je-

denfalls einer Arbeitsleistung für die Firma M. auch überführt werden kann.

Kann aber ein konkreter dringender Tatverdacht mangels Verwertbarkeit der Erkenntnisse des Detektiveinsatzes nicht nachgewiesen werden, scheitert auch die hilfsweise ausgesprochene ordentliche Kündigung. Sie ist nicht sozial gerechtfertigt im Sinne von § 1 Abs. 2 KSchG.

Der Beklagten steht auch keine Erstattung der Detektivkosten für den Einsatz im Monat Juni 2015 zu aus § 280 Abs. 1 BGB.

1. Ein Arbeitnehmer hat wegen Verletzung arbeitsvertraglicher Pflichten dem Arbeitgeber die durch das Tätigwerden eines Detektivs entstandenen notwendigen Kosten zu ersetzen, wenn der Arbeitgeber aufgrund eines konkreten Tatverdachts gegen den Arbeitnehmer einem Detektiv die Überwachung eines Arbeitnehmers überträgt und der Arbeitnehmer einer vorsätzlichen Vertragsverletzung überführt wird (BAG 26. September 2013 – 8 AZR 1026/12; BAG 28. Oktober 2010 – 8 AZR 547/09). Zu ersetzen sind die Aufwendungen des Geschädigten nach § 249 BGB aber nur, soweit diese nach den Umständen des Falls als notwendig anzusehen sind (BAG 26. September 2013 – 8 AZR 1026/12).

2. Vorliegend mag unterstellt werden, dass die Beklagte den Detektiv auf der Grundlage eines ausreichenden konkreten Tatverdachts beauftragt hat. Es fehlt schon an einer Überführung des Klägers wegen einer vorsätzlichen Vertragspflichtverletzung. Die Beklagte macht die Erkenntnisse des Detektivs schon selbst nicht für eine Tatkündigung, sondern nur für eine Verdachtskündigung geltend.

3. Hinzu kommt, dass die Beklagte an der Verwertung der Erkenntnisse gehindert ist, siehe oben. Eine Beauftragung eines Detektivs für die Gewinnung von Erkenntnissen, die anschließend nicht verwertet werden dürfen, ist nicht notwendig.

Die Beklagte hat auch keinen Anspruch auf Auskunftserteilung über die Konkurrenztätigkeit des Klägers aus dem Arbeitsvertrag iVm. § 242 BGB.

1. Kann der Arbeitgeber mit hoher Wahrscheinlichkeit dartun, dass sein Arbeitnehmer ihm während des bestehenden Arbeitsverhältnisses unerlaubte Konkurrenz gemacht hat, dann ist der Arbeitnehmer verpflichtet, über die von ihm getätigten Geschäfte Auskunft zu erteilen und Rechnung zu legen (BAG 21. Oktober 1970 – 3 AZR 479/69).

Vorliegend ist der Beklagten die Darlegung der hohen Wahrscheinlichkeit der Konkurrenztätigkeit mangels Verwertbarkeit der Erkenntnisse aus den Detektivermittlungen aber nicht gelungen.

2. Die weiteren Stufen der Stufenklage waren nicht Gegenstand des Berufungsverfahrens.

Zwar kann das Berufungsgericht, das den Anspruch auf Auskunft verneint, gleichzeitig die weiteren Stufen durch einheitliches Endurteil abweisen, wenn diesen jegliche Grundlage entzogen wurde, denn das Beharren auf einer erstinstanzlichen Entscheidung über die weiteren Stufen wäre dann eine prozessunökonomische bloße Formelei (Zöller/Greger, ZPO 31. Aufl. § 254 Rn. 14). So liegt der Fall aber vorliegend nicht. Zwar wurde der Auskunftsanspruch vorliegend verneint, aber nur mangels Beweisbarkeit. Dem Schadenersatzanspruch ist aber noch nicht endgültig jegliche Grundlage entzogen.

3. Die Zulassung der Revision beruht auf § 72 Abs. 2 Nr. 1 ArbGG. Der Frage des Beweisverwertungsverbotes von Erkenntnissen aus gezielten Datenerhebungen über Nichtstraftatbestände wird grundsätzliche Bedeutung beigemessen.

Zum Anspruch auf Entfernung einer Abmahnung nach Ende des Arbeitsverhältnisses

(**Landesarbeitsgericht Schleswig-Holstein**, Urteil vom 19. Juli 2016 – 1 Sa 37/16 –)

Dem Anspruch auf Entfernung zu Unrecht erteilter Abmahnungen fehlt regelmäßig das erforderliche Leistungsinteresse (Rechtsschutzbedürfnis), wenn das Arbeitsverhältnis zwischenzeitlich beendet wurde.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Parteien streiten über die Ansprüche des Klägers auf Entfernung von drei Abmahnungen aus seiner Personalakte.

Der Kläger war ab dem 01.05.2007 bei der Beklagten beschäftigt. § 21 des schriftlichen Arbeitsvertrags lautet:

„§ 21 Untersuchung der gesundheitlichen Eignung

Der Mitarbeiter erklärt sich bereit, sich auf Verlangen der Arbeitgeberin ärztlich untersuchen zu lassen. Die hierdurch anfallenden Kosten trägt die Arbeitgeberin. Der Mitarbeiter entbindet den untersuchenden Arzt insofern von der ärztlichen Schweigepflicht, als das Untersuchungsergebnis Einfluss auf die Erfüllung der arbeitsvertraglich vorausgesetzten Einsatzfähigkeit des Mitarbeiters haben kann“.

Am 16.12.2014 genehmigte die Beklagte dem Kläger für die Zeit vom 10. bis 28.08.2015 Urlaub. Aufgabe des Klägers war ab September 2014, für die Produktionsstätte der Beklagten in B. eine neue CNC-Fräse zu erwerben und in Betrieb zu nehmen. Am 04.05.2015 erklärte der Geschäftsführer der Beklagten sinngemäß, wegen Verzögerungen bei den Arbeiten zur Vorbereitung der Installation der Fräse könne der Urlaub bestimmter Mitarbeiter – darunter der Kläger als Verantwortlicher – in Gefahr sein.

Am 06.05.2015 sprach der Kläger dann mit dem Geschäftsführer und danach der Geschäftsführerin der Beklagten über die Frage der Urlaubsgewährung. Er bat um eine schriftliche Bestätigung dahingehend, dass ihm der Urlaub genehmigt sei. Der weitere Inhalt dieser Gespräche ist streitig.

Ab dem 07.05.2015 meldete sich der Kläger unter Vorlage ordnungsgemäß ausgestellter Arbeitsunfähigkeitsbescheinigungen bei der Beklagten arbeitsunfähig. Mit Schreiben vom 07.05.2015 lud die Beklagte den Kläger zu einer Vorstellung beim Betriebsarzt zur Feststellung der gesundheitlichen Eignung für die übernommene Arbeitsaufgabe für den 08.05.2015 ein. Der Kläger lehnte die Untersuchung unter Hinweis auf seine Arbeitsunfähigkeit und einen fehlenden berechtigten Anlass ab. Mit Schreiben vom 21.05.2015 erteilte die Beklagte dem Kläger aufgrund dieser Ablehnung unter Hinweis auf § 21 des Arbeitsvertrags eine Abmahnung.

Am 22.05.2015 bestätigte der von der Beklagten eingeschaltete medizinische Dienst der Krankenkasse die vom Hausarzt festgestellte Arbeitsunfähigkeit.

Am 10.06.2015 sollte sich der Kläger auf Veranlassung der Beklagten zu einer arbeitsmedizinischen Untersuchung bei der C. GmbH einfinden. Unter Vorlage eines in M. ausgestellten ärztlichen Attests seines Hausarztes vom 09.06.2015 teilte der Kläger mit, er könne diese Termin nicht wahrnehmen. Mit Schreiben vom 30.07.2015 erteilte ihm die Beklagte wegen dieses Sachverhalts eine weitere Abmahnung. Schließlich erteilte die Beklagte dem Klä-

ger am 07.08.2015 eine dritte Abmahnung, weil er sich am 05.08.2015 nicht zur ärztlichen Untersuchung eingefunden habe.

In erster Instanz hat der Kläger – soweit für das Berufungsverfahren von Interesse – die Entfernung der drei Abmahnungen aus der Personalakte verlangt.

Das Arbeitsgericht hat der Klage hinsichtlich der hier in Rede stehenden Streitgegenstände in vollem Umfang stattgegeben. Zur Begründung hat es im Wesentlichen ausgeführt: Die Abmahnungen seien unwirksam. Es fehle an einer Rechtsgrundlage für die Anordnung der betriebsärztlichen Untersuchung. § 21 des Arbeitsvertrags sei unwirksam, da er den Kläger unangemessen benachteilige. Die Klausel regele eine voraussetzungslose, jederzeitige Untersuchungspflicht unter teilweiser Aufhebung der ärztlichen Schweigepflicht und greife damit unzulässig in das allgemeine Persönlichkeitsrecht des Arbeitnehmers ein.

Gegen das am 04.01.2016 zugestellte Teil-Urteil hat die Beklagte am 25.01.2016 Berufung eingelegt und diese am 04.03.2016 begründet.

Zur Begründung ihrer Berufung führt sie aus:

Die Abmahnungen seien berechtigt. § 21 des Arbeitsvertrags sei im Hinblick auf die einschlägige Rechtsprechung dahin auszulegen, dass die Untersuchungspflicht nach § 21 „bei gegebener Veranlassung" bestehe. Auch zeige § 21 S. 3, dass eine Untersuchung nur möglich sein solle, wenn Zweifel daran bestünden, dass der Mitarbeiter seinen vertraglichen Pflichten nachkommen könne. Nach Beendigung des Arbeitsverhältnisses sei die Klage auch insoweit unzulässig geworden.

Der Kläger hat beantragt, die Berufung zurückzuweisen.

Er erwidert: Wegen der zwischenzeitlichen Erfüllung der Zahlungsansprüche fehle der Berufung teilweise das Rechtsschutzbedürfnis. Trotz zwischenzeitlicher Beendigung des Arbeitsverhältnisses fehle seiner Klage auf Entfernung der Abmahnungen nach einem neueren Urteil des Bundesarbeitsgerichts nicht das Leistungsinteresse.

Aus den Gründen:

B. Die Berufung ist begründet, soweit die Beklagte die Abweisung der Anträge auf Entfernung der Abmahnungen vom 21.05., 30.07. und 07.08.2015 begehrt.

I. Die Anträge auf Entfernung der Abmahnungen vom 21.05., 30.07. und 07.08.2015 sind unzulässig. Es fehlt das erforderliche Leistungsinteresse (Rechtsschutzbedürfnis), da das Arbeitsverhältnis der Parteien zwischenzeitlich beendet ist.

1. Nach einer Entscheidung des Bundesarbeitsgerichts vom 14.09.1994 (5 AZR 632/93) steht dem Arbeitnehmer nach Beendigung des Arbeitsverhältnisses im Regelfall ein Anspruch auf Entfernung einer zu Unrecht erteilten Abmahnung aus der Personalakte nicht mehr zu. Etwas anderes kann dann gelten, wenn objektive Anhaltspunkte dafür vorliegen, dass die Abmahnung dem Arbeitnehmer auch noch nach Beendigung des Arbeitsverhältnisses schaden kann (Rn 23). Ein entsprechendes Interesse wird nicht dadurch begründet, dass der Arbeitgeber sich bei der Erteilung des Endzeugnisses von den Abmahnungen leiten lässt. Denn der Arbeitnehmer kann sein Interesse daran, insgesamt nicht falsch beurteilt zu werden, in einem Zeugnisrechtsstreit durchsetzen (BAG, a.a.O., Rn 25).

Der Kläger hat sich auf eine Entscheidung des Bundesarbeitsgerichts vom 16.11.2010 (9 AZR 573/09) berufen, in der ein nachvertraglicher Anspruch des Arbeitnehmers auf Einsicht in seine Personalakte unter Hinweis auf die Pflicht des Arbeitgebers, keine unrichtigen Daten über den Arbeitnehmer aufzubewahren, begründet wird. Der Arbeitnehmer könne seine Rechte auf Beseitigung oder Korrektur unrichtiger Daten in seiner Personalakte nur geltend machen, wenn er von deren Inhalt bereits Kenntnis habe (BAG, a.a.O., Rn 42).

Hieraus ist der Schluss gezogen worden, damit habe sich die Entscheidung des Bundesarbeitsgerichts vom 14.11.1994 erledigt (so etwa LAG Berlin-Brandenburg, Beschl. v. 18.07.2011 – 10 Ta 1325/11 –; KR-Fischermeier, 10. Aufl., § 626 BGB, Rn 283).

2. Demgegenüber hat der zuständige zweite Senat des Bundesarbeitsgerichts in einer Entscheidung vom 19.04.2012 (2 AZR 233/11) an seiner Rechtsprechung aus dem Jahre 1994 uneingeschränkt festgehalten und ausdrücklich ausgeführt, nach beendetem Arbeitsverhältnis könne ein Anspruch auf Entfernung von Abmahnungen nur ausnahmsweise gegeben sein, wenn objektive Anhaltspunkte dafür bestehen, eine Abmahnung könne dem Arbeitnehmer auch noch nach Beendigung des Arbeitsverhältnisses schaden (a.a.O., Rn 51).

3. Das Berufungsgericht folgt dem fachlich zuständigen zweiten Senat und hält ebenfalls eine Klage auf Entfernung von Abmahnungen im beendeten Arbeitsverhältnis für regelmäßig unzulässig, da hierfür ein Rechtsschutzbedürfnis nicht besteht. Anders als der Kläger und die von ihm zitierte Rechtsprechung und Literatur meint, hat das Bundesarbeitsgericht in seinem Urteil vom 16.11.2010 allein zum Anspruch des Arbeitnehmers auf Einsichtnahme in eine Personalakte nach Beendigung des Arbeitsverhältnisses Stellung genommen. Mit der Entscheidung ist dem Kläger kein Recht auf Entfernung einer Abmahnung aus der Personalakte zugesprochen worden. Das Bundesarbeitsgericht hat nur festgestellt, dass Voraussetzung für einen solchen Anspruch der Einblick in die Personalakte ist. Zum hier in Rede stehenden Entfernungsanspruch verhält sich diese Entscheidung nicht. Insoweit verbleibt es dabei, dass der Kläger ein Leistungsinteresse darlegen muss. Es ist also vorzutragen, dass objektive Anhaltspunkte dafür bestehen, dass die Abmahnung ihm auch noch nach Beendigung des Arbeitsverhältnisses schaden kann.

4. Hierfür gibt es keine Anhaltspunkte. Der Kläger hat hierzu auch nichts dargelegt. Die Beklagte ist weder berechtigt, noch verpflichtet, die Personalakte an andere Arbeitgeber weiterzuleiten. Die – potenziell unrichtigen – Eintragungen in der Personalakte sind auch nicht mehr zur Kenntnisnahme durch betriebsinterne Mitarbeiter bestimmt.

Zum Umfang des Einsichtsrechts eines Einzelbetriebsrates in Bruttolohn- und Gehaltslisten

(**Landesarbeitsgericht Schleswig-Holstein**, Beschluss vom 9. Februar 2016 – 1 TaBV 43/15 –)

Einem neben drei weiteren Betriebsräten in einem Unternehmen etablierten Einzelbetriebsrat steht ein Recht auf Einsichtnahme in die Gehaltslisten sämtlicher Arbeitnehmer des Unternehmens – mit Ausnahme der leitenden Angestellen – zwecks Überprüfung des Gleichbehandlungsgrundsatzes zu, da dieser Grundsatz unternehmensbezogen gilt.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Beteiligten streiten über den Umfang des Einsichtsrechts des antragstellenden Betriebsrats in die bei der Antragsgegnerin (Arbeitgeberin) geführten Bruttolohn- und Gehaltslisten.

Die Arbeitgeberin führt den Omnibuslinienverkehr im Rahmen des H. Verkehrsverbunds durch. Für ihr Unternehmen sind vier Betriebsräte errichtet, darunter der Antragsteller sowie die Betriebsräte in B., Q. und E. Es besteht ein Gesamtbetriebsrat. Der antragstellende Betriebsrat besteht aus elf Mitgliedern und hat einen Betriebsausschuss gebildet.

Mit Schreiben vom 29.01.2015 begehrte der Antragsteller die Einsichtnahme in die Bruttolohn- und Gehaltslisten sämtlicher Mitarbeiter des Unternehmens. Die Arbeitgeberin lehnte dies mit dem Hinweis ab, der Betriebsrat sei nur für die S. Mitarbeiter zuständig und könne daher nur Einsicht in deren Gehaltslisten erhalten. Darauf hat der Betriebsrat das vorliegende Beschlussverfahren eingeleitet.

Das Arbeitsgericht hat nach dem Antrag des Betriebsrats erkannt und zur Begründung im Wesentlichen ausgeführt: Weitere Betriebsräte und der Gesamtbetriebsrat seien am vorliegenden Verfahren nicht zu beteiligen, da sie nicht in ihren Rechten betroffen seien. Der Antrag sei begründet. Dies folge aus § 80 Abs. 2 Satz 2 BetrVG i.V.m. dem arbeitsrechtlichen Gleichbehandlungsgrundsatz. Dieser greife auch dann ein, wenn eine entgeltverteilende Entscheidung des Arbeitgebers nicht auf einen Betrieb beschränkt sei. Das Einsichtnahmerecht des Betriebsrats auch in die Lohn- und Gehaltslisten anderer Betriebe diene dazu, dem Betriebsrat Kenntnis darüber zu verschaffen, ob die Arbeitgeberin entgegen dem Gleichbehandlungsgrundsatz Leistungen gewähre. Datenschutzrechtliche Bedenken bestünden nicht.

Gegen diesen am 18.06.2015 zugestellten Beschluss hat die Arbeitgeberin am 25.06.2015 Beschwerde eingelegt.

Aus den Gründen:

Das Arbeitsgericht hat dem Antrag des Betriebsrats zu Recht und im Wesentlichen auch mit zutreffender Begründung stattgegeben. Auf diese wird zunächst Bezug genommen. Im Hinblick auf die Beschwerdebegründung sind die vorliegenden Ausführungen veranlasst.

I. Beteiligte des Verfahrens sind nur der antragstellende Betriebsrat und die Arbeitgeberin. Die weiteren Betriebsräte und der Gesamtbetriebsrat sind nicht am Verfahren beteiligt.

1. Nach § 83 Abs. 3 ArbGG haben in einem Beschlussverfahren neben dem Antragsteller diejenigen Stellen ein Recht auf Anhörung, die nach dem BetrVG im Einzelfall am Verfahren beteiligt sind. Beteiligte in Angelegenheiten des BetrVG ist jede Stelle, die durch die begehrte Entscheidung in ihrer betriebsverfassungsrechtlichen Stellung unmittelbar betroffen ist (ständige Rechtsprechung, z.B. BAG, Beschl. v. 25.09.2012 – 1 ABR 17/12 – [...], Rn. 11).

2. Danach sind vorliegend nur der Antragsteller und die Arbeitgeberin Beteiligte des Verfahrens.

Weitere Beteiligte werden durch den Beschluss im vorliegenden Verfahren in ihrer betriebsverfassungsrechtlichen Rechtsstellung nicht betroffen. Entgegen der Auffassung der Arbeitgeberin steht bei einem stattgebenden Beschluss nicht fest, dass das streitige Einsichtsrecht allen anderen Betriebsräten und/oder dem Gesamtbetriebsrat nicht zusteht.

Geht es dem Betriebsrat in Zusammenhang mit dem Einsichtsrecht nach § 80 Abs. 2 Satz 2 BetrVG um die Wahrnehmung allgemeiner Aufgaben nach § 80 Abs. 1 BetrVG, kann das Einsichtsrecht nämlich sowohl dem Betriebsrat, als auch dem Gesamtbetriebsrat zustehen (Richardi/Thüsing, BetrVG, 15. Aufl., § 80 Rn. 88). Nichts anderes gilt für ein mögliches Einsichtsrecht der weiteren Betriebsräte der Arbeitgeberin. Das hängt letztlich damit zusammen, dass das Einsichtsrecht nur der Vorbereitung der Wahrnehmung von weiteren Aufgaben und/oder Mitbestimmungsrechten des Betriebsrats dient. Erst wenn feststeht, welche konkrete betriebsverfassungsrechtliche Aufgabe sich für den Betriebsrat aus der Einsichtnahme in die Lohn- und Gehaltslisten ergibt, kann festgestellt werden, in wessen Zuständigkeit (Betriebsrat oder Gesamtbetriebsrat) diese fällt.

Wird also dem Antrag stattgegeben, bedeutet dies nur, dass das Einsichtsrecht auch dem Antragsteller dieses Verfahrens zusteht, nicht aber, dass es anderen Betriebsräten nicht zusteht. Nichts anderes gilt bei Antragsabweisung. Diese Entscheidung wirkt nur im Verhältnis zwischen dem antragstellenden Betriebsrat und der Arbeitgeberin. Über den Umfang des Einblicksrechts weiterer Betriebsräte oder insbesondere des Gesamtbetriebsrats ist damit nichts gesagt.

IV. Der Antrag ist begründet.

Das vom Betriebsrat geltend gemachte Einsichtsrecht folgt aus § 80 Abs. 2 Satz 2 BetrVG. Nach dieser Vorschrift sind dem Betriebsrat auf Verlangen jederzeit die zur Durchführung seiner Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen; in diesem Rahmen ist u.a. der Betriebsausschuss berechtigt, in die Listen über die Bruttolöhne und -gehälter Einblick zu nehmen.

Die Voraussetzungen der Vorschrift liegen vor.

1. Zu den Aufgaben des Betriebsrats nach § 80 Abs. 2 Satz 2 BetrVG gehören namentlich auch die in § 80 Abs. 1 genannten allgemeinen Aufgaben des Betriebsrats. Nach § 80 Abs. 1 Nr. 1 BetrVG hat der Betriebsrat die allgemeine Aufgabe, darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden. Dieses Überwachungsrecht umfasst das gesamte zugunsten der Arbeitnehmer geschaffene normative Recht, einschließlich des Richterrechts. Hierzu zählt auch der Gleichbehandlungsgrundsatz (BAG v. 14.01.2014, Rn. 23; Fitting, 27. Aufl., § 80, Rn. 6; Richardi, a.a.O., Rn. 17; Däubler/Kittner, BetrVG, 14. Aufl., § 80, Rn. 127).

2. Das Einsichtsrecht besteht allerdings nur, soweit es zur Durchführung der Aufgaben des Betriebsrats erforderlich ist. Auch diese Voraussetzung liegt hier vor. Die Einsichtnahme in die Gehaltslisten sämtlicher Arbeitnehmer des Unternehmens mit Ausschluss der leitenden Angestellten dient der Überprüfung, ob die Arbeitgeberin den Gleichbehandlungsgrundsatz im Unternehmen wahrt.

a) Der Gleichbehandlungsgrundsatz gilt nach der Rechtsprechung des Bundearbeitsgerichts grundsätzlich unternehmensbezogen. Eine Unterscheidung zwischen Arbeitnehmern verschiedener Betriebe ist nur aus sachlichen Gründen zulässig, die vom Arbeitgeber darzulegen sind (BAG v. 03.12.2008 – 5 AZR 74/08 – [...], Rn. 16).

Zur Überwachung dieses Gleichbehandlungsgrundsatzes ist die Einsichtnahme in die Bruttolohn- und Gehaltslisten aller Arbeitnehmer mit Ausnahme der leitenden Angestellten des Unternehmens erforderlich, weil denkbar ist, dass die Arbeitgeberin in einem Betrieb allgemeine Leistungen nach einem generalisierenden Prinzip gewährt und im Betrieb des Antragstellers nicht. Das kann, soweit es um finanzielle Zuwendungen geht, durch eine Einsichtnahme in die Bruttolohn- und Gehaltsliste festgestellt werden.

b) Allerdings kann der Betriebsrat nicht – etwa im Wege der Prozessstandschaft – für einzelne Arbeitnehmer die Einhaltung des Gleichbehandlungsgrundsatzes durchsetzen. Diese sind insoweit auf den Individualrechtsweg angewiesen. Der Betriebsrat ist aber berechtigt, wegen eines Verstoßes gegen den Gleichbehandlungsgrundsatz beim Arbeitgeber auf Abhilfe zu drängen, und auch verpflichtet, den Arbeitnehmer gegenüber dem Arbeitgeber zu unterstützen (Fitting, a.a.O., Rn. 15). Daneben ist der Betriebsrat auch für die Umsetzung des Gleichbehandlungsgrundsatzes im Betrieb im Rahmen der betrieblichen Lohngestaltung zuständig. Auch wenn eine verteilende Entscheidung des Arbeitgebers sich über mehrere Betriebe eines Unternehmens erstreckt, folgt hieraus nicht die Zuständigkeit des Gesamtbetriebsrats (BAG v. 23.03.2010 – 1 ABR 82/08).

c) Einen konkreten Anlass oder gar einen Verstoß der Arbeitgeberin gegen den Gleichbehandlungsgrundsatz muss der Betriebsrat nicht darlegen. Das Einblicksrecht ist nicht anlassbezogen (BAG v. 14.01.2014 – 1 ABR 54/12 – juris, Rn. 23).

d) Datenschutzrechtliche Bedenken bestehen gegen die Einsichtgewährung nicht.

Bruttoentgeltlisten enthalten personenbezogene Daten im Sinne von § 2 Abs. 1 BDSG, die von Arbeitgebern zur Durchführung des Arbeitsverhältnisses nach § 32 Abs. 1 Satz 1 BDSG zulässigerweise erhoben, verarbeitet und genutzt werden. Gewährt die Arbeitgeberin einem Betriebsratsmitglied nach § 80 Abs. 2 Satz 2 Hs. 2 BetrVG Einsicht in die Bruttoentgeltlisten, handelt es sich um eine nach § 32 Abs. 1 BDSG zulässige Form der Datennutzung. Dies folgt schon daraus, dass die Beteiligungsrechte der Interessenvertretung der Beschäftigten nach § 32 Abs. 3 BDSG durch die nach Abs. 1 dieser Bestimmung erlaubte Datennutzung nicht berührt werden. Zu den Interessenvertretungen der Beschäftigten zählt auch der Betriebsrat. Hinzu kommt, dass dieser selbst Teil der verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG ist (BAG, a.a.O., Rn. 28).

Mit dem Bundesarbeitsgericht ist davon auszugehen, dass die Einsichtsgewährung keine Weitergabe von Daten an Dritte darstellt.

e) Dem Anspruch steht auch nicht entgegen, dass der Betriebsrat nicht für sämtliche Arbeitnehmer des Unternehmens zuständig ist.

Das Auskunftsrecht des Arbeitgebers erstreckt sich auch in anderen Fällen auf Mitarbeiter, die nicht durch den Betriebsrat vertreten werden. Nach § 80 Abs. 2 Satz 1 BetrVG erstreckt sich etwa die Unterrichtung auch auf die Beschäftigung von Personen, die nicht in einem Arbeitsverhältnis zum Arbeitgeber stehen. Das Bundesarbeitsgericht hat bereits seit langem anerkannt, dass der Informationsanspruch des Betriebsrats sich auch auf freie Mitarbeiter, für die der Betriebsrat ebenfalls nicht zuständig ist, bezieht (BAG v. 15.12.1998 – 1 ABR 9/98 –).

f) Schließlich besteht auch keine vorrangige Zuständigkeit des Gesamtbetriebsrats.

aa) Richtig ist, dass im Bereich der zwingenden Mitbestimmung für das Verhältnis der betriebsverfassungsrechtlichen Organe der Grundsatz der Zuständigkeitstrennung gilt. Hier sind ausschließlich entweder die einzelnen Betriebsräte oder der Gesamtbetriebsrat oder der Konzernbetriebsrat zuständig. Die gesetzliche Zuständigkeitsverteilung ist zwingend und unabdingbar (BAG v. 14.11.2006 – 1 ABR 4/06 – juris, Rn. 34). Dieser Grundsatz der Zuständigkeitstrennung gilt im Prinzip auch in Angelegenheiten, die nicht der zwingenden Mitbestimmung unterliegen (Fitting, § 50, Rn. 11) mit hier nicht in Betracht kommenden Einschränkungen.

bb) Vorliegend geht es dem Betriebsrat aber gerade nicht um die Ausübung von Mitbestimmungsrechten. Wie bereits oben ausgeführt, dient die Einsichtnahme erst der Vorbereitung der Wahrnehmung von Aufgaben durch den Betriebsrat. In diesem Stadium steht noch gar nicht fest, ob der Betriebsrat ein Mitbestimmungsrecht ausüben will, und damit stellt sich auch die Frage der Zuständigkeit noch nicht. Für die Information und Unterstützung der Arbeitnehmer zur Geltendmachung ihrer Rechte ist jedenfalls der örtliche Betriebsrat zuständig. Stellt ein Betriebsrat im Rahmen seiner Überwachungsaufgaben Rechtsverstöße fest, hat er den Arbeitgeber auf sie hinzuweisen und auf Abhilfe zu drängen. Beeinträchtigt ein Rechtsverstoß die Rechte von Arbeitnehmern, hat der Betriebsrat auch diese zu informieren und auf die Möglichkeit gerichtlicher Schritte hinzuweisen (GK-BetrVG, 10. Aufl., § 80, Rn. 28; Fitting, § 80, Rn. 15).

g) Der Beschluss des Betriebsrats B./G., wonach die Arbeitgeberin aufgefordert wird, dem hier antragstellenden Betriebsrat die Einsicht in die Gehaltsliste in die von ihr vertretenen Arbeitnehmer nicht zu gewähren, ist erkennbar unerheblich. Der Beschluss eines Betriebsrats eines anderen Betriebs kann die betriebsverfassungsrechtliche Zuständigkeit des Antragstellers nicht beeinträchtigen. In einem etwaigen Beschlussverfahren, das vom B. Betriebsrat angekündigt worden ist, könnte sich die Arbeitgeberin jederzeit auf die gesetzliche Zuständigkeitsregelung und den Beschluss dieser Kammer beziehen.

Berichte, Informationen, Sonstiges

BayLDA: Datenschutzaufsichtsbehörden prüfen grenzüberschreitende Datenübermittlungen

In einer koordinierten schriftlichen Prüfungsaktion nehmen zehn deutsche Datenschutzaufsichtsbehörden Übermittlungen personenbezogener Daten in das Nicht-EU-Ausland genauer unter die Lupe. Die Prüfung soll dabei auch der Sensibilisierung von Unternehmen für gerade die Verarbeitungsprozesse dienen, bei denen personenbezogene Daten in Nicht-EU-Länder übermittelt werden – wie es bspw. bei Cloud Computing häufig der Fall ist.

In den letzten Jahren haben grenzüberschreitende Übermittlungen von personenbezogenen Daten in der Privatwirtschaft weiter massiv zugenommen. Zu den Ursachen dieser Entwicklung zählen die wirtschaftliche Globalisierung wie auch die stetige Ausbreitung von Dienstleistungen und Produkten des sog. Cloud Computing. Selbst viele kleinere und mittlere Unternehmen in Deutschland verarbeiten inzwischen zahlreiche personenbezogene Daten (z.B. von Kunden, Mitarbeitern oder Bewerbern) häufig auf Servern externer Dienstleister, oft außerhalb der Europäischen Union. Dies ist vor allem bei Angeboten wie dem sog. Software as a Service der Fall. Ein klassisches Beispiel hierfür sind Office-Anwendungen „aus dem Internet", die standortunabhängig und flexibel genutzt werden können. Viele dieser Dienste stammen jedoch von US-Unternehmen und setzen deshalb meist die Übermittlung personenbezogener Daten in die USA und/oder in andere Nicht-EU-Staaten voraus. Die bisherige Erfahrung der Datenschutzaufsichtsbehörden zeigt, dass sich Unternehmen bei Nutzung solcher Produkte nicht immer der Tatsache bewusst sind, dass dadurch eine Übermittlung personenbezogener Daten in Nicht-EU-Staaten stattfindet und entsprechende datenschutzrechtliche Konsequenzen daraus resultieren.

Möchte ein Unternehmen personenbezogene Daten in Länder außerhalb der Europäischen Union übermitteln, so muss es zuerst prüfen, ob überhaupt sichergestellt werden kann, dass die Daten auch nach der Übermittlung noch angemessen geschützt bleiben – andernfalls muss die Übermittlung unterbleiben. Entscheidend ist daher, im Unternehmen frühzeitig eine Sensibilisierung dafür zu erzeugen, ob und ggf. im Rahmen welcher Verarbeitungen das Unternehmen personenbezogene Daten in Nicht-EU-Staaten übermitteln möchte oder vielleicht sogar bereits übermittelt. Finden solche Übermittlungen statt, so muss sich das Unternehmen zwingend Gedanken machen, inwieweit diese auf eine datenschutzrechtliche Grundlage gestützt werden können oder nicht.

Vor diesem Hintergrund werden zehn deutsche Datenschutzaufsichtsbehörden (Bayern, Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und Sachsen- Anhalt) in den nächsten Wochen eine koordinierte schriftliche Prüfungsaktion zur Abfrage von Übermittlungen personenbezogener Daten durch nicht-öffentliche Stellen, d.h. insbesondere Unternehmen, in Nicht-EU-Staaten durchführen. Im Rahmen der Prüfung werden rund 500 Unternehmen angeschrieben, die nach dem Zufallsprinzip ausgewählt wurden. Die Aufsichtsbehörden haben dabei Wert darauf gelegt, Unternehmen unterschiedlicher Größenordnungen und verschiedener Branchen einzubeziehen.

Ein wichtiges Ziel der Prüfung liegt in der Sensibilisierung der Unternehmen für Datenübermittlungen in Länder außerhalb der Europäischen Union. Um Unternehmen das Auffinden solcher Übermittlungen zu erleichtern, wird auch gezielt nach dem Einsatz von Produkten und Leistungen externer Anbieter gefragt, die – nach bisherigen Erfahrungen der Aufsichtsbehörden – mit einer Übermittlung personenbezogener Daten in Nicht-EU-Staaten verbunden sind. Gefragt wird zum Beispiel nach der Inanspruchnahme externer Leistungen und Produkte in Bereichen wie Fernwartung, Support, Ticketing-Bearbeitung, aber auch Customer Relationship Management oder Bewerbermanagement. Die Unternehmen werden dann aufgefordert, die entsprechenden von ihnen genutzten Dienstleistungen und Produkte konkret zu nennen.

Sofern personenbezogene Daten in Nicht-EU-Staaten übermittelt werden, sind die kontrollierten Unternehmen darüber hinaus aufgefordert anzugeben, auf welcher datenschutzrechtlichen Grundlage die Übermittlungen erfolgen. Mitgeteilt werden muss bspw., ob für das Zielland durch Beschluss der Europäischen Kommission ein angemessenes Datenschutzniveau anerkannt ist (dazu zählt auch der sog. EU-U.S Privacy Shild), ob Standardvertragsklauseln als Grundlage verwendet werden, ob die Übermittlungen auf Einwilligungen der Betroffenen gestützt werden o. a.

„Übermittlungen personenbezogener Daten in Nicht-EU-Staaten gehören inzwischen auch bei vielen mittelständischen Unternehmen zum Alltag, nicht zuletzt aufgrund der immer stärkeren Verbreitung von Angeboten des Cloud Computing. Unternehmen müssen sich aber dessen bewusst sein, dass hierfür besondere datenschutzrechtliche Anforderungen gelten. Durch die koordinierte Prüfaktion, an der sich zehn deutsche Datenschutzaufsichtsbehörden beteiligen, wollen wir auch die Sensibilität der Unternehmen in diesem Bereich erhöhen," betont Thomas Kranig, der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht. „Ausgehend von der Beantwortung des Fragebogens kann

und wird das Bayerische Landesamt für Datenschutzaufsicht dort, wo ach dies als notwendig zeigt, auch in eine tiefere Prüfung einsteigen."

(Pressemitteilung vom 10.11.2016)

BfDI: Datenschutz bei Gesundheits-Apps und Wearables mangelhaft

Gesundheits- und Fitness-Apps und die dazugehörigen Wearables boomen. Doch viele Anbieter missachten gesetzliche Anforderungen. Nutzerinnen und Nutzer werden nicht oder nur mangelhaft darüber informiert, welche ihrer sensiblen Gesundheitsdaten von wem und zu welchem Zweck gespeichert werden. Gesammelte Daten können oftmals nicht gelöscht werden.

Der Markt für Apps im Gesundheitsbereich boomt. Das Angebot umfasst weltweit geschätzt rund eine Million Angebote mit Gesundheitsbezug. Egal ob Fitness-, Gesundheits-, Lifestyle-Apps, Sport- oder medizinische Apps, gemeinsam ist allen, dass sie die Körperdaten ihrer Nutzer elektronisch erfassen. Um besser zu verstehen, was mit diesen sensiblen Daten geschieht, haben Datenschutzbehörden aus Bund und Ländern stichprobenartig Geräte und Apps von verschiedenen Anbietern überprüft.

Dabei zeigt sich, dass Hersteller, Betreiber und Verkäufer der getesteten Geräte und Apps die Nutzer oft nicht ausreichend darüber informieren, was mit ihren Daten geschieht. Stichpunktartige Anfragen der Datenschützer nach Auskunft zu gespeicherten Daten wurden mit pauschalen Verweisen auf Datenschutzerklärungen beantwortet oder wegen Nicht-Zuständigkeit abgewiesen. Viele Hersteller sind in Deutschland nur mit Serviceniederlassungen präsent, während ihr Hauptsitz in anderen EU- oder Dritt-Staaten liegt. Erst unter der ab Mai 2018 EU-weit gültigen Datenschutzgrundverordnung können deutsche Aufsichtsbehörden Beschwerden deutscher Verbraucher wirksamer bearbeiten. Sie appellieren daher an Bürgerinnen und Bürger vor dem Kauf und dem Einsatz von Wearables und Gesundheits-Apps genau auf den Schutz ihrer Daten zu achten.

So erfüllen die meisten der untersuchten Datenschutzerklärungen nicht die gesetzlichen Anforderungen. Sie sind in der Regel zu lang, schwer verständlich und enthalten zu essentiellen Datenschutzfragen nur pauschale Hinweise. Viele Erklärungen liegen nicht einmal in deutscher Sprache vor. Oftmals wurde auch nur auf die generelle Datenschutzerklärung des Unternehmens verwiesen, die kaum konkreten Bezug zu dem Wearable und den besonders schützenswerten Gesundheitsdaten hat.

Unbefugte Weitergabe der Gesundheitsdaten an Dritte

Oft werden die durch die Geräte erhobenen Gesundheitsdaten durch externe Dritte verarbeitet. Durch die unklaren Regelungen zur Datenverarbeitung entgleiten diese Daten dabei der Kontrolle durch die Nutzer. Zwar scheinen Einzelinformationen wie Körpergewicht, zu-

rückgelegte Schritte, Dauer des Schlafes oder Herzfrequenz für sich betrachtet oftmals wenig aussagekräftig. In der Regel werden diese Daten jedoch mit eindeutigen Personenkennungen oder auch Standortdaten verknüpft. Bei einer dauerhaften Nutzung von Wearables fallen damit so viele Informationen an, dass sich ein präzises Bild des Tagesablaufs und Gesundheitszustands der jeweiligen Nutzer ergibt.

Viele der Geräte und Apps bieten die Möglichkeit, aufgezeichnete Fitness-Daten mit Freunden zu teilen. Häufig fehlt dabei ein Warnhinweis, dass die Weitergabe der sensiblen Nutzerdaten nur dann geschehen darf, wenn der Nutzer dieses ausdrücklich wünscht und bewusst hierin einwilligt. Einige Hersteller geben an, dass sie die Fitness-Daten der Nutzer für Forschungszwecke und Marketing verwenden und an verbundene Unternehmen weitergeben. Die Nutzer erfahren jedoch auch hier häufig nicht, um wen es sich dabei handelt, noch können sie der Weitergabe ihrer Daten widersprechen.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff warnt daher: Fitness- und Bewegungsdaten, wie sie von vielen Wearables erhoben werden, verraten sehr viel über das Leben und die Gesundheit ihrer Nutzer. Vor dem Kauf von Wearables und der Installation der dazugehörigen Apps auf dem Smartphone sollten sich die Nutzer fragen, ob sie wissen, was mit ihren Gesundheitsdaten geschieht und an wen sie weitergegeben werden. Auch die Hersteller und Betreiber der Geräte und Apps sind in der Pflicht. Viele Probleme ließen sich vermeiden, wenn Fitnessdaten lediglich lokal auf einem Smartphone gespeichert und verarbeitet würden.

Löschen der Daten kaum möglich

Oft bieten Geräte und die damit verbundenen Nutzerkonten keine Möglichkeit, Daten selbst vollständig zu löschen. Will man etwa ein gebrauchtes Gerät weiterverkaufen, so genügt es nicht, die App zu löschen, um bereits gesammelte Daten zu vernichten. Bedenken bereiten den Datenschützern auch die technischen Analysetools mit denen Hersteller nachverfolgen, wie die Geräte oder Apps genutzt werden. Hier fehlt der Nachweis, dass gesammelte Daten tatsächlich anonym sind. Daher besteht die Gefahr, dass diese Daten für Werbezwecke und zur Profilbildung verwendet werden.

Bereits im April 2016 hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder von den Herstellern von Gesundheits-Apps und Wearables mehr Transparenz gefordert sowie korrekte Einwilligungserklärungen und ein Bekenntnis zur Datensparsamkeit. Die jetzt vorliegenden Untersuchungsergebnisse unterstreichen die Dringlichkeit der Forderungen der Datenschutzkonferenz.

(Pressemitteilung Nr. 19/2016 vom 05.12.2016)

Literaturhinweise

Buchbesprechungen

Matthias Lachenmann, **Datenübermittlung im Konzern,** Dissertation an der Universität Oldenburg, Hrsg. Prof. Dr. Jürgen Taeger, Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2016, S. 398, 49,80 €

Der Schwerpunkt der Dissertation von Lachenmann widmet sich noch der Rechtslage nach dem BDSG. Speziell dargestellt wird die DS-GVO im 3. Kapitel des Buches, wobei sich nach einer Einführung in den wesentlichen Regelungsinhalt anschließend konzernintern zu berücksichtigende Rechte betroffener Personen, Zulässigkeitsvoraussetzungen der Datenverarbeitung und -übermittlung nebst der Möglichkeiten der konzerninternen Auftragsverarbeitung dargestellt werden. Zutreffend hält der Autor dabei an der rechtlichen Privilegierung auch im Rahmen der DS-GVO fest, d.h. dass der Verarbeiter für die Verarbeitung an sich, nicht jedoch für die Weitergabe an den Auftragnehmer einer Erlaubnis bedarf. Bei der Frage der Privilegierung von Übermittlungen im Konzern (ErwG 48) sieht der Autor zutreffend kein Konzernprivileg, jedoch eine Unterstützung bei Datenübermittlungen, die auf einer Interessenabwägung beruhen. Dabei sind auch die Ausführungen zur Schaffung von gemeinsam verantwortlichen Stellen von Relevanz.

Die vorherstehenden Kapitel 1 bis 2 beleuchten vollständig alle sich aus der derzeitigen Rechtslage stellenden Fragen von Datenverarbeitungen mit

Konzernbezug, wobei der Darstellung der unterschiedlichen rechtlichen Grundlagen der konzerninternen Datenübermittlung besondere Aufmerksamkeit gewidmet wird. Umfassend (25 Seiten) gewürdigt wird in Kapitel 2 IX der Erlaubnistatbestand des § 32 BDSG für eine Übermittlung von Beschäftigtendaten, wobei das konzerndimensionale Arbeitsverhältnis insbesondere eine Rolle spielt. Von Praxisrelevanz sind die Ausführungen zur Einwilligung der Betroffenen als Rechtsgrundlage der Datenübermittlung und deren Fortbestand bei gesellschaftsrechtlichen Änderungen des Konzerns. Ändert sich durch eine Umwandlung die wirtschaftliche und rechtliche Identität der verantwortlichen Stelle nicht oder ändert sich die verantwortliche Stelle im Wege der Gesamtrechtsnachfolge, wirken die Einwilligungen fort.

Für denjenigen, der sich zusammenfassend über die Aussagen des Buches informieren will, sind die in Kapitel 4 wiedergegebenen 9 Thesen und die nachfolgenden, in 57 kurzen Abschnitten bestehenden prägnanten Zusammenfassungen der Ergebnisse lesenswert.

Das Buch hat seinen besonderen Wert darin, dass es das Thema in eindeutig abschließender Weise zunächst an Hand des BDSG abhandelt, dann jedoch den Ausblick auf das kommende Recht in vergleichender Weise, insbesondere insoweit sich die Rechtslage ändern wird, umfassend darstellt. Eine Veröffentlichung, die jeder, der mit Datenverarbeitungen im Konzern befasst ist, in seinen Literaturbestand aufnehmen sollte.

(Prof. Peter Gola, Königswinter)

Daniel Schmid, **Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen** – Eine datenschutzrechtliche Betrachtung der Auslagerung von Kunden-, Personal- und Mandantendaten, Duncker & Humblot, 2017, Internetrecht und Digitale Gesellschaft, Band 5, 291 S., Print: 79,90 €, E-Book: 71,90 €

Cloud Computing, also die flexible und bedarfsabhängige Bereitstellung bzw. Nutzung von IT-Ressourcen, nimmt aufgrund der möglichen Kostenersparnis in kleinen und mittelständischen Unternehmen eine immer größere Rolle ein. Die Nutzung von Cloud-Diensten stellt diese Unternehmen vor datenschutzrechtliche Herausforderungen. Das gilt besonders derzeit, da es mit der Safe-Harbor-Entscheidung des EuGH, dem EU-US Privacy Shield und der Europäischen Datenschutzgrundverordnung zu einigen weitreichenden Änderungen im europäischen Datenschutzrecht gekommen ist bzw. kommen wird. Diese Untersuchung geht der Frage nach, ob kleine und mittelständische Unternehmen bzw. Rechtsanwaltskanzleien mit Sitz in Deutschland ihre Kunden-, Personal- bzw. Mandantendaten im Rahmen eines sog. Software-as-a-Service (SaaS) Dienstes an einen deutschen, europäischen oder US-amerikanischen Cloud-Anbieter datenschutzkonform auslagern können. Dabei wird u.a. ein Schwerpunkt auf die Auftragsdatenverarbeitung und die Möglichkeiten eines internationalen Datentransfers am Beispiel eines US-amerikanischen Cloud-Anbieters gelegt.

(Redaktion)

Felix Zimmermann, **Der Schutz des publizistischen Systems vor Werbeplatzierungen** – Gesetzgeberische Spielräume und verfassungsrechtliche Grenzen bei der Regulierung von Product Placements und anderen Werbeplatzierungen in elektronischen Medien, Hamburger Schriften zum Medien-, Urheber- und Telekommunikationsrecht, Bd. 9, Nomos Verlag, 2016, 522 S., broschiert, 129,– €

Werbung in Medieninhalten wird als ein Weg angesehen, die Finanzierungskrise für Inhalte abzumildern. Nach dem verfassungsrechtlichen Trennungsgrundsatz dürfen Werbung und Medieninhalt nicht vermischt werden. Doch nicht jede Werbeplatzierung ist insofern von gleicher Relevanz. Das Buch zeigt, welche Spielräume und Grenzen der Gesetzgeber bei der Regulierung von Werbeplatzierungen zu beachten hat. Dabei verfolgt es den Ansatz, den Trennungsgrundsatz stets auf die Ursachen für dessen Fundierung zurückzuführen, nämlich die Programmautonomie und das Rezipientenvertrauen. Diese Aspekte streiten je nach Art und Thema der Werbeplatzierung und des Medieninhalts mal mehr und mal weniger für die Trennung und Kennzeichnung von Werbung. Unter Berücksichtigung verfassungs- und europarechtlicher Vorgaben wird die einfach-rechtliche Lage untersucht. Dabei wird festgestellt, dass im Rundfunkstaatsvertrag verfassungswidrige Regelungen vorliegen – vor allem in Bezug auf Kennzeichnungsvorschriften.

(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.

Eckhardt, Jens, **Anwendungsbereich des Datenschutzrechts – geklärt durch den EuGH?** CR 2016, S. 786 ff.
Erörtert wird die Entscheidung des EuGH (RDV 2016, 326) zum Personenbezug von IP-Adressen. Das Gericht hatte zwar nur die Frage zu entscheiden, ob die dynamische IP-Adresse für den Betreiber einer Webseite per se ein personenbezogenes Datum ist. In der Sache musste er beantworten, wann das Datenschutzrecht zur Anwendung kommt. Der EuGH hatte sich darüber hinaus mit der weiteren Frage zu befassen, ob die "schwarz-weiß"-Regelung in § 15 TMG mit der Richtlinie 95/46/EG vereinbar ist, da sie keine Interessenabwägung als Rechtsgrundlage für die Speicherung der dynamischen IP-Adresse durch den Webseitenbetreiber vorsieht. Der Beitrag arbeitet zum einen heraus, wie der EuGH die Grundsatzfrage nach der Bestimmbarkeit einer Person geklärt hat (I.) und geht zum anderen der Frage nach, wie die Zulässigkeit der Speicherung dynamischer IP-Adressen angesichts der Erforderlichkeit einer Zulässigkeit aufgrund einer Interessenabwägung beurteilt werden muss (II.). Zu beiden Aspekten der Entscheidung wird zudem untersucht, ob und inwieweit die Entscheidung unter der DS-GVO die Rechtsanwendung bestimmen wird.

Gerpott, Thorsten J., **Vorschlag der Kommission zur Weiterentwicklung des europäischen Rechtsrahmens für den Telekommunikationssektor,** K&R 2016, S. 801
Die Europäische Kommission hat im September 2016 Entwürfe für eine Richtlinie und eine Verordnung zur Weiterentwicklung des Rechts- und Institutionenrahmens für elektronische Kommunikationsnetze und -dienste veröffentlicht. Dieser Beitrag gibt einen Überblick bezüglich zentraler Änderungen des bisherigen Unionsrechts, die mit den Vorschlägen verbunden sind, und nimmt eine erste Bewertung aus regulierungsökonomischer Sicht vor.

Körner, Marita, **Die Datenschutz-Grundverordnung und die nationale Regelungsmöglichkeiten für Beschäftigtendatenschutz,** NZA 2016, S. 1383
Die Verfasserin lotet die Reichweite des Art. 88 DS-GVO aus und meldet Kritik an dem Vorhaben des BMI zur Übernahme des § 32 BDSG in das BDSG-neu an, indem sie die Einhaltung des Minimumstandards der DS-GVO nach Art. 88 Abs. 2 anmahnt.

Kort, Michael, **Die Zukunft des deutschen Beschäftigungsdatenschutzes,** ZD 2016, S. 555
Der Autor zeigt auf, dass Art. 88 DS-GVO viele Fragen offen lässt, insbesondere nach der Reichweite und dem zeitlichen Rahmen für eine Ausfüllung. Offen gehalten wird, ob § 32 BDSG als Ausfüllung der Öffnungsklausel aufrecht erhalten bleiben kann. Ferner geht er einer Reihe von Anwendungsfällen der DS-GVO bei der Verarbeitung im Beschäftigungsverhältnis nach.

Moos, Flemming/Rothkegel, Tobias, **Nutzung von Scoring-Diensten im Online-Versandhandel,** ZD 2016, S. 561
Aufgezeigt wird der Einsatz der ständig technisch fortentwickelten Scoringsysteme in Betrachtung des insoweit bestehenden Spannungsfelds zwischen BDSG, AGG und DS-GVO.

Piltz, Carlo, **Die Datenschutz-Grundverordnung (IV)**, K&R 2016, S. 777
Im Anschluss an den dritten Teil der Beitragsreihe (Heft 11/2016) zur Datenschutz-Grundverordnung (DS-GVO) befasst sich dieser vierte Teil mit den Anforderungen an Datenübermittlung in Drittländer und betrachtet zudem die Regelungen zur Errichtung von Aufsichtsbehörden.

Spelge, Karin, **Der Beschäftigtendatenschutz nach Wirksamwerden der Datenschutz-Grundverordnung,** DuD 2016, S. 775
Nach Spelge lässt die DS-GVO weder ein Unterschreiten noch eine Ausweitung des Schutzniveaus zu. Soweit § 32 Abs. 2 BDSG (= § 24 Abs. 2 BDSG-neu) die nicht automatisierte bzw. nicht dateiorganisierte Verarbeitung von Beschäftigtendaten dem Beschäftigtendatenschutz unterstellt, sei die Bestimmung nichtig. Zudem könne der Verstoß gegen die Meldepflicht des Art. 88 Abs. 3 DS-GVO dazu führen, dass jede nationale Regelungskompetenz verloren gehe.

Ist die Bahn im postfaktischen Zeitalter angekommen?

Lassen Sie Ihre Daten nicht unbeaufsichtigt

Lassen Sie Ihr Gepäck nicht unbeaufsichtigt. Diesen Hinweis an Flughäfen und Bahnhöfen kennt man. Deshalb passt man gut auf, dass sich Langfinger nicht am Gepäck vergreifen. Das ist aber nicht alles, was in der Bahn geklaut werden kann. Dort wird in Zügen der zweiten Klasse auf verschiedenen ICE-Strecken WLAN für die Bahnkunden angeboten. Das kostet nichts, und es ist denkbar einfach zu bedienen. Man ruft eine Seite auf und klickt den Button zum Einverständnis mit den Geschäftsbedingungen.

Dabei werden die IP-Adresse und MAC-Adresse – also die Kennung des verwendeten Endgeräts abfragt und für die WLAN-Nutzung freigeschaltet. Bei Anfragen an andere Webseiten ist es wichtig, Sicherheitsmaßnahmen zu treffen, wie das Mitsenden eines sog. Tokens. Das ist ein elektronischer Schlüssel, um unbefugte Datenzugriffe auf eine Verbindung auszuschließen. Die Bahn hat mitgeteilt, besondere Sicherheitsmerkmale in ihr WLAN eingebaut zu haben. Trotzdem könne sie die Sicherheit ihrer Verbindungen und den Schutz vor Datenklau nicht komplett garantieren. Dafür sei der Fahrgast selbst verantwortlich.

Offenes WLAN ist praktisch, und die meisten wollen auf möglichst unkomplizierten Zugang zum Netz nicht verzichten. Der Wirtschaftsstandort Deutschland ist darauf angewiesen. Aber was im Netz unkompliziert und smart ist, ist rechtlich oft problematisch. Verantwortungsloser Umgang mit Daten ist zwar an der Tagesordnung; er birgt aber auch große gesellschaftliche Risiken. Wir müssen auf unsere Persönlichkeit im Netz schon selber aufpassen.

Die Bahn rät deshalb dazu, eine VPN-Verbindung beim Datenaustausch zu nutzen oder ausschließlich auf https-Seiten zu surfen. Dieser Hinweis ist wichtig, und er gehört nicht ins Kleingedruckte. Wer offen mit Netzdiensten wirbt, sollte auch auf die Risiken hinweisen. Passend wäre eine Ansage im Zug: „Lassen Sie Ihre Daten nicht unbeaufsichtigt und nutzen Sie unser WLAN nur, wenn Sie die Sicherheit des Netzes verantworten können."