ISSN 0178-8930

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

2/2019

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

HANSEN/WALCZAK, Pseudonymisierung à la DS-GVO und verwandte Methoden

KEBER, Mythen der Datenschutzgrundverordnung – Erlesenes aus (knapp) 300 Tagen DS-GVO

HERMANN, Datenschutz in Prüfungsverfahren nach DS-GVO und BDSG

THIEL, Querschnittsprüfung der LfD Niedersachsen zur Umsetzung der DS-GVO in Unternehmen

Kurzbeiträge

GOLA, Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (40): Offene Fragen bei der Beschäftigtendatenverarbeitung: Gehaltsabrechnung durch Steuerberater und Verarbeitungen beim Betriebsrat

Rechtsprechung

Aus dem Inhalt

EUGH, Videoaufzeichnung von Polizeibeamten in einer Polizeidienststelle während der Vornahme von Verfahrenshandlungen und Veröffentlichung auf einer Video-Website

BVERWG, Informantenschutz gegenüber Verstorbenen

BVERFG, Mitbestimmung bei der Anweisung zur Vorlage einer Arbeitsunfähigkeitsbescheinigung

BVERWG, Dienstliches Gespräch als äußere Einwirkung im Sinne des Dienstunfallrechts (Ls)

BVERWG, Auskunftsanspruch hinsichtlich einer aus öffentlichen Mitteln finanzierten Verwandtenbeschäftigung

OLG SCHLESWIG, Zur Haftung für nicht autorisierte Entscheidungen im Online-Banking (Ls)

35. Jahrgang
Februar 2019
Seiten 51–104

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Die neue Datenschutz-Grundverordnung für Mitarbeiter

Informieren - Sensibilisieren - Dokumentieren

Die bewährte Mitarbeiterinformation Datenschutz liegt jetzt in neuer aktualisierter Fassung vor. Sie ist auf das neue Datenschutzrecht (DS-GVO und BDSG 2018) ausgerichtet und wurde grafisch neu gestaltet.

Mit dieser Mitarbeiterinformation können Sie alle Ihre Mitarbeiterinnen und Mitarbeiter zu den Grundlagen des Datenschutzes informieren und für dessen Bedeutung und Notwendigkeit sensibilisieren.

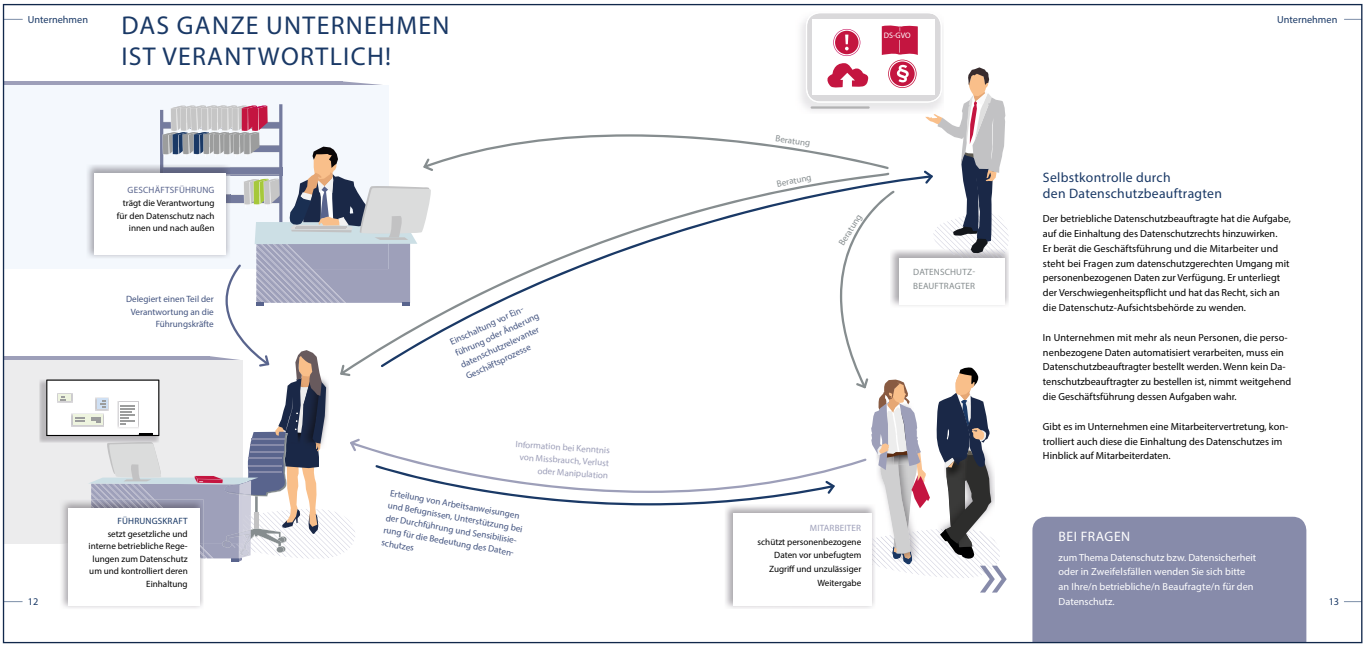
GDD e.V.
Mitarbeiterinformation Datenschutz

Merkblatt für Mitarbeiterinnen und Mitarbeiter
zu DS-GVO und BDSG
28. Auflage 2018 - Broschüre - 21 x 21 cm
ISBN 978-3-89577-790-5
20 Seiten, Staffelpreise

„So informieren Sie Ihre Mitarbeiter einfach und anschaulich zum neuen Datenschutzrecht!“

Judith Todd
Kundenbetreuung

Musterseite



Muster unter www.datakontext.com

DATAKONTEXT GmbH Tel. 02234/98949-30 Fax 02234/98949-32 www.datakontext.com bestellung@datakontext.com

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht

35. Jahrgang 2019
Heft 2
Seiten 51–104

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 51

Veranstaltungen 52

Aufsätze

Marit HANSEN/Benjamin WALCZAK
Pseudonymisierung à la DS-GVO und verwandte Methoden **53**

Prof. Dr. Tobias KEBER
Mythen der Datenschutzgrundverordnung – Erlesenes aus (knapp) 300 Tagen DS-GVO **58**

Maximilian HERMANN
Datenschutz in Prüfungsverfahren nach DS-GVO und BDSG **64**

Barbara THIEL
Querschnittsprüfung der LfD Niedersachsen zur Umsetzung der DS-GVO in Unternehmen **68**

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (40): Offene Fragen bei der Beschäftigtendatenverarbeitung: Gehaltsabrechnung durch Steuerberater und Verarbeitungen beim Betriebsrat **73**

Rechtsprechung

Videoaufzeichnung von Polizeibeamten in einer Polizeidienststelle während der Vornahme von Verfahrenshandlungen und Veröffentlichung auf einer Video-Website (EuGH, Urteil vom 14.02.2019) **77**

Informantenschutz gegenüber Verstorbenen
(BVerwG, Urteil vom 24.10.2018) **81**

Mitbestimmung bei der Anweisung zur Vorlage einer Arbeitsunfähigkeitsbescheinigung
(BVerfG, Urteil vom 15.10.2018) **81**

Dienstliches Gespräch als äußere Einwirkung im Sinne des Dienstunfallrechts (Ls)
(BVerwG, Beschluss vom 11.10.2018) **83**

Auskunftsanspruch hinsichtlich einer aus öffentlichen Mitteln finanzierten Verwandtenbeschäftigung
(BVerwG, Beschluss vom 27.09.2018) **83**

Zur Haftung für nicht autorisierte Entscheidungen im Online-Banking (Ls)
(OLG Schleswig, Urteil vom 29.10.2018) **88**

Bekanntgabe der privaten Mobilfunknummer an den Arbeitgeber
(LAG Thüringen, Urteil vom 16.05.2018) **88**

Umstellung auf automatisierte Personalaktenführung
(OVG Münster, Urteil vom 17.12.2018) **92**

Einsicht eines Ratsmitglieds in Gewerbesteuerakten (Ls)
(OVG Münster, Beschluss vom 06.11.2018) **95**

Zu den Voraussetzungen einer von einem Verstoß „betroffenen Person" i.S.d. Datenschutzgrundverordnung
(LG Wiesbaden, Beschluss vom 05.11.2018) **95**

Berichte, Informationen, Sonstiges

Wirksamkeit eines Kopftuchverbots? **100**

Liebeskontakte per Internet **100**

Literaturhinweise

Buchbesprechungen

Simitis, Spiros/Hornung, Gerrit/Spieker, Indra gen. Döhmann (Hrsg.), Datenschutzrecht – DS-GVO und BDSG
(GOLA) **101**

Schmitt, Florian, Die (unangekündigte) Datenschutzkontrolle des BfDI im Anwendungsbereich des BDSG und des TKG
(FRANCK) **101**

Neuerscheinungen

Aufsätze **103**

Nachgefasst 104

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

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

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

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

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

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

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

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

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

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

Prof. Dr. Karl LINNENKOHL, Universität Kassel

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

Prof. Dr. Michael RONELLENFITSCH, Hessischer Datenschutzbeauftragter

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

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

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

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

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 1/2019; DATAKONTEXT, Frechen, C.H. Beck

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

Urheber- und Verlagsrechte:
Sie sind einschließlich der Veröffentlichung als PDF im Online-Archiv vorbehalten. Sie erstrecken sich auch auf die veröffentlichten Gerichtsentscheidungen und deren Leitsätze; diese sind geschützt, soweit sie vom Einsender oder von der Schriftleitung erstellt oder bearbeitet sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen: Diese bedürfen zur Auswertung einer Genehmigung des Verlages.
Der Verlag gestattet in der Regel die Herstellung von Fotokopien zu innerbetrieblichen Zwecken, wenn dafür eine Gebühr an die VG Wort, Abteilung Wissenschaft, Goethestraße 49, 80336 München, entrichtet wird, von der die Zahlungsweise zu erfragen ist.

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

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

Erscheinungsweise
6 x jährlich

Bezugspreis

Jahresabonnement	€ 139,–
Einzelheft	€ 25,–

MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

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

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

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

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

Satz
alka mediengestaltung gmbh
Willmuthstraße 30, 53332 Bornheim-Sechtem

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

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

Zeitschrift für
Datenschutz–, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
35. Jahrgang 2019 Heft 2
Seiten 51 – 104

RDV
Recht der Datenverarbeitung

35. Jahrgang · April 2019 · Seiten 51 – 104

Editorial

Cookies – Vorhang zu und alle Fragen offen

„Mit § 15 Abs. 3 TMG wird Art. 5 Abs. 3 der Richtlinie 2002/58 umgesetzt". So der Generalanwalt Szpunar in Rn. 21 (vgl. auch Rn. 101) seiner Schlussanträge zur Rechtssache C-673/17 (Planet49 GmbH) vom 21.03.2019. Diese Aussage hat weitreichende Konsequenzen. Nach der fast einhelligen Auffassung in Deutschland setzen die Datenschutznormen im 4. Abschnitt des TMG die durch die DS-GVO aufgehobene Datenschutzrichtlinie und gerade nicht die ePrivacy-RiLi um. Nach der Kollisionsregelung des Art. 95 DS-GVO ist die DS-GVO maßgeblich. (Dazu Schwartmann/Klein, Art. 6 DS-GVO, Rn. 141 in Schwartmann/Jaspers/Thüsing/Kugelmann, HK-DS-GVO/BDSG).

Was bedeutet dieser Widerspruch? § 15 Abs. 3 TMG sieht vor, dass man in die Erstellung von pseudonymen Nutzerprofilen durch Onlinedienste unter anderem zu Werbezwecken einwilligen kann, indem man dem als Nutzer nicht widerspricht („opt out)". Das reicht nach der DS-GVO nicht aus. Art. 6 Abs. 1 S. 1 a) DS-GVO, der ErwG 32 auslegt, verlangt für eine Einwilligung eine eindeutige bestätigende Handlung. Stillschweigen oder vorangekreuzte Kästchen reichen nicht („opt in"). Beim Einsatz von Tools zur Reichweitenmessung („cookies") ist dieser Widerspruch zwischen dem Datenschutzrecht (DS-GVO) und dem Recht des elektronischen Geschäftsverkehrs (ePrivacy-RiLi/TMG) bedeutsam. DS-GVO bedeutet „opt in". Ob ePrivacy-RiLi in der Umsetzung des TMG „opt out" bedeuten kann, muss in Sachen Planet49 der Europäische Gerichtshof entscheiden.

Der Generalanwalt hält in Rn. 122 für eine wirksame Einwilligung ein „opt in" für erforderlich. Das war zu erwarten. Überraschend ist aber, dass er den 4. Abschnitt des TMG als Umsetzung der Richtlinie 2002/58 begreift. Ob die Kommission die Richtlinie in dieser Form in Deutschland als umgesetzt betrachtet, ist gerade bezogen auf ein „opt out" offen. (COCOM11-20 v. 04.10.2011, S. 5). Folgt der EuGH dem Generalanwalt, dann würde die Kollisionsregel des Art. 95 DS-GVO Anwendung finden. Die DS-GVO träte zurück, weil sie im Regelungsbereich der Richtlinie 2002/58 keine zusätzlichen Pflichten, wie das „opt in"-Erfordernis auferlegen darf. Es bliebe bei der Anwendbarkeit des 4. Abschnitts des TMG. Konsequenz: Cookies sind bis zu einer anders lautenden Entscheidung des EuGH oder der ePrivacy-VO per „opt out-Einwilligung" zulässig. Zum einen wäre die Diskussion von Schwartmann/Benedikt/Jacquemain in PinG 2018, 150 ff., ob es nach der DS-GVO für die Zulässigkeit von Cookies auf „opt in" oder Interessenabwägung ankommt, damit hinfällig. Zum anderen käme im Rahmen des TMG nur noch die „opt out-Einwilligung" nach § 15 Abs. 3 in Betracht, weil weder ePrivacy-RiLi noch TMG eine Interessenabwägung vorsieht.

Die schlüssige Auffassung der DSK, wonach die Datenschutzvorschriften des TMG und damit § 15 Abs. 3 TMG durch die DS-GVO abgelöst sind, ist aus berufenem Munde qualifiziert bestritten. Rechtsanwender können sich aus gutem Grund fragen, ob ihre „Cookie-Praxis" bis zur Klärung im Anwendungsfall an den großzügigen Vorgaben des TMG ausgerichtet werden kann. So müsste es auch die Datenschutzerklärung wiedergeben. Die ausführliche Darstellung in den Schlussanträgen zu den Anforderungen an eine „opt in-Einwilligung" wäre für Deutschland also zunächst ohne Bedeutung.

Bei Cookies ist es ein wenig wie in Brechts „Der gute Mensch von Sezuan". Dort heißt es: „Wir stehen selbst enttäuscht und sehn betroffen. Den Vorhang zu und alle Fragen offen." Auch bei Cookies schien der Vorhang zu. Nun sind alle Fragen offen. Enttäuscht und betroffen dürfte nicht jeder sein.

Professor Dr. Rolf Schwartmann

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

Termin	Thema	Ort	Kontakt
07.05.2019	Löschen nach DS-GVO	Köln	GDD e.V. und DATAKONTEXT
06.-07.05.2019	Neues Datenschutzrecht kompakt	Köln	GDD e.V. und DATAKONTEXT
13.05.2019	Mobile Endgeräte im Zeitalter von DS-GVO und ePrivacy-Verordnung	Köln	GDD e.V. und DATAKONTEXT
14.05.2019	Grundlagen der Auftragsverarbeitung	Köln	GDD e.V. und DATAKONTEXT
16.05.2019	Datenschutz international	Köln	GDD e.V. und DATAKONTEXT
20.05.2019	Videoüberwachung nach BDSG 2018 und DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
20.-24.05.2019	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
03.06.2019	Teleworking unter Beachtung von Datenschutz und Sicherheit	Köln	GDD e.V. und DATAKONTEXT
04.06.2019	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
04.-06.06.2019	SAP ERP für Datenschutzbeauftragte	Düsseldorf	GDD e.V. und DATAKONTEXT
17.06.2019	Strafverfolgung, Whistleblowing, Internal Investigations – Datenschutz und Strafrecht	Köln	GDD e.V. und DATAKONTEXT
24.06.2019	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V. und DATAKONTEXT
02.-03.07.2019	Datenschutz im Gesundheitswesen	Köln	GDD e.V. und DATAKONTEXT
05.-07.08.2019	GDD-Sommer-Workshop	Timmendorfer Strand	GDD e.V. und DATAKONTEXT
03.09.2019	Hacker-Tools für Datenschutzbeauftragte	Stuttgart	GDD e.V. und DATAKONTEXT
10.09.2019	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Stuttgart	GDD e.V. und DATAKONTEXT
09.-13.09.2019	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
16.09.2019	Planung und Umsetzung der Überwachungsaufgabe des DSB	Köln	GDD e.V. und DATAKONTEXT
16.09.2019	Datenschutz und Betriebsrat unter der DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
17.09.2019	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
19.09.2019	Die ePrivacy-Verordnung im Zusammenspiel mit der DS-GVO	Düsseldorf	GDD e.V. und DATAKONTEXT
23.09.2019	Mobile Endgeräte im Zeitalter von DS-GVO und ePrivacy-Verordnung	Köln	GDD e.V. und DATAKONTEXT
24.09.2019	Beschäftigtendatenverarbeitung nach DS-GVO und BDSG 2018	Köln	GDD e.V. und DATAKONTEXT
26.09.2019	Big Data-Analysen nach DS-GVO und BDSG 2018	Köln	GDD e.V. und DATAKONTEXT
30.09.2019	Grundlagen der Auftragsverarbeitung	Köln	GDD e.V. und DATAKONTEXT

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

Aufsätze

Marit Hansen/Benjamin Walczak

Pseudonymisierung à la DS-GVO und verwandte Methoden[1]

Aufgrund der voranschreitenden Digitalisierung vieler Lebensbereiche von immer mehr Menschen wächst auch die Fülle an Informationen, die über jede und jeden gesammelt werden. Der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, wie er in der Datenschutz-Grundverordnung (DS-GVO) gefordert ist, kann durch vielfältige organisatorische und technische Maßnahmen gewährleistet oder unterstützt werden.

Ein in der DS-GVO konkret genanntes Mittel ist die Pseudonymisierung, die als einzige Maßnahme mit einer Begriffsbestimmung (Art. 4 Nr. 5 DS-GVO) hervorgehoben wird. Pseudonymisierung wird ferner erwähnt im Zusammenhang mit der Verarbeitung personenbezogener Daten zu einem anderen Zweck als ursprünglich vorgesehen (Art. 6 Abs. 4 lit. e DS-GVO), als beispielhafte Maßnahme bei der Erfüllung der Anforderung „Datenschutz durch Technikgestaltung" (Art. 25 Abs. 2 DS-GVO), als Maßnahme zur Gewährleistung eines ausreichenden Schutzniveaus (Art. 32 Abs. 1 lit. a DS-GVO), als mögliche branchenspezifische Verhaltensregel für die Verarbeitung personenbezogener Daten (Art. 40 Abs. 2 lit. d DS-GVO) und als Maßnahme zur Gewährleistung der geforderten Garantien bei der Verarbeitung personenbezogener Daten für wissenschaftliche, statistische und archivarische Zwecke (Art. 89 Abs. 1 DS-GVO sowie Erwägungsgrund 156).

Pseudonymisierung kann eine datenschutzfördernde Maßnahme sein, indem die Identität eines Individuums in einem spezifischen Kontext verborgen wird. Zugleich kann eine Pseudonymisierung dazu beitragen, das Risiko für die Rechte und Freiheiten der betroffenen Personen zu verringern und im Fall eines Datenschutzverstoßes die negativen Folgen zu mindern.

I. Der Begriff der Pseudonymisierung

Ein Wort zur Warnung vorab: In verschiedenen Disziplinen spielen die Begriffe „Pseudonymisierung" und „Pseudonym" eine Rolle, ohne dass es bisher einheitliche Definitionen gegeben hätte. Schon die Verwendung in verschiedenen juristischen Normen stellen auf verschiedene Qualitäten der Pseudonyme/Pseudonymisierung ab (beispielsweise im Signaturgesetz, im Telemediengesetz oder im alten LDSG Schleswig-Holstein). Ähnliches gilt für die Annäherung an das Thema aus technischer Sicht.[2]

In diesem Beitrag soll zwar primär auf die DS-GVO-Definition zu Pseudonymisierung Bezug genommen werden. Jedoch garantieren die technischen Verfahren, die mehr oder weniger für eine Pseudonymisierung geeignet sein können, allein häufig noch nicht, dass die Anforderungen an eine Pseudonymisierung im Sinne der DS-GVO erfüllt werden. Dies kann zudem von weiteren Faktoren abhängen wie beispielsweise von den zu pseudonymisierenden Daten selbst oder etwaigem Zusatzwissen.

Dies vorausgeschickt, nehmen wir einen Blick in die Definition in Art. 4 Nr. 5 der DS-GVO:

„‚Pseudonymisierung' [bezeichnet] die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden".

Es handelt sich demnach um eine Verarbeitung von personenbezogenen Daten derart, dass das Resultat – die pseudonymisierten Daten – ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden kann. Bei diesen zusätzlichen Informationen handelt es sich um solche Daten, durch die sich die Daten individuell zuordnen lassen, beispielsweise eine Tabelle mit einer Zuordnung zwischen Namen und Pseudonym oder eine Berechnungsfunktion, die eine solche Zuordnung leistet (siehe Abb. 1).

Diese Definition setzt am Kern des Datenschutzrechts, dem Personenbezug von Daten (Art. 4 Nr. 1 DS-GVO), an: Ziel ist eine Entkopplung der ursprünglich personenbezogenen Daten von den betroffenen Personen. Im Falle einer –

1 In diesen Beitrag sind Erkenntnisse aus dem Forschungsprojekt „Forum Privatheit" (Förderkennzeichen 16KIS0747) eingeflossen, das mit Mitteln des Bundesministeriums für Bildung, und Forschung (BMBF) gefördert wird.

2 Pfitzmann/Hansen, A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, Version 0.34, 10.08.2010 http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf; Art.-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, 14/DE WP 216.

"in der DS-GVO nicht legaldefinierten – Anonymisierung ist die durch die Veränderung der Daten erreichte Entkopplung von den zugehörigen Personen irreversibel, anders als bei der Pseudonymisierung. Anonymisierte Daten sind also nicht mehr personenbezogen und unterfallen demnach auch nicht mehr der DS-GVO. Allerdings ist der Sprachgebrauch hier oft unscharf, beispielsweise garantieren sog. „anonymisierte Gerichtsurteile" in der Regel keinesfalls, dass die betroffenen Personen nicht feststellbar sind. Auch kann der technische Fortschritt dazu führen, dass ein Personenbezug in vormals als anonymisiert eingestuften Daten zu einem späteren Zeitpunkt hergestellt werden kann.[3]

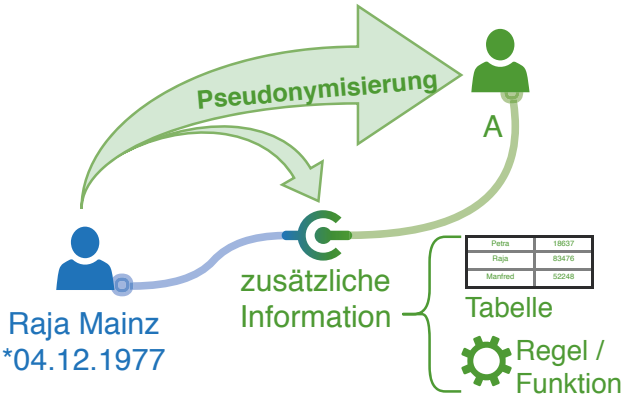


Abb. 1: Veranschaulichung der Pseudonymisierung nach DS-GVO

Sowohl bei Anonymisierung als auch bei Pseudonymisierung handelt es sich um Datenverarbeitungen, die den Datenschutzgrundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) unterstützen.

Unter dem Begriff „Pseudonym", der in der DS-GVO ebenfalls nicht definiert wird, versteht man einen Identifikator, eine Kennung oder ein Kennzeichen anstelle des echten Namens einer Person. Dies muss nicht eine einzelne Zeichenkette sein, sondern kann auch aus mehreren Attributen bestehen. Das Vorhandensein eines Pseudonyms garantiert noch keine Pseudonymisierung im Sinne der DS-GVO. Stattdessen führt die DS-GVO Kennungen auf, die sich vom echten Namen unterscheiden, beispielsweise die Online-Kennungen (siehe Erwägungsgründe 30 und 64 sowie Art. 4 Nr. 1 DS-GVO) oder andere Identifikatoren wie in Art. 87 DS-GVO, der die Verarbeitung der nationalen Kennziffer oder andere Kennzeichen von allgemeiner Bedeutung regelt. Agiert eine betroffene Person unter Pseudonym, beispielsweise gegenüber einem Verantwortlichen wie einem Online-Händler, ist damit noch nicht gesagt, ob der echte Namen dem Verantwortlichen bekannt ist, ob dieser das Pseudonym zuordnen kann oder sogar vergeben hat, ob die betroffene Person eigenständig ein Pseudonym gewählt hat und ob durch die mehrfache Verwendung Profilbildungen möglich sind. Diese Fallkonstellation unterscheidet sich von der üblichen Pseudonymisierung, bei der bereits ein personenbezogener Datenbestand vorhanden ist, von dem der Verantwortliche in einem weiteren Verarbeitungsschritt eine pseudonymisierte Version erstellt.

II. Anforderungen an eine Pseudonymisierung

Durch den Einsatz einer Pseudonymisierung allein ist eine Verarbeitung personenbezogener Daten nicht automatisch rechtmäßig. Sie kann jedoch ein wichtiger Baustein sein, um eine entsprechende Verarbeitung im Einklang mit der DS-GVO zu ermöglichen.

Zu unterscheiden ist dabei der Einsatz eines Pseudonymisierungsverfahrens als technische Schutzmaßnahme im Sinne der Risikoverminderung (Art. 32 DS-GVO) oder zur Erfüllung der Anforderung „Datenschutz durch Technikgestaltung" (Art. 25 DS-GVO) einerseits oder als Ermöglichung einer kompatiblen Weiterverarbeitung nach Art. 6 Abs. 4 DS-GVO andererseits.

In beiden Anwendungsfällen kommt ein Pseudonymisierungsverfahren als eine von mehreren Maßnahmen zum Einsatz; die Pseudonymisierung ist sowohl in Art. 6 Abs. 4 DS-GVO als auch in Art. 32 Abs. 1 DS-GVO ein Punkt in jeweils nicht abschließenden Maßnahmenlisten. Ein eingesetztes Pseudonymisierungsverfahren und dessen Wirkung müssen stets im Zusammenhang und verbunden mit den anderen Maßnahmen bewertet werden.

In der DS-GVO werden keine konkreten Verfahren für eine Pseudonymisierung vorgegeben, allerdings werden in der Begriffsbestimmung in Art. 4 Nr. 5 DS-GVO, in Art. 32 Abs. 1 DS-GVO und im Erwägungsgrund 26 DS-GVO drei Kernanforderungen formuliert:

- Ein Pseudonymisierungsverfahren soll unter der Bedingung, dass eine Nichtverfügbarkeit der zusätzlichen Informationen garantiert ist, eine anonymisierende Wirkung haben. Das bedeutet: Personenbezogene Daten sollen so verarbeitet werden, „dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können". Trotz der unter bestimmten Bedingungen bestehenden anonymisierenden Wirkung bleibt aufgrund der Existenz der zusätzlichen Informationen der Personenbezug bestehen; es liegt bei der Pseudonymisierung eben keine irreversible Anonymisierung vor.
- Die Zuordnung der pseudonymisierten Daten zu Identitätsinformationen (z.B. als Tabelle oder Formel) soll einem besonderen Schutz durch technische und organisatorische Maßnahmen gegen (unberechtigte) Zugriffe unterliegen. Für die Nutzenden der pseudonymisierten Daten dürfen diese zusätzlichen Informationen also nicht im Zugriff stehen, sie sind aber vorhanden. Hier kann es Situationen geben, in denen ein gezielter Zugriff auf diese Informationen erforderlich ist, beispielsweise um für einzelne Datensätze eine Zuordnung zu einer Person vorzunehmen.
- Ein eingesetztes Pseudonymisierungsverfahren muss dem Stand der Technik entsprechen; die Wirksamkeit muss regelmäßig überprüft, bewertet und evaluiert werden.

3 Dies kann besondere Sorgfaltspflichten erfordern, vgl. Roßnagel/Scholz, Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.

Die konkreten Anforderungen an eine Pseudonymisierung sind dabei abhängig von der beabsichtigten Wirkung. Die beiden im Folgenden beschriebenen anonymisierenden[4] und risikomindernden Wirkungen[5] sind dabei nicht isoliert, sondern in der Praxis kombiniert zu betrachten.

1. Anonymisierende Wirkung

Mit einer Pseudonymisierung kann von einer verantwortlichen Stelle beabsichtigt werden, dass die pseudonymisierten Daten – ohne Hinzuziehen zusätzlicher Informationen – für eine weitere Verarbeitung zunächst einmal die gleichen Eigenschaften haben sollen wie anonymisierte Daten: Eine Zuordnung zu einer spezifischen betroffenen Person muss ausgeschlossen sein. Anonym sind die Daten gemäß Erwägungsgrund 26 DS-GVO, wenn „die betroffene Person nicht oder nicht mehr identifiziert werden kann". Ohne die Existenz der zusätzlichen Informationen würden demnach die Daten nicht personenbezogen nach den Kriterien des Art. 4 Abs. 1 sein.

Die Zuordenbarkeit der pseudonymisierten Daten zu einer spezifischen Person muss für jedes Pseudonymisierungsverfahren geprüft und ausgeschlossen werden. Berücksichtigt werden müssen alle Mittel, die nach allgemeinem Ermessen zur Identifizierung durch die verantwortliche Stelle oder eine andere Person genutzt werden können. Explizit erwähnt wird in Erwägungsgrund 26 DS-GVO als ein Mittel der Identifizierung das Aussondern (im Sinne von „Vereinzeln"/ „singling out"); die einzelnen pseudonymisierten Daten sind also explizit auch im Zusammenhang mit den anderen Daten zu bewerten. Bei der Bewertung, welche anderen Mittel zur Identifizierung genutzt werden können, sollen sowohl die aktuell verfügbare Technologie als auch zukünftige technologische Entwicklungen berücksichtigt werden.

Insgesamt muss also neben dem aktuellen Risiko einer Identifizierung auch die erwartbare Risikoentwicklung betrachtet werden. Dementsprechend muss ggf. auch eine „Schutzreserve" vorgesehen sein.[6] Werden die Daten zudem über einen längeren Zeitraum verwendet, müssen Prüfungen des Risikos einer Zuordenbarkeit regelmäßig erfolgen und ggf. entsprechende Maßnahmen getroffen werden, da mit der Zeit durch bessere Verknüpfungsmöglichkeiten oder neues Zusatzwissen eine Identifizierung leichter möglich sein könnte.

Sind diese Bedingungen einer anonymisierenden Wirkung erfüllt, ist dies jedoch nicht gleichbedeutend mit einer Anonymisierung. Diese würde gemäß Erwägungsgrund 26 DS-GVO voraussetzen, dass eine Identifizierung überhaupt nicht mehr möglich ist. Die pseudonymisierten Daten sind demnach stets als personenbezogene Daten zu behandeln.

2. Risikomindernde Wirkung

Eine zweite Wirkung eines Pseudonymisierungsverfahrens ist die Minderung des Risikos für die Rechte und Freiheiten der betroffenen Personen. Im Allgemeinen verringert eine Pseudonymisierung von Daten das Risiko, allerdings ist diese Wirkung zum einen abhängig von der konkreten Ausgestaltung des Verfahrens.

Insbesondere ist die gesonderte und gesicherte Aufbewahrung der „zusätzlichen Informationen" gemäß Art. 4 Abs. 5, d.h. die Zuordnung der pseudonymisierten Daten zu Identitätsdaten, von Bedeutung. Im Pseudonymisierungsverfahren kann diese Zuordnung von einem unabhängigen Dritten übernommen werden, sodass auch die verantwortliche Stelle die pseudonymisierten Daten nicht einer speziellen betroffenen Person zuordnen kann.

Gemäß Erwägungsgrund 29 kann das Pseudonymisierungsverfahren jedoch auch vollständig in der Hand des Verantwortlichen bleiben, „wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um – für die jeweilige Verarbeitung – die Umsetzung dieser Verordnung zu gewährleisten". Dabei muss die Zuordnungsregel gesondert aufbewahrt werden und der Zugriff auf wenige befugte Personen begrenzt werden.

In beiden Fällen ist die Zuordnungsregel durch Sicherungsmaßnahmen besonders zu schützen, hierfür gelten die Vorgaben des Art. 32 DS-GVO.

Ferner muss das Pseudonymisierungsverfahren dokumentiert werden. In jedem Fall sind bei der Dokumentation von Verarbeitungstätigkeiten die Vorgaben des Art. 30 DS-GVO zu erfüllen. Um eine Nachprüfbarkeit sowohl für eigene Zwecke als auch im Rahmen der Rechenschaftspflicht zu gewährleisten, müssen weitere Informationen über das Verfahren dokumentiert werden, beispielsweise die Beschreibung des konkreten Verfahrens einschließlich der die Pseudonymisierung durchführenden „befugten Personen"; dies können auch unabhängige Dritte sein. Sollte eine Re-Identifizierung der pseudonymisierten Daten (also eine Zuordnung von einzelnen oder allen Daten zu den betroffenen Personen) unter bestimmten Bedingungen vorgesehen sein, ist auch zu dokumentieren, wer unter welchen Bedingungen auf welche Weise diese Verarbeitung vornimmt.

III. Risiken bei einer Pseudonymisierung

Das naheliegende Risiko eines Pseudonymisierungsverfahrens ist das Risiko der Zuordnung der Daten zu einer betroffenen Person. Wie beschrieben werden daher hohe Anforderungen an das Pseudonymisierungsverfahren und die Sicherung der Zuordnungsinformationen gestellt.

Allerdings müssen bei der Risikobewertung einer Pseudonymisierung verschiedene Angriffsszenarien berücksichtigt werden. Neben dem Versuch, eine Zuordnungsliste und damit den Zusammenhang zwischen spezifischen Personen und pseudonymisierten Daten bzw. Pseudonymen herzustellen, kann eine unbefugte Zuordnung auch auf anderen Wegen versucht werden. Dabei unterscheiden sich die Ansätze darin, ob zu einem bekannten Pseudonym die betroffene Person identifiziert werden soll oder das zu einer betroffenen Person passende Pseudonym gefunden werden soll

4 Genauer: die Zuordnung zu einer Person vermeidenden Wirkung.

5 Roßnagel, Pseudonymisierung personenbezogener Daten, ZD 2018, 246 ff.

6 Schaar, DS-GVO: Geänderte Vorgaben für die Wissenschaft – Was sind die neuen Rahmenbedingungen und welche Fragen bleiben offen?, ZD 2016, 224 f.

oder über eine betroffene Person lediglich die Information eingeholt werden soll, ob sie überhaupt in einem Datensatz enthalten ist oder nicht. Allen Szenarien ist gleich, dass sie ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen. Im Wesentlichen können vier Methoden unterschieden werden:[7]

- Ausprobieren: Werden Pseudonyme auf Grundlage von überschaubaren Identitätsdaten erstellt, können bei Verwendung einer mathematischen Zuordnungsregel alle möglichen Identitätsdaten ausprobiert werden, bis die Identität zu einem Pseudonym aufgedeckt wurde.
- Aussondern („singling out", „herausgreifen"): Aus den nach der Pseudonymisierung noch enthaltenen Daten können gegebenenfalls durch die Kombination mehrerer Merkmale einzelne Personen identifiziert werden, weil ihre Merkmalskombination einmalig ist.
- Verknüpfen („linking", „verketten"): Die pseudonymisierten Daten können mit anderen Datensätzen verknüpft werden, wodurch eine Identifizierung von Personen ermöglicht wird.
- Schlussfolgerungen („inferring"): Mit zusätzlichem Wissen können aus den pseudonymisierten Daten Rückschlüsse auf betroffene Personen gezogen werden – z.B. aus dem Notenspiegel einer Schulklasse ohne Einsen kann geschlussfolgert werden, dass ein bestimmter Schüler auch keine sehr gute Note hat.

Für alle diese Risiken gibt es Gegenmaßnahmen wie z.B. die Generalisierung von Daten bis hin zum Verfälschen oder Hinzufügen von fiktiven Daten, die allerdings die Datenqualität reduzieren können.[8] Die Maßnahmen müssen folglich abhängig vom Zweck der Verarbeitung gewählt werden.

Ein weiteres Risiko der Pseudonymisierung liegt im bereits erwähnten Homonymfehler, also der Zuweisung des gleichen Pseudonyms an zwei unterschiedliche Personen. In diesem Fall verlieren die pseudonymisierten Daten Integrität und bei einer Zuordnung der Pseudonym-Daten zu einer betroffenen Person durch die verantwortliche Stelle (z.B. bei einem Auskunftsersuchen) werden fremde Informationen preisgegeben. Dieses Risiko kann durch die geeignete Wahl eines Pseudonymisierungsverfahrens verringert oder sogar ausgeschlossen werden.[9]

Erwähnt werden soll an dieser Stelle, dass die Weiternutzung pseudonymisierter Daten nach Erreichen der damit verbundenen Zwecke und Wegfall der Erforderlichkeit nicht durch einfaches Löschen der Pseudonyme ermöglicht werden kann. Eine Anonymisierung ist in der Regel nicht durch das Entfernen der Zuordnung oder der Pseudonyme zu erreichen, sondern muss als eigenständiges Verfahren erfolgen, für das spezielle Anforderungen der Anonymisierung gelten.[10]

IV. Verfahren der Pseudonymisierung

In vielen Anwendungsfällen werden Daten pseudonymisiert, um die Datensätze für statistische oder wissenschaftliche Auswertungen weiter zu nutzen, ohne einen direkten Personenbezug herzustellen. Die Verkettbarkeit der Datensätze kann für diesen Zweck wichtig sein, doch können abhängig vom Kontext dabei unterschiedliche Arten von Pseudonymen zum Einsatz kommen.

Die Stärke des Schutzes mithilfe einer Pseudonymisierung oder anderen Identitätsverschleierungen hängt davon ab, wie hoch die Kosten sowie der Zeitaufwand für eine direkte oder indirekte Zuordnung zu Personen durch Dritte einzuschätzen sind. Organisatorisch kann das Schutzniveau durch eine besondere Trennung der eigentlichen Datenverarbeitung von der Erstellung der Pseudonyme – z.B. durch unabhängige Dritte – erhöht werden. Zudem können unterschiedliche technische Verfahren zur Erstellung von Pseudonymen gewählt werden, die die Stärke des Schutzes vor einer Identifizierung der betroffenen Personen beeinflussen können. Dazu ist ein besonderes Augenmerk auf mögliche Fehler und Unzulänglichkeiten der Datenverarbeitung im Zusammenhang mit der Pseudonymisierung und den Umgang mit pseudonymisierten Daten zu legen, beispielsweise das Beibehalten von Quasi-Identifikatoren, die Verwendung von verkettungsermöglichenden Daten oder eine unzureichende Berücksichtigung von Hintergrundwissen oder Auffälligkeiten im Datenbestand, die das Risiko einer etwaigen Zuordenbarkeit erhöhen.[11]

1. Erstellung von Pseudonymen

Die Zuordnung eines Pseudonyms zu einem Datensatz kann auf unterschiedliche Weisen erfolgen. Generell stehen zwei Verfahren zu Verfügung: eine Pseudonym-Erstellung[12] in Listen oder durch ein Berechnungsverfahren. Beiden gemein ist, dass man nur in Kenntnis der Liste bzw. des Berechnungsverfahrens ein Pseudonym einer Person zuordnen können darf und aufgrund der Möglichkeit der Zuordnung diese zusätzlichen Informationen gesondert aufzubewahren und durch technische und organisatorische Maßnahmen zu schützen sind.

Besonders zu beachten ist außerdem für die meisten Anwendungsfälle, dass die Zuweisung eines Pseudonyms an zwei unterschiedliche Personen zu vermeiden ist. So wäre auszuschließen, dass ein Auskunftsersuchen einer der beiden Personen zu einer Preisgabe der Daten der anderen Person führen kann.

2. Pseudonym-Erstellung in Listen

Bei einer Pseudonym-Erstellung in Listen werden Identitätsdaten anhand einer Tabelle Pseudonymen zugeordnet (siehe Abb. 2). Bei der Pseudonymisierung muss der Verantwortliche darauf achten, dass die Pseudonyme dabei keinen inhaltlichen oder funktionalen Bezug zu den Identitätsdaten haben. Ein Durchnummerieren der Pseudonyme ist dabei

7 Art.-29-Datenschutzgruppe, WP 216, 2014, 11 f.

8 Ebd., WP 216, 12.

9 Schwartmann/Weiß (Hrsg.), Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen, 2018, 28.

10 Ebd., 25.

11 Hansen, Art. 4 Nr. 5 DS-GVO, Rn. 57, in: Simitis et al. (Hrsg.), Datenschutzrecht – DS-GVO mit BDSG, 2019.

12 Nicht jede Pseudonym-Erstellung und Ersetzung der Identitätsdaten erfüllt die Anforderungen der DS-GVO an eine Pseudonymisierung.

nicht zu empfehlen, da ggf. aus dem Pseudonym Informationen ableitbar sind wie der Zeitpunkt der Aufnahme in die Datenbank oder die Position im Alphabet. Beides kann die Identifizierung für unbefugte Dritte erleichtern.

Zufällig vergebene Pseudonyme vermeiden dieses Risiko, allerdings sind auf diesem Weg Homonymfehler möglich, d.h. zwei unterschiedlichen Identitäten wird zufällig das gleiche Pseudonym zugewiesen. Um dies auszuschließen, kann es sinnvoll sein, vor der Neuvergabe eines Pseudonyms zu prüfen, ob es neu ist. Ist dies nicht möglich, muss die Länge der Pseudonyme so gewählt werden, dass derlei Fehler sehr unwahrscheinlich sind.

ID	Pseudonym (selbst gewählt)	Pseudonym (nummeriert)	Pseudonym (zufällig)
Petra Agridou *13.11.1972	MickeyMouse	56483	18637
Raja Mainz *04.12.1977	Tux_0412	56484	83476
Manfred Ohm *09.12.1981	Manfred_Ohm	56485	52248

Abb. 2: Darstellung verschiedener Pseudonyme

Sollen die Nutzenden eines Systems selbst ihre Pseudonyme wählen, ist dabei zu beachten, dass ein inhaltlicher Bezug zwischen Pseudonym und Identitätsdaten vonseiten des Verantwortlichen, der die pseudonymisierten Daten verarbeitet, nicht ausgeschlossen werden kann. Selbst wenn der Verantwortliche die Nutzenden über solche Identifizierungsrisiken informiert, kann er nicht sicher sein, dass die strengen Vorgaben an die Pseudonymisierung erfüllt werden. Hierbei handelt es sich in der Regel nicht um eine Pseudonymisierung gemäß DS-GVO.[13]

3. Pseudonym-Erstellung durch Berechnungsverfahren

Ein anderer Weg der Pseudonym-Erstellung ist die Zuordnung des Pseudonyms durch ein Berechnungsverfahren. Hierbei entfällt das Speichern einer Tabelle mit den Zuordnungen von Identitätsdaten zu Pseudonymen. Da allerdings sichergestellt werden muss, dass nicht auch Dritte aus den Identitätsdaten das Pseudonym berechnen können, muss das Verfahren abgesichert werden, z.B. mit einem geheimen kryptographischen Schlüssel.

Daher bietet sich als eine Form der Pseudonymisierung die Verwendung eines Blockchiffrieralgorithmus an, mit dem aus dem Schlüssel und den Identitätsdaten ein Pseudonym berechnet wird. Auch eine kryptographische Prüfsumme der Identitätsdaten kann für die Erzeugung eines Pseudonyms genutzt werden. Bei beiden Techniken ist darauf zu achten, dass der Stand der Technik beachtet wird und z.B. ein ausreichend langer Schlüssel verwendet wird. Maßgeblich muss auch hier sein, die erwartbare technische Entwicklung zu berücksichtigen.

Insbesondere muss das Verfahren gegen Aufzählungsangriffe gesichert sein. Das sind Angriffe, bei denen so lange Identitätsdaten als Eingabe der Berechnungsfunktion ausprobiert werden, bis die Identitätsdaten zu einem vorhandenen Pseudonym gefunden wurden. Wird zum Beispiel das Pseudonym mithilfe einer Einweg-Funktion (Hash-Funktion) lediglich aus einer Telefonnummer berechnet, kann aus dem Pseudonym zwar nicht unmittelbar die Telefonnummer ermittelt werden, jedoch lässt sich leicht für jede mögliche Telefonnummer das zugehörige Pseudonym berechnen. Mit der so erstellten Liste (Rainbow-Table) ließe sich ein zuvor unbekanntes Pseudonym einer Telefonnummer zuordnen. Dieser Angriff ist für jeden beschränkten Wertebereich möglich. Eine verschlüsselte Hash-Funktion, bei dem ein geheim zu haltender Parameter (Salt-Wert) einfließt, kann diese Gefahr verringern.

V. Ausblick

Pseudonymisierung ist ein wichtiges Instrument in der Datenschutz-Grundverordnung zum Schutz der betroffenen Personen. Allerdings wird dieser Schutz nicht von jedem Verfahren der Pseudonym-Erstellung erreicht. Um die Spreu vom Weizen zu trennen und das Mittel der Pseudonymisierung einfach und rechtssicher in der Praxis nutzbar zu machen, können Best-Practice-Ansätze und Standardisierungen von technischen Methoden und organisatorischen Einbettungen in die Abläufe der Verantwortlichen helfen. Der Nutzen starker, etablierter Verfahren der Pseudonymisierung wird zukünftig sowohl in dem erhöhten Schutz der betroffenen Personen liegen als auch in den Ermöglichungs- und Erleichterungsfunktionen einer Weiterverarbeitung pseudonymisierter personenbezogener Daten, zum Beispiel für statistische Zwecke.[14]

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

Benjamin Walczak
arbeitet seit 2017 als Informatiker beim ULD. Sein Schwerpunkt liegt in der Analyse und Bewertung von Konzepten und Techniken zur Umsetzung datenschutzrechtlicher Anforderungen.

Foto: Olaf Bathke, Kiel

13 Hansen, Art. 4 Nr. 5 DS-GVO, Rn. 36, in: Simitis et al. (Hrsg.), Datenschutzrecht – DS-GVO mit BDSG, 2019.

14 Schwartmann/Weiß (Hrsg.), Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz, 2017, 15 f.

Prof. Dr. Tobias Keber

Mythen der Datenschutzgrundverordnung – Erlesenes aus (knapp) 300 Tagen DS-GVO

Kurz vor der datenschutzrechtlichen Zeitenwende am 25.5.2018 überboten sich die Medien gegenseitig mit der Darstellung von Sachverhalten, die durch die DS-GVO künftig wesentlich erschwert oder gar unmöglich würden. Nach Abflachen einer Empörungswelle wurde der nächste Skandal schon herbeigeschrieben, wobei eine auflagenstarke Tageszeitung des Axel Springer Verlags besonderes Engagement zeigte. Andererseits liefert nicht jede Analyse der öffentlichkeitswirksam aufbereiteten Sachverhalte einen datenschutzrechtlich völlig unzutreffenden Befund. Nachfolgend sollen daher vier im öffentlichen Diskurs besonders hervorgetretene Episoden auf ihren juristischen Wahrheitsgehalt untersucht werden.

I. Mythos, Logos und die DS-GVO

Für die Sophisten stand der Mythos im Gegensatz zum Logos. Während ein Mythos zwar den Anspruch auf die von ihm behauptete Wahrheit erhebt, der Sache nach aber als märchenhafte Erzählung erscheint, bezeichneten sie mit Logos den Versuch, durch verstandesgemäße Beweise die Wahrheit einer Behauptung zu begründen. Für Aristoteles gehörte der Mythos ins Theater, Logos (als „echte" Wissenschaft) galt als Inbegriff der Vernunft.[1] Überträgt man das Gesagte auf den Untersuchungsgegenstand, so steht Logos für die juristische Subsumtion eines Lebenssachverhaltes unter die einschlägigen Rechtsnormen, hier vornehmlich die DS-GVO.

Der Suchbegriff „DS-GVO" und „Wahnsinn" weist bei Google Trends[2] 2018 in den Monaten Mai, Juni, Oktober sowie Ende des Jahres 2018 signifikante Spitzen auf.[3] Grob kann man diese den nachfolgend näher analysierten Episoden zuordnen. Dessen ungeachtet ist die Auswahl hier subjektiv. Angesichts des begrenzten Umfangs kann nicht auf den ebenso viel diskutierten alerten Metzgermeister,[4] die unter #Klingelgate bekannt gewordene Posse um 220.000 städtische Klingelschilder in Wien oder die in einer Mainzer Arztpraxis ausgelegte Einwilligungserklärung eingegangen werden, wonach der Unterzeichner „mit seiner Unterschrift bestätigt, die neue Datenschutz-Grundverordnung erhalten und gelesen zu haben, sowie deren Bedingungen zu akzeptieren".[5]

II. Viele Visitenkarten, eine Schublade und (k)ein Dateisystem

Ein besonders intensiv ventiliertes Narrativ betraf Visitenkarten. Am 15.5.2018 war bei "Die Welt" und anderen zu lesen, bereits die Annahme einer Visitenkarte eines Geschäftspartners lege einen Datenschutzverstoß nahe, wenn nicht im selben Moment über die mit diesen Daten beabsichtigte Verarbeitung informiert werde.[6] Auf reichweitenstarken YouTube-Kanälen witzelte man über den synallagmatischen Austausch von Visitenkarten (nur) gegen Ausgabe einer (die Karten im Größenformat deutlich übertreffenden) Datenschutzerklärung, die bei Geschäftsterminen vorzuhalten und zu übergeben wäre.[7] Um Versachlichung der Debatte bemüht, steuerte u.a. der BayLfD mit einem Statement zu Visitenkarten als einer schon seit 200 Jahren etablierten Merkhilfe zur sozialen Interaktion entgegen.[8] Der Autor hat sich vor diesem Hintergrund die Frage gestellt, ob eine (freilich hypothetisch) langjährig gelebte Praxis (noch) rechtmäßig sein kann, erhaltene Visitenkarten lose in einer von drei Schubladen eines Schreibtischcontainers abzulegen, wo sich über die Zeit durchaus 300-400 Karten gesammelt haben dürften.

Der Reihe nach und beginnen wir – streng dem Logos des DS-GVO-Prüfungsschemas verpflichtet – bei der Frage des sachlichen Anwendungsbereichs. Nach Art. 2 Abs. 1 DS-GVO betrifft dieser nicht nur die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, sondern auch die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Die Visitenkartenschublade könnte

1 Eingehend dazu Meyer, Bedeutungsgenese der Begriffe „Mythos" und „Logos" in der griechischen Antike, Archiv für Begriffsgeschichte 1999, S. 35 – 63 (60 ff.).

2 Der Online-Dienst „Google-Trends" der Google LLC stllt Informationen dazu bereit, welche Suchbegriffe wie oft von Nutzern der Suchmaschine eingegeben wurden. Anschließend werden die Ergebnisse in Relation zum totalen Suchaufkommen gesetzt.

3 Recherche abrufbar durch Eingabe der Begriffe DS-GVO und Wahnsinn, abrufbar unter https://trends.google.de/trends/explore?q=DS-GVO%20wahnsinn&geo=DE.

4 Dazu etwa Schmidt, l+f: Das DS-GVO-Absurditätenkabinett, Beitrag abrufbar unter https://www.heise.de/security/meldung/l-f-Das-DS-GVO-Absurditaetenkabinett-4057866.html.

5 Vgl. dazu Keber/Sehl/Schneider, 7 DS-GVO-Mythen im Rechtscheck, Beitrag bei Legal Tribune Online vom 28.1.2019, abrufbar unter https://www.lto.de/recht/feuilleton/f/europaeischer-datenschutztag-DS-GVO-kuriose-faelle-rechtliche-bewertung/. Beim Sozialen Netzwerk Twitter hat der Verfasser den #XFilesGDPR initiiert, wo sich mittlerweile eine beachtliche Sammlung skurriler Konstellationen rund um die DS-GVO findet.

6 Seibel, Jetzt werden sogar Visitenkarten zur Datenschutz-Falle, Artikel abrufbar unter https://www.welt.de/wirtschaft/article176468214/DS-GVO-Visitenkarten-werden-durch-neue-EU-Regel-zum-Datenschutz-Problem.html;
Hüfner, DS-GVO: Jetzt werden sogar Visitenkarten zum Datenschutz-Problem https://t3n.de/news/DS-GVO-visitenkarten-1080318/.

7 Das YouTube Video „DS-GVO Wahnsinn: So absurd wird es WIRKLICH, wenn man sich daran hält" der Kölner Rechtsanwaltskanzlei Wilde Beuge Solmecke (nach eigenen Angaben Europas größter Rechtskanal) wurde bis dato über 300.000 mal aufgerufen (Stand: 30. Januar 2019). Es ist abrufbar unter: https://www.youtube.com/watch?v=Q_P6Q3fkZB8.

8 BayLfD, Kurz-Information 11: Visitenkarten in der Welt der Datenschutz-Grundverordnung, Papier abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki11.html.

ein Fall nichtautomatisierter Verarbeitung personenbezogener Daten sein, was ein „Dateisystem" voraussetzt. Artikel 4 Nr. 6 DS-GVO definiert dieses als „strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird". Um personenbezogene Daten i.S.v., Artikel 4 Nr. 1 (Name, Anschrift, Telefonnummer etc.) geht es ohne Frage, problematisch ist das Merkmal der strukturierten Sammlung. Bedingt erhellend insoweit ist ErwG 15 Satz 3 DS-GVO, wonach Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, nicht in den Anwendungsbereich der Verordnung fallen sollen.

In der englischen Sprachfassung ist von „filing system" die Rede, einer Begrifflichkeit, wie sie sich schon in der (auch im Übrigen Art. 4 Nr. 6 DS-GVO ähnelnden) englischen Sprachfassung der Datenschutzrichtlinie 95/46[9] (Art. 2 lit. c) fand. Im Gegensatz zur DS-GVO führte die deutsche Sprachfassung des Art. 2 lit. c) RiLi 95/46 allerdings nicht den Begriff des Dateisystems, sondern nur den der „Datei".[10] Erkennt man darin letztlich nur einen Übersetzungsfehler im alten Recht, der mit der DS-GVO korrigiert wurde,[11] ist für die Interpretation des Art. 4 Nr. 6 DS-GVO das Urteil des EuGH in Sachen Zeugen Jehovas[12] relevant, in dem der Gerichtshof den Begriff der „Datei" (filing system) der Datenschutzrichtlinie im Rahmen der Vorlage eines finnischen Gerichts ausgelegt hat. Einem denkbar weiten Ansatz folgend heißt es in Randnummer 61 des Urteils:

„Insofern ist die Frage, nach welchem genauen Kriterium und in welcher genauen Form die Sammlung der von den einzelnen Verkündigern erhobenen personenbezogenen Daten tatsächlich strukturiert ist, ohne Belang, soweit in dieser Sammlung die Daten über eine bestimmte bereits aufgesuchte Person leicht wiederauffindbar sind, was jedoch das vorlegende Gericht anhand sämtlicher Umstände des Ausgangsverfahrens zu prüfen hat."

Erstens stellt der Gerichtshof das Merkmal der Strukturierung damit faktisch anforderungslos und ersetzt es durch den Aspekt einer leichten Wiederauffindbarkeit. Zweitens ist deren Bewertung nicht Sache des EuGH, sondern tatrichterliche Aufgabe. Mit guten Gründen (und Erfahrungswerten) lässt sich die leichte Auffindbarkeit einer einzelnen Visitenkarte unter mehreren hundert Karten im Fall der Visitenkartenschublade also verneinen. Anders verhält es sich, wenn bei Annahme oder Ablage der Karten die (spätere) Überführung in ein geordnetes (z.B. analoge Rollkartei mit A-Z Register) oder automatisches System (Adressdatenverwaltung, bspw. Outlook) geplant ist. Weil die Haushaltsausnahme in Art. 2 Abs. 2 lit.c) DS-GVO („ausschließlich persönliche Tätigkeit") bei der Kontaktanbahnung mittels Visitenkarten in aller Regel nicht greifen dürfte,[13] wäre der Anwendungsbereich der DS-GVO eröffnet.

Während die Rechtfertigung der Datenverarbeitung durch den Empfänger angesichts einer ihm übergebenen Visitenkarte wenig Probleme bereitet,[14] werfen die Transparenz- und Informationspflichten gem. Art. 12 ff. DS-GVO schwierige(re) Fragen auf. Nach Ansicht des BayLfD ist der Zeitpunkt der Entgegennahme der Karten streng von der zeitlich nachgelagerten Phase zu unterscheiden, in der diese Daten (gegebenenfalls automatisiert) verarbeitet werden.[15] Danach löst die Entgegennahme der Visitenkarte für sich genommen noch keine Informationspflicht aus. Die dann wesentlich interessantere, nachgelagerte Phase erhält in der Stellungnahme des BayLfD bemerkenswert wenig Raum. Die Beschreibung eines praktisch verwertbaren Lösungsansatzes vermisst man auch in der „DSK Orientierungshilfe zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung", wo das Visitenkartenproblem ebenfalls adressiert wird. Sibyllinisch heißt es dort:

„Visitenkarten, die von den betroffenen Personen auf Messen oder sonstigen Veranstaltungen ausdrücklich zur Informationszusendung oder weiteren geschäftlichen Kontaktaufnahme hinterlassen werden, können grundsätzlich eine wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO darstellen, wenn infolge weiterer Umstände für den Verantwortlichen eine Nachweisbarkeit der Einwilligung gegeben ist."[16]

Damit wird nicht nur die Frage des Vorliegens einer Einwilligung und diejenige ihrer Nachweisbarkeit vermengt. Auch welche weiteren Umstände relevant sein sollen, bleibt das Geheimnis der DSK. Wesentlich entschlossener fiel die Einschätzung des ehemaligen Bundesbeauftragten für den Datenschutz Schaar aus. Die Übergabe einer Businesscard erfolge regelmäßig durch den Inhaber, damit der Empfänger Kontakt mit ihm aufnehme. Damit sei der Inhaber der Karte auch insoweit informiert, dass der Empfänger die Daten in seinem Adressverzeichnis erfasst. Datenschutzrechtliche Informationspflichten gäbe es nur, wenn die Daten zu anderen Zwecken, etwa zur Überprüfung der Kreditwürdigkeit, herangezogen würden.[17]

9 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, abgedruckt in: Fink/Schwartmann/Cole/Keber, Europäisches und Internationales Medienrecht, 2. Aufl. A 100.

10 Vor diesem Hintergrund und zur nichtautomatisierten Datei in § 3 Abs. 2 S. 2 BDSG a.F.: Gola/Schomerus, BDSG, 12. Auflage 2015, § 3 Rn. 20.

11 Schwartmann/Mühlenbeck, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 4 Rn 91.

12 EuGH , Urteil vom 10.07.2018 – C-25/17. Vgl. dazu auch die Anmerkung Hoeren, ZD 2018, 469.

13 Vgl. dazu ErwG 18 sowie unten, 2.

14 In Betracht kommen eine konkludente Einwilligung, Art. 6 Abs. 1 lit. a) DS-GVO, Übergabe der Karte als vorvertragliche Maßnahme, Art. 6 Abs. 1 Buchstabe b) DS-GVO und die Verarbeitung zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f) DS-GVO.

15 So der BayLfD in der aktuellen Kurz-Information 11: Visitenkarten in der Welt der Datenschutz-Grundverordnung, Papier abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki11.html.

16 DSK Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO), Stand 7.11.2018, S. 9. Papier abrufbar unter https://www.datenschutzkonferenz-online.de/orientierungshilfen.html.

17 Schaar, Die notwendige Zumutung Datenschutz, Gastbeitrag bei Heise, online abrufbar unter https://www.heise.de/newsticker/meldung/Analyse-zur-DS-GVO-von-Peter-Schaar-Die-notwendige-Zumutung-Datenschutz-4057260.html.

Das klingt im Lichte der Ausnahmevorschrift des Artikel 13 Abs. 4 DS-GVO nachvollziehbar, wonach die Informationspflicht entfällt, wenn ein Betroffener über die Informationen bereits verfügt. Wortlaut („wenn und soweit") und Systematik des Artikel 13 Abs. 4 DS-GVO gebieten allerdings eine enge Interpretation. Auch wenn der Inhaber der Visitenkarte damit rechnet, dass der Empfänger die Daten (zum Zweck einer Kontaktaufnahme) in ein Adressverzeichnis aufnimmt, so ist ihm nicht bekannt, ob dies über ein Visitenkartenkarussell erfolgt oder durch Eingabe der Daten bei Outlook. Gleichgültig ist das dem Betroffenen nicht, denn die Gefahr einer Weitergabe der Adressdaten durch den Empfänger an Dritte – auch an die Anbieter (nicht nur, aber vor allem berufsorientierter) Sozialer Netzwerke durch Hochladen des Adressbuchs – ist hoch. Kaum in Betracht kommt eine Übertragung, bzw. analoge Anwendung der in Artikel 14 Absatz 5 lit. b) DS-GVO geregelten Ausnahme vom Informationsgebot bei unverhältnismäßigem Aufwand[18] oder eine Beschränkung der Informationspflicht nach § 32 I Nr. 1 BDSG. Denn diese Bestimmung ist wegen ihrer so in der DS-GVO nicht angelegten Differenzierung unionsrechtswidrig.[19]

Best Practice könnte nach alledem sein, auf der in der Regel vorhandenen Unternehmenswebseite die dort ohnehin bestehende Datenschutzerklärung um einen Abschnitt „Verfahren mit Visitenkarten" zu erweitern und dort anzugeben, was mit den Visitenkarten passiert. Der Empfänger einer Visitenkarte kontaktiert nun per Mail den Inhaber der Karte und bedankt sich für das nette Gespräch (anlässlich dessen die Karte übergeben wurde). In dieser Mail befindet sich in der Fußzeile ein standardisierter Hinweis darauf, dass der Umgang mit Visitenkarten in der Datenschutzerklärung auf der Unternehmenswebseite dokumentiert ist.[20]

III. Geschwärzte Kinderfotos und (kirchliches) Datenschutzrecht

Die Bild-Zeitung berichtete am 2.8.2018 über den katholischen Kindergarten St. Katharina in Dormagen (NRW), wo man dem Artikel zu Folge auf Fotos in den Erinnerungs-Mappen der Kinder die Gesichter der umstehenden, ebenfalls KiTA-angehörigen Freundinnen und Spielkameraden geschwärzt hatte.[21] Aus Angst, gegen die neue, verschärfte Datenschutz-Grundverordnung zu verstoßen, habe sich die KiTa-Leitung zu diesem Schritt entschlossen, da man sich nicht sicher war, ob die zu Beginn der Kindergartenzeit unterschriebene Einwilligungserklärung insoweit ausreiche.

Der Anwendungsbereich der DS-GVO ist eröffnet, wobei man bei den Bildern in der KiTA an das „Haushaltsprivileg" des Art. 2 Abs. 2 lit. c) DS-GVO denken könnte. Dann müsste es aber um eine Tätigkeit im ausschließlich persönlichen oder familiären Kontext gehen, die sich – wie die französische und die englische Sprachfassung („household", „domestique") deutlicher als die deutsche Formulierung zeigen – in der häuslichen (Privat-)Sphäre abspielt. Im Lichte von ErwG 18 zur DS-GVO und der Rechtsprechung des EuGH zur Vorgängervorschrift in der Datenschutzrichtlinie 95/46[22] ist das nicht zu begründen. Der nächste Prüfungsschritt führt, da es sich im fraglichen Fall um eine katholische KiTA handelt, in das an die DS-GVO zum 24.5.2018 angepasste Gesetz über den Kirchlichen Datenschutz (KDG). Auch insoweit gilt für die Verarbeitung personenbezogener Daten ein Verbot mit Erlaubnisvorbehalt, wobei § 6 KDG entsprechende Tatbestände – etwa eine Einwilligung der von der Verarbeitung betroffenen Person – vorsieht. Danach wäre eine Rechtfertigung für die Anfertigung und Verbreitung der Bildnisse der Kinder auf Grundlage einer Einwilligung ihrer Eltern grundsätzlich möglich (§ 6 Absatz 1 lit. b) KDG).[23]

Personenbezogene Daten liegen bei den Bildnissen der Kinder vor, gegebenenfalls sind sogar „besondere Kategorien personenbezogener Daten betroffen. Das sind nach der Begriffsbestimmung in § 4 Ziffer 2 KDG unter anderem solche personenbezogene Daten, aus denen die rassische und ethnische Herkunft oder religiöse oder weltanschauliche Überzeugungen hervorgehen" sowie genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person oder auch Gesundheitsdaten einer natürlichen Person. Personenfotos lassen regelmäßig die rassische und ethnische Herkunft der Abgebildeten erkennen. Damit wäre jede in den KiTA-Erinnerungsalben enthaltene Fotografie eine besonders sensible Datenverarbeitung.

Vor dem Hintergrund des Art. 91 DS-GVO[24] wird man insoweit aber auch deren Wertung in Erwägungsgrund 51 Satz 3 übertragen können, wonach die Verarbeitung von Lichtbildern nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden kann. Anders soll dies unter der Ägide der DS-GVO nur sein, wenn biometrische Daten erfasst werden; was etwa bejaht werden kann, wenn mit einem Smart-Phone erstellte Bilder einer Person in einem Sozialen Netzwerk hochgeladen werden und damit physische bzw. physiologische Merkmale des menschlichen Körpers maschinenlesbar gemacht werden.[25]

18 Schwartmann/Schneider, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 13, Rn. 65.

19 Dix, in: Simitis, Hornung, Spieker (Hrsg.), Datenschutzrecht, Artikel 13, Rn. 23.

20 Nahe liegt, den Hinweis in der Fußzeile einer E-Mail sogleich als Link auf die entsprechende Passage in der Datenschutzerklärung auszugestalten. Dieser Praxis steht entgegen, dass sicherheitsbewusste E-Mail Empfänger Links in E-Mails von Empfängern, die sie (noch) nicht näher kennen, grundsätzlich nicht ausführen.

21 Tischendorf, Hilfe, die haben alle meine Freunde angemalt, Artikel der Bild online verfügbar unter: https://www.bild.de/regional/duesseldorf/datenschutz/kindergarten-schwaerzt-alle-abschiedsfotos-56508006.bild.html.

22 Vgl. zu Artikel 3 Absatz 2 zweiter Gedankenstrich der Richtlinie 95/46 EuGH, Urteil v. 06.11.2003, C-101/01 Lindqvist, Rn. 54 ff.

23 Im hier zu betrachtenden Fall geht es nicht um Bilder zum Zweck der im Aufgabenbereich der KiTAs liegenden Entwicklungsdokumentation, wofür (trägerspezifisch) besondere gesetzliche Erlaubnistatbestände greifen können.

24 Nach Art. 91 DS-GVO und Erwägungsgrund 165 dürfen Kirchen und religiöse Vereinigungen oder Gemeinschaften umfassende Regelungen zum Datenschutz erlassen. Die Regelungen müssen allerdings im Einklang mit der Datenschutz-Grundverordnung stehen.

25 Jaspers/Schwartmann/Mühlenbeck, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 9, Rn. 72.

In der Kindertagesstätte ging es – soweit ersichtlich – nur um Abzüge der Personenfotos auf Papier, so dass es sich nach Sinn und Zweck der Vorgaben nicht um die Verarbeitung besonderer Kategorien personenbezogener Daten handelt. Mit diesem Ergebnis negierte man auch nicht das besondere Schutzbedürfnis der Kinder, dem bei den Anforderungen an die Einwilligung (ggfs. beider Erziehungsberechtigter als Träger der elterlichen Verantwortung (§§ 1626 BGB)) und den korrespondierenden Informationspflichten Rechnung zu tragen wäre.

§ 8 KDG enthält Vorgaben für die Einwilligung. Nach Absatz 1 der Vorschrift muss auf ihren konkreten Zweck sowie die Folgen ihrer Verweigerung hingewiesen werden, und die Einwilligung muss auf einer freien Entscheidung der betroffenen Person beruhen. Nach § 8 Abs. 2 KDG bedarf sie der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Nach Absatz 5 der Vorschrift muss der Verantwortliche die Einwilligung nachweisen können. Was genau in der Einwilligungserklärung der KiTA in Dormagen stand, lässt sich von hier aus nicht sagen. Die Fortgeltung der zu Beginn der Kindergartenzeit noch unter altem Datenschutzregime unterschriebenen Einwilligungserklärung[26] ist jedenfalls nicht ausgeschlossen, so sie denn hinreichend präzise formuliert war. Der Fortgeltung der Alteinwilligung nicht entgegen steht die (nach neuem Recht gesteigerte) Informationspflicht nach Artikel 13 DS-GVO,[27] die das KDG in § 15 spiegelt.

Kurz gesagt gilt also: Geschwärzte Kindergesichter in KiTA-Erinnerungsalben müssen nicht sein, soweit die Eltern aller betroffenen Kinder rechtswirksam und hinreichend informiert eingewilligt haben.

IV. Kaffee und Kuchen für 70 plus

Die Schwäbische Zeitung berichtete am 23.11.2018 über einen Seniorennachmittag für Menschen über 70 Jahre, dessen Planung durch das Datenschutzrecht erheblich erschwert worden sei. Der Veranstalter, ein DRK-Ortsverein, hatte für die Einladung der Zielgruppe in den Vorjahren immer Adresslisten von den Ortsverwaltungen erhalten, was unter dem Regime der DS-GVO nun nicht mehr möglich sei.[28]

Dieser Ansicht ist zunächst insoweit zuzustimmen, als der Anwendungsbereich der DS-GVO eröffnet ist. Die Datenverarbeitung überschreitet die Grenzen der Haushaltsausnahme deutlich. Zu unterscheidende Verarbeitungsschritte sind hier die Weitergabe der Meldedaten der Ortverwaltungen als öffentliche Stellen auf der einen und die Nutzung dieser Daten durch den DRK-Ortsverein als verantwortliche, nicht öffentliche Stelle[29] auf der anderen Seite.

Während sich der letztgenannte Verarbeitungsschritt gegebenenfalls mit berechtigten Interessen[30] rechtfertigen ließe, stellt sich für den ersten Verarbeitungsschritt die Frage, auf welchen Rechtfertigungstatbestand abgestellt werden kann, da Einwilligungen der einzuladenden Seniorinnen und Senioren insoweit nicht vorlagen. Der Sachverhalt ließe vor dem Hintergrund einer (Art. 6 Abs. 1 lit e, 6 Abs. 3 Satz 1 lit. b DS-GVO konkretisierenden) Datenübermittlung durch öffentliche Stellen an nichtöffentliche Stellen im Sinne des § 25 Absatz 2 BDSG denken, allerdings bestehen im Bundesmeldegesetz (BMG) insoweit speziellere Vorgaben, § 1 Absatz 2 Satz 1 BDSG. Mit Blick auf Erlaubnistatbestände im BMG muss man dann noch sehen, dass dieses Gegenstand des noch andauernden Anpassungsprozesses der nationalen Rechtslage durch das 2. Datenschutz-Anpassungsgesetzes ist.[31] Soweit gegenwärtig ersichtlich, betreffen diese Änderungen indes nicht die nachfolgend untersuchten Vorgaben zur Gruppenauskunft nach § 46 BMG.[32]

Nach § 46 Absatz 1 Satz 1 BMG darf eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Personen (Gruppe der 70-jährigen mit Namen und Anschrift) nur erteilt werden, wenn sie im öffentlichen Interesse liegt. Die Kombination der Tatbestandsmerkmale „darf nur" und „öffentliche Interessen" kann man nun so lesen, dass die Übermittlung von Meldedaten auf Grundlage einer Gruppenauskunft nach § 46 BMG an Vereine grundsätzlich nicht in Betracht kommt, da der verfolgte Zweck üblicherweise auf andere Weise erreicht werden kann, etwa durch öffentliche Aufrufe, Zeitungsanzeigen oder Postwurfsendungen und es in der Regel an einem öffentlichen Interesse fehle.[33] Dass die Seniorinnen und Senioren eine persönliche Ansprache wünschen, was nur in Gestalt einer persönlichen Einladung per Post möglich sein soll, erschließt sich nicht. Die dem Seniorennachmittag vorgeschaltete Datenverarbeitung ist damit tatsächlich so nicht möglich, was aber keine unmittelbare Folge der DS-GVO ist.

26 Eingehend zu Alteinwilligungen und ErwG 171 vgl. Schwartmann/Klein, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Artikel 6, Rn. 18. Vgl. ferner Art-29-Datenschutzgruppe WP 259, 29 sowie das GDD Praxishilfe XIII, S. 9.

27 Schwartmann/Klein, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Artikel 6, Rn. 19.

28 Artikel von Kircheis, abrufbar unter https://www.schwaebische.de/landkreis/alb-donau-kreis/emerkingen_artikel,-datenschutz-macht-probleme-beim-seniorennachmittag-_arid,10968694.html.

29 Das Deutsche Rote Kreuz e.V. ist föderal gegliedert in Bundesverband, Landes-, Bezirks-, Kreisverbände und Ortsvereine. Die Gliederungen arbeiten sämtlich auf der Basis von einheitlichen, systematisch aufeinander aufbauenden Satzungen zusammen, die die Rechte und Pflichten im Rahmen der Mitgliedschaft im Deutschen Roten Kreuz regeln. Die Ortsvereine führen die satzungsmäßigen Aufgaben des Deutschen Roten Kreuzes, u.a. die Förderung der Gesundheit, der Wohlfahrt und der Jugend, vorbehaltlich besonderer Vorgaben in den aufeinander aufbauenden Satzungen in eigener Verantwortung durch.

30 Art. 6 Abs. 1 lit. f DS-GVO, Versorgung der über 70jährigen mit Kaffee und Kuchen im Rahmen der Wohlfahrtspflege?

31 Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU), BT Drucksache 19/4674 v. 1.10.2018, Art. 16, Änderungen des Bundesmeldegesetzes, S. 33 ff.).

32 Zu den geplanten Änderungen im BMG vgl. die Stellungnahmen der Sachverständigen Bock und Aden in der Expertenanhörung vom 10.12.2018. Dokumente abrufbar unter https://www.bundestag.de/dokumente/textarchiv/2018/kw41-de-datenschutz-anpassung/572348.

33 So die Ansicht des LfD Niedersachsen im Informationspapier abrufbar unter https://www.lfd.niedersachsen.de/themen/melderecht/datenschutz-im-melderecht-56172.html Stand des Dokuments: November 2017. In diese Richtung jetzt auch BayLDA: Aktuelle Kurz-Information 5 – Melderegisterdaten und Gratulationen, Informationspapier abrufbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki05.html.

V. Weihnachtsaktion ohne Datenschutz

Am 15.11.2018 berichtete der Bayerische Rundfunk über das mittelfränkische Roth, wo die Datenschutzgrundverordnung einer schönen Tradition auf dem Christkindelsmarkt ein vorläufiges Ende bereitet haben soll.[34] Bis dahin hatten Kinder in der Vorweihnachtszeit Wunschzettel an den Weihnachtsbaum auf dem Marktplatz in Roth gehängt. Neben den Weihnachtswünschen der Kinder (Fahrt im Feuerwehrauto der örtlichen freiwilligen Feuerwehr, Besuch beim Bürgermeister, Sachgeschenke) waren dort ihre Kontaktdaten (Vorname, Name, Anschrift) zu lesen. Nach der früheren Praxis gab die Stadt die jährlich bis zu 4000 Wunschzettel an externe Sponsoren weiter, die die Wünsche gegebenenfalls erfüllten. Im November 2018 ließ die Stadt allerdings verlautbaren, die Aktion könne mit Rücksicht auf die Vorgaben der DS-GVO nicht mehr durchgeführt werden. Sich schützend vor potentiell verletzte Kinderseelen werfend intervenierte am 20.11.2018 der private Radiosender Antenne Bayern und stellte medienwirksam ("Antenne Bayern rettet Weihnachtstradition")[35] eine Einwilligungserklärung zum Ausdruck bereit, die von den Eltern der Kinder unterschrieben und den für die Wunschzettelaktion Verantwortlichen übergeben werden konnte.

Für die Lösung des Falls sind einerseits die Situation vor und das Verfahren nach dem 20.11.2018 sowie andererseits zwei größere Verarbeitungsschritte zu unterscheiden.[36] Der erste Verarbeitungsschritt betrifft die Sammlung/Erhebung der Daten am städtischen Weihnachtsbaum, der zweite Schritt die Weitergabe der Wunschzettel an die Sponsoren, wobei hierfür streng genommen noch ein weiterer Prozess in Gestalt einer Sortierung (welcher Wunsch wird an welchen Sponsor weitergegeben – „Wunsch-Matching") vorgeschaltet ist. Beginnen wir mit der Analyse der Situation vor der Intervention von Antenne Bayern am 20.11.2018:

Die Eröffnung des sachlichen Anwendungsbereichs der DS-GVO erschließt sich jedenfalls mit Blick auf die erste Verarbeitungsphase (noch) nicht ohne weiteres. Art. 2 Abs. 1 DS-GVO adressiert auch die nichtautomatisierte Verarbeitung personenbezogener Daten, Voraussetzung ist dann aber wie oben gesehen, dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Selbst bei einem weiten Verständnis fällt es schwer, bei knapp 4000 beliebig an einen Baum gehängten Zetteln von einer „Struktur" zu sprechen; jedenfalls, wenn man dies nicht auf eine bloß theoretische Auffindbarkeit (irgendwo an diesem Baum) beschränkt.

Ungeachtet dessen geht es im Fall um eine Datenverarbeitung der Stadt Roth als öffentliche Stelle, was über Art. 6 Abs. 1 lit. e), Abs 2 und 3 DS-GVO ins Bundes-, bzw. Landesrecht führt und angesichts der Handlungen der Stadt Roth den Anwendungsbereich des Bayerischen Datenschutzgesetzes nach § 1 Abs. 1 Satz BayDSG auslöst. Jenes bestimmt in Art. 2 Satz 1 BayDSG,[37] dass für die Verarbeitung personenbezogener Daten durch öffentliche Stellen vorbehaltlich anderweitiger Regelungen die Vorschriften der DS-GVO auch außerhalb des sachlichen Anwendungsbereichs des Art. 2 Abs. 1 und 2 DS-GVO gelten, also auch für die hier in Frage stehende nichtautomatisierte Verarbeitung außerhalb eines Dateisystems.

Zu prüfen sind dann (Zeitphase vor dem 20.11.2018) gesetzliche Erlaubnistatbestände.[38] Für den ersten Verarbeitungsschritt (Veranstaltung der Aktion) kommt Art. 4 BayDSG in Betracht. Absatz 1 der Vorschrift erlaubt die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle, wenn dies zu ihrer Aufgabenerfüllung erforderlich ist. Aufgaben der Gemeinde sind nach Art. 7 Absatz 1 der Bayerischen Gemeindeordnung (GO) alle Angelegenheiten der örtlichen Gemeinschaft, wobei insoweit auf die nicht abschließende („insbesondere") Aufzählung in Art. 83 Abs. 1 der Bayerischen Verfassung verwiesen wird, der unter anderem die örtliche Kulturpflege nennt. Traditionell werden dem eigenen Wirkungskreis der Gemeinden u.a. ihre Selbstverwaltung, die Daseinsvorsorge, aber auch die diesbezügliche Öffentlichkeitsarbeit zugerechnet. Mit Blick auf die Erforderlichkeit i.S.d. Art. 4 BayDSG ließe sich zwar kritisch fragen, wie weit sich dies mit Blick auf eine derartige Wunschzettelaktion (ernsthaft) bejahen lässt. Erforderlichkeit nimmt der EuGH jedoch zum Teil schon dann an, wenn ohne die betreffende Tätigkeit ein legitimes Ziel nur weniger effizient erfüllt werden kann.[39]

Vor dem Hintergrund gesetzlicher Erlaubnistatbestände problematischer ist der zweite Verarbeitungsschritt, die Übermittlung der Wunschzettel mit den personenbezogenen Daten an Dritte (Sponsoren). In Betracht kommt Art. 5 BayDSG, der bestimmte Datenübermittlungen legitimiert und zwischen der Übermittlung öffentlicher Stellen untereinander (Absatz 1 Nr. 1) und der Übermittlung von einer öffentlichen Stelle an eine nicht öffentliche Stelle (Absatz 1 Nr. 2) unterscheidet. Vor diesem Hintergrund lässt sich ersterenfalls die Übermittlung der Wunschzetteldaten an die örtliche Feuerwehr rechtfertigen, soweit es um eine Spazierfahrt mit einem Löschfahrzeug geht. Geht es um die Weitergabe von Daten an private Sponsoren, die Sachgeschenke zum Gegenstand haben, kommt Nr. 2 der Vorschrift in Betracht, der eine Interessenabwägung vorsieht.

Mit Urteil vom 27. September 2018 hat das Bundesverwaltungsgericht entschieden,[40] dass die Regelung zur Über-

34 Https://www.br.de/nachrichten/bayern/wunschzettel-aktion-in-roth-faellt-wegen-datenschutzgruenden-aus,R9UKMr1.

35 Https://www.antenne.de/programm/sendungen/die-stefan-meixner-show/antenne-bayern-rettet-rother-weihnachtsaktion-euer-wunschzettel-ans-christkind.

36 Vgl. hierzu insgesamt auch Veil, Die Wunschzettel am Weihnachtsbaum der Stadt Roth, Artikel v. 24.11.2018 bei CR Online, abrufbar unter https://www.cr-online.de/blog/tag/wunschzettel/.

37 BayDSG, in der Fassung vom 15.05.2018.

38 Fragen zu technisch-organisatorischen Maßnahmen oder Maßnahmen zur Zugangssicherung zum Wunschzettelbaum sollen hier nicht adressiert werden.

39 Zur Rechtsprechung des EuGH eingehend EDPS, Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit, Dokument vom 11.04.2017, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_de.pdf.

40 BVerwG 7 C 5.17, Entscheidung abrufbar unter https://www.bverwg.de/de/270918U7C5.17.0.

mittlung in Art. 5 Abs. 1 S. 1 Nr. 2 BayDSG mit den Vorgaben der DS-GVO nicht vereinbar sei. Begründet hat das Gericht diese Einschätzung mit dem Argument, dass sich die landesrechtliche Vorschrift nicht in dem durch die Öffnungsklauseln in Art. 6 Abs. 2 und 3 determinierten Rahmen halte, weil danach nur eine Konkretisierung der Regelungen von Art. 6 Abs. 1 Unterabs. 1 Buchst. c und e DS-GVO erlaubt sei, während die landesrechtliche Bestimmung der Sache nach an Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO anknüpfe, der wegen seines Satz 2 für Behörden gerade gesperrt sei. Anders sei dies – so das Gericht in seiner Begründung mit Hinweis auf die Kommentarliteratur[41] – nur, wenn die Behörde als Teilnehmer im Privatrechtsverkehr auftrete. Vor diesem Hintergrund liegt es nahe, diesen Ausnahmefall auch für solche Konstellationen anzudenken, in denen eine behördliche Stelle deshalb (ausnahmsweise) wie ein Teilnehmer im Privatrechtsverkehr erscheint, weil für sie – zumindest partiell – eine grundrechtsspezifische Gefährdungslage besteht. Das wäre bei Maßnahmen im Bereich der Selbstverwaltungsangelegenheiten der Gemeinden der Fall.

Unabhängig davon kommt jedenfalls nach dem 20.11.2018 eine einwilligungsbasierte Datenverarbeitung in Betracht, die den Informationspflichten, Artt. 13 Abs. 1, Abs. 2 DS-GVO (u.a. Dauer der Speicherung, Hinweis auf Betroffenenrechte) hinreichend Rechnung tragen müsste. Das von Antenne Bayern zur Verfügung gestellte Formular (das sich die Stadt durch An-/Übernahme zu eigen gemacht hat) erschöpfte sich in dem Hinweis „Ich bin damit einverstanden, dass meine Kontaktdaten und der Wunsch meines Kindes im Rahmen der Wunscherfüllung an Dritte (z.B. Sponsoren) weitergeleitet werden. Die Kontaktdaten werden von der Stadt Roth nur im Rahmen der Wunschaktion und nicht für Werbezwecke o.ä. verwendet.“[42]

Selbst wenn man es mit der herrschenden Auffassung für möglich hält, den Transparenz- und Informationspflichten auch gestuft und über Medienbrüche hinweg zu entsprechen,[43] fehlt im Formular die unmittelbar auf erster Ebene vorzuhaltende[44], hinreichend konkrete Information über die Empfänger, der pauschale Verweis auf „Dritte (z.B. Sponsoren)“ reicht insoweit nicht. Die weiteren Angaben (2nd Level: Beschwerderecht, Dauer der Speicherung, Rechtsgrundlage der Verarbeitung u.a.) hätte man über weiterführende Hinweise auf einer verlinkten Webseite adressieren können. Dies ist – soweit ersichtlich – aber nicht erfolgt. Rechtlich möglich ist eine derartige Wunschzettelbaum-Aktion nach alledem schon, nur eben nicht so, wie es in Roth (zunächst) gelaufen ist. Zu diesem Ergebnis gelangt dem Grunde nach auch ein Statement der Europäischen Kommission vom 21.11.2018.[45] Dass dieser neuerdings eine Kompetenz zur (authentischen) Interpretation der DS-GVO zukäme, wäre allerdings: ein Mythos.

VI. Fazit

Die vier schillernden Episoden aus der Welt der datenschutzrechtlichen Praxis nach dem 25.5.2018 liefern nach ihrer Analyse im Lichte des Logos der DS-GVO keinen einheitlichen Befund. Grundsätzlich macht das neue Regelungsregime Erinnerungsalben mit Bildern der Spielkameraden im Kindergarten ebenso wenig unmöglich, wie die Einladung zum Seniorennachmittag mit Kaffee und Kuchen unter allen Umständen am Datenschutz scheitert. Entscheidend ist das "Wie genau" der Verarbeitung personenbezogener Daten, was bei dem Visitenkartenbeispiel ebenso eine zentrale Rolle spielt, wie bei der Wunschzettel-Aktion auf dem Weihnachtsmarkt. Die von DS-GVO-Kritikern bemühten Narrative funktionieren im öffentlichen Diskurs nur deshalb so gut, weil sie keinen Raum für Differenzierung lassen. Ein "Es kommt darauf an" als Leitmotiv juristisch seriöser Arbeit macht die öffentlichkeitswirksame Kommunikation für Datenschützer deutlich schwerer. Diese schicksalshafte Last ist aber keine spezifische Folge der DS-GVO.

Prof. Dr. Tobias Keber
Professur für Medienrecht und Medienpolitik in der digitalen Gesellschaft an der Hochschule der Medien (HdM) Stuttgart. Lehrbeauftragter für Internet- und Multimediarecht am Mainzer Medieninstitut (Johannes Gutenberg-Universität Mainz). Vorsitzender des Wissenschaftlichen Beirats der Gesellschaft für Datenschutz und Datensicherheit (GDD) sowie im Leitungsgremium des Instituts für Digitale Ethik (IDE) an der Hochschule der Medien.

41 Albers/Veit, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand 1. Mai 2018, Art. 6 DS-GVO Rn. 46; Heberlein, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 51 f.; Schulz, in: Gola, Datenschutz-Grundverordnung, Art. 6 DS-GVO Rn. 56; Frenzel, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 6 Rn. 26.

42 Formular abrufbar unter https://www.antenne.de/programm/sendungen/die-stefan-meixner-show/antenne-bayern-rettet-rother-weihnachtsaktion-euer-wunschzettel-ans-christkind.

43 Dazu WP 260 Rev. 1 v. 11.4.2018, S. 19 f.

44 Vgl. GDD-Praxishilfe DS-GVO VII – Transparenzpflichten bei der Datenverarbeitung, Version 2.1, Stand April 2018 https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf.

45 Unter der Überschrift „Klarstellung: EU-Datenschutz verbietet keine Wunschzettel-Aktionen zu Weihnachten“ heißt es dort: „Die Europäische Datenschutzgrundverordnung verbietet in keiner Weise Wunschzettel-Aktionen zu Weihnachten. Berichte, die auf das Gegenteil schließen lassen, sind falsch. Um Geschenke an die Kinder zu liefern, dürfen die Kontaktdaten der Familie aufgenommen werden – vorausgesetzt, die Eltern stimmen zu. Das sind die Regeln, die schon seit 20 Jahren gelten. Die Datenschutzgrundverordnung hat daran nichts geändert.“ Das Statement ist abrufbar unter: https://ec.europa.eu/germany/news/20181121-klarstellung-eu-datenschutz-verbietet-keine-wunschzettel-aktionen-zu-weihnachten_de.

Maximilian Hermann, LL. M.

Datenschutz in Prüfungsverfahren nach DS-GVO und BDSG

In Prüfungsverfahren[1] liegt es in der Natur der Sache, dass personenbezogene Daten verarbeitet werden. Prüfungsverfahren dienen der Leistungsbeurteilung von Prüflingen. Eine Leistungsbeurteilung kann dabei nur dann erfolgen, wenn genügend Informationen über den zu beurteilenden Prüfling vorliegen. Durch die Verarbeitung personenbezogener Daten von Prüflingen erhalten Prüfungseinrichtungen viele Informationen über die Prüflinge. Es geht dabei u.a. um Daten über persönliche Verhältnisse, Leistungsvermögen, Gesundheit und Stressresistenz.[2] Der Datenschutz in Prüfungsverfahren ist nicht gänzlich neu. Durch das Inkrafttreten der DS-GVO werden Prüfungsverfahren jedoch in vielen relevanten Bereichen auf völlig neue rechtliche Grundlagen gestellt. Der Aufsatz widmet sich dabei spezifischen Fragestellungen, die sich in Prüfungsverfahren in öffentlich-rechtlichen Prüfungseinrichtungen, wie staatlichen Hochschulen oder Justizprüfungsämtern, ergeben.

I. Personenbezogene Daten in Prüfungsverfahren

Die DS-GVO definiert den Begriff der personenbezogenen Daten in Art. 4 Nr. 1 DS-GVO. Vergleicht man die Datenverarbeitungsvorgänge in Prüfungsverfahren mit dieser Definition, lassen sich eine Vielzahl von personenbezogenen Daten in Prüfungsverfahren identifizieren.

Zunächst ist hier an Namen, Alter, Geschlecht und Anschrift der Prüflinge zu denken. Auch die Matrikel- oder Prüfnummern sind personenbezogene Daten. Dabei ist es unerheblich, ob der Prüfer den Prüfling im Zeitpunkt der Korrektur und der Bewertung der Prüfungsarbeit identifizieren kann oder nicht.[3] Auch Lichtbilder der Prüflinge, die für eine Prüfungsakte oder den Studierendenausweis verwendet werden, sind personenbezogene Daten.[4] Wird mit den Prüflingen per E-Mail kommuniziert, kommt der E-Mail-Adresse dann Personenbezug zu, wenn anhand der in der Adresse angegebenen Informationen eine Identifikation der Person möglich ist. Auch die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung sind personenbezogene Daten.[5] Der Inhalt der Antworten spiegelt nämlich den Kenntnisstand und das Kompetenzniveau des Prüflings in einem bestimmten Bereich sowie gegebenenfalls seine Gedankengänge, sein Urteilsvermögen und sein kritisches Denken wider.[6] Im Fall einer handschriftlich verfassten Prüfung enthalten die Antworten zudem Informationen über die Handschrift.[7]

Im Rahmen von Prüfungsverfahren werden nicht nur personenbezogene Daten der Prüflinge verarbeitet. In der Regel sind auch personenbezogene Daten Dritter berührt, die am Prüfungsverfahren beteiligt sind. Insbesondere geben Prüfer in schriftlichen Arbeiten Bewertungen ab und versehen die Arbeiten mit korrekturbezogenen Anmerkungen. So kommt im Inhalt dieser Anmerkungen die Ansicht oder Beurteilung des Prüfers in Bezug auf die individuelle Leistung des Prüflings in der Prüfung und insbesondere in Bezug auf dessen Kenntnisse und Kompetenz in dem betreffenden Bereich zum Ausdruck. Diese Anmerkungen zielen im Übrigen gerade darauf ab, die Beurteilung der Leistung des Prüflings durch den Prüfer zu dokumentieren und können Auswirkungen auf die Rechte und Interessen des Prüflings haben.[8] Dem steht auch nicht entgegen, dass die Anmerkungen des Prüfers zu den vom Prüfling in der Prüfung abgegebenen Antworten Informationen darstellen, die aufgrund des Inhalts, ihres Zwecks und ihrer Auswirkungen mit dem betreffenden Prüfling verknüpft sind, zugleich Informationen über den Prüfer darstellen. Ein und dieselbe Information kann nämlich mehrere natürliche Personen betreffen und folglich für diese Personen personenbezogene Daten darstellen.[9]

II. Keine Privilegierung zu Forschungszwecken

Die Durchführung von Prüfungsverfahren obliegt in vielen Fällen Hochschulen und damit wissenschaftlichen Einrichtungen. Datenverarbeitungen zu wissenschaftlichen Zwecken werden an verschiedenen Stellen der DS-GVO privilegiert. Insbesondere enthält Art. 89 Abs. 2 DS-GVO eine Öffnungsklausel zugunsten der Mitgliedsstaaten, die Rechte der betroffenen Personen bei Verarbeitungen zu wissenschaftlichen Forschungszwecken einzuschränken.[10] Handelt es sich bei den zu wissenschaftlichen Forschungszwecken verarbeiteten Daten um besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO, sieht Art. 9 Abs. 2 lit. j DS-GVO eine Öffnungsklausel zugunsten der Mitgliedsstaaten vor, Ausnahmen vom grundsätzlichen Verarbeitungsverbot des Art. 9 Abs. 1 DS-GVO zu normieren.[11]

1 Der Verfasser hat sich im Zuge seiner Masterarbeit mit dem Datenschutz in Prüfungsverfahren nach DS-GVO und BDSG beschäftigt. Die Arbeit ist online abrufbar unter: https://epb.bibl.th-koeln.de/frontdoor/index/index/docId/1285.

2 Vgl. Schwartmann/Hermann, Forschung & Lehre 7/18, S. 578.

3 EuGH, Urt. v. 20.12.2017, C-434/16, Rn. 30 – Nowak.

4 Enthalten diese Bilder biometrische Daten, ist der Anwendungsbereich von Art. 9 DS-GVO eröffnet.

5 EuGH, Urt. v. 20.12.2017, C-434/16 – Nowak.

6 EuGH, Urt. v. 20.12.2017, C-434/16, Rn. 37 – Nowak.

7 EuGH, Urt. v. 20.12.2017, C-434/16, Rn. 37 – Nowak.

8 Vgl. EuGH, Urt. v. 20.12.2017, C-434/16, Rn. 43 – Nowak.

9 Vgl. EuGH, Urt. v. 20.12.2017, C-434/16, Rn. 44 – Nowak.

10 Der deutsche Gesetzgeber hat mit § 27 Abs. 2 BDSG von der Öffnungsklausel Gebrauch gemacht.

Voraussetzung für die Privilegierung ist jedoch, dass es sich um Verarbeitungen zu wissenschaftlichen Forschungszwecken handelt. Wird man die wissenschaftliche Forschung und Lehre noch unter die Privilegierungen der DS-GVO fassen können, ist dies für Prüfungsverfahren nicht der Fall.[12] Prüfungsverfahren sind nicht als Teil der Lehre zu qualifizieren. Dies ergibt sich unmittelbar aus dem Zweck der Prüfungsverfahren: Prüfungsverfahren dienen nicht dazu, neues Wissen und neue Erkenntnisse zu gewinnen, sondern erlerntes Wissen abzurufen und anzuwenden. Es findet daher viel mehr eine Leistungsbeurteilung des Prüflings in dieser Hinsicht statt. Diese Leistungsbeurteilung ist nicht unter den Begriffen Forschung und Lehre zu fassen.

III. Bestimmung des Verantwortlichen

Werden personenbezogene Daten in Prüfungsverfahren verarbeitet, ist zu prüfen, wen die gesetzlich normierten Pflichten treffen. Dies ist in erster Linie der Verantwortliche. Der Verantwortliche nach der Definition des Art. 4 Nr. 7 DS-GVO wird zum Adressaten der Pflichten der DS-GVO und so zur Einhaltung der datenschutzrechtlichen Grundsätze verpflichtet.

Nach dem Wortlaut des Art. 4 Nr. 7 DS-GVO können natürliche oder juristische Personen, Behörden, eine Einrichtung oder eine andere Stelle Verantwortlicher sein. Der Begriff des Verantwortlichen ist daher ein Oberbegriff für verschiedene in Betracht kommende Normadressaten.[13]

Für Prüfungsverfahren im öffentlichen Bereich ist der Begriff der Behörde prägend. Die Behörde ist jedoch weder in Art. 4 Nr. 7 DS-GVO noch an einer anderen Stelle in der DS-GVO näher definiert. Ebenfalls das BDSG oder die Landesdatenschutzgesetze enthalten keine Legaldefinition. Deshalb bedarf es zur näheren Bestimmung des Begriffs eines Rückgriffs auf die Legaldefinition des Verwaltungsverfahrensgesetzes.[14]

Gem. § 1 Abs. 4 VwVfG ist Behörde jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt. Dabei ist ein funktionelles, d.h. aufgabenorientiertes und kein organisatorisches, Verständnis zugrunde zu legen.[15] Ausgehend von der funktionalen Ausrichtung der DS-GVO sind in diesem Zusammenhang keine grundsätzlichen Konflikte des deutschen Rechts mit dem EU-Datenschutzrecht erkennbar.[16] Dieses funktionelle Verständnis ist auch aus datenschutzrechtlichen Erwägungen notwendig. Die Stelle, die personenbezogene Daten verarbeitet, hat den transparentesten Blick auf die Datenverarbeitungsprozesse und entscheidet über Zweck und Mittel der Datenverarbeitung. Sie ist damit in der Lage, die datenschutzrechtlichen Vorgaben zu erfüllen und damit das Ziel, den Einzelnen vor unrechtmäßiger Verarbeitung seiner personenbezogenen Daten zu schützen, zu erreichen. In Abgrenzung zu einem bloßen Behördenteil ist darauf abzustellen, ob eine gewisse organisatorische Selbstständigkeit besteht.[17] Indizien sind hierfür insbesondere die Unabhängigkeit vom Wechsel des Amtsinhabers, die Selbstständigkeit der Aufgabenerledigung sowie die Möglichkeit, die eigenen Angelegenheiten in einem gewissen Umfang selbst zu gestalten.[18] Entscheidend für den Behördenbegriff sind die aufgezeigten Maßstäbe. Es kommt nicht darauf an, ob die Bezeichnung „Behörde“ ausdrücklich geführt wird.[19] Danach sind unselbstständige Arbeitseinheiten einer Behörde im Regelfall keine Behörde.

Nimmt man diese Kriterien als Maßstab, ist zu erkennen, dass beispielsweise Justizprüfungsämter, die für die Abnahme der ersten juristischen Staatsprüfung zuständig sind[20] und Landesjustizprüfungsämter, die für die Abnahme der zweiten juristischen Staatsprüfung zuständig sind[21], als eigene Behörden zu qualifizieren sind. Die Prüfungsämter bestehen unabhängig eines Wechsels des Amtsinhabers. Sie sind zwar den Oberlandesgerichten[22] bzw. dem Justizministerium[23] angegliedert. Diese organisatorische Verbindung mit einer anderen Behörde schließt aber die Behördeneigenschaft nicht aus.[24] Aufgrund gesetzlicher Bestimmungen treten sie eigenständig auf. Sie sind in ihrer Aufgabenerledigung weitestgehend selbstständig und können ihre Aufgaben im gesetzlich zugewiesenen Rahmen selbst gestalten.

Ob Prüfungsausschüsse an Hochschulen als Behörden zu qualifizieren sind und damit Verantwortliche nach Art. 4 Nr. 7 DS-GVO sind, hängt davon ab, welche Regelungen die jeweiligen Prüfungsordnungen, bezogen auf den Prüfungsausschuss, enthalten und wie die Stellung des Prüfungsausschusses innerhalb der Hochschule ausgestaltet ist. Sind die Regelungen so ausgestaltet, dass der Prüfungsausschuss eine ähnliche Stellung wie die dargestellten Prüfungsämter hat, ist der Prüfungsausschuss als Behörde zu qualifizieren. Er ist dann auch Verantwortlicher nach Art. 4 Nr. 7 DS-GVO, und ihn treffen alle Vorgaben der DS-GVO und der nationalen Regelungen.[25] Er kann dann, bezogen auf das Prüfungsverfahren, nicht mehr als unselbstständiger Teil der Hochschule angesehen werden.[26]

IV. Datenminimierung durch Pseudonymisierung

Datenverarbeitungen in Prüfungsverfahren haben den Grundsätzen des Art. 5 DS-GVO zu entsprechen. Insbesondere müssen personenbezogene Daten nach Art. 5 Abs. 1

11 Zum Beispiel § 27 Abs.1 u. Abs. 3 BDSG.

12 So auch Golla, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, Teil C, § 23, Rn. 77.

13 Schwartmann/Mühlenbeck, in: HK-DS-GVO/BDSG, Art. 4 Nr. 7, Rn. 108.

14 Dieser Rückgriff auf die Definition der Behörde nach dem Verwaltungsverfahrensgesetz ist nicht nur notwendig, sondern auch zulässig, vgl. Klar/Kühling, in: Kühling/Buchner, DS-GVO, § 2 BDSG, Rn. 4.

15 Schwartmann/Mühlenbeck, in: HK-DS-GVO/BDSG, Art. 4 Nr. 7, Rn. 114.

16 Vgl. Petri, in: Simitis, Hornung, Spiecker, Datenschutzrecht, Art. 4 Nr. 7, Rn. 19.

17 Klar/Kühling, in: Kühling/Buchner, DS-GVO, § 2 BDSG, Rn. 4.

18 Klar/Kühling, in: Kühling/Buchner, DS-GVO, § 2 BDSG, Rn. 4.

19 Schmitz, in: Stelkens/Bonk/Sachs, VwVfG, § 1, Rn. 237.

20 § 3 Abs. 1 JAG-NRW.

21 § 48 Abs. 1 JAG-NRW.

22 § 3 Abs. 1 S. 2 JAG-NRW.

23 § 48 Abs. 1 S. 2 JAG-NRW.

24 Vgl. Schmitz, in: Stelkens/Bonk/Sachs, VwVfG, § 1, Rn. 240.

25 Je nach Ausgestaltung in der jeweiligen Prüfungsordnung können die Voraussetzungen einer gemeinsamen Verantwortlichkeit erfüllt sein, sodass es Art. 26 DS-GVO zu beachten gilt.

26 Vgl. Schmitz, in: Stelkens/Bonk/Sachs, VwVfG, § 1, Rn. 242.

lit. c DS-GVO dem Zweck angemessen und sachlich relevant sein. Zudem muss die Datenverarbeitung auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein. Nach der DS-GVO unzulässig ist damit die Verarbeitung personenbezogener Daten, die für den verfolgten Zweck inadäquat, unerheblich oder entbehrlich ist.[27] Wesentliche Ausprägung des Grundsatzes der Datenminimierung ist die Forderung nach Pseudonymisierung und Anonymisierung.[28]

In Prüfungsverfahren kommt der Pseudonymisierung eine besondere Rolle zu. Insbesondere bei der Erstellung von Klausuren ist der Grundsatz der Datenminimierung zu beachten. Mit Hilfe der Pseudonymisierung kann dafür gesorgt werden, dass der Umfang der Verarbeitung personenbezogener Daten wesentlich beschränkt wird. So ist es angezeigt, dass auf Klausuren der (Klar-)Name der Prüflinge nicht auftaucht, sondern etwa durch ein Pseudonym ersetzt wird. Ein denkbares Pseudonymisierungsverfahren für Prüfungsverfahren stellt die Zuteilung von Prüfnummern dar. Dabei erhält jeder Prüfling eine Prüfnummer, die mit seinem Namen und weiteren (prüfungsrelevanten) Daten verknüpft ist. Der für das Prüfungsverfahren Verantwortliche hat alleine Zugriff auf eine Zuordnungsübersicht, die die Verknüpfung der Prüfnummern mit dem jeweiligen Prüfling zulässt. Diese Zuordnungsübersicht muss mit den notwendigen technischen und organisatorischen Maßnahmen vor Zugriffen Unbefugter abgesichert werden.

Hand in Hand mit der datenschutzrechtlich angezeigten Pseudonymisierung geht die Objektivität der Prüfer einher. Diese sind dann nicht in der Lage den Prüfling zu identifizieren und eine objektive Beurteilung der Prüfungsleistung wird gefördert. Prüfungsrechtlich ist die Pseudonymisierung von schriftlichen Prüfungsarbeiten nicht zwingend. Der prüfungsrechtliche „Grundsatz der Anonymität“, gilt, wenn die Prüfungsordnung dies vorsieht oder eine ständige Übung dieser Art besteht.[29] Eine rechtliche Verpflichtung, das Prüfungsverfahren durchgängig pseudonym zu gestalten, existiert derzeit nicht.[30] Ohne explizite Regelung liegt es daher im pflichtgemäßen Ermessen des Verantwortlichen für das Prüfungsverfahren, ein pseudonymisiertes Prüfungsverfahren vorzusehen, so dass jede sachlich vertretbare Lösung statthaft ist.[31]

Die Anwendung der oben dargestellten datenschutzrechtlichen Prinzipien haben jedoch direkte Auswirkungen auf die Gestaltung von Prüfungsverfahren. Räumt das Prüfungsrecht dem Prüfungsamt ein Ermessen ein, darüber zu entscheiden, dass Prüfungsverfahren pseudonym zu gestalten, bestimmt das Datenschutzrecht, den Datenverarbeitungsprozess „Prüfungsverfahren“ insbesondere nach den Grundsätzen des Art. 5 DS-GVO auszugestalten. Vor allem der Grundsatz der Datenminimierung des Art. 5 Abs. 1 lit. c DS-GVO fordert im Ergebnis, dass Daten, die für den verfolgten Zweck unerheblich sind, nicht verarbeitet werden dürfen.[32] Die Bearbeitung und Bewertung einer schriftlichen Arbeit ist auch dann möglich, wenn der Prüfer den Prüfling nicht namentlich kennt. Weiter ist es auch nicht notwendig, dass der Prüfer den Prüfling namentlich zuordnen kann. Mit der Pseudonymisierung von schriftlichen Prüfungsarbeiten steht den Prüfungseinrichtungen eine alternative Methode zur Verfügung, die es ermöglicht, den angestrebten Zweck auch bei Verarbeitung weniger personenbezogener Daten zu erreichen. Diese datenschutzrechtlichen Vorgaben müssen Einfluss auf das Ermessen der Prüfungsbehörde haben, ob das Prüfungsverfahren pseudonymisiert ausgestaltet wird oder nicht. Ein pseudonymisiertes Prüfungsverfahren fördert auch die Objektivität der Prüfer und sorgt im Ergebnis für die Steigerung der Chancengleichheit zwischen den Prüflingen. Diese Synergie zwischen Prüfungs- und Datenschutzrecht kann auch über mehrere Prüfungszyklen aufrechterhalten bleiben, wenn beispielsweise im Sinne einer Best-Practice-Lösung Prüfnummern von Prüfungszyklus zu Prüfungszyklus geändert werden. Prüfungsverfahren an Hochschulen dürften auch schon dann die von Art. 5 Abs. 1 lit. c DS-GVO gesteckten Maßstäbe erfüllen, wenn als Pseudonym auf den schriftlichen Arbeiten die Matrikelnummer der Prüflinge verwendet wird. So kann auf Seiten der Prüfungsbehörde der Aufwand der Gestaltung eines datenschutzkonformen Prüfungsverfahrens gering gehalten werden, denn die Matrikelnummer bekommt der Prüfling bereits mit Einschreibung in den jeweiligen Studiengang zugeteilt. Die Neuanlegung eines Kennziffernsystems ist damit nicht notwendig, im Sinne der aufgezeigten Best-Practice-Lösung aus datenschutzrechtlicher Sicht aber wünschenswert.

V. Einsicht in Prüfungsarbeiten

Die DS-GVO legt in Kapitel III umfassende Betroffenenrechte fest, die mit entsprechenden Pflichten der Verantwortlichen in Prüfungseinrichtungen korrespondieren.

Relevant für Prüfungsverfahren ist insbesondere Art. 15 DS-GVO, wonach der betroffenen Person das Recht zusteht, in angemessenen Zeitabständen insbesondere Auskunft darüber zu verlangen, ob und welche personenbezogenen Daten verarbeitet werden. Bei den Antworten der Prüflinge in schriftlichen Arbeiten handelt es sich um personenbezogene Daten. Diese werden zwar in der Regel nicht automatisiert verarbeitet, die Prüfungsunterlagen werden aber in strukturierten, wenn auch analogen, Akten aufbewahrt. Somit liegt eine Speicherung in einem Dateisystem i. S. d. Art. 2 Abs. 1 DS-GVO vor.[33] Sie sind damit grundsätzlich vom Auskunftsanspruch des Art. 15 DS-GVO erfasst.

In vielen gesetzlichen Regelungen zu Prüfungsverfahren finden sich spezifische Vorgaben zur Einsicht in Prüfungsunterlagen.[34] Diese Regelungen kollidieren mit dem Auskunftsanspruch nach der DS-GVO. Wie dargestellt handelt es sich bei den Antworten der Prüflinge in schriftlichen Arbeiten um personenbezogene Daten.

27 Jaspers/Schwartmann/Hermann, in: HK-DS-GVO/BDSG, Art. 5, Rn. 46.

28 Jaspers/Schwartmann/Hermann, in: HK-DS-GVO/BDSG, Art. 5, Rn. 46.

29 Niehues/Fischer/Jeremias, Prüfungsrecht, Rn. 324.

30 Vgl. BVerwG Beschl. v. 14.03.1979 – 7 B 16.79, DÖV 1979, 752; Beschl. v. 25.05.1999 – 6 B 65.98, NVwZ-RR 1999, 745; Niehues/Fischer/Jeremias, Prüfungsrecht, Rn. 324.

31 Vgl. Niehues/Fischer/Jeremias, Prüfungsrecht, Rn. 324.

32 Vgl. Jaspers/Schwartmann/Hermann, in: HK-DS-GVO/BDSG, Art. 5, Rn. 46.

33 Vgl. Pabst, in: HK-DS-GVO/BDSG, Art. 2, Rn. 30.

34 Bsp. § 23 Abs. 2 JAG NRW.

Inhaltlich sehen die einschlägigen prüfungsrechtlichen Regelungen oftmals Verfahren zur Einsicht in die Prüfungsarbeiten vor, die nicht deckungsgleich mit dem Umfang des Auskunftsanspruchs nach Art. 15 DS-GVO sind. Insbesondere wird von den Fristenregelungen des Art. 12 Abs. 3 DS-GVO und von der Verpflichtung zur Herausgabe einer Kopie der Daten abgewichen. Oftmals wird in den Regelungen auch bestimmt, wann und wo die Einsicht in die Prüfungsunterlagen zu erfolgen hat.

Auch unter der Geltung der DS-GVO werden die bereichsspezifischen Regelungen nicht gegenstandslos, denn Art. 23 DS-GVO enthält eine Öffnungsklausel, die den nationalen Gesetzgeber dazu ermächtigt, unter bestimmten Voraussetzungen die Betroffenenrechte der DS-GVO zu beschränken. Grundgedanke des Art. 23 DS-GVO ist es, für bestimmte Fälle Rechte von Betroffenen, die sich aus der DS-GVO ergeben, beschränken zu können oder bestehende Beschränkungen aufrecht zu erhalten. Art. 23 Abs. 1 DS-GVO fordert kein formelles Gesetz. Auch in Verordnungen und Satzungen können Einschränkungen geregelt werden.[35]

Art. 23 Abs. 1 DS-GVO regelt die Tatbestände, die eine Beschränkung von Betroffenenrechten ermöglichen. Für die genannten Regelungen zur Einsicht in Prüfungsunterlagen kommt Art. 23 Abs. 1 lit. e DS-GVO in Betracht. Danach sollen Beschränkungen zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedsstaates, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit zulässig sein. Die konkret benannten Interessen haben dabei lediglich den Charakter von Regelbeispielen.[36] In der Konsequenz können also auch weitere, in Art. 23 Abs. 1 lit. e DS-GVO nicht aufgeführte Interessen benannt werden.[37]

Für Prüfungseinrichtungen ist es elementar, dass die Einsicht in die Prüfungsunterlagen strukturiert erfolgt. Dies wird bereits dadurch deutlich, dass an Prüfungsverfahren oftmals eine Vielzahl von Prüflingen teilnimmt. Die Prüflinge erstellen umfangreiche Lösungen in Form von mehreren beschriebenen Seiten, deren Struktur durch wiederkehrende Auskunftsansprüche nicht verloren gehen darf. Daneben darf das Funktionieren der öffentlichen Prüfungseinrichtungen nicht dadurch erschwert werden, dass unkoordiniert Einsichten in Prüfungsunterlagen zu erfolgen haben. Diese organisatorischen Herausforderungen würden die öffentliche Aufgabe der Prüfungseinrichtungen, insbesondere das Durchführen von Prüfungsverfahren, erheblich gefährden. Es liegt somit auch im berechtigten Interesse der Prüflinge, dass hier Regelungen getroffen werden, die der Erfüllung der Aufgaben der Prüfungseinrichtungen förderlich sind.

Art. 23 Abs. 2 DS-GVO formuliert inhaltliche Mindestanforderungen an gesetzliche Vorschriften im Sinne des Abs. 1, wobei diese, aufgrund des Begriffs „gegebenenfalls“, nur dann zu berücksichtigen sind, wenn es im konkreten Fall einer solchen Angabe bedarf.[38] Um die inhaltlichen Mindestanforderungen des Art. 23 Abs. 2 DS-GVO zu erfüllen, muss die beschränkende Rechtsvorschrift zunächst erkennen lassen, zu welchem Zweck Daten verarbeitet werden.[39] Zusätzlich ergibt sich aus Art. 23 Abs. 2 DS-GVO, dass der Umfang der Beschränkung zu skizzieren ist und kompensatorische Verfahrensgarantien und Schutzvorkehrungen nach Art. 23 Abs. 2 lit. d, f, g und h DS-GVO enthalten sein müssen.

Als Anwendungsfall des Art. 23 DS-GVO kommt § 23 Abs. 2 JAG-NRW in Betracht. Dieser regelt die Einsichtsmöglichkeit des Prüflings in seine Prüfungsarbeiten. Die Norm lässt erkennen, dass die Daten zum Zwecke der Durchführung des Prüfungsverfahrens verarbeitet werden. Dies ergibt sich insbesondere daraus, dass die Einsicht auch die Gutachten der Prüfer umfasst. Ohne diese Begutachtung kann der Zweck der Verarbeitung, die Durchführung des Prüfungsverfahrens mit der Leistungsbeurteilung als elementarem Bestandteil, nicht erfolgen. Mit den Prüfungsunterlagen werden auch die Kategorien der personenbezogenen Daten grundsätzlich in der Norm bezeichnet. Der Umfang der vorgenommenen Beschränkung wird dadurch deutlich, dass die Norm genau bezeichnet, welche Daten eingesehen werden können (§ 23 Abs. 2 S. 1 JAG-NRW), wo die Einsicht zu erfolgen hat (§ 23 Abs. 2 S. 2 JAG-NRW) und welche zeitliche Beschränkung, nämlich binnen eines Monats nach Bekanntgabe der Prüfungsentscheidung, für die Stellung des Antrags auf Einsichtnahme gilt (§ 23 Abs. 2 S. 3 JAG-NRW).

Diese Grundsätze lassen sich auf vergleichbare Regelungen in anderen Prüfungsordnungen übertragen, die die Einsichtnahme in Prüfungsunterlagen regeln. Treffen die maßgeblichen Prüfungsordnungen keine Regelungen zu Akteneinsicht, kann sich der Anspruch auf Akteneinsicht aus § 29 VwVfG bzw. entsprechender Vorschriften der Verwaltungsverfahrensgesetze der Länder ergeben. Nach den oben aufgezeigten Grundsätzen sind auch diese Regelungen als von Art. 23 DS-GVO getragene Abweichungen von Art. 15 DS-GVO zu qualifizieren. Den Prüflingen wird die Akteneinsicht, und damit die Auskunft, nicht per se verwehrt. Es finden lediglich Modifizierungen bezüglich des Verfahrensablaufs zur Einsichtnahme statt.

VI. Fazit

Bei der Durchführung von Prüfungsverfahren werden eine Vielzahl von personenbezogenen Daten der an dem Verfahren Beteiligten verarbeitet. Insbesondere die Antworten der Prüflinge sind personenbezogene Daten. Von den Privilegierungen zu wissenschaftlichen Forschungszwecken ist die Durchführung von Prüfungen, auch an Hochschulen, nicht erfasst. Für die Bestimmung des Verant wortlichen von Prüfungsverfahren im öffentlichen Bereich

35 Stender-Vorwachs, in: BeckOK Datenschutzrecht, Art. 23, Rn. 10.

36 Bäcker, in: Kühling/Buchner, DS-GVO, Art. 23, Rn. 22.

37 Vgl. Pabst, in: HK-DS-GVO/BDSG, Art. 23, Rn. 38.

38 Vgl. Paal, in: Paal/Pauly, DS-GVO, Art. 23, Rn. 44.

39 Vgl. Pabst, in: HK-DS-GVO/BDSG, Art. 23, Rn. 65.

ist der Begriff der Behörde prägend. Unter Beachtung der jeweiligen Entscheidungsstrukturen in einer Prüfungseinrichtung, ist der für die Datenverarbeitung Verantwortliche im Einzelfall zu identifizieren. Bei der Erstellung von Klausuren ist der Grundsatz der Datenminimierung zu beachten. Dieser hat Auswirkungen auf das Ermessen der Prüfungsbehörde, das Prüfungsverfahren pseudonym auszugestalten. Bestehende Regelungen zur Klausureinsicht gelten auch unter der DS-GVO weiter, sofern sie kompensatorische Maßnahmen vorsehen. Wird die Akteneinsicht nicht per se verwehrt, sondern finden lediglich Modifizierungen des Verfahrensablaufs statt, sind die vom Auskunftsanspruch des Art. 15 DS-GVO abweichenden Regelungen als von Art. 23 DS-GVO getragene Ausnahmen zu qualifizieren.

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

Foto: Thilo Schmülgen/TH Köln

Barbara Thiel

Querschnittsprüfung der LfD Niedersachsen zur Umsetzung der DS-GVO in Unternehmen

Schon vor ihrem Geltungsbeginn am 25. Mai 2018 sah sich die Datenschutz-Grundverordnung (DS-GVO) scharfer Kritik ausgesetzt – auch und vor allem aus Kreisen der Wirtschaft. Die DS-GVO, so die Vorwürfe, würden den Aufwand für Datenschutz unverhältnismäßig in die Höhe schrauben. Tatsächlich verlangt die Verordnung unter anderem von Wirtschaftsunternehmen, sich an einige Neuerungen anzupassen. So gilt es etwa, die Informations- und Dokumentationspflichten zu erfüllen, ein Verzeichnis von Verarbeitungstätigkeiten zu führen, bestehende Rechtsgrundlagen für die Verarbeitung personenbezogener Daten und Verträge mit Auftragsverarbeitern zu prüfen und ggf. anzupassen sowie insgesamt interne Prozesse zu hinterfragen bzw. zu ändern.

Auch für die Aufsichtsbehörden sieht die DS-GVO neue Aufgaben und damit einhergehend eine veränderte Rolle vor. Neben einer modifizierten Beratungs- und Unterstützungsfunktion gesteht die Verordnung den Datenschutzbehörden auch umfangreiche Aufsichtsbefugnisse und weit reichende Sanktionsmöglichkeiten zu. Deshalb fragten sich zum Geltungsbeginn viele Verantwortliche, wie die Aufsichtsbehörden nun unter den neuen Voraussetzungen agieren würden. Die Frage stand im Raum, ob die Behörden sofort umfassende Prüfungen durchführen und darauf drakonische „Strafen" in Millionenhöhe folgen lassen würden.

Nicht diese Befürchtungen, sondern der Wunsch, sich möglichst frühzeitig einen Überblick über den Stand der Umsetzung in Niedersachsen zu verschaffen, veranlasste die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen, nur einen Monat nach Geltung der DS-GVO eine branchenübergreifende Prüfung einzuleiten, die als solche die bislang größte Prüfung in der Geschichte der Behörde darstellt.

Um das mit dieser Prüfung verbundene Arbeitsvolumen bewältigen zu können, wurde die Prüfung in Form eines Projekts angelegt. Vorteil dieser Arbeitsform ist es, dass die Projektgruppenmitglieder losgelöst von den üblichen Strukturen überwiegend eigenverantwortlich die gestellten Aufgaben bewältigen und notwendige Entscheidungen nicht auf dem Dienstweg, sondern von einer dafür eingesetzten Lenkungsgruppe gemeinsam getroffen und dadurch auf eine breitere Basis gestellt werden. Durch die Bildung eines referatsübergreifenden Projektteams konnte zudem die Expertise verschiedener Fachreferate zusammengeführt und für die Prüfung optimal genutzt werden.

Die Ausgangslage für diese Prüfung war dabei wenig vielversprechend: In einer repräsentativen Befragung des Branchenverbandes Bitkom unter mehr als 500 Unternehmen aus Deutschland hatte noch im Mai 2018 nur ein Viertel der Befragten angegeben, die Vorgaben der DS-GVO bis zum Stichtag umsetzen zu können – und das trotz zweijähriger Übergangsfrist. Nun galt es also herauszufinden, was das für Niedersachsen bedeutete.

I. Aufklärung vor Sanktion

Im Rahmen dieser Prüfung waren insgesamt 50 Unternehmen unterschiedlicher Größe aufgefordert, eine Vielzahl von Fragen zu zehn Bereichen des Datenschutzes zu beantworten. Im Vordergrund stand und steht dabei nicht der Kontrollaspekt. Es geht im Ansatz nicht darum, möglichst viele Fehler zu finden und Bußgelder zu verhängen. Erklärtes Ziel

dieser Prüfung ist es vielmehr, eine Bestandsaufnahme durchzuführen, die Antwort geben soll auf die Frage: Wie gut haben die niedersächsischen Unternehmen die neuen Anforderungen umgesetzt, welche die DS-GVO mit sich bringt? Und in welchen Bereichen sind nach wie vor Handlungsbedarfe vorhanden, die es aufzuarbeiten gilt?

Das Hauptanliegen der LfD Niedersachsen war und ist es also, zu identifizieren, ob und wo es bei den verantwortlichen Stellen noch Nachholbedarf gibt. Im Interesse von Aufklärung und Sensibilisierung – eine der neuen in der DS-GVO verankerten Aufgaben der Aufsichtsbehörden – soll zudem mit der Prüfung das Bewusstsein für den Datenschutz im Allgemeinen und die Vorschriften der DS-GVO im Speziellen gestärkt werden. Fest steht allerdings auch: Sofern während der Prüfung gravierende Verstöße gegen die DS-GVO festgestellt werden, sind auch weitergehende Maßnahmen bis hin zu der Verhängung eines Bußgeldes möglich.

II. Fragen auf Basis der KMU-Checkliste

Der für die Querschnittsprüfung entwickelte Fragebogen[1] beruht auf der „Checkliste für die Umstellung kleinerer Unternehmen auf die Datenschutzgrundverordnung“, welche die LfD Niedersachsen im November 2017 veröffentlicht hatte. Mit dieser Liste hatte die LfD Niedersachsen den Unternehmen sechs Monate vor dem 25. Mai 2018 eine Hilfestellung zur Vorbereitung auf die DS-GVO gegeben. Sie sollte die Unternehmen in die Lage versetzen, Bereiche zu identifizieren, in denen sie bereits gut aufgestellt waren und wo es noch Handlungs- bzw. Optimierungsbedarf gab. Bereits zu diesem Zeitpunkt hatte die LfD Niedersachsen immer wieder öffentlich – zum Beispiel in vielen Vorträgen auf Veranstaltungen der Industrie- und Handelskammern – , darauf hingewiesen, dass die Inhalte dieser Checkliste zum Gegenstand zukünftiger Prüfungen gemacht würden.

Mit den zehn Fragenkomplexen der Querschnittsprüfung werden die nach Ansicht der LfD Niedersachsen für Verantwortliche wesentlichen Bereiche der DS-GVO angesprochen. Sie befassen sich mit dem Verzeichnis von Verarbeitungstätigkeiten und den Rechtsgrundlagen für die Datenverarbeitung, mit der Einhaltung der Betroffenenrechte, mit dem technischen Datenschutz, der Datenschutz-Folgenabschätzung, der Auftragsverarbeitung, der Bestellpflicht für Datenschutzbeauftragte, den Meldepflichten und last but not least der Einhaltung der Rechenschaftspflicht. Zudem sollen die Unternehmen generell darstellen, wie sie sich auf die DS-GVO vorbereitet haben, welche Unternehmensbereiche involviert waren und welche Maßnahmen initiiert wurden.

III. Unternehmensauswahl

Auch wenn der Fragebogen auf einer Checkliste für kleine und mittelständische Unternehmen beruht, sollten kleine und mittlere Betriebe gerade nicht Teil der Querschnittsprüfung sein. Vielmehr gingen die Fragen an 20 große und 30 mittelgroße Unternehmen aus verschiedenen Branchen, die ihren Sitz in Niedersachsen haben und bei denen davon ausgegangen werden konnte, dass sie schon nach altem Datenschutzrecht entsprechend aufgestellt waren und damit besser und zügiger auf die neuen Vorgaben reagieren konnten.

Bei der konkreten Auswahl der Unternehmen spielten verschiedene Aspekte eine Rolle:

- So sollten nicht allein Firmen der Region Hannover geprüft werden, sondern Unternehmen aus ganz Niedersachsen – von der Küste bis Göttingen, von Osnabrück bis Helmstedt.
- Darüber hinaus sollte die Auswahl auch Unternehmen beinhalten, die nicht nur die Daten ihrer Mitarbeiterinnen und Mitarbeiter verarbeiten, sondern vor allem auch die Daten ihrer Kundinnen und Kunden. Bei letzteren sollte es sich zudem möglichst nicht nur um Geschäftskunden, sondern verstärkt auch um solche aus dem Consumer-Bereich handeln.
- Ferner sollten viele verschiedene Branchen abgedeckt werden – von Versicherungen über den Finanzbereich und den Handel bis hin zu Wirtschafts- und Steuerberatern. Von Versorgungsunternehmen und Personaldienstleistungen über Wach- und Schließgesellschaften bis hin zur Touristikbranche.
- Um eine übermäßige Belastung einzelner Unternehmen zu vermeiden, sollten diese außerdem nicht in der jüngsten Vergangenheit „Teilnehmer“ anderer Schwerpunktprüfungen der LfD Niedersachsen gewesen sein.
- Schließlich sollten die Firmen eine Größe haben, die zur Bestellung eines Datenschutzbeauftragten verpflichtet. Der kleine Handwerksbetrieb oder Einzelhändler sollte nicht betroffen sein.

Innerhalb einer Frist von sechs Wochen sollten die ausgewählten Unternehmen die Fragen schriftlich beantworten. Auf Antrag konnte diese Frist verlängert werden, was von einigen Unternehmen in Anspruch genommen wurde. Beantwortet wurde der Fragebogen letztlich von allen angeschriebenen Unternehmen.

IV. Abfrage der Unternehmensprozesse

Besonderer Wert wird in dieser Prüfung auf die Darstellung der Prozesse in den betroffenen Unternehmen („Wie stellen Sie sicher, dass…?“) gelegt. Da sie, die Prozesse, die grundsätzliche Vorgehensweise und Methodik wiederspiegeln, geben gerade sie grundlegend Aufschluss darüber, wie gut ein Verantwortlicher in der Lage ist, die Anforderungen der DS-GVO zu erfüllen.

Die Fragen wurden bewusst offen gestellt, um den Unternehmen die Möglichkeit zu eröffnen, ihre Antworten auf ihre konkrete Situation und Größe anzupassen. Gleichzeitig lässt diese Vorgehensweise Hinweise darauf zu, wie weit die einzelnen Anforderungen der DS-GVO bei den Unternehmen bereits erkannt und prozessual umgesetzt wurden. Denn nur durch die Verankerung der datenschutzrechtlichen Anforderungen in konkrete Unternehmensprozesse kann gewährleis-

1 Der Fragebogen kann auf der Webseite der LfD Niedersachsen abgerufen werden: https://www.lfd.niedersachsen.de/download/132359.

tet werden, dass die Anforderungen nicht nur im Einzelfall, sondern kontinuierlich und dauerhaft erfüllt werden. Viele Firmen haben zudem bereits ein Qualitätsmanagementsystem etabliert und sind vor diesem Hintergrund mit der Methodik des kontinuierlichen Verbesserungsprozesses vertraut. Neue datenschutzorientierte Prozesse können in dieses System integriert werden, was regelmäßige Evaluierungen und gegebenenfalls Anpassungen ermöglicht. Zudem erleichtert die dokumentierte prozessuale Verankerung die Erfüllung der Rechenschaftspflicht auf Seiten der Verantwortlichen.

V. Eigenverantwortliche Darstellung von Lösungswegen statt Multiple-Choice

Auf eine kleinteilige Abfrage der Erfüllung rechtlicher Vorgaben wurde bewusst verzichtet, weil andernfalls zwangsläufig auch ein Teil des Lösungsweges vorgezeichnet worden wäre. Das eigene (Mit-) Denken hätte nicht mehr in dem Maße im Vordergrund gestanden, wie es bei offenen Fragen der Fall ist. Denn: Bei einer Vielzahl von kleinteiligen Fragen ist es für den Fragenden anhand der Antworten nicht mehr erkennbar, ob der Befragte auch ohne die konkreten Fragen an diese Details gedacht hätte. Mit dem von der LfD Niedersachsen gewählten Ansatz müssen die Befragten ihren Lösungsweg vielmehr eigenverantwortlich darstellen und gleichzeitig dokumentieren, dass sie sich mit der Thematik in ihrem Unternehmen auseinander gesetzt, die rechtlichen Anforderungen auf ihre konkrete Situation übertragen sowie die erforderlichen Prozesse entwickelt und implementiert haben.

Für die Befragten ist dieser Weg der Fragestellung durchaus mit Herausforderungen verbunden – besonders im Vergleich zu einem Multiple-Choice Fragebogen. Doch die stärkere Aussagekraft der Antworten rechtfertigt den Aufwand, der den Unternehmen zugemutet wird. Die Antworten lassen Rückschlüsse darauf zu, in welchen Unternehmen das Thema DS-GVO wirklich angekommen ist. Wo wird der Datenschutz schon gelebt, wo ist er zur Chefsache geworden und wo ist er eher noch eine Randerscheinung, die man zwar zur Kenntnis genommen aber noch nicht wirklich ins Unternehmen hineingetragen hat?

VI. Detaillierter Kriterienkatalog zur Auswertung

Die mit der Art der Fragestellung verbundene besondere Herausforderung gilt jedoch nicht nur für die Befragten, sondern ebenso für die Mitarbeiterinnen und Mitarbeiter der LfD Niedersachsen. Denn die Auswertung einer solchen Prüfung mit einer Vielzahl offener Fragen ist weitaus (zeit-) aufwändiger, als die eines Multiple-Choice Fragebogens. Teilweise wurden mehrere hundert Seiten Unterlagen von den Unternehmen eingereicht.

Um hierbei den Überblick zu behalten und eine einheitliche Bewertung der Antworten zu gewährleisten, wurde zu den zehn Themenkomplexen ein detaillierter Katalog bestehend aus circa 200 Einzelkriterien erarbeitet. Die Kriterien basieren dabei auf den rechtlichen Anforderungen der DS-GVO. Mit dem Katalog ist neben der Gewährleistung einer konsistenten Bewertung auch eine (weitere) Hilfestellung bezweckt. Denn anhand der Kriterien soll verdeutlicht werden, was ein Verantwortlicher alles zu beachten hat, um datenschutzkonform aufgestellt zu sein. Daher wird der Kriterienkatalog am Ende der Querschnittsprüfung veröffentlicht und so allen (niedersächsischen) Unternehmen zugänglich gemacht werden.

VII. Fokus auf methodischem Vorgehen

In Hinblick auf das Ziel der Querschnittsprüfung, einen Überblick über den Umsetzungstand der DS-GVO in den Unternehmen zu erhalten, wurde bei den Kriterien der Fokus teilweise ausschließlich auf das methodische Vorgehen gelegt und keine inhaltliche Auswertung vorgenommen. Dies ist insbesondere bei den Datenschutz-Folgenabschätzungen der Fall. Das heißt, für diese wird „nur“ bewertet, ob die dazu eingereichten Unterlagen zumindest die Inhalte nach Art. 35 Abs. 7 DS-GVO enthalten. So wird zum Beispiel geprüft, ob eine Einstufung der Schwere eines Risikos stattfindet und diese begründet wird. Es wird dagegen nicht geprüft, ob die konkrete Einstufung von Seiten der Aufsichtsbehörde für richtig gehalten wird. Denn eine detaillierte inhaltliche Prüfung würde den für die Querschnittsprüfung kalkulierten zeitlichen Prüfungsrahmen bei knapp 200 vorgelegten Datenschutz-Folgenabschätzungen schlichtweg sprengen.

VIII. Ampelfarbe pro Fragenkomplex

Zu jedem Kriterium sind drei Bewertungen dazu möglich, ob ein Kriterium erfüllt ist: ja, nein oder teilweise. Alle Einzelkriterien, die es zu einer Frage der zehn Komplexe gibt, werden anschließend zu einer Gesamtbewertung pro Fragenkomplex zusammengefasst und einer Ampelfarbe (rot/gelb/grün) zugeordnet.

Mit „Grün“ werden die Komplexe bewertet, die inhaltlich weitestgehend zufriedenstellend beantwortet wurden, mit nur geringen Abweichungen bei der Bewertung der Einzelkriterien. Bei „Grün“ sieht die LfD Niedersachsen keinen konkreten Handlungsbedarf auf Seiten der Unternehmen zu diesem Bereich. Mit „Gelb“ werden die Fragenkomplexe eingestuft, bei denen es noch Handlungsbedarf gibt. Solche Handlungsbedarfe sind dann festzustellen, wenn die Einzelkriterien häufiger mit „teilweise“ oder zum Teil auch mit „nein“ bewertet werden mussten. Auf „Rot“ stehen schließlich die Komplexe, bei denen die Antworten auf erheblichen Handlungsbedarf schließen lassen. Hier wurden die Einzelkriterien überwiegend mit „teilweise“ und „nein“ bewertet.

Der LfD Niedersachsen ist durchaus bewusst, dass die Nichterfüllung von Kriterien zum Teil auch daraus resultieren kann, dass das eine oder andere Unternehmen den Erwartungshorizont der Aufsichtsbehörde hinsichtlich der Detailtiefe der Ausführungen nicht richtig eingeschätzt hat. Hier ist jedes der geprüften Unternehmen im Nachgang ge-

fordert, den jeweiligen individuellen Anpassungsbedarf auf Basis der mitgeteilten Prüfungsergebnisse zu erkennen und bei Bedarf die Unternehmensprozesse anzupassen.

Die eingereichten Unterlagen werden zudem nur in dem für die Prüfung des Kriterienkataloges erforderlichen Rahmen gesichtet und ausgewertet, nicht darüber hinaus. Somit steht am Ende der Querschnittsprüfung eine konkrete Aussage darüber, inwieweit die Unternehmen die bewerteten Kriterien erfüllt haben. Es kann jedoch keine Aussage darüber getroffen werden, inwieweit die von den Unternehmen eingereichten Unterlagen insgesamt inhaltlich datenschutzkonform ausgestaltet waren.

IX. Transparente Kommunikation der Ergebnisse

Den geprüften Unternehmen, denen die Ampelfarbe „grün" oder „gelb" zugeordnet worden ist und bei denen demzufolge insgesamt – über alle Fragen hinweg – kein Handlungsbedarf oder nur in wenigen Fällen ein solcher gesehen wird, wird voraussichtlich bis Ende März ihr jeweiliges Prüfungsergebnis pro Fragenkomplex schriftlich mitgeteilt werden. Mit der Mitteilung des schriftlichen Prüfungsergebnisses wird für diese Unternehmen die Querschnittsprüfung beendet sein.

In diesem Zusammenhang wird vor allem darauf einzugehen sein, welche Fragen das Unternehmen aus Sicht der LfD zufriedenstellend beantwortet hat und wo noch Handlungsbedarf gesehen wird. Zudem wird jedem Unternehmen auch der detaillierte Kriterienkatalog mit der unternehmensspezifischen Bewertung jedes einzelnen Kriteriums zur Verfügung gestellt. Die geprüften Firmen haben auf diese Weise die Möglichkeit, nachzuvollziehen, welchen Maßstab die LfD Niedersachsen an die Antworten angelegt hat und wie sie zur (Gesamt-) Bewertung der einzelnen Prüfungsfragen gekommen ist.

Mit dieser Darstellung schafft die LfD Niedersachsen Transparenz und wird zugleich dem in der DS-GVO verankerten Auftrag der Aufklärung, Information und Sensibilisierung gerecht. Die Unternehmen erhalten konkrete, nachvollziehbare Hinweise, in welchen Bereichen die Antworten noch Verbesserungspotenzial erkennen lassen. Zugleich sollen die Unternehmen dadurch motiviert werden, dieses Verbesserungspotenzial auch tatsächlich zu nutzen, um dadurch letztlich einen verbesserten Datenschutz für die Betroffenen zu gewährleisten.

X. Vor-Ort-Termine

In gleicher Weise werden auch die Unternehmen, bei denen zum Teil oder auch verbreitet erhebliche Handlungsbedarfe erkannt wurden, über das Ergebnis der Prüfung informiert. Allerdings wird es sich bei dieser Mitteilung zunächst nur um ein Zwischenergebnis handeln können. Es wird vielmehr erforderlich sein, die Unternehmen dazu aufzufordern, zu den Feststellungen der Aufsichtsbehörde Stellung zu nehmen. Erst auf dieser Basis wird es möglich sein, zu einer vertieften Beurteilung der Sachlage durch die Aufsichtsbehörde zu kommen. Soweit dies anhand der schriftlichen Unterlagen nicht möglich sein sollte, werden zudem weitergehende Kontrollmaßnahmen im Rahmen von Vor-Ort-Terminen zu veranlassen sein.

Diese Termine sollen primär dazu dienen, die durch die Aufsichtsbehörde gewonnenen Erkenntnisse in einem persönlichen Gespräch zu erläutern und gemeinsam mit den Unternehmen insbesondere die Bereiche, in denen erheblicher Handlungsbedarf gesehen wird, vertieft zu erörtern. Es bleibt abzuwarten, in welcher Weise die Unternehmen auf diese aufsichtsbehördlichen Aktivitäten reagieren und ob und inwieweit sie bereit sind, etwaige datenschutzrechtliche Verstöße abzustellen. Nicht auszuschließen ist, dass es in Einzelfällen auch zur Verhängung eines Bußgeldes kommen kann. Dabei wird u.a. zu berücksichtigen sein, wie schwerwiegend der jeweilige Verstoß ist und wie das Unternehmen damit umgegangen ist.

Voraussichtlich im Mai 2019 wird die LfD der Öffentlichkeit einen Abschlussbericht über die Prüfung vorlegen.

XI. Fazit

Die Querschnittsprüfung der LfD Niedersachsen kam für manche Unternehmen sicherlich überraschend und vielleicht auch überraschend früh – war die Datenschutz-Grundverordnung doch erst wenige Wochen anzuwenden. Doch der Zeitpunkt war genau richtig: Um Themen zu identifizieren, bei denen auf Unternehmensseite noch Unsicherheit herrscht, um zu erkennen, wo von Seiten der LfD verstärkt Beratung angeboten werden sollte, und schließlich, um die Unternehmen wachzurütteln und für die neuen Anforderungen zu sensibilisieren. Jetzt heißt es, die Prüfung abzuschließen und mit den Erkenntnissen weiter zu arbeiten. Die Ergebnisse – das zeigt sich schon jetzt – sind spannend und wie erwartet aufschlussreich.

Nicht zuletzt erhofft sich die LfD durch die Prüfung auch Hinweise für ihre eigene Arbeit. So könnten sich zum Beispiel Schwerpunktprüfungen in bestimmten Branchen anschließen. Zudem ist es denkbar, dass für Bereiche mit besonders hohem Beratungs- und Aufklärungsbedarf neue Orientierungshilfen und Handlungsempfehlungen erarbeitet werden (müssen).

Barbara Thiel

Barbara Thiel wurde am 18. Dezember 2014 vom Niedersächsischen Landtag zur Landesbeauftragten für den Datenschutz nach Artikel 62 der Niedersächsischen Verfassung gewählt und nach der Wahl von der Landesregierung mit Wirkung vom 1. Januar 2015 für die Dauer von acht Jahren berufen.

Barbara Thiel wuchs in Salzgitter auf. Sie studierte u.a. Rechtswissenschaften an der Georg-August-Universität Göttingen und legte dort ihr Erstes Juristisches Staatsexamen ab. Nach ihrem Referendariat und Zweitem Juristischen Staatsexamen in Niedersachsen war sie unter anderem im Niedersächsischen Innenministerium, beim Niedersächsischen Landesrechnungshof sowie beim Landkreis Wolfenbüttel tätig. Zuletzt war Thiel Dezernentin bei der Region Hannover.

GDD-FORUM

Fortbildungsveranstaltung gem. Art. 38 DS-GVO/ §§ 5, 6, 38 BDSG

Ein Jahr DS-GVO

Erfahrungen und Lösungen im Umgang mit dem neuen Datenschutzrecht

Ein Jahr nach Geltung der DS-GVO und dem zeitgleichen Inkrafttreten des BDSG gibt es weiterhin viele offene Fragen, wie das neue Datenschutzrecht umzusetzen ist. Diese Fragen betreffen die Zulässigkeit der Datenverarbeitung, die Organisation der Betroffenenrechte bis hin zur technischen Umsetzung der Löschpflichten.

Weiterhin ist von Interesse, wie die Aufsichtsbehörden die Neuregelungen bewerten, welche Umsetzungsmaßnahmen erwartet und welche Anforderungen an die Rechenschaftspflicht gestellt werden. Auch die Kriterien an die Verhängung der ersten Bußgelder sind richtungsweisend.

Das GDD-Forum „Ein Jahr DS-GVO" beleuchtet diese und weitere Praxisfragen des neuen Datenschutzrechts. Es bietet die Möglichkeit, direkt mit Experten und Vertretern der Datenschutzaufsicht Fachfragen zu erörtern.

27.05.2019 in KÖLN

10.00–17.00 Uhr

Referenten

Dr. Tobias Jacquemain, LL.M.

RA Andreas Jaspers

Ulrich Kelber

Gabriela Krader

Thomas Kranig

RA Thomas Müthlein

Maria Christina Rost

Prof. Dr. Rolf Schwartmann

Sichern Sie sich Ihren fachlichen Vorsprung!

DATAKONTEXT

Jetzt informieren und anmelden unter www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

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

Kurzbeiträge

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (40): Offene Fragen bei der Beschäftigtendatenverarbeitung: Gehaltsabrechnung durch Steuerberater und Verarbeitungen beim Betriebsrat

Ausgewählt und kommentiert von Prof. Peter Gola*

Der am 4.2.2019 von dem LfDI Baden-Württemberg vorgelegte 34. Tätigkeitsbericht über das Jahr 2018 geht ausführlich auf zwei den Beschäftigtendatenschutz betreffende Streitfragen ein. Dabei geht es zum einen um die Übertragung der Gehaltsabrechnung an einen Steuerberater als Auftragsverarbeiter und zum anderen um die Rolle des Betriebsrats als eigenverantwortliche Stelle.

I. Ausgelagerte Gehaltsabrechnung

1. Typischer Fall einer Auftragsverarbeitung

Die Aufsichtsbehörden sind sich nach wie vor einig, dass ein Outsourcing der Gehaltsabrechnung regelmäßig den Tatbestand einer Auftragsverarbeitung (Art. 4 Nr. 8 DS-GVO) erfüllt, der unter den Voraussetzungen des Art. 28 DS-GVO gestattet ist. Dies folgt daraus, dass auch nach der DS-GVO der Auftragsverarbeiter kein „Dritter" (Art. 4 Nr. 10 DS-GVO) ist, sondern ein „fiktiv interner" Empfänger (Art. 4 Nr. 9 DS-GVO); dies jedenfalls dann, wenn er weisungsgebunden zu nichts anderem befugt wird als zu dem, das der Auftraggeber auch selbst an Verarbeitungen durchführen dürfte.[1] Zwischen dem den Auftrag erteilenden Verantwortlichen und seinem Auftragsverarbeiter besteht ein „Innenverhältnis" auf Grund dessen die Verarbeitung durch den Auftragsverarbeiter grundsätzlich dem Verantwortlichen zugerechnet wird. Dem steht nicht entgegen, dass, wenn der Auftragsverarbeiter über ein umfassenderes Know-how als sein Auftraggeber verfügt, dieser ihm einen gewissen Spielraum für selbständige Entscheidungen einräumen kann.[2] Dies gilt insbesondere für die Delegation der Entscheidung über die technisch-organisatorischen Fragen der Verarbeitung.

Dieser Sachverhalt ändert zwar nichts daran, dass es sich bei der Weitergabe der Mitarbeiterdaten an den Auftragsverarbeiter stets um eine unter dem Verbot mit Erlaubnisverhalt des Art. 6 Abs. 1 DS-GVO stehenden Verarbeitungsfall der Offenlegung von personenbezogenen Daten handelt (Art. 4 Nr. 2 DS-GVO). Andererseits bleibt es dabei, dass dieser Vorgang auch unter Anwendung der DS-GVO weiterhin „privilegiert" ist,[3] wenn der Datenempfänger – wie es bei der Auslagerung der Gehaltsabrechnung regelmäßig der Fall ist – keine maßgebende Eigenkompetenz bei der Verwendung der überlassenen Daten hat und der Auftraggeber allein über Zweck der Datenverarbeitung entscheidet.

Aufgrund der in der DS-GVO getroffenen Verantwortlichkeiten von Auftraggeber und Auftragnehmer besteht nämlich weiterhin kein gesonderter Schutzbedarf der betroffenen Person bei Einschaltung eines Auftragsverarbeiters. Es bedarf keiner gesonderten Rechtsgrundlage, wenn die Nutzung der Daten unter Einhaltung der Regelungen der Verordnung zur Auftragsvergabe erfolgt.[4] Insofern kann Art. 28 DS-GVO als eigenständige Befugnisnorm verstanden werden.[5]

Vertretbar mag es auch sein, die zwischen Auftraggeber und Auftragnehmer vereinbarte Datenverarbeitung als einheitlichen Verarbeitungsvorgang (Art. 4 Nr. 2 DS-GVO) einzuordnen, für den es nur eine einheitliche Prüfung geben kann.[6]

Damit steht es auch unter Geltung der DS-GVO grundsätzlich außer Frage, dass die Auslagerung der Gehaltsabrechnung keiner speziellen Rechtfertigung bedarf, wenn sie nach in Art. 28 DS-GVO für die Auftragsverarbeitung festgelegten Bedingungen vollzogen wird.

2. Beispiele selbstständiger Dienstleistungen im Personalbereich

Keine Auftragsverarbeitung liegt dagegen vor, wenn der beauftragte Dienstleister gemäß seinem Berufsbild die Daten zwecks eigenverantwortlicher Tätigkeit erhält. Als Beispiele aus dem Bereich der Gehaltszahlung zählt das DSK-Kurzpapier auf die Einbeziehung eines Bankinstituts bei dem Gehaltstransfer, eines Postdienstes für den Transport der Gehaltsnachweise an den Mitarbeiter oder auch die Datenweitergabe bei der Einschaltung eines Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer) in Personalangelegenheiten.[7]

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

1 So u.a. Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Rn. 9, wobei aber der Hinweis, dass nur die Datenweitergabe in Form der Übermittlung dem Erlaubnisvorbehalt des Art. 6 Abs. 1 unterliege, nicht zutrifft.

2 Kurzpapier Nr. 13 – Auftragsverarbeitung der DSK- Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf.

3 Gola, in: Gola, DS-GVO Art 4 Rn.; Schmitz/v. Dall'Armi, ZD 2016, 427 (429).

4 Plath, in: Plath, DS-GVO Art. 28 Rn. 3.

5 Krohm/Müller-Peltzner, RDV 2016, 307.

6 Vgl. Plath, in: Plath, Art. 28 Rn. 3; zur Diskussion vgl. Petri, in: Simitis/Hornung/Spiecker, Art. 28 Rn. 29 ff.

3. Der Steuerberater als Gehaltsabrechner

Zwischen zumindest drei Aufsichtsbehörden wird jedoch die Frage, ob ein Steuerberater, wenn er die Gehaltsabrechnung übernimmt, Auftragsdatenverarbeiter seines Mandanten wird, unterschiedlich bewertet.[8] Einerseits wurde und wird dies vom BayLDA verneint,[9] da die freiberufliche und eigenverantwortliche Tätigkeit des Steuerberaters der Weisungsgebundenheit einer Auftragsverarbeitung auch dann entgegenstehe, wenn er nur die Lohnbuchhaltung für einen Mandanten durchführt. Da ein Steuerberater nach dem Steuerberaterrecht bei seinen Tätigkeiten weisungsungebunden und eigenverantwortlich sei, gelte das auch für den Fall der Übernahme der Gehaltsabrechnung. Er könne sich nicht, wie allgemeine Dienstleister bei der Lohnabrechnung allein auf Weisungen des Mandanten berufen.[10] Konsequenz ist dann, dass auch für den Fall der Übertragung der Gehaltsabrechnung kein gesonderter Vertrag zur Auftragsverarbeitung mit den Mandanten geschlossen werden muss;[11] jedoch aber eine die Übermittlung der Daten gestattende Erlaubnisnorm von Nöten ist, die der LfDI Baden Württemberg jedoch nicht zu erkennen vermag.

Andererseits wird aber auch für den bei der Gehaltsabrechnung eingeschalteten Steuerberater die Funktion als Auftragsverarbeiter nunmehr von der LDI NRW dann bejaht,[12] sofern – ähnlich wie bei einem Lohnbüro – von der Steuerkanzlei nur und ausschließlich die Lohnbuchhaltung des Mandanten geführt wird. Bei gemischten Tätigkeiten – eigenverantwortliche Steuerberatung sowie weisungsgebundene Dienstleistungen – sei zu differenzieren: Im Hinblick auf weisungsgebundene Dienstleistungen sei eine Auftragsverarbeitung gegeben; bei der Beauftragung mit Tätigkeiten aufgrund steuerberatungsrechtlicher Vorschriften eine Datenverarbeitung in eigener Verantwortung dagegen nicht.[13]

Dem schloss sich der LfDI Baden-Württemberg in seinem 34. Tätigkeitsbericht an (Seite 57, Ziffer 1.10):"Übernimmt ein Steuerberater neben seiner eigentlichen Steuerberatertätigkeit (Hilfe in Steuersachen) zusätzlich weitere Aufgaben, handelt es sich um Auftragsverarbeitung im Sinne des Artikels 28 DS-GVO und bedarf einer entsprechenden Vereinbarung mit dem datenschutzrechtlich verantwortlichen Auftraggeber." Dies begründet er u.a. wie folgt: „Seit dem Beschluss des Bundesverfassungsgerichts vom 27. Januar 1982 (1 BvR 807/80 –, BStBl II 1982, 281, BVerfGE 59, 302-329) steht fest, dass das Buchführungsprivileg für steuerberatende Berufe (§ 5 Absatz 1 des Steuerberatungsgesetzes) nicht für die laufende Lohnbuchhaltung gilt. Begründet wird dies damit, dass es sich bei der laufenden Lohnbuchhaltung um reine Routinearbeiten handelt, die „sich als eine nicht durch besondere rechtliche Erwägungen geprägte schematisierte Subsumtion von Lohnzahlungsvorgängen unter die amtlichen Lohnsteuertabellen und das betriebliche Lohnkonto darstellt". Folgerichtig wurde das Steuerberatungsgesetz angepasst; nach § 6 Nummer 4 des Steuerberatungsgesetzes gilt das Verbot der unbefugten Hilfeleistung in Steuersachen (u.a.) nicht für die laufende Lohnabrechnung. Für die Frage, ob der Steuerberater solche Arbeiten als Verantwortlicher im Sinne des Artikels 4 Nummer 7 DS-GVO oder als Auftragsverarbeiter im Sinne des Artikel 4 Nummer 8 DS-GVO erledigt, kommt diesem Umstand, dass es sich bei der laufenden Lohnbuchhaltung um rein mechanische Verarbeitungsvorgänge handelt, die keine besondere Qualifikation der steuerberatenden Berufe erfordert, entscheidende Bedeutung zu. Denn dies hat zur Folge, dass der für die Mitarbeiterdaten Verantwortliche die Befugnis behält, Zwecke und Mittel der Verarbeitung zu bestimmen. Dem steht auch nicht entgegen, dass der Steuerberater ansonsten, soweit er dem Steuerberaterprivileg unterfallende Arbeiten erledigt, zweifelsfrei als Verantwortlicher tätig wird. Denn es ist anerkannt, dass je nach konkreter Tätigkeit und Zusammenhang dieselbe Organisation hinsichtlich bestimmter Verarbeitungen als Verantwortlicher und hinsichtlich anderer Verarbeitungen als Auftragsverarbeiter handeln kann (Hartung, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 2. Auflage 2018, Art. 4 Nr. 8 DS-GVO Rn. 7; ebenso: Arbeitspapier Nr. 169 der Artikel-29-Datenschutzgruppe, S. 35).

Soll die Lohnbuchhaltung durch den Steuerberater nicht im Rahmen eines Auftragsverhältnisses nach Artikel 28 DS-GVO erfolgen, sondern tritt der Steuerberater selbst als datenschutzrechtlich Verantwortlicher auf, bedarf es einer Rechtsgrundlage, die den Auftraggeber berechtigt, die personenbezogenen Daten seiner Beschäftigten dem Steuerberater zu übermitteln, und gleichzeitig bedarf es einer Rechtsgrundlage, die den Steuerberater zur (eigenverantwortlichen) Verarbeitung der Beschäftigtendaten berechtigt. Soweit es um die Verarbeitung personenbezogener Daten durch den Steuerberater für Zwecke der laufenden Lohnabrechnung geht, kann als Rechtsgrundlage jedenfalls nicht auf § 11 des Steuerberatungsgesetzes abgestellt werden, da es sich insoweit nicht um Daten handelt, die der „Erfüllung der Aufgaben nach diesem Gesetz" (Hilfe in Steuersachen) dienen. Hinzu kommt, dass die Lohnbuchhaltung auch die Verarbeitung besonderer Kategorien personenbezogener Daten, sog. sensitiver Daten, beinhaltet, wie etwa Gesundheitsdaten oder Daten, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen. Sensitive Daten dürfen nur unter den (zusätzlichen) Voraussetzungen des Artikels 9 Absatz 2 DS-GVO verarbeitet werden. Die Verarbeitung solcher Daten durch den Steuerberater als (Eigen-)Verantwortlichen lässt sich indes unter keinen dieser Ausnahmetatbestände des Artikels 9 Absatz 2 DS-GVO subsumieren. Auch die Ausnahmeregelung des § 26 Absatz 3 des Bundesdatenschutzgesetzes (BDSG) hilft hier nicht

7 DSK, Fn. 2.

8 Kramer, Beauftragung eines Steuerberaters – AV oder nicht?, DatenschutzPraxis 11/2018, 18.

9 So auch die Steuerberaterkammer: https://www.bstbk.de/de/presse/news/2018-07-30_Lohn_Gehaltsbuchfuehrung/index.html.

10 Https://www.lda.bayern.de/media/FAQ_Steuerberater_keine_ADV.pdf.

11 Steuerberaterkammer, Fn. 7.

12 LfDI NRW: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Datenverarbeitung-in-der-Steuerberatung/Datenverarbeitung-in-der-Steuerberatung.html.

13 LfDI NRW, Fn. 10.

weiter. Denn weder verarbeitet der Steuerberater die sensitiven Daten „für Zwecke des Beschäftigungsverhältnisses“, noch ist die Verarbeitung „zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich“. Fehlt es somit an der Berechtigung, solche Daten zu verarbeiten, schließt dies insgesamt eine Lohnbuchhaltung als Verantwortlicher aus. Dagegen ist die Weitergabe auch sensitiver Daten im Rahmen eines Auftragsverhältnisses nach Artikel 28 DS-GVO grundsätzlich unproblematisch. Auch das Kurzpapier Nummer 13 der Datenschutzkonferenz steht dieser Auffassung entgegen anderslautender Behauptung nicht entgegen. Wenn dort in Anhang B die Tätigkeit von Berufsgeheimnisträgern pauschal von der Auftragsverarbeitung ausgeschlossen wird, ist dies jedenfalls nicht so zu verstehen, dass dies grundsätzlich auch für solche zusätzlich übernommenen Hilfstätigkeiten gilt, die keinen unmittelbaren Bezug zur Kerntätigkeit des Geheimnisträgers haben.

Übernimmt ein Steuerberater neben seiner eigentlichen Steuerberatertätigkeit (Hilfe in Steuersachen) zusätzlich weitere Aufgaben, handelt es sich um Auftragsverarbeitung im Sinne des Artikels 28 DS-GVO und bedarf einer entsprechenden Vereinbarung mit dem datenschutzrechtlich verantwortlichen Auftraggeber.“

4. Konsequenzen der unterschiedlichen Bewertung

Ob die Frage, welche der Bewertungen des Sachverhalts bei der Beauftragung eines Steuerberaters mit der Gehaltsabrechnung zutreffend ist, von gravierender praktischer Relevanz ist, hängt davon ab, ob die bei fehlender Auftragsverarbeitung stattfindende Datenübermittlung auf Zulässigkeitsgrenzen stößt. So wie die zur Fertigung einer Steuererklärung erforderliche Übermittlung zulässig ist, muss dies doch auch für die weniger Entscheidungsspielräume bietende Gehaltsberechnung gelten, indem sich der Arbeitgeber auf Art. 6 Abs. 1 lit. f und ggf. Art. 9 Abs. 2 lit. g DS-GVO stützen kann. Vorrangig wäre ggf. sogar § 26 Abs. 1 Satz 1 und Abs. 3 BDSG, da die Übermittlung erforderlich ist, um sich aus dem Beschäftigungsverhältnis ergebenden Rechte und Pflichten auszuüben oder zu erfüllen.

Solange sich zu dieser Frage keine einheitliche Auffassung der Aufsichtsbehörden gebildet hat, sollten sich Arbeitgeber nach der Auffassung der für sie zuständigen Aufsichtsbehörde richten und danach ihre vertraglichen Beziehungen mit der Steuerberaterpraxis gestalten, wenngleich nicht zu erwarten ist, dass eine Aufsichtsbehörde ihre Ansicht per Bußgeld durchzusetzen versucht, solange Uneinigkeit der Aufsichtsbehörden besteht.

II. Die eigenverantwortliche Rolle des Betriebsrats

1. Die Rolle des Betriebsrats nach der DS-GVO

Erneut problematisiert wird, ob der Betriebsrat als eigener Verantwortlicher im Sinne der DS-GVO in Betracht kommt oder ob er entsprechend der langjährigen Rechtsprechung des BAG[14] weiterhin dem Arbeitgeber als Verantwortlichem zuzurechnen ist.[15] Der LfDI Baden-Württemberg verneint letzteres wohl als erste Aufsichtsbehörde eindeutig.

Die Beantwortung der Frage nach der Eigenverantwortlichkeit von Betriebsräten ergibt sich nach Auffassung des LfDI BW aus der DS-GVO selbst: Entscheidet der Betriebsrat – wie es der Fall ist – selbst über die Zwecke und Mittel der Verarbeitung personenbezogener Daten, sei er als eigener Verantwortlicher anzusehen. Auch wenn der Arbeitgeber nach dem BetrVG letztlich über die dem Betriebsrat zur Verfügung gestellten Mittel entscheide, zeige die praktische Erfahrung, dass die Frage, welches Mittel ein Betriebsrat zur Erfüllung seiner Aufgaben nutzt, in der Regel durch diesen selbst bestimmt wird. Der Betriebsrat entscheide selbst, ob er bspw. eine Excel-Liste oder eine handschriftliche Liste von Mitarbeiterdaten anlegte oder wie er Vorgänge, die ihm von den Beschäftigten des Unternehmens gemeldet werden, dokumentiert, verwalte oder ablegte.[16] Auch bzgl. der weiteren Voraussetzung, d.h. über die Zwecke der Verarbeitung personenbezogener Daten entscheide der BR selbst, auch wenn ihm diese abstrakt vom Betriebsverfassungsgesetz vorgegeben werde.

2. Konsequenzen aus der Eigenständigkeit

Bei der Frage, welche Konsequenzen sich aus der Einstufung des Betriebsrats als eigener Verantwortlicher ergeben, weist der LfDI darauf hin, dass selbst für die Datenverarbeitung verantwortlich zu sein auch bedeute, den von der DS-GVO auferlegten Pflichten als Verantwortlicher nachzukommen. Somit müssen auch Betriebsräte bspw. Auskunftsansprüche und Löschverpflichtungen erfüllen.

Fraglich sei, ob bei Missachtung der Pflichten Bußgelder verhängt werden können. Normadressat von Bußgeldern sind in aller Regel die Verantwortlichen. Somit kommen auch Bußgelder gegen Betriebsräte in Betracht. Problematisch sei, inwieweit der Betriebsrat nach nationalem Recht rechts- und vermögensfähig ist. Die Beantwortung dieser Frage sei in der Vergangenheit von der Rechtsprechung unterschiedlich beantwortet worden. In einem Fall hat der Bundesgerichtshof dem Betriebsrat jedoch zumindest eine begrenzte Rechtsfähigkeit zugesprochen.[17] Es bleibe daher abzuwarten, wie sich die Thematik in Zukunft entwickele.

Dem LfDI BW ist die umstrittene Rechtslage durchaus bewusst. Insbesondere die Folge, dass der Betriebsrat beim Vorliegen der entsprechenden Voraussetzungen einen eigenen Datenschutzbeauftragten benennen muss, kann bei entsprechenden ggf. gerichtlich zu entscheidenden Initiativen von Mitarbeitervertretungen zur Aufhellung der Sachlage beitragen.

14 NZA 1998, 385.

15 Vgl. z.B. Gola, in: Gola (Hrsg.), DS-GVO, 2. Aufl. Art. 4 Rn. 56. Ferner Kranig/Wybitul, ZD 2019, 1, Baumgärtner/Honsch, ZD 2019, 99.

16 LfDI BW – 34. Tätigkeitsbericht 2018 – 1. 34 schwerpunke 38.

17 Vgl. BGH, Urteil v. 25.10.2012 – III ZR 266/11.

GDD-FORUM

Fortbildungsveranstaltung gem. Art. 38, Abs. 2 DS-GVO/ §§ 5, 6, 38 BDSG

Ihr Dialog mit der Datenschutzaufsicht

Informationen aus erster Hand

Der Dialog geht weiter: Die Umsetzung des neuen Datenschutzrechts aus DS-GVO und BDSG löst immer noch viele Praxisfragen aus. Diese werden in den Workingpaper des Datenschutzausschusses, Hinweisen der Datenschutzkonferenz oder den Arbeitspapieren der jeweiligen Aufsichtsbehörden nur zum Teil oder diskussionswürdig beantwortet.

Aus dem Inhalt:

- Marketing und Datenschutz
- Informationspflichten
- Anforderungen an die Datenschutz-Folgenabschätzung
- Anforderungen an die Rechenschaftsplicht

Termin/Ort

26. Juni 2019 in Hannover

10.00–17.15 Uhr

Referenten

Dr. Stefan Brink

RA Andreas Jaspers

Prof. Dr. Rolf Schwartmann

Barbara Thiel

Jetzt informieren und anmelden unter www.datakontext.com

Sichern Sie sich Ihren fachlichen Vorsprung!

DATAKONTEXT

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

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

Rechtsprechung

Videoaufzeichnung von Polizeibeamten in einer Polizeidienststelle während der Vornahme von Verfahrenshandlungen und Veröffentlichung auf einer Video-Website

(**Europäischer Gerichtshof**, Urteil vom 14. Februar 2019 – C 345/17 –)

1. **Art. 3 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass die von einem Bürger erfolgte Aufzeichnung von Polizeibeamten in einer Polizeidienststelle auf Video während der Aufnahme einer Aussage und die Veröffentlichung des so aufgezeichneten Videos auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, in den Anwendungsbereich dieser Richtlinie fällt.**
2. **Art. 9 der Richtlinie 95/46 ist dahin auszulegen, dass ein Sachverhalt wie der des Ausgangsverfahrens, d. h. die Aufzeichnung von Polizeibeamten in einer Polizeidienststelle auf Video während der Aufnahme einer Aussage und die Veröffentlichung des so aufgezeichneten Videos auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, eine Verarbeitung personenbezogener Daten allein zu journalistischen Zwecken im Sinne dieser Bestimmung darstellen kann, sofern aus diesem Video hervorgeht, dass diese Aufzeichnung und diese Veröffentlichung ausschließlich zum Ziel hatten, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten, was zu prüfen Sache des vorlegenden Gerichts ist.**

Sachverhalt:

15 Herr B. filmte in den Räumlichkeiten einer Dienststelle der lettischen nationalen Polizei die Aufnahme seiner Aussage im Rahmen eines Ordnungswidrigkeitenverfahrens.

16 Er veröffentlichte das so aufgezeichnete Video (im Folgenden: in Rede stehendes Video), das Polizeibeamte und deren Tätigkeit in der Polizeidienststelle zeigte, auf der Website www.youtube.com. Diese Website bietet Nutzern die Möglichkeit, Videos zu veröffentlichen, anzuschauen und zu teilen.

17 Nach dieser Veröffentlichung stellte die nationale Datenschutzbehörde in einer Entscheidung vom 30. August 2013 fest, dass Herr B. gegen Art. 8 Abs. 1 des Datenschutzgesetzes verstoßen habe, da er die Polizeibeamten in ihrer Eigenschaft als betroffene Personen nicht nach Maßgabe dieser Vorschrift über den Zweck der Verarbeitung der sie betreffenden personenbezogenen Daten informiert habe. Herr B. habe der nationalen Datenschutzbehörde auch keine Informationen über den Zweck der Aufzeichnung des in Rede stehenden Videos und dessen Veröffentlichung auf einer Website erteilt, die belegt hätten, dass der verfolgte Zweck mit dem Datenschutzgesetz in Einklang gestanden habe. Die nationale Datenschutzbehörde forderte Herrn B. daher auf, die Löschung des Videos auf der Website www.youtube.com und anderen Websites zu veranlassen.

18 Herr B. erhob bei der Administratīvā rajona tiesa (Verwaltungsgericht erster Instanz, Lettland) eine Klage, mit der er beantragte, die Rechtswidrigkeit dieser Entscheidung der nationalen Datenschutzbehörde festzustellen und ihm Ersatz für die Schäden zuzusprechen, die ihm seiner Ansicht nach entstanden sind. Er trug vor, er habe mit der Veröffentlichung des in Rede stehenden Videos die Aufmerksamkeit der Gesellschaft auf ein seiner Auffassung nach rechtswidriges Handeln der Polizei lenken wollen. Das Verwaltungsgericht wies die Klage ab.

19 Mit Urteil vom 11. November 2015 wies die Administratīvā apgabaltiesa (Regionales Verwaltungsgericht, Lettland) das Rechtsmittel von Herrn B. gegen die Entscheidung der Administratīvā rajona tiesa (Verwaltungsgericht erster Instanz) zurück.

20 Die Administratīvā apgabaltiesa (Regionales Verwaltungsgericht) begründete ihre Entscheidung damit, dass in dem in Rede stehenden Video die Polizeidienststelle sowie mehrere Polizeibeamten in Ausübung ihres Amtes zu sehen seien und die Kommunikation mit den Polizeibeamten bei der Vornahme von Verwaltungshandlungen sowie die Stimmen von Polizeibeamten, von Herrn B. und seines Begleiters zu hören seien.

21 Im Übrigen könne nicht festgestellt werden, ob das Recht von Herrn B. auf freie Meinungsäußerung oder das Recht anderer Personen auf Privatsphäre Vorrang haben müsse, da Herr B. nicht angegeben habe, zu welchem Zweck er das in Rede stehende Video veröffentlicht habe. Auch zeige das Video weder aktuelle Ereignisse, die für die Gesellschaft von Interesse wären, noch ein unehrenhaftes Verhalten von Polizeibeamten. Da Herr B. das in Rede stehende Video weder zu journalistischen Zwecken im Sinne des Gesetzes über die Presse und andere Masseninformationsmedien noch zu künstlerischen oder literarischen Zwecken erstellt habe, sei Art. 5 des Datenschutzgesetzes nicht anwendbar.

22 Die Administratīvā apgabaltiesa (Regionales Verwaltungsgericht) gelangte daher zu dem Ergebnis, dass Herr B. durch das Filmen der Polizeibeamten bei der Ausübung ihres Amtes, ohne ihnen den Zweck der Verarbeitung ihrer personenbezogenen Daten mitzuteilen, gegen Art. 8 Abs. 1 des Datenschutzgesetzes verstoßen habe.

23 Herr B. erhob beim vorlegenden Gericht, der Augstākā tiesa (Oberster Gerichtshof, Lettland), Kassationsbeschwerde gegen das Urteil der Administratīvā apgabaltiesa (Regionales Verwaltungsgericht) und berief sich dabei auf sein Recht auf freie Meinungsäußerung.

24 Er machte insbesondere geltend, dass das in Rede stehende Video Beamte der nationalen Polizei zeige, d. h. öffentliche Personen an einem für die Öffentlichkeit zugänglichen Ort, die daher nicht in den persönlichen Anwendungsbereich des Datenschutzgesetzes fielen.

25 Das vorlegende Gericht hat zum einen Zweifel, ob das Filmen von Polizeibeamten in einer Polizeidienststelle bei der Ausübung ihres Amtes und die Veröffentlichung des so aufgezeichneten Videos im Internet in den Anwendungsbereich der Richtlinie 95/46 fällt. Es ist insoweit zwar der Ansicht, dass das Verhalten von Herrn B. nicht unter die in Art. 3 Abs. 2 der Richtlinie genannten Ausnahmen vom Anwendungsbereich dieser Richtlinie falle, weist jedoch darauf hin, dass es im vorliegenden Fall um eine Aufzeichnung gehe, die nur ein einziges Mal erfolgt sei, und dass Herr B. die Polizeibeamten bei der Ausübung ihres öffentlichen Amtes, d. h., während sie als Vertreter der öffentlichen Gewalt gehandelt hät-

ten, gefilmt habe. Unter Bezugnahme auf Nr. 95 der Schlussanträge des Generalanwalts Bobek in der Rechtssache Rīgas satiksme (C 13/16, EU:C:2017:43) weist das vorlegende Gericht darauf hin, dass das Hauptanliegen, das den Schutz personenbezogener Daten rechtfertige, aber das mit der groß angelegten Verarbeitung dieser Daten verbundene Risiko sei.

26 Zum anderen möchte das vorlegende Gericht wissen, wie der Ausdruck „allein zu journalistischen Zwecken" in Art. 9 der Richtlinie 95/46 auszulegen ist und ob dieser Ausdruck einen Sachverhalt erfassen kann, wie er Herrn B. zur Last gelegt wird.

27 Unter diesen Umständen hat die Augstākā tiesa (Oberster Gerichtshof) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Fallen Tätigkeiten wie die im vorliegenden Fall in Rede stehende Aufzeichnung von Polizeibeamten in einer Polizeidienststelle bei der Vornahme von Verfahrenshandlungen und die Veröffentlichung des aufgezeichneten Videos auf der Website www.youtube.com in den Geltungsbereich der Richtlinie 95/46?

2. Ist die Richtlinie 95/46 dahin auszulegen, dass die genannten Tätigkeiten als eine Verarbeitung personenbezogener Daten zu journalistischen Zwecken im Sinne von Art. 9 dieser Richtlinie angesehen werden können?

Zu den Vorlagefragen

Zur ersten Frage

28 Mit seiner ersten Frage möchte das vorlegende Gericht wissen, ob Art. 3 der Richtlinie 95/46 dahin auszulegen ist, dass die Aufzeichnung von Polizeibeamten in einer Polizeidienststelle auf Video während der Aufnahme einer Aussage und die Veröffentlichung des so aufgezeichneten Videos auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, in den Anwendungsbereich dieser Richtlinie fällt.

29 Die Richtlinie 95/46 gilt nach ihrem Art. 3 Abs. 1 „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen".

30 Der Begriff „personenbezogene Daten" im Sinne dieser Bestimmung bezieht sich nach der Definition in Art. 2 Buchst. a der Richtlinie 95/46 auf „alle Informationen über eine bestimmte oder bestimmbare natürliche Person". Als bestimmbar wird eine Person angesehen, „die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu … einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen Identität sind".

31 Nach der Rechtsprechung des Gerichtshofs fällt das von einer Kamera aufgezeichnete Bild einer Person unter den Begriff „personenbezogene Daten" im Sinne von Art. 2 Buchst. a der Richtlinie 95/46, sofern es die Identifikation der betroffenen Person ermöglicht (vgl. Urteil vom 11. Dezember 2014, Ryneš, C 212/13, EU:C:2014:2428, Rn. 22).

32 Im vorliegenden Fall geht aus der Vorlageentscheidung hervor, dass die Polizeibeamten auf dem in Rede stehenden Video zu sehen und zu verstehen sind, so dass davon auszugehen ist, dass die Bilder der so aufgezeichneten Personen personenbezogene Daten im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 darstellen.

33 Der Begriff „Verarbeitung personenbezogener Daten" bezeichnet nach Art. 2 Buchst. b der Richtlinie 95/46 „jeden … Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten".

34 In Bezug auf eine Videoüberwachungsanlage hat der Gerichtshof bereits entschieden, dass eine Videoaufzeichnung von Personen auf einer kontinuierlichen Speichervorrichtung, der Festplatte der Überwachungsanlage, gemäß Art. 2 Buchst. b und Art. 3 Abs. 1 der Richtlinie 95/46 eine automatisierte Verarbeitung personenbezogener Daten darstellt (vgl. in diesem Sinne Urteil vom 11. Dezember 2014, Ryneš, C 212/13, EU:C:2014:2428, Rn. 23 und 25).

35 In der mündlichen Verhandlung vor dem Gerichtshof hat Herr B. vorgetragen, dass er zur Aufzeichnung des in Rede stehenden Videos eine Digitalkamera verwendet habe. Dabei handelt es sich um eine Videoaufzeichnung von Personen auf einer kontinuierlichen Speichervorrichtung, dem Speicher der Kamera. Eine solche Aufzeichnung stellt somit eine automatisierte Verarbeitung personenbezogener Daten im Sinne von Art. 3 Abs. 1 der Richtlinie 95/46 dar.

36 Insoweit ist der Umstand, dass eine solche Aufzeichnung nur ein einziges Mal erfolgt ist, ohne Bedeutung für die Frage, ob dieser Vorgang in den Anwendungsbereich der Richtlinie 95/46 fällt. Wie sich nämlich aus dem Wortlaut von Art. 2 Buchst. b in Verbindung mit Art. 3 Abs. 1 dieser Richtlinie ergibt, gilt diese für „jeden Vorgang", der eine Verarbeitung personenbezogener Daten im Sinne dieser Bestimmungen darstellt.

37 Der Gerichtshof hat ferner entschieden, dass der Vorgang, der darin besteht, personenbezogene Daten auf eine Website zu stellen, ebenfalls als eine solche Verarbeitung anzusehen ist (vgl. in diesem Sinne Urteile vom 6. November 2003, Lindqvist, C 101/01, EU:C:2003:596, Rn. 25, und vom 13. Mai 2014, Google Spain und Google, C 131/12, EU:C:2014:317, Rn. 26).

38 Insoweit hat der Gerichtshof im Übrigen klargestellt, dass es zur Wiedergabe von Informationen auf einer Internetseite eines Hochladens dieser Seite auf einen Server sowie der erforderlichen Vorgänge bedarf, um diese Seite den mit dem Internet verbundenen Personen zugänglich zu machen. Diese Vorgänge erfolgen zumindest teilweise in automatisierter Form (vgl. in diesem Sinne Urteil vom 6. November 2003, Lindqvist, C 101/01, EU:C:2003:596, Rn. 26).

39 Somit stellt die Veröffentlichung einer Videoaufzeichnung – wie das in Rede stehende Video –, die personenbezogene Daten enthält, auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, eine ganz oder teilweise automatisierte Verarbeitung dieser Daten im Sinne von Art. 2 Buchst. b und Art. 3 Abs. 1 der Richtlinie 95/46 dar.

40 Gemäß Art. 3 Abs. 2 der Richtlinie 95/46 findet diese Richtlinie im Übrigen auf zwei Arten der Verarbeitung personenbezogener Daten keine Anwendung. Dabei handelt es sich zum einen um Verarbeitungen, die für die Ausübung von Tätigkeiten erfolgen, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union in seiner vor dem Inkrafttreten des Vertrags von Lissabon geltenden Fassung, und in jedem Fall Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich. Zum anderen schließt diese Bestimmung Verarbeitungen personenbezogener Daten aus, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen werden.

41 Da die in Art. 3 Abs. 2 der Richtlinie 95/46 vorgesehenen Ausnahmen zur Unanwendbarkeit der Regelung zum Schutz personenbezogener Daten führen, die die Richtlinie vorsieht, und damit von dem ihr zugrunde liegenden Ziel, den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten – wie das durch Art. 7 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) garantierte Recht auf Achtung des Privat- und Familienlebens sowie das durch Art. 8 der Charta garantierte Recht auf Schutz personenbezogener Daten – sicherzustellen, abweichen, müssen sie eng ausgelegt werden (vgl. in diesem Sinne Urteile vom 27. September 2017, Puškár, C 73/16, EU:C:2017:725, Rn. 38, und vom 10. Juli 2018, Jehovan todistajat, C 25/17, EU:C:2018:551, Rn. 37).

42 Was das Ausgangsverfahren anbelangt, geht aus den beim Gerichtshof eingereichten Unterlagen hervor, dass zum einen die Aufzeichnung und die Veröffentlichung des in Rede stehenden Videos weder als eine Verarbeitung personenbezogener Daten angesehen werden können, die für die Ausübung von Tätigkeiten erfolgte, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, noch als eine Verarbeitung betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates oder die Tätigkeiten des Staates im strafrechtlichen Bereich im Sinne von Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46. Insoweit hat der Gerichtshof bereits entschieden, dass die Tätigkeiten, die in der genannten Vorschrift beispielhaft aufgeführt werden, allesamt spezifische Tätigkeiten des Staates oder staatlicher Stellen sind, die mit den Tätigkeitsbereichen von Privatpersonen nichts zu tun haben (vgl. in diesem Sinne Urteil vom 27. September 2017, Puškár, C 73/16, EU:C:2017:725, Rn. 36 und die dort angeführte Rechtsprechung).

43 Zum anderen erfolgte die im Ausgangsverfahren in Rede stehende Verarbeitung personenbezogener Daten aufgrund dessen, dass Herr B. das in Rede stehende Video ohne Zugangsbeschränkung auf einer Video-Website veröffentlicht hat, auf der die Nutzer Videos versenden, anschauen und teilen können, wodurch personenbezogene Daten einer unbestimmten Zahl von Personen zugänglich gemacht wurden, nicht im Rahmen der Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (vgl. entsprechend Urteile vom 6. November 2003, Lindqvist, C 101/01, EU:C:2003:596, Rn. 47, vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 44, vom 11. Dezember 2014, Ryneš, C 212/13, EU:C:2014:2428, Rn. 31 und 33, und vom 10. Juli 2018, Jehovan todistajat, C 25/17, EU:C:2018:551, Rn. 42).

44 Des Weiteren kann der Umstand, dass Polizeibeamte im Rahmen der Ausübung ihres Amtes auf Video aufgezeichnet werden, nicht zum Ausschluss einer solchen Art der Verarbeitung personenbezogener Daten aus dem Anwendungsbereich der Richtlinie 95/46 führen.

45 Wie die Generalanwältin in Nr. 29 ihrer Schlussanträge ausgeführt hat, sieht diese Richtlinie nämlich keine Ausnahme vor, die Verarbeitungen personenbezogener Daten, die Beamte betreffen, vom Anwendungsbereich dieser Richtlinie ausschließen würde.

46 Aus der Rechtsprechung des Gerichtshofs geht ferner hervor, dass Informationen nicht deshalb nicht als „personenbezogene Daten" einzustufen sind, weil sie im Kontext einer beruflichen Tätigkeit stehen (vgl. in diesem Sinne Urteil vom 16. Juli 2015, ClientEarth und PAN Europe/EFSA, C 615/13 P, EU:C:2015:489, Rn. 30 und die dort angeführte Rechtsprechung).

47 Nach alledem ist auf die erste Frage zu antworten, dass Art. 3 der Richtlinie 95/46 dahin auszulegen ist, dass die Aufzeichnung von Polizeibeamten in einer Polizeidienststelle auf Video während der Aufnahme einer Aussage und die Veröffentlichung des so aufgezeichneten Videos auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, in den Anwendungsbereich dieser Richtlinie fällt.

Zur zweiten Frage

48 Mit seiner zweiten Frage möchte das vorlegende Gericht wissen, ob Art. 9 der Richtlinie 95/46 dahin auszulegen ist, dass ein Sachverhalt wie der des Ausgangsverfahrens, d. h. die Aufzeichnung von Polizeibeamten in einer Polizeidienststelle auf Video während der Aufnahme einer Aussage und die Veröffentlichung des so aufgezeichneten Videos auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, eine Verarbeitung personenbezogener Daten zu journalistischen Zwecken im Sinne dieser Bestimmung darstellt.

49 Zunächst ist festzustellen, dass die Bestimmungen einer Richtlinie nach ständiger Rechtsprechung des Gerichtshofs mit Blick auf ihre Ziele und das mit ihr eingeführte System auszulegen sind (Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 51 und die dort angeführte Rechtsprechung).

50 Wie sich aus ihrem Art. 1 ergibt, soll die Richtlinie 95/46 den Mitgliedstaaten den freien Verkehr personenbezogener Daten ermöglichen und gleichzeitig den Schutz der Grundrechte und Grundfreiheiten, insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung dieser Daten gewährleisten. Dieses Ziel lässt sich jedoch nur erreichen, wenn berücksichtigt wird, dass die genannten Grundrechte in einem gewissen Maß mit dem Grundrecht der Freiheit der Meinungsäußerung in Einklang gebracht werden müssen. Im 37. Erwägungsgrund der Richtlinie 95/46 wird klargestellt, dass mit ihrem Art. 9 bezweckt wird, zwei Grundrechte miteinander in Einklang zu bringen, nämlich zum einen den Schutz der Privatsphäre und zum anderen die Freiheit der Meinungsäußerung. Diese Aufgabe obliegt den Mitgliedstaaten (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 52 bis 54).

51 Der Gerichtshof hat bereits entscheiden, dass in Anbetracht der Bedeutung, die der Freiheit der Meinungsäußerung in jeder demokratischen Gesellschaft zukommt, die damit zusammenhängenden Begriffe, zu denen der des Journalismus gehört, weit ausgelegt werden müssen (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 56).

52 So ergibt sich aus den Vorarbeiten zur Richtlinie 95/46, dass die in ihrem Art. 9 vorgesehenen Befreiungen und Ausnahmen nicht nur für Medienunternehmen, sondern für jeden gelten, der journalistisch tätig ist (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 58).

53 Nach der Rechtsprechung des Gerichtshofs sind „journalistische Tätigkeiten" solche Tätigkeiten, die zum Zweck haben, Informationen, Meinungen oder Ideen, mit welchem Übertragungsmittel auch immer, in der Öffentlichkeit zu verbreiten (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 61).

54 Zwar ist es Sache des vorlegenden Gerichts, zu prüfen, ob im vorliegenden Fall die Verarbeitung personenbezogener

Daten, die Herr B. vorgenommen hat, diesem Zweck entspricht, jedoch kann der Gerichtshof diesem Gericht die für die ihm obliegende Beurteilung erforderlichen Auslegungshinweise geben.

55 So schließt der Umstand, dass Herr B. kein Berufsjournalist ist, in Anbetracht der in den Rn. 52 und 53 des vorliegenden Urteils angeführten Rechtsprechung des Gerichtshofs es offenbar nicht aus, dass die Aufzeichnung des in Rede stehenden Videos und dessen Veröffentlichung auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, unter diese Bestimmung fallen können.

56 Insbesondere kann der Umstand, dass Herr B. diese Aufzeichnung auf einer solchen Website, im vorliegenden Fall der Website www.youtube.com, online gestellt hat, für sich genommen dieser Verarbeitung personenbezogener Daten nicht die Eigenschaft als „allein zu journalistischen Zwecken" im Sinne von Art. 9 der Richtlinie 95/46 erfolgt nehmen.

57 Es muss nämlich die Entwicklung und die Vervielfältigung der Mittel zur Kommunikation und zur Verbreitung von Informationen berücksichtigt werden. Wie der Gerichtshof bereits entschieden hat, ist der Träger, mit dem die verarbeiteten Daten übermittelt werden – ob es sich um einen klassischen Träger wie Papier oder Radiowellen oder aber um einen elektronischen Träger wie das Internet handelt –, nicht ausschlaggebend für die Beurteilung, ob es sich um eine Tätigkeit „allein zu journalistischen Zwecken" handelt (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 60).

58 Allerdings kann, wie die Generalanwältin in Nr. 55 ihrer Schlussanträge ausgeführt hat, nicht davon ausgegangen werden, dass jegliche im Internet veröffentlichte Information, die sich auf personenbezogene Daten bezieht, unter den Begriff der „journalistischen Tätigkeiten" fiele und daher für sie die in Art. 9 der Richtlinie 95/46 vorgesehenen Abweichungen und Ausnahmen gälten.

59 Im vorliegenden Fall ist es Sache des vorlegenden Gerichts, zu prüfen, ob aus dem in Rede stehenden Video hervorgeht, dass die Aufzeichnung und die Veröffentlichung dieses Videos ausschließlich zum Ziel hatten, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 62).

60 Dabei kann das vorlegende Gericht u. a. berücksichtigen, dass das in Rede stehende Video nach den Angaben von Herrn B. auf einer Website veröffentlicht wurde, um die Aufmerksamkeit der Gesellschaft auf die angeblich vorschriftswidrigen Praktiken der Polizei zu lenken, die während der Aufnahme seiner Aussage angewandt worden seien.

61 Es ist jedoch darauf hinzuweisen, dass die Feststellung derartiger vorschriftswidriger Praktiken keine Voraussetzung für die Anwendbarkeit von Art. 9 der Richtlinie 95/46 ist.

62 Hingegen könnte dann, wenn sich erweisen sollte, dass die Aufzeichnung und die Veröffentlichung dieses Videos nicht ausschließlich zum Ziel hatten, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten, nicht davon ausgegangen werden, dass die Verarbeitung der im Ausgangsverfahren in Rede stehenden personenbezogenen Daten „allein zu journalistischen Zwecken" erfolgte.

63 Des Weiteren ist darauf hinzuweisen, dass die in Art. 9 der Richtlinie 95/46 vorgesehenen Befreiungen und Ausnahmen nur in dem Umfang angewandt werden dürfen, in dem sie sich als notwendig erweisen, um zwei Grundrechte, nämlich das Recht auf Schutz der Privatsphäre und das Recht auf freie Meinungsäußerung, miteinander in Einklang zu bringen (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 55).

64 Um ein Gleichgewicht zwischen diesen beiden Grundrechten herzustellen, erfordert der Schutz der Privatsphäre demnach, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Datenschutz, die in den Kapiteln II, IV und VI der Richtlinie 95/46 vorgesehen sind, auf das absolut Notwendige beschränken (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C 73/07, EU:C:2008:727, Rn. 56).

65 Es ist darauf hinzuweisen, dass Art. 7 der Charta, der das Recht auf Achtung des Privat- und Familienlebens betrifft, Rechte enthält, die den in Art. 8 Abs. 1 der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (im Folgenden: EMRK) gewährleisteten Rechten entsprechen, und dass diesem Art. 7 gemäß Art. 52 Abs. 3 der Charta somit die gleiche Bedeutung und Tragweite beizumessen ist wie Art. 8 Abs. 1 EMRK in seiner Auslegung durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (Urteil vom 17. Dezember 2015, WebMindLicenses, C 419/14, EU:C:2015:832, Rn. 70). Gleiches gilt für Art. 11 der Charta und Art. 10 EMRK (vgl. in diesem Sinne Urteil vom 4. Mai 2016, Philip Morris Brands u. a., C 547/14, EU:C:2016:325, Rn. 147).

66 Insoweit geht aus dieser Rechtsprechung hervor, dass der Europäische Gerichtshof für Menschenrechte für die Zwecke der Abwägung zwischen dem Recht auf Achtung des Privatlebens und dem Recht auf freie Meinungsäußerung eine Reihe relevanter Kriterien entwickelt hat, die zu berücksichtigen sind, darunter der Beitrag zu einer Debatte von allgemeinem Interesse, der Bekanntheitsgrad der betroffenen Person, der Gegenstand der Berichterstattung, das vorangegangene Verhalten der betroffenen Person, Inhalt, Form und Auswirkungen der Veröffentlichung, die Art und Weise sowie die Umstände, unter denen die Informationen erlangt worden sind, und deren Richtigkeit (vgl. in diesem Sinne EGMR, 27. Juni 2017, Satakunnan Markkinapörssi Oy und Satamedia Oy/Finnland, CE:ECHR:2017:-0627JUD000093113, § 165). Ebenso muss die Möglichkeit berücksichtigt werden, dass der für die Verarbeitung Verantwortliche Maßnahmen ergreift, die es ermöglichen, das Ausmaß des Eingriffs in das Recht auf Privatsphäre zu verringern.

67 Im vorliegenden Fall geht aus der dem Gerichtshof vorgelegten Akte hervor, dass nicht ausgeschlossen werden kann, dass die Aufzeichnung und die Veröffentlichung des in Rede stehenden Videos, die erfolgt sind, ohne dass die betroffenen Personen über diese Aufzeichnung und deren Zwecke informiert wurden, einen Eingriff in das Grundrecht auf Achtung des Privatlebens dieser Personen, d. h. der in diesem Video zu sehenden Polizeibeamten, darstellt.

68 Sollte es sich erweisen, dass die Aufzeichnung und die Veröffentlichung des in Rede stehenden Videos ausschließlich zum Ziel hatten, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten, so ist es Sache des vorlegenden Gerichts, zu beurteilen, ob die in Art. 9 der Richtlinie 95/46 vorgesehenen Befreiungen und Ausnahmen sich als notwendig erweisen, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen, und ob sich diese Befreiungen und Ausnahmen auf das absolut Notwendige beschränken.

69 Nach alledem ist auf die zweite Frage zu antworten, dass Art. 9 der Richtlinie 95/46 dahin auszulegen ist, dass ein Sachverhalt wie der des Ausgangsverfahrens, d. h. die Aufzeichnung von Polizeibeamten in einer Polizeidienststelle auf Video wäh-

rend der Aufnahme einer Aussage und die Veröffentlichung des so aufgezeichneten Videos auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, eine Verarbeitung personenbezogener Daten allein zu journalistischen Zwecken im Sinne dieser Bestimmung darstellen kann, sofern aus diesem Video hervorgeht, dass diese Aufzeichnung und diese Veröffentlichung ausschließlich zum Ziel hatten, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten, was zu prüfen Sache des vorlegenden Gerichts ist.

Informantenschutz gegenüber Verstorbenen

(**Bundesverwaltungsgericht,** Beschluss vom 24. Oktober 2018 – 20 F 15.16 –)

1. **Das Wohl des Bundes im Sinne des § 99 Abs. 1 Satz 2 Alt. 1 VwGO kann auch nach dem (mutmaßlichen) Tod eines Informanten die Geheimhaltung seiner persönlichen Daten erforderlich machen. Denn das für die Gewinnung von Informanten notwendige Vertrauen in die Verlässlichkeit von Vertraulichkeitszusagen ist zu gewährleisten.**
2. **Liegt der (mutmaßliche) Tod eines Informanten länger als etwa 30 Jahre zurück, bedarf die Notwendigkeit einer weiteren Geheimhaltung bei weit zurückliegenden, abgeschlossenen Vorgängen zusätzlicher Erläuterungen.**

Beschluss

In der Verwaltungsstreitsache hat der Fachsenat des Bundesverwaltungsgerichts für Entscheidungen nach § 99 Abs. 2 VwGO am 24. Oktober 2018 durch den Vorsitzenden Richter am Bundesverwaltungsgericht Dr. Häußler, den Richter am Bundesverwaltungsgericht Prof. Dr. Burmeister und die Richterin am Bundesverwaltungsgericht Dr. Eppelt beschlossen:

Die Sperrerklärung des Beigeladenen vom 31. Januar 2017 ist rechtswidrig, soweit sie sich auf Schwärzungen auf den Seiten 45, 46, 51 Nr. 1 und 4, 53 Nr. 1 und 4, 95, 97, 119, 135, 174 und 186 des Vorganges mit der Signatur „BND-Archiv 24856_OT“ sowie die Schwärzungen in dem Datenbankauszug zu der Verwaltungsnummer 16 214 in den Zeilen 2 bis 9 unter der Überschrift „Grunddaten Person“ bezieht.

Im Übrigen wird der Antrag der Klägerin abgelehnt.

Mitbestimmung bei der Anweisung zur Vorlage einer Arbeitsunfähigkeitsbescheinigung

(Bundesverwaltungsgericht, Beschluss vom 15. Oktober 2018 – 5 P 9.17 –)

Das Mitbestimmungsrecht des § 52 Abs. 1 Satz 1 PersVG HB ist umfassend und wird durch die beispielhaften Aufzählungen von mitbestimmungspflichtigen Maßnahmen in § 63 Abs. 1, § 65 Abs. 1 sowie § 66 Abs. 1 PersVG HB nicht eingeschränkt (Aufgabe der bisherigen Rechtsprechung).

Sachverhalt:

Die Beteiligten streiten darüber, ob die Verpflichtung einzelner Beschäftigter zur Vorlage einer Arbeitsunfähigkeitsbescheinigung ab dem ersten Krankheitstag der Mitbestimmung des Personalrats unterliegt.

Antragsteller ist der Personalrat beim Senator für Umwelt, Bau und Verkehr der Hansestadt Bremen, dem Beteiligten. Mit Schreiben vom 20. Juli 2012 wies die Personalstelle des Beteiligten die Arbeitnehmerin Frau S. an, wegen ihrer häufigen Kurzzeiterkrankungen in den vergangenen 12 Monaten ab sofort eine Arbeitsunfähigkeitsbescheinigung ab dem ersten Krankheitstag vorzulegen. Zuvor hatte die Personalstelle den Antragsteller von der beabsichtigten Anordnung in Kenntnis gesetzt und mitgeteilt, dass die Angelegenheit aus ihrer Sicht nicht der Mitbestimmung des Personalrats unterliege, weil es sich nicht um eine personalvertretungsrechtliche Maßnahme im Sinne des § 58 Abs. 1 Satz 1 PersVG HB handele. Der Antragsteller vertrat die Auffassung, dass die Anordnung eine der Mitbestimmung unterliegende Maßnahme darstelle.

Aus den Gründen:

Das Oberverwaltungsgericht geht zu Recht davon aus, dass die Anordnung des Beteiligten gegenüber einzelnen Arbeitnehmern, die Arbeitsunfähigkeitsbescheinigung ab dem ersten Krankheitstag vorzulegen, als Maßnahme (1.), die weder unter eine gesetzliche oder tarifliche Regelung noch unter einen der Katalogtatbestände in den §§ 63, 65 oder 66 PersVG HB fällt (2.), gemäß § 52 Abs. 1 Satz 1 PersVG HB der Mitbestimmung des Personalrats unterliegt (3.).

1. Die gegenüber einzelnen Beschäftigten ergehende Anordnung gemäß § 5 Abs. 1 Satz 3 des Gesetzes über die Zahlung des Arbeitsentgelts an Feiertagen und im Krankheitsfall (Entgeltfortzahlungsgesetz) vom 26. Mai 1994 (BGBl. I S. 1014, 1065), zuletzt geändert durch Gesetz vom 16. Juli 2015 (BGBl. I S. 1211) – EntgFG – die ärztliche Bescheinigung über das Bestehen der Arbeitsunfähigkeit bereits ab dem ersten Krankheitstag vorzulegen, ist, wie das Oberverwaltungsgericht zu Recht annimmt, eine Maßnahme im Sinne des § 58 Abs. 1 Satz 1 PersVG HB. Danach setzt die Mitbestimmung voraus, dass eine der Mitbestimmung des Personalrats unterliegende Maßnahme beabsichtigt ist. Unter einer Maßnahme im personalvertretungsrechtlichen Sinn ist jede auf die Veränderung des bestehenden Zustandes abzielende Handlung oder Entscheidung der Dienststellenleitung zu verstehen, die den Rechtsstand der Beschäftigten berührt und durch deren Durchführung das Beschäftigungsverhältnis oder die Arbeitsbedingungen eine Änderung erfahren (stRspr, vgl. z.B. BVerwG, Beschluss vom 17. Mai 2017 – 5 P 2.16 – Buchholz 250 § 75 BPersVG Nr. 127 Rn. 10 m.w.N.). So liegt es hier. Gemäß § 5 Abs. 1 Satz 1 EntgFG ist der Arbeitnehmer verpflichtet, dem Arbeitgeber die Arbeitsunfähigkeit und deren voraussichtliche Dauer unverzüglich mitzuteilen. Wenn die Arbeitsunfähigkeit länger als drei Kalendertage dauert, hat er gemäß § 5 Abs. 1 Satz 2 EntgFG eine ärztliche Bescheinigung über das Bestehen der Arbeitsunfähigkeit sowie deren voraussichtliche Dauer spätestens an dem darauffolgenden Arbeitstag vorzulegen. Abweichend davon ist der Arbeitgeber gemäß § 5 Abs. 1 Satz 3 EntgFG berechtigt, die Vorlage der ärztlichen Bescheinigung früher zu verlangen. Macht der Arbeitgeber von diesem einseitigen, in seinem nicht

gebundenen Ermessen liegenden Bestimmungsrecht Gebrauch, trifft er gegenüber den betroffenen Beschäftigten eine von der gesetzlichen Regelung des § 5 Abs. 1 Satz 1 EntgFG abweichende Sonderregelung und verändert damit deren arbeitsvertragliche Nebenpflichten.

2. Zwischen den Beteiligten steht zu Recht nicht im Streit, dass die Anordnung gegenüber einzelnen Beschäftigten, eine Arbeitsunfähigkeitsbescheinigung bereits ab dem ersten Krankheitstag vorzulegen, weder unter eine gesetzliche oder tarifliche Regelung noch unter einen der Katalogtatbestände in den §§ 63, 65 oder 66 PersVG HB fällt.

3. Die Anordnung gegenüber einzelnen Beschäftigten, eine ärztliche Arbeitsunfähigkeitsbescheinigung ab dem ersten Krankheitstag vorzulegen, ist gemäß § 52 Abs. 1 Satz 1 PersVG HB mitbestimmungspflichtig. Danach hat der Personalrat die Aufgabe, für alle in der Dienststelle weisungsgebunden tätigen Personen in allen sozialen, personellen und organisatorischen Angelegenheiten gleichberechtigt gemäß den Bestimmungen der §§ 58 bis 62 PersVG HB mitzubestimmen. Wie das Oberverwaltungsgericht zu Recht annimmt, ist der Personalrat dementsprechend berechtigt, an allen innerdienstlichen Maßnahmen des Dienststellenleiters mitzuwirken. Dieses Mitbestimmungsrecht beansprucht uneingeschränkte Geltung. Das ergibt die an Wortlaut (a), Gesetzessystematik (b), Sinn und Zweck der gesetzlichen Regelung (c) sowie der Gesetzgebungsgeschichte (d) ausgerichtete Auslegung der Norm.

a) Bereits der Wortlaut des § 52 Abs. 1 Satz 1 PersVG HB, wonach der Personalrat zur Mitbestimmung „in allen sozialen, personellen und organisatorischen Angelegenheiten“ aufgerufen ist, weist deutlich in die Richtung eines umfassenden und uneingeschränkten Mitbestimmungsrechts. Denn nach dem Alltags- und Fachsprachgebrauch spricht ganz Überwiegendes dafür, ihn dahin zu verstehen, dass der Personalrat in ausnahmslos jeder der genannten Angelegenheiten mitzubestimmen hat. Dies ist allerdings nicht zwingend.

b) Der systematische Zusammenhang zwischen § 52 Abs. 1 Satz 1 PersVG HB einerseits und § 63 Abs. 1 und 2, § 65 Abs. 1 und 3 sowie § 66 Abs. 1 und 3 PersVG HB andererseits verbietet die Annahme einer Einschränkung des Mitbestimmungsrechts nach der zuerst genannten Bestimmung.

Nach § 63 Abs. 1, § 65 Abs. 1 und § 66 Abs. 1 PersVG HB erstreckt sich das Recht der Mitbestimmung des Personalrats, soweit eine gesetzliche oder tarifliche Regelung nicht besteht oder die Zuständigkeit des Gesamtpersonalrats nicht gegeben ist, insbesondere auf die nachfolgend aufgeführten Maßnahmen. Die Bestimmungen enthalten einen beispielhaften und nicht abschließenden Katalog von Mitbestimmungstatbeständen, wie sich bereits aus dem der Aufzählung jeweils vorangestellten Wort „insbesondere“ und ihren jeweiligen Überschriften ergibt („Beispiele für Mitbestimmung …“). Darin erschöpft sich die Bedeutung der Katalogtatbestände. Insbesondere ist ihnen nicht auch der Wille des Gesetzgebers zu entnehmen, dass andere Maßnahmen des Dienststellenleiters der Mitbestimmung des Personalrats nur dann unterliegen sollen, wenn sie in ihren Auswirkungen auf die Dienststelle und die Beschäftigten den beispielhaft geregelten Maßnahmen in etwa gleichkommen, sie einem der Beispielsfälle nach Art und Bedeutung vergleichbar sind. Soweit das Bundesverwaltungsgericht dies in seiner bisherigen Rechtsprechung anders gesehen hat (vgl. BVerwG, Beschlüsse vom 17. Juli 1987 – 6 P 13.85 – Buchholz 251.3 § 66 BrPersVG Nr. 1 S. 1 <3 f.>, vom 11. November 1993 – 6 PB 4.93 – juris Rn. 4 und vom 24. Juni 2014 – 6 P 1.14 – Buchholz 251.8 § 73 RhPPersVG Nr. 1 Rn. 17 f.), hält der Senat daran – mit Blick auf die Rechtslage nach dem Bremischen Personalvertretungsgesetz – aus den nachstehenden Gründen nicht fest.

Es kann hier dahingestellt bleiben, welche Bedeutung beispielhaften Mitbestimmungskatalogen in den Personalvertretungsgesetzen des Bundes und anderer Länder beizumessen ist. Das Bundesverwaltungsgericht hat bereits in seiner früheren Rechtsprechung zum Ausdruck gebracht, dass sich für das bremische Landesrecht eine unüberprüfte Übertragung der für das Bundesrecht und das sonstige Landesrecht entwickelten Rechtsgrundsätze verbietet (vgl. BVerwG, Beschlüsse vom 17. August 1989 – 6 P 11.87 – BVerwGE 82, 288 <291> und vom 11. November 1993 – 6 PB 4.93 – juris Rn. 4). Deshalb ist auch bei der Ermittlung der Bedeutung der hier in Rede stehenden Mitbestimmungskataloge den Besonderheiten der bremischen Rechtslage Rechnung zu tragen. Eine solche Eigenheit stellen die so genannten Unberührtheitsklauseln der § 63 Abs. 2, § 65 Abs. 3 und § 66 Abs. 3 PersVG HB dar. Nach diesen wird durch die ihnen jeweils vorangestellten beispielhaften Aufzählungen von Mitbestimmungstatbeständen die Allzuständigkeit des Personalrats nach § 52 Abs. 1 Satz 1 PersVG HB nicht berührt. Diese Bestimmungen steuern maßgeblich sowohl die Auslegung des § 52 Abs. 1 Satz 1 PersVG HB als auch diejenige der § 63 Abs. 1, § 65 Abs. 1 und § 66 Abs. 1 PersVG HB.

Ihnen ist zum einen zu entnehmen, dass § 52 Abs. 1 Satz 1 PersVG HB eine Allzuständigkeit des Personalrats hinsichtlich der Mitbestimmung in sozialen, personellen und organisatorischen Angelegenheiten begründet. Der Begriff „Allzuständigkeit“ ist hier dahin zu verstehen, dass das Bremische Personalvertretungsgesetz dem Personalrat – abweichend von den Personalvertretungsgesetzen des Bundes und anderer Bundesländer – ein umfassendes bzw. allumfassendes gleichberechtigtes Mitbestimmungsrecht in allen insoweit in Bezug genommenen (innerdienstlichen) Angelegenheiten gewährt (vgl. BVerwG, Beschlüsse vom 30. Oktober 1964 – 7 P 2.64 – BVerwGE 19, 359 <361>, vom 18. März 1981 – 6 P 27.79 – BVerwGE 62, 55 <58> und vom 17. Juli 1987 – 6 P 13.85 – Buchholz 251.3 § 66 BrPersVG Nr. 1 S. 1 <3 f.>; Rust, in: Arbeitnehmerkammer Bremen <Hrsg.>, Gemeinschaftskommentar zum BremPersVG, 2016, § 52 Rn. 12). Mithin handelt es sich bei § 52 Abs. 1 Satz 1 PersVG HB um eine Generalklausel, die im Gegensatz zu einer enumerativen und abschließenden Aufzählung einzelner Mitbestimmungstatbestände ein uneingeschränktes Mitbestimmungsrecht im Rahmen ihres Anwendungsbereichs verleiht (vgl. Altvater, in: Altvater/Baden/Berg/Kröll/Noll/Seulen, BPersVG, 9. Aufl. 2016, vor § 66 Rn. 23).

Den Unberührtheitsklauseln ist zum anderen zu entnehmen, dass dieses umfassende Mitbestimmungsrecht durch § 63 Abs. 1, § 65 Abs. 1 und § 66 Abs. 1 PersVG HB keine Einschränkung erfährt. Dies folgt zweifelsfrei aus der Wendung, dass durch die Aufzählungen in diesen Bestimmungen die Allzuständigkeit „nicht berührt“ wird. Damit wird zugleich zum Ausdruck gebracht, dass die Katalogtatbestände einzelne der Mitbestimmung unterfallende Fallgestaltungen (lediglich) hervorheben. Sie beschränken hingegen das bereits aus § 52 Abs. 1 Satz 1 PersVG HB folgende umfassende Mitbestimmungsrecht nicht (so auch: Altvater, in: Altvater/Baden/Berg/Kröll/Noll/Seulen, BPersVG, 9. Aufl. 2016, § 104 Rn. 7; Dannenberg, in: Arbeitnehmerkammer Bremen <Hrsg.>, Gemeinschaftskommentar zum BremPersVG, 2016, § 65 Rn. 30; Fischer/Goeres/Gronimus,

GKÖD, Band V, Stand März 2018, K § 75 Rn. 120; Oetjens, in: Arbeitnehmerkammer Bremen <Hrsg.>, Gemeinschaftskommentar zum BremPersVG, 2016, § 63 Rn. 24; Rust, in: Arbeitnehmerkammer Bremen <Hrsg.>, Gemeinschaftskommentar zum BremPersVG, 2016, § 52 Rn. 135).

Dem steht die Rechtsprechung des Bundesverfassungsgerichts nicht entgegen. Soweit dieses aufgezeigt hat, dass das Wort „insbesondere" vor den beispielhaften Aufzählungen der Mitbestimmungstatbestände die Richtung der möglichen Gegenstände der Beschlussfassung andeutet (BVerfG, Urteil vom 27. April 1959 – 2 BvF 2/58 – BVerfGE 9, 268 <289>), kann dem nicht entnommen werden, dass die Katalogtatbestände das Mitbestimmungsrecht nach § 52 Abs. 1 Satz 1 PersVG HB beschränken (a.A. BVerwG, Beschluss vom 17. Juli 1987 – 6 P 13.85 – Buchholz 251.3 § 66 BrPersVG Nr. 1 S. 1 <3 f.>). Die Erwägung des Bundesverfassungsgerichts bezieht sich ausschließlich auf die Abgrenzung der innerdienstlichen von den außerdienstlichen Angelegenheiten und nicht auch auf die Frage einer Einschränkung des Mitbestimmungsrechts nach § 52 Abs. 1 Satz 1 PersVG HB.

c) Sinn und Zweck des § 52 Abs. 1 Satz 1 PersVG HB stützen das bisherige Auslegungsergebnis. Die Bestimmung ist Ausdruck einer „radikal personalvertretungsfreundlichen Konzeption" (vgl. BVerwG, Beschluss vom 30. Oktober 1964 – 7 P 2.64 – BVerwGE 19, 359 <360>; Großmann/Mönch/Rohr, Bremisches Personalvertretungsgesetz, 1979, § 52 Rn. 1 und § 63 Rn. 7) und verfolgt insbesondere den Zweck, mitbestimmungsfreie Räume in innerdienstlichen Angelegenheiten weitgehend zu vermeiden. Damit stände entgegen der Auffassung des Beteiligten auch nicht im Einklang, das Mitbestimmungsrecht aus Gründen der Praktikabilität sowie den Erfordernissen einer effektiven und modernen Verwaltung zu beschränken.

d) Die Gesetzgebungsgeschichte unterstützt ebenfalls die Auslegung, dass § 52 Abs. 1 Satz 1 PersVG HB dem Personalrat ein umfassendes Mitbestimmungsrecht bei allen innerdienstlichen Maßnahmen des Dienstherrn einräumt, das die Beispielskataloge in den § 63 Abs. 1, § 65 Abs. 1 und § 66 Abs. 1 PersVG HB nicht einschränken. Die Unberührtheitsklausel in den § 63 Abs. 2, § 65 Abs. 3 und § 66 Abs. 3 PersVG HB wurde durch das Bremische Personalvertretungsgesetz vom 5. März 1974 (Brem. GBl. S. 131) angefügt. Anlass dafür war eine Gesetzesinitiative der CDU-Fraktion in der Bremischen Bürgerschaft, die neben anderen Reformen des geltenden Personalvertretungsgesetzes die Streichung des Wortes „insbesondere" in dem Katalog über die Mitbestimmung in personellen Angelegenheiten in § 65 Abs. 1 PersVG HB bei gleichzeitiger Erweiterung der Katalogtatbestände zum Ziel hatte (vgl. Bürgerschafts-Drs. 8/545). Dieser Vorschlag fand nicht nur keine Mehrheit, sondern der bremische Gesetzgeber hob die Allzuständigkeit des Personalrats durch eine Gesetzesänderung in zweifacher Weise hervor: Erstens wurde in den amtlichen Überschriften der §§ 63, 65 und 66 PersVG HB jeweils das Wort „Beispiele" eingefügt, womit das ebenfalls das Beispielhafte zum Ausdruck bringende „insbesondere" in den ersten Absätzen noch einmal bekräftigt wurde, zweitens wurde den Beispielskatalogen die Unberührtheitsklausel angefügt (vgl. Bürgerschafts-Drs. 8/644 und Bürgerschafts-Drs. 8/848 Anhang 1, Anlage Nr. 9). Es kann hier offenbleiben, ob diese Rechtsänderung die bisherige Rechtslage lediglich klarstellte oder ob sie darüber hinaus sogar eine Ausweitung der Mitbestimmung beinhaltete. Eindeutig ist jedenfalls, dass der Gesetzgeber die Allzuständigkeit des Personalrats gestärkt hat, indem er ihre Unabhängigkeit vom Inhalt der Beispielskataloge ausdrücklich betont und damit deutlich zum Ausdruck gebracht hat, dass er diese nicht als Eingrenzung der Allzuständigkeit verstanden wissen wollte.

Dienstliches Gespräch als äußere Einwirkung im Sinne des Dienstunfallrechts (Ls)

(Bundesverwaltungsgericht, Beschluss vom 11. Oktober 2018 – 2 B 3.18 –)

Auch nicht-körperliche Einwirkungen können äußere Einwirkungen im Sinne des Dienstunfallrechts (z.B. § 31 Abs. 1 Satz 1 BeamtVG) sein; dies gilt auch für dienstliche Gespräche (hier: über ein außerdienstliches Verhalten des Beamten mit der Ankündigung einer disziplinarrechtlichen Prüfung). Bei Letzteren ist allerdings Voraussetzung, dass während des Dienstgesprächs durch dessen Verlauf, durch die Art der Äußerungen (z.B. aggressives Anbrüllen) oder durch deren Inhalt (z.B. Beleidigungen, Beschimpfungen) der Rahmen der Sozialadäquanz überschritten wird. Ein im Rahmen des „Normalen" bleibendes Gespräch mit dienstrechtlichem Anlass genügt nicht (im Anschluss an BVerwG, Urteil vom 9. April 1970 – 2 C 49.68 – BVerwGE 35, 133 <134 f.>).

Auskunftsanspruch hinsichtlich einer aus öffentlichen Mitteln finanzierten Verwandtenbeschäftigung

(Bundesverwaltungsgericht, Urteil vom 27. September 2018 – 7 C 5.17 –)

1. **Ist die Entscheidung zur Zulässigkeit der Übermittlung von personenbezogenen Daten in den privaten Bereich dem Grunde nach durch den Gesetzgeber getroffen worden, steht einer Übertragung der in Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO formulierten materiellen Anforderungen zur gebotenen inhaltlichen Ausformung der Datenverarbeitung nichts entgegen.**

2. **Bei einem presserechtlichen Auskunftsanspruch ist – in gleicher Weise wie bei Unterlassungsansprüchen gegen Presseveröffentlichungen – bei der Schutzbedürftigkeit und Schutzwürdigkeit personenbezogener Daten danach zu unterscheiden, ob die Intim-, die Privat- oder die Sozialsphäre betroffen ist.**

3. **Im Fall einer aus öffentlichen Mitteln finanzierten Verwandtenbeschäftigung im häuslichen Bereich eines Abgeordneten überwiegt das Informationsinteresse der Presse, die Höhe der gezahlten Bruttovergütung zu erfahren, die schutzwürdigen Belange des Abgeordneten und der von ihm beschäftigten Verwandten.**

Sachverhalt:

Der Kläger, Journalist bei einer Tageszeitung, macht einen presserechtlichen Auskunftsanspruch gegenüber dem Landtagsamt des Beklagten geltend.

Mit Bescheid vom 12. September 2013 lehnte die Präsidentin des Bayerischen Landtags den Antrag des Klägers ab, ihm Auskunft über das von dem Beigeladenen zu 1 als Landtagsabgeordneten an die Beigeladene zu 2, seine Ehefrau, für ihre Tätigkeit als Sekretärin im häuslichen Abgeordnetenbüro gezahlte Bruttogehalt in der Zeit zwischen 1995 und 2013 zu erteilen. Diese Kosten wurden vom Landtag nach Maßgabe des Bayerischen Abgeordnetengesetzes erstattet.

Auf die hiergegen erhobene Klage verurteilte das Verwaltungsgericht den Beklagten, dem Kläger Auskunft darüber zu erteilen, welche jährliche Bruttovergütung der Beigeladene zu 1 für die Beschäftigung der Beigeladenen zu 2 als Sekretärin im häuslichen Abgeordnetenbüro des Beigeladenen zu 1 zwischen 2000 und dem 30. September 2013 geltend gemacht hat.

Auf die Berufung des Beklagten hat der Verwaltungsgerichtshof das Urteil des Verwaltungsgerichts geändert und die Klage abgewiesen.

Aus den Gründen:

Die zulässige Revision des Klägers ist begründet. Das Berufungsurteil beruht auf einer Verletzung von Bundesrecht (§ 137 Abs. 1 Nr. 1 VwGO). Der Verwaltungsgerichtshof hat den geltend gemachten presserechtlichen Auskunftsanspruch unter Verstoß gegen Art. 5 Abs. 1 Satz 2 GG verneint (1.). Auf der Grundlage der tatsächlichen Feststellung des Verwaltungsgerichtshofs kann der Senat in der Sache selbst entscheiden und die Berufung gegen das stattgebende Urteil des Verwaltungsgerichts zurückweisen (§ 144 Abs. 3 Satz 1 Nr. 1 VwGO; 2.).

1. Die Auslegung und Anwendung des landesrechtlichen Presseauskunftsanspruchs durch den Verwaltungsgerichtshof ist einer revisionsgerichtlichen Prüfung zugänglich (a). Die Ablehnung des Anspruchs ist nicht mit Bundesrecht vereinbar (b).

a) Der Verwaltungsgerichtshof hat über den geltend gemachten Anspruch nach Art. 4 Bayerisches Pressegesetz (BayPrG) in der Fassung der Bekanntmachung vom 19. April 2000 (GVBl 2000, 340) in Anwendung revisiblen Rechts entschieden.

Ein Instanzgericht wendet revisibles Recht auch insoweit an, als es sich bei der Auslegung und Anwendung irrevisiblen Rechts durch revisibles Recht gebunden sieht (stRspr; vgl. etwa BVerwG, Urteile vom 16. Januar 2003 – 4 CN 8.01 – BVerwGE 117, 313 <317> und vom 1. Oktober 2014 – 6 C 35.13 – Buchholz 11 Art. 5 Abs. 1 GG Nr. 3 Rn. 20). Der Kläger stützt seinen presserechtlichen Auskunftsanspruch auf Art. 4 Abs. 1 BayPrG, wonach die Presse gegenüber Behörden ein Auskunftsrecht hat, das sie unter anderem durch ihre Redakteure ausüben kann. Der Verwaltungsgerichtshof hat die Annahme einer dem Anspruch entgegenstehenden, aufgrund beamtenrechtlicher oder sonstiger gesetzlicher Vorschriften bestehenden Verschwiegenheitspflicht (Art. 4 Abs. 2 Satz 2 BayPrG) dahingehend begründet, dass die verfassungsrechtlich geschützten Persönlichkeitsrechte der Beigeladenen (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) das durch Art. 5 Abs. 1 Satz 2 GG geschützte Auskunftsinteresse des Klägers überwögen. Insoweit beruht die Anwendung der irrevisiblen Vorschrift des Art. 4 BayPrG auf einer bestimmten Gewichtung und Abwägung nach Maßgabe revisiblen Rechts.

b) Die Auslegung und Anwendung von Art. 4 BayPrG durch den Verwaltungsgerichtshof ist nicht mit dem verfassungsrechtlichen Schutz der Presse aus Art. 5 Abs. 1 Satz 2 GG vereinbar.

aa) Nach Art. 4 Abs. 2 Satz 2 BayPrG darf der Presseauskunftsanspruch nur verweigert werden, soweit aufgrund beamtenrechtlicher oder sonstiger gesetzlicher Vorschriften eine Verschwiegenheitspflicht besteht. Bundesrechtlich nicht zu beanstanden ist der Ansatz des Verwaltungsgerichtshofs, wonach sich Verschwiegenheitspflichten im Sinne von Art. 4 Abs. 2 Satz 2 BayPrG aus Grundrechten Dritter, hier dem Recht der Beigeladenen, auf informationelle Selbstbestimmung ergeben können und in diesem Fall eine Abwägung des verfassungsrechtlich geschützten Interesses der Presse mit dem Interesse der Beigeladenen vorzunehmen ist (UA S. 5). Dies entspricht dem für den in Art. 5 Abs. 1 Satz 2 GG verbürgten verfassungsunmittelbaren presserechtlichen Auskunftsanspruch geltenden Maßstab, wonach ein solcher Anspruch besteht, soweit ihm berechtigte schutzwürdige Interessen privater oder öffentlicher Stellen an der Vertraulichkeit der Information nicht entgegenstehen (vgl. BVerwG, Urteil vom 16. März 2016 – 6 C 65.14 – BVerwGE 154, 222 Rn. 16 m.w.N.). Dabei sind die widerstreitenden Grundrechtspositionen in einen angemessenen Ausgleich zu bringen; im Wege praktischer Konkordanz ist jeweils abzuwägen, ob dem Informationsinteresse der Presse aufgrund der Pressefreiheit oder einem schützenswerten Interesse betroffener Dritter der Vorzug zu geben ist. (BVerfG, Kammerbeschluss vom 28. August 2000 – 1 BvR 1307/91 – NJW 2001, 503 <505>).

bb) Gleichfalls nicht zu beanstanden ist die Auffassung des Verwaltungsgerichtshofs, dass eine Abwägung nur dann eröffnet ist, wenn der mit der Weitergabe personenbezogener Daten verbundene Eingriff in das Grundrecht auf informationelle Selbstbestimmung sich auf eine bereichsspezifische Ermächtigungsgrundlage stützen kann, die insbesondere den Anforderungen an die Normenklarheit genügt (BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 u.a. – BVerfGE 65, 1<44>; BVerwG, Urteil vom 15. Januar 2012 – 6 C 9.11 – BVerwGE 141, 329 Rn. 27).

Der Verwaltungsgerichtshof nimmt insoweit nur die Offenbarungspflichten nach dem Gesetz über die Rechtsverhältnisse der Mitglieder des Bayerischen Landtags (Bayerisches Abgeordnetengesetz – BayAbgG) in der Fassung der Bekanntmachung vom 6. März 1996 (GVBl S. 82), zuletzt geändert durch Gesetz vom 24. April 2017, in den Blick. Die dem zugrunde liegende Rechtsauffassung, dass damit die Offenlegung mandatsbezogener Informationen grundsätzlich abschließend geregelt werde, und der daraus folgende absolute Schutz der von diesen Vorschriften nicht erfassten Informationen verfehlt die Anforderungen des Art. 5 Abs. 1 Satz 2 GG.

(1) Nach Art. 4a Abs. 3 BayAbgG in Verbindung mit den vom Landtag erlassenen Verhaltensregeln ist der Abgeordnete zur Anzeige und Veröffentlichung bestimmter persönlicher Verhältnisse, etwa Art und Höhe bestimmter Einkünfte, verpflichtet. Der Verwaltungsgerichtshof weist zwar zutreffend darauf hin, dass die Regelungen über die Erstattung der Kosten für Arbeits-, Dienst- und Werkverträge zur Unterstützung der parlamentarischen Tätigkeit des Abgeordneten eine Offenlegung der Sachverhalte nicht vorsehen und durch die Festlegungen im Haushaltsgesetz lediglich die Erstattungshöchstbeträge öffentlich bekannt sind. Ob dies im Gegenschluss die Annahme rechtfertigt, insoweit scheide eine weitere mandatsbezogene Transparenz aus, erscheint zweifelhaft. Denn Art. 4a Abs. 3 BayAbgG zielt auf die Offenlegung von Umständen, die auf mögliche Interessenverflechtungen und wirtschaftliche Abhängigkeiten und damit auf eine Gefährdung der Unabhängigkeit des Abgeordne-

ten durch Loyalitätskonflikte sowie eine Beeinträchtigung der Repräsentations- und Funktionsfähigkeit des Landtags schließen lassen (vgl. BVerfG, Urteil vom 4. Juli 2007 – 2 BvE 1-4/06 – BVerfGE 118, 277 <352 ff.>), während es vorliegend um die sachangemessene Verwendung öffentlicher Gelder geht. An die Auslegung des Landesrechts durch den Verwaltungsgerichtshof ist der Senat indessen nicht gebunden; ihr steht Art. 5 Abs. 1 Satz 2 GG entgegen.

Der verfassungsrechtlich gewährleistete Vermittlungs- und Kontrollauftrag der Presse gebietet, dass – von einzelnen behördlichen Funktionsbereichen besonderen Charakters abgesehen – die dem Auskunftsanspruch entgegenstehenden Ausschlussgründe einen punktuellen Zuschnitt aufweisen, mit dem konkret umrissenen gegenläufigen Schutzgütern Rechnung getragen wird, und zwar beschränkt auf das Maß, in dem bei materieller Betrachtung tatsächlich ein Schutzbedarf erkennbar ist. Ungeachtet seiner rechtlichen Verortung darf ein genereller, abwägungsfester Vorrang eines privaten oder öffentlichen Vertraulichkeitsinteresses vor dem Informationsinteresse der Presse nur dann normiert werden, wenn dies demjenigen Abwägungsergebnis entspricht, das in aller Regel in Einzelfällen tatsächlich erzielt würde (vgl. BVerwG, Urteil vom 25. März 2015 – 6 C 12.14 – BVerwGE 151, 348 Rn. 30). Angesichts des Doppelstatus des Abgeordneten als Mandatsträger und Privatperson darf das Abgeordnetengesetz zwar sowohl der Freiheit des Mandats als auch den persönlichen Belangen des Abgeordneten als Schutzgütern Rechnung tragen. Dass insbesondere bei den individuellen Interessen des Abgeordneten ein Schutzbedarf anzunehmen ist, der sich generalisierend gegenüber dem Informationsinteresse der Presse sollte durchsetzen können, ist aber weder dargetan noch sonst ersichtlich.

(2) Ausgehend von seiner Rechtsauffassung verschließt sich der Verwaltungsgerichtshof der Heranziehung weiterer Rechtsvorschriften, die den Anforderungen für einen Eingriff in das informationelle Selbstbestimmungsrecht genügen und deswegen Grundlage einer umfassenden Abwägung sein können.

Eine solche Vorschrift findet sich zwar weder allein im presserechtlichen Normbestand, wovon der Verwaltungsgerichtshof zu Recht ausgeht, noch in Gestalt einer eigenständigen Rechtsgrundlage in den datenschutzrechtlichen Bestimmungen. Die presserechtliche Anspruchsgrundlage ist jedoch insoweit um datenschutzrechtliche Vorgaben zu ergänzen.

(2.1) Art. 4 Abs. 2 BayPrG ist insoweit unzureichend. Denn im Unterschied zu anderen in den Landespressegesetzen geregelten Auskunftsansprüchen werden die schutzwürdigen Interessen der betroffenen Dritten nicht einmal erwähnt; ein Bezug auf diese Schutzgüter wird allein über die dort benannten Verschwiegenheitspflichten hergestellt, ohne dies zu konkretisieren (vgl. Hornung, AfP 2017, 390 <393>; Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand September 2003, Art. 19 BayDSG Rn. 11a).

(2.2) Diese Lücke wird nicht (mehr) durch eine datenschutzrechtliche Rechtsgrundlage ausgefüllt.

Maßgeblich ist die Rechtslage nach Inkrafttreten der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Warenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DS-GVO; ABl. L 119 S. 1) und der hierauf bezogenen Anpassung des nationalen Rechts durch die Neufassung des Bayerischen Datenschutzgesetzes (BayDSG) vom 15. Mai 2018 (GVBl S. 230). Diese Rechtsänderung ist im Revisionsverfahren zu beachten, denn das Berufungsgericht, entschiede es anstelle des Revisionsgerichts, hätte sie seinerseits zu berücksichtigen (BVerwG, Urteil vom 28. Juli 2016 – 7 C 7.14 – Buchholz 451.91 Europ. UmweltR Nr. 65 Rn. 14 m.w.N.). Für den im Wege der allgemeinen Leistungsklage geltend gemachten Auskunftsanspruch ist mangels abweichender Regelungen die Rechtslage im Zeitpunkt der gerichtlichen Entscheidung maßgeblich.

Nach Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG ist eine Übermittlung personenbezogener Daten zulässig, wenn der Empfänger eine nicht öffentliche Stelle ist, diese Stelle ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat; dies gilt auch, soweit die Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben wurden, übermittelt werden. Diese Vorschrift, die nach Art. 1 Abs. 1 Satz 1 BayDSG insbesondere das behördliche Handeln regelt und nach Art. 2 BayDSG auch außerhalb des Anwendungsbereiches der Datenschutz-Grundverordnung – d.h. auch bei nicht automatisierter Verarbeitung der Daten und außerhalb einer Tätigkeit im Anwendungsbereich des Unionsrechts – an deren Vorgaben zu messen ist (siehe Bayerischer Landtag, Drs. 17/19628 S. 32), ist allerdings keine taugliche Rechtsgrundlage. Mit ihrem 1. Halbsatz tritt die Vorschrift zwar an die Stelle des im Wesentlichen gleichlautenden Art. 19 Abs. 1 Nr. 2 BayDSG a.F., der ebenso wie die vergleichbare Bestimmung des § 16 Abs. 1 Nr. 2 BDSG a.F. als Grundlage für Auskünfte an die Presse angesehen worden ist (vgl. Wilde/Ehmann/Niese/Knoblauch, a.a.O., Art. 19 BayDSG Rn. 11a, 14 f.; Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 16 Rn. 10; siehe auch Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 16 Rn. 13, 15). Vor dem Hintergrund der Änderungen im Unionsrecht kann die bisherige Rechtslage jedoch nicht fortgeschrieben werden (so aber etwa auch die Begründung des Gesetzentwurfs zur Parallelvorschrift in § 25 Abs. 2 Nr. 2 BDSG, BT-Drs. 18/11352 S. 96).

Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG ist mit der Datenschutz-Grundverordnung nicht vereinbar. Die Datenschutz-Grundverordnung gilt gemäß Art. 288 Abs. 2 AEUV unmittelbar. Sie ist grundsätzlich weder auf eine Umsetzung angewiesen, noch ist dies überhaupt zulässig; selbst eine Normwiederholung im nationalen Recht ist dem Grunde nach ausgeschlossen. Nur im Rahmen ausdrücklicher Ermächtigungen können ihre Regelungen vom nationalen Gesetzgeber spezifiziert, präzisiert und konkretisiert werden (siehe Selmayr/Ehmann, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung Rn. 80 ff. sowie die Erläuterungen in BT-Drs. 18/11325 S. 73 f.). Nach dem Hinweis in der amtlichen Überschrift findet Art. 5 BayDSG seine Rechtfertigung in Art. 6 Abs. 2 bis 4 DS-GVO, soweit dem nationalen Gesetzgeber darin Regelungsspielräume eingeräumt werden. Jedenfalls auf Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG trifft dies nicht zu.

Auf die Öffnungsklausel in Art. 6 Abs. 2 und 3 DS-GVO kann diese Norm schon deswegen nicht gestützt werden, weil danach nur eine Konkretisierung der Regelungen von Art. 6 Abs. 1 Unterabs. 1 Buchst. c und e DS-GVO erlaubt ist, während die landesrechtliche Bestimmung an Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO anknüpft. Als Norm, die die Reichweite dieses Erlaubnistatbestands klarstellend verdeutlicht und deswegen nach Maßgabe von Erwägungsgrund 8 zur DS-GVO, d.h. wegen der Kohärenz und Verständlichkeit der Regelung, mit dem grund-

sätzlichen Normwiederholungsverbot ausnahmsweise vereinbar ist (so Wilde/Ehmann/Niese/Knoblauch, a.a.O., Art. 5 BayDSG Rn. 15 f.), kann die Vorschrift ebenso wenig Bestand haben. Denn im Unterschied zur Vorgängervorschrift des Art. 7 Buchst. f der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr – Datenschutz-Richtlinie – (ABl. L 281 S. 31) gilt Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO nach Unterabs. 2 nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Eine Unterscheidung nach „eigennützigen" und „fremdnützigen" Aufgaben ist nicht möglich. Erfasst sind vielmehr die durch Gesetz übertragenen Aufgaben im Rahmen der Eingriffs- und Leistungsverwaltung. Damit fällt jegliche Datenverarbeitung in Erfüllung hoheitlicher Funktionen, wozu auch die Beantwortung von Presseanfragen zählt, unter den Ausschlusstatbestand und ist den Erlaubnistatbeständen nach Art. 6 Abs. 1 Unterabs. 1 Buchst. c und e DS-GVO zuzuordnen. Denn die hoheitliche behördliche Tätigkeit ist ausweislich von Erwägungsgrund 47 Satz 5 immer auf eine gesonderte Ermächtigungsgrundlage angewiesen. Dieses Erfordernis kann nicht durch einen umfassenden Auffangtatbestand überspielt werden. Demgegenüber ist der Erlaubnistatbestand des Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO einschlägig, wenn die Behörde als Teilnehmer im Privatrechtsverkehr auftritt (Albers/Veit, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand 1. Mai 2018, Art. 6 DS-GVO Rn. 46; Heberlein, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 51 f.; Schulz, in: Gola, Datenschutz-Grundverordnung, Art. 6 DS-GVO Rn. 56; Frenzel, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 6 Rn. 26).

Auch Art. 6 Abs. 4 DS-GVO ermöglicht dem nationalen Gesetzgeber nicht, den Erlaubnistatbestand des Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO hinsichtlich seines persönlichen Geltungsbereichs zu erweitern. Es ist bereits nicht ersichtlich, dass der Landesgesetzgeber von einem solchen Verständnis des Art. 6 Abs. 4 DS-GVO ausgegangen ist. Die Begründung des Gesetzentwurfs verweist insofern auf eine Ergänzung der spezifischen Zweckänderungserlaubnisse in Art. 5 Abs. 1 Satz 1 Nr. 2 Halbs. 2 BayDSG (Bayerischer Landtag, Drs. 17/19628 S. 34), die sich an Art. 6 Abs. 4 DS-GVO messen lassen müssen. Auch bei der bundesrechtlichen Parallelvorschrift des § 25 Abs. 2 Nr. 2 BDSG fehlt in der Begründung des Gesetzentwurfs – im Unterschied zu §§ 23 und 24 BDSG – ein entsprechender Hinweis (BT-Drs. 18/11325 S. 95 f.; anders die ausdrückliche Bezugnahme auf Art. 6 Abs. 4 DS-GVO in der Begründung des Gesetzentwurfs zur gleichlautenden Vorschrift des § 22 Abs. 2 Nr. 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vom 3. Mai 2018 <GVBl. S. 82>, LT-Drs. 19/5726 S. 127 f.). Jedenfalls ist Art. 6 Abs. 4 DS-GVO keine neben Art. 6 Abs. 2 und 3 DS-GVO stehende übergreifende Öffnungsklausel; er bezieht sich vielmehr allein auf die Zweckänderungsbefugnis im Rahmen der nach Art. 6 Abs. 1 DS-GVO nach Maßgabe von Art. 6 Abs. 2 und 3 DS-GVO zulässigen Datenverarbeitung (vgl. Albers/Veit, a.a.O., Art. 6 DS-GVO Rn. 71 f., 77; Heberlein, a.a.O., Art. 6 DS-GVO Rn. 48; Reimer, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 67; Buchner/Petri, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 182 f., 199 f.; siehe aber auch Schulz, a.a.O., Art. 6 DS-GVO Rn. 216, 239 ff.).

(2.3) Scheiden hiernach Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG und in gleicher Weise die vorrangige Bestimmung des Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO als eigenständige Rechtsgrundlage für die Übermittlung personenbezogener Daten im Rahmen eines presserechtlichen Auskunftsanspruchs aus, kann letztere gleichwohl zur inhaltlichen Ausfüllung und Konkretisierung dieses Anspruchs herangezogen werden, der dann den Anforderungen des Gesetzesvorbehalts für einen Eingriff in das Recht auf informationelle Selbstbestimmung genügt. Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO ist, wie dargelegt, auf behördliche Tätigkeiten nicht anwendbar, weil die Übermittlung von personenbezogenen Daten in den privaten und folglich weniger kontrollierten Bereich einer ausdrücklichen gesetzlichen Entscheidung bedarf. Ist diese Entscheidung allerdings dem Grunde nach durch den Gesetzgeber getroffen worden, steht einer Übertragung der dort formulierten materiellen Anforderungen zur gebotenen inhaltlichen Ausformung der Datenverarbeitung, die grundlegenden datenschutzrechtlichen Anforderungen genügt, nichts entgegen.

2. Die auf dieser Grundlage eröffnete umfassende Abwägung der widerstreitenden Interessen fällt zugunsten des Auskunftsanspruchs des Klägers aus, so dass das erstinstanzliche Urteil wiederherzustellen ist (§ 144 Abs. 3 Satz 1 Nr. 1 VwGO).

a) Der Kläger hat unter Berufung auf seine Tätigkeit als Journalist und die Berichterstattung über die sogenannte Verwandtenaffäre im Zusammenhang mit der Beschäftigung von Familienangehörigen durch Landtagsabgeordnete ein berechtigtes Interesse an der Informationsübermittlung dargelegt. Mit Blick auf die Garantie der institutionellen Eigenständigkeit der Presse (BVerfG, Urteil vom 5. August 1966 – 1 BvR 586/62 u.a. – BVerfGE 20, 162 <175 f.>; BVerwG, Urteil vom 13. Dezember 1984 – 7 C 139.81 – BVerwGE 70, 310 <311>) und das Verbot einer publizistischen Relevanzprüfung (vgl. BVerwG, Urteil vom 16. März 2016 – 6 C 65.14 – BVerwGE 154, 222 Rn. 18) ist mehr nicht zu fordern. Insbesondere ist unbeachtlich, ob der Kläger bereits jetzt Anhaltspunkte für eine missbräuchliche Inanspruchnahme der Kostenerstattung durch den Beigeladenen zu 1 aufzeigen kann. Das ist der journalistischen Bewertung nach der begehrten Auskunftserteilung vorbehalten.

Nichts Abweichendes ergibt sich aus dem Hinweis des Beklagten auf das Urteil des Europäischen Gerichts vom 25. September 2018 – T-639/15 u.a. [ECLI:EU:T:2018:602], Psara/Parlament. Die dortigen Ausführungen zu den engen Voraussetzungen, unter denen eine Herausgabe personenbezogener Daten von Abgeordneten des Europäischen Parlaments in Betracht kommt (Rn. 52 ff., 71 ff.), beziehen sich auf eine andere Rechtslage. Das Erfordernis des Nachweises der Notwendigkeit der Übermittlung personenbezogener Daten ergibt sich ausdrücklich aus Art. 8 Buchst. b der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr – EU-DatenschutzVO – (ABl. 2001, L 8 S. 1), der bei der Prüfung eines Antrags auf Informationszugang auf der Grundlage der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission – TransparenzVO – (ABl. L 145 S. 43) bei dem absoluten Ablehnungsgrund nach deren Art. 4 Abs. 1 Buchst. b (Schutz der Privatsphäre und der Integrität des Einzelnen) heranzuziehen und in vollem Umfang anwendbar ist (EuGH, Urteile vom 29. Juni 2010 – C-28/08 P [ECLI:EU:C:2010:378], Bavarian Lager – Rn. 63 ff., 77 und vom 16. Juli 2015 – C-615/13 P [ECLI:EU:C:2015:

489], Client Earth u.a. – Rn. 44 ff.). Ansatzpunkte für eine Übertragbarkeit der dortigen Erwägungen ergeben sich nicht daraus, dass das Erfordernis der Notwendigkeit als Ausdruck des Verhältnismäßigkeitsgrundsatzes verstanden wird (EuG, Urteil vom 25. September 2018 – T-639/15 u.a. – Rn. 72), der auch in anderen unionsrechtlich determinierten Regelungszusammenhängen zu beachten ist. Soweit die Verhältnismäßigkeitsprüfung nach der EU-DatenschutzVO auch eine Prüfung des mit der Datenübermittlung verfolgten Ziels umfasst und damit den Ansatz der TransparenzVO jedenfalls ergänzt, wird dem im Rahmen von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO durch das Erfordernis eines berechtigten Interesses Rechnung getragen. Im Übrigen findet der Verhältnismäßigkeitsgrundsatz in Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO seinen Niederschlag in der Regelung, dass die Datenübermittlung erforderlich sein muss. Danach müssen sich die Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige beschränken (EuGH, Urteil vom 4. Mai 2017 – C-13/16 [ECLI:EU:C:2017:336], Rigas satiksme – Rn. 30 m.w.N.; siehe auch Erwägungsgrund 39 zur DS-GVO). Dem ist hier Genüge getan; denn das journalistische Aufklärungsinteresse ist zwingend auf die begehrten Auskünfte zu den gezahlten und erstatteten Bruttogehältern angewiesen; ein milderes Mittel zur Interessenwahrung gibt es nicht.

b) Demgegenüber ist das schutzwürdige Interesse der Beigeladenen am Ausschluss der Datenübermittlung geringer zu bewerten.

Bei einem presserechtlichen Auskunftsanspruch ist – in gleicher Weise wie bei Unterlassungsansprüchen gegen Presseveröffentlichungen – bei der Schutzbedürftigkeit und Schutzwürdigkeit personenbezogener Daten danach zu unterscheiden, ob die Intim-, die Privat- oder die Sozialsphäre betroffen ist (vgl. etwa OVG Berlin-Brandenburg, Beschluss vom 28. Oktober 2011 – 10 S 33/11 – NVwZ-RR 2012, 107 Rn. 25; Hornung, AfP 2017, 390 <994 f.>; Gersdorf, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, Stand 1. Mai 2017, GG Art. 2 Rn. 42 ff.). In Konkretisierung des Verhältnismäßigkeitsgrundsatzes dient diese Unterscheidung als Orientierungspunkt für die Beurteilung der Intensität der Grundrechtsbeeinträchtigung und für die Gewichtung der diese Beeinträchtigung rechtfertigenden Gründe (BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 – BVerfGE 65, 1 <45>). Eingriffe in die Sozialsphäre sind unter erleichterten Voraussetzungen zulässig, so dass der Persönlichkeitsschutz weniger weit reicht als in den Fällen der Betroffenheit der Intim- und Privatsphäre (vgl. BVerfG, Kammerbeschlüsse vom 7. Mai 1997 – 1 BvR 1974/93, 1 BvR 1987/93 – NJW 1997, 2669 <2700> und vom 21. August 2006 – 1 BvR 2606/04 u.a. – NJW 2006, 3406 <3408>).

Die Angaben zu dem vom Beigeladenen zu 1 an die Beigeladene zu 2 für die Beschäftigung im häuslichen Abgeordnetenbüro gezahlten Bruttogehalt sind der Sozialsphäre zuzurechnen. Diese umfasst die gesamte Teilnahme am öffentlichen Leben, also die Gegebenheiten, in denen der Einzelne in Kontakt mit anderen tritt.

Auch wenn öffentliche Stellen am betreffenden Arbeitsverhältnis nicht beteiligt sind und es folglich nicht dem öffentlichen Dienst zuzuordnen ist, haben die Angaben als Grundlage für eine Kostenerstattung aus Steuermitteln einen gesteigerten Öffentlichkeitsbezug. Die Schutzwürdigkeit personenbezogener Daten entfällt zwar nicht allein deswegen, weil Leistungen aus öffentlichen Kassen bezahlt und Aufwendungen daraus beglichen werden. Das Informationsinteresse überwiegt aber wegen der besonderen Umstände, die das Beschäftigungsverhältnis prägen. Die Vorgaben der Kostenerstattung an Abgeordnete für Arbeits-, Dienst- und Werkverträge in Art. 6 Abs. 7 BayAbG a.F., Art. 8 Abs. 1 BayAbgG n.F. zeichnen sich durch eine gegenüber der sonstigen Spesenverwendung aus öffentlichen Mitteln vergleichsweise freie Verfügbarkeit aus. Zu diesem Vertrauensvorschuss hinzu trat – unmittelbar oder aufgrund der sogenannten Altfallregelung – die Möglichkeit einer sogenannten Verwandtenbeschäftigung im häuslichen Bereich, die durch die Möglichkeit einer besonders vorteilhaften Ausgestaltung des Arbeitsvertrages und insbesondere der Bezahlung ein gewisses abstraktes Missbrauchspotenzial in sich trägt. Diese Missbrauchsanfälligkeit rechtfertigt ein Aufklärungsinteresse der Presse, die aufgrund der begehrten Auskünfte überprüfen kann, ob sich die Vergütung im Rahmen des Angemessenen bewegt. Dabei ist die Höhe der im Haushalt für die Kostenerstattung bereitgestellten Mittel nach der verbindlichen Wirkung der Erläuterungen zum Haushalt ein Indiz für die Angemessenheit der Beschäftigungsvergütung. Danach waren die Mittel mit einer Vollzeitstelle nach TVL Entgeltgruppe 6 für eine Büroarbeitskraft und eine 2/3-Stelle nach TVL Entgeltgruppe 13 für einen wissenschaftlichen Mitarbeiter bemessen (vgl. Bericht des Bayerischen Obersten Rechnungshofes vom 12. August 2013, S. 17).

Die Schutzwürdigkeit der Belange der Beigeladenen zu 2 ist nicht abweichend zu bewerten. Sie steht zwar nicht wie der Mandatsträger im Lichte der Öffentlichkeit. Sie ist jedoch ein Beschäftigungsverhältnis eingegangen, das – wie ausgeführt – Besonderheiten aufweist und insoweit keine „reine Privatangelegenheit“ darstellt, was die Schutzwürdigkeit darauf bezogener persönlicher Daten mindert. Die Finanzierung des Beschäftigungsverhältnisses aus öffentlichen Mitteln und der wegen der Orientierung der Erstattungsregelungen an den Kosten für eine Büroarbeitskraft und zusätzlich einen wissenschaftlichen Mitarbeiter bestehende Rechtfertigungsdruck führen auch bei ihr dazu, dass der Schutz ihres Persönlichkeitsrechts hinter der Pressefreiheit zurücktreten muss. Eine „Stigmatisierung“ der Beigeladenen zu 2 ist mit der Offenlegung der Bruttobezüge nicht verbunden. Sollten sich aus der Bewertung der Angemessenheit der Vergütung kritische Nachfragen ergeben, muss sie sich dem als Folge einer selbst gewählten Vertragsgestaltung stellen. Schließlich ist das Steuergeheimnis nicht betroffen, denn das Bruttogehalt lässt Rückschlüsse auf persönliche Steuermerkmale nicht zu.

Durch die Offenlegung der Daten wird auch die Freiheit des Abgeordnetenmandats des Beigeladenen zu 1 nicht verletzt. Die Inanspruchnahme von Leistungen für die Amtsausstattung berührt zwar nicht die politische Willensbildung im parlamentarischen Raum, die den Kern der Mandatsausübung bildet; sie ermöglicht aber die Ausübung des Mandats (vgl. zur Inanspruchnahme der Sachleistungspauschale für die Amtsausstattung nach § 12 Abs. 1 Satz 1 AbgG im Rahmen der Mandatsfreiheit nach Art. 38 Abs. 1 Satz 2 GG: BVerwG, Urteil vom 16. März 2016 – 6 C 65.14 – BVerwGE 154, 222 Rn. 22 f. m.w.N.), die grundsätzlich nicht durch störende Einflüsse beeinträchtigt werden soll. Auf den Schutz der Freiheit des Mandats kann sich der Beigeladene zu 1 auch nach dem Ausscheiden aus dem Landtag berufen. Es kommt insoweit nicht auf konkrete Nachwirkungen aus dem Mandatsverhältnis im Zeitpunkt der Erfüllung des Auskunftsanspruchs an; entscheidend sind vielmehr die „Vorwirkungen“ einer auch nachträglich drohenden Veröf-

fentlichung bestimmter Angaben. Der Abgeordnete soll sein Mandat grundsätzlich ungestört ausüben können, ohne eine spätere Offenlegung befürchten zu müssen. Die oben dargestellte landesrechtliche Ausgestaltung der Erstattung von Auslagen für Beschäftigungsverhältnisse, schränkt die Schutzwürdigkeit der Freiheit des Mandats jedoch ein. Anders als in dem dem Urteil vom 16. März 2016 – 6 C 65.14 – (a.a.O.) zugrunde liegenden Fall der allgemeinen Amtsausstattung für Schreibgeräte und Digitalkameras im Wege einer Sachleistungspauschale, gibt es im vorliegenden Fall konkrete an die Qualifikation der Mitarbeiter anknüpfende Vorgaben für die Angemessenheit der Beschäftigungsverhältnisse, die wegen des dadurch möglichen Fremdvergleichs die Schutzwürdigkeit der Freiheit des Mandats geringer erscheinen lassen.

Zur Haftung für nicht autorisierte Entscheidungen im Online-Banking (Ls)

(**Oberlandesgericht Schleswig,** Beschluss vom 29. Oktober 2018 – 5 U 290/18)

1. **Im Rahmen des § 675u BGB a.F. ist es bei einer nicht autorisierten Online-Überweisung Sache der Bank darzulegen und zu beweisen, dass es sich um ein außerhalb ihres Einflussbereichs liegendes und auch bei Anwendung der gebotenen Sorgfalt nicht vermeidbares Ereignis handelte.**
2. **Bei missbräuchlicher Verwendung von PIN und TAN im Online-Banking rechtfertigen allein die Aufzeichnungen der Nutzung eines Zahlungsauthentifizierungsinstruments und die Prüfung der Authentifizierung im Sinne von § 675b Satz 3 Nr. 4 BGB die Anwendung der Grundsätze des Anscheinsbeweises für eine grob fahrlässige Pflichtverletzung des Kunden nicht.**
3. **Auch ein Anscheinsbeweis auf alternativer Grundlage, der Zahlungsdienstnutzer habe entweder den Zahlungsvorgang autorisiert oder aber grob fahrlässig gegen seine Pflichten aus § 6751 BGB verstoßen, kommt sowohl nach der Auffassung des Schleswig-Holsteinischen Oberlandesgerichts als auch des Bundesgerichtshofs in seinem Urteil vom 26.01.2016 nicht in Betracht.**

Bekanntgabe der privaten Mobilfunknummer an den Arbeitgeber

(**Landesarbeitsgericht Thüringen,** Urteil vom 16. Mai 2018 – 6 Sa 442/17 –)

1. **Die Erhebung/Erfassung der privaten Mobiltelefonnummer eines Arbeitnehmers gegen seinen Willen ist wegen des darin liegenden äußerst schwerwiegenden Eingriffs in das allgemeine Persönlichkeitsrecht des Arbeitnehmers nur dann ausnahmsweise zulässig, wenn der Arbeitgeber ohne Kenntnis der Mobiltelefonnummer im Einzelfall eine legitime Aufgabe, für die der Arbeitnehmer eingestellt ist, nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und ihm eine andere Organisation der Aufgabenerfüllung nicht möglich oder nicht zumutbar ist.**
2. **Schafft ein kommunaler Arbeitgeber die Rufbereitschaft für Notfälle im Gesundheitsamt für die Dauer der Nachtzeit von 19:01 bis 5:59 Uhr aus Kostengründen ab, um im Notfall einen der Beschäftigten nach dem Zufallsprinzip ggf. auch über das Mobiltelefon aus seiner Freizeit heraus zur Arbeitsleistung heranzuziehen, wählt er damit eine risikobehaftete Arbeitsorganisation. Diese rechtfertigt nicht den in der Herausgabe der Mobiltelefonnummer liegenden Eingriff in die Persönlichkeitsrechte der Beschäftigten, denn grundsätzlich entscheidet jeder Arbeitnehmer selbst, für wen, wann und wo er durch Bekanntgabe der Mobiltelefonnummer erreichbar sein will.**
3. **Verweigert ein Arbeitnehmer die datenschutzrechtlich unzulässige Erfassung der Mobiltelefonnummer hat er einen Anspruch auf Rücknahme und Entfernung einer deshalb erteilten Abmahnung aus der Personalakte.**

Sachverhalt:

Die Parteien streiten über einen Anspruch des Klägers gegen den Beklagten auf Rücknahme und Entfernung einer Abmahnung aus der Personalakte.

Der Kläger war bei dem beklagten Landkreis als Sachbearbeiter Hygiene/Infektionsschutz im Gesundheitsamt beschäftigt.

Im Aufgabenbereich des Beklagten konnten bezogen auf die Hygiene/Infektionsschutz Gefährdungsanlagen entstehen, welche ein Tätigwerden auch außerhalb von Dienstzeiten erforderlich machen. Darunter waren katastrophenähnliche Szenarien wie der Ausbruch von hoch infektiösen Krankheiten zu verstehen. Auch bei auftretenden Problemen beim Trinkwasser oder mikrobiologischer Belastung von Wasser in Schwimmbädern und Badeseen waren Sofortmaßnahmen der Mitarbeiter im Bereich der Hygiene/Infektionsschutz vorgesehen.

Bis zum 31.12.2016 sicherte der Beklagte diese Maßnahmen dadurch ab, dass außerhalb der Dienstzeit eine Rufbereitschaft eingerichtet wurde. Für die erforderliche Kontaktaufnahme wurde ein Diensthandy zur Verfügung gestellt. Hierfür erhielten die Mitarbeiter, welche zur Rufbereitschaft eingeteilt waren, eine zusätzliche Vergütung in Form von Freizeitausgleich oder Geldzahlung.

Unter Berufung auf Grundsätze der Wirtschaftlichkeit und Sparsamkeit sowie aufgrund von Überlastungsanzeigen des Sachgebietes Hygiene/Infektionsschutz entschied sich der Beklagte, die Absicherung von notwendigen Tätigkeiten außerhalb angeordneter Arbeitszeiten oder Rufbereitschaftszeiten anders zu organisieren. Ab dem 1.1.2017 wurde Rufbereitschaft außerhalb der gewöhnlichen Dienstzeit beschränkt auf Samstage, Sonntag, Feiertage und so genannte Brückentage auf die Zeit von 7:00 Uhr bis 19:00 Uhr. Für diesen Zeitraum erhielten die im Voraus festgelegten Mitarbeiter jeweils nach wie vor ein Diensthandy. Außerhalb dieser Zeiten in der Zeit von 19:01 Uhr bis 6:59 Uhr sollte nach den Vorstellungen des Beklagten über die Rettungsleitstelle, versucht werden,

einen der sieben im Bereich Hygiene/Infektionsschutz beschäftigten Mitarbeiter auf irgend einem Wege zu kontaktieren. Dabei war es dem Zufall bzw. der Willkür des entsprechenden Mitarbeiters des Rettungsdienstzweckverbandes überlassen, zu welchem Mitarbeiter versucht wurde, Kontakt aufzunehmen. Zu diesem Zwecke verlangte der Beklagte von den Mitarbeiter die Mitteilung der Wohnanschrift, der privaten Festnetz- und auch der Mobiltelefonnummern, damit diese Kontaktaufnahme in Notfällen auch außerhalb jeglicher Dienstzeit und außerhalb vorher angeordneter Rufbereitschaftszeit möglich war.

Nach einigem vorgerichtlichen Streit über die Verpflichtung des Klägers, seine angeforderten Kontaktdaten herauszugeben, erteilte der Beklagte dem Kläger unter dem 24.5.2017 eine Abmahnung unter anderem deshalb, weil er seine Mobiltelefonnummer nicht innerhalb der geforderten Frist mitgeteilt habe.

Mit Urteil vom 12.10.2017 hat das Arbeitsgericht den Beklagten verurteilt, die Abmahnung vom 24.5.2017 zurückzunehmen und aus der Personalakte des Klägers zu entfernen. Der Anspruch auf Herausgabe der Mobilfunknummern bestehe nicht, weil kein Anspruch erkennbar sei, dass der Kläger außerhalb seiner Dienstzeit ständig rund um die Uhr für den Arbeitgeber zum Zwecke einer möglichen Arbeitsaufnahme erreichbar zu sein habe.

Gegen dieses ihm am 3.11.2017 zugestellte Urteil hat der Beklagte Berufung eingelegt.

Aus den Gründen:

Die Klage ist begründet. Der Kläger hat gegen den Beklagten einen Anspruch auf Entfernung der Abmahnung vom 24.5.2017 aus seiner Personalakte. Anspruchsgrundlage ist § 242 BGB i.V.m. § 1004 BGB analog.

Arbeitnehmer können in entsprechender Anwendung von §§ 242, 1004 Abs. 1 Satz 1 BGB die Entfernung einer zu Unrecht erteilten Abmahnung aus ihrer Personalakte verlangen. Der Anspruch besteht unter anderem, wenn die Abmahnung auf einer unzutreffenden rechtlichen Bewertung des Verhaltens des Arbeitnehmers beruht (st. Rechtspr. vgl. statt vieler BAG 9.9.2015, 7 ABR 69/13, AP News 2016, 5 Rn 39). Ist nur eine von mehreren in einer Abmahnung beanstandeten Verhaltensweisen zu Unrecht als Pflichtverstoß bewertet worden, ist die gesamte Abmahnung aus der Personalakte zu entfernen (BAG 13.3.1991 – 5 AZR 133/90, NZA 1991, 768).

So ist es hier, denn es fehlt hinsichtlich des auch in der Abmahnung enthaltenen Vorwurfs, seine Mobiltelefonnummer nicht an den Beklagten herausgegeben zu haben, an einer Verletzung von Pflichten aus dem Arbeitsvertrag durch den abgemahnten Kläger. Er war nicht verpflichtet, seine Mobiltelefonnummer dem Beklagten bekannt zu geben.

Es kann offenbleiben, ob der Beklagte einen Anspruch gegen den Kläger hat, diesen außerhalb der Arbeitszeit, außerhalb von Bereitschaftszeiten und außerhalb der (zum Teil abgeschafften) Rufbereitschaft zur Arbeitsleistung heranzuziehen, das ist hier nicht streitentscheidend. Die Kammer lässt auch offen, ob sich – das Bestehen eines solchen Anspruchs zu Gunsten der Beklagten unterstellt – hieraus abstrakt ein grundsätzlicher Anspruch auf Bekanntgabe der Mobiltelefonnummer ableiten lassen könnte, denn jedenfalls im hier zu entscheidenden Fall besteht dieser Anspruch konkret nicht. Der Beklagte verlangt die Bekanntgabe von personenbezogenen Daten; dieses Verlangen unterliegt den Beschränkungen des Datenschutzrechts gem. § 33 Abs. 1 ThürDSG i.V.m. § 79 Abs. 1 ThürBG in ihrer derzeit geltenden Fassung; weder die DS-GVO noch entsprechende Änderungen des ThürDG oder ThürBG waren zum Zeitpunkt der letzten mündlichen Verhandlung in Kraft. Danach ist dem Beklagten hier die Erhebung der Mobiltelefonnummer des Klägers untersagt, denn weder liegt eine Einwilligung des Klägers vor, noch liegen die Voraussetzungen der Zulässigkeit der Datenerhebung gegen den Willen des Klägers vor, noch hat der Beklagte einen Anspruch gegen den Kläger auf Erteilung einer Einwilligung hierzu.

Die Zulässigkeit der Erhebung von persönlichen Daten durch Arbeitgeber richtet sich nach § 79 Abs. 1 ThürBG. Diese Norm ist gem. § 33 Abs. 1 ThürDSG hinsichtlich der Erhebung und Nutzung von personenbezogenen Daten von Arbeitnehmern, die in einem privatrechtlich ausgestalteten Arbeits- oder Ausbildungsverhältnis zu einer öffentlichen Stelle im Sinne des ThürDSG stehen, entsprechend anwendbar. Öffentliche Stellen im Sinne des ThürDSG sind nach der Legaldefinition in § 2 Abs. 1 ThürDSG unter anderem Gemeindeverbände. Der Beklagte ist als Landkreis nach den §§ 86 ff ThürKO als kommunale Gebietskörperschaft Gemeindeverband in diesem Sinne. Der Kläger als Arbeitnehmer befindet sich zu ihm in einem privatrechtlich ausgestalteten Arbeitsverhältnis.

Nach § 79 Abs. 1 ThürBG ist die Verarbeitung personenbezogener Daten außerhalb der Einwilligung eines betroffenen Arbeitnehmer nur zulässig, soweit sie zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt.

Auch die nicht automatisierte Erfassung von Daten ist Verarbeitung in diesem Sinne (§ 3 Abs. 3 Nr. 1 ThürDSG). Die Mobiltelefonnummer ist ein personenbezogenes Datum (§ 3 Abs. 1 ThürDSG). Der Kläger ist als direkt Befragter Betroffener.

Eine Einwilligung des Klägers liegt nicht vor. Eine besondere Rechtsvorschrift, welche die Erfassung der Mobiltelefonnummer des Klägers erlaubt liegt auch nicht vor.

Die Herausgabe der Mobiltelefonnummer des Klägers an den Beklagten ist weder zur Durchführung des Arbeitsverhältnisses noch zu Zwecken des Personaleinsatzes erforderlich. Die anderen Alternativen des § 79 Abs. 1 ThürBG kommen erkennbar nicht in Betracht.

Der Begriff der Erforderlichkeit in diesem Sinne bedeutet nicht, dass die Daten für den Arbeitgeber unverzichtbar sein müssen (BAG 22.10.1986, 5 AZR 660/85). Ausreichend ist, wenn der Arbeitsgeber ohne ihre Kenntnis oder Nutzung im konkreten Einzelfall eine legitime Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann.

Dabei ist zu beachten, dass der Arbeitgeber aufgrund seiner aus Art. 12 und Art. 14 GG getragenen unternehmerischen Freiheit Arbeitsablauf und Arbeitsorganisation und damit den Zweck der Datenerhebung grundsätzlich vorformen darf. Für den Beklagten als kommunale Gebietskörperschaft gilt dies in ähnlichem Maße aufgrund der in Art. 28 GG und Art. 91 Abs. 2 ThürVerf garantierten kommunalen Selbstverwaltungsgarantie. Kollidiert diese insoweit unternehmerische Vorgabe mit Grundrechten von Arbeitnehmern, hier dem Grundrecht auf informationelle Selbstbestimmung, ist ein schonender Ausgleich dieser Rechtspositionen vorzunehmen (ähnlich zu § 32 BDSG: NK-ArbR/Birk BDSG § 32 Rn 86).

Der mit einer Datenerhebung verbundene Eingriff in das allgemeine Persönlichkeitsrecht des Arbeitnehmers muss in diesem Rahmen einer Abwägung der beiderseitigen Interessen

nach dem Grundsatz der Verhältnismäßigkeit standhalten (so schon BAG 22.10.1986, 5 AZR 660/85). Dieser verlangt, dass der Eingriff geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen. Es dürfen keine anderen, zur Zielerreichung gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkenden Mittel zur Verfügung stehen. Die Verhältnismäßigkeit im engeren Sinne ist gewahrt, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Die Datenerhebung, -verarbeitung oder -nutzung darf keine übermäßige Belastung für den Arbeitnehmer darstellen und muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen (so zum vergleichbar, teilweise identisch wie § 79 Abs. 1 ThürBG formuliertem § 32 BDSG: BAG 29.6.2017 – 2 AZR 597/16, NZA 2017, 1179 mwN.).

Danach ist es hier nicht zulässig, die Mobiltelefonnummer vom Kläger zu erheben, denn der in der Herausgabe der Nummer liegende Eingriff in sein Persönlichkeitsrecht wiegt außerordentlich schwer und steht außer Verhältnis zu den ihn rechtfertigenden Gründen.

In der Erfassung der Mobiltelefonnummer liegt ein erheblicher Eingriff in das Persönlichkeitsrecht des Klägers. Soweit der Beklagte in Zweifel zieht, dass überhaupt ein Eingriff vorliegt und dieser allenfalls gering sein könnte, weil es unwahrscheinlich sei, dass der Beklagte von der durch Bekanntgabe der Mobiltelefonnummer gegebenen Möglichkeit einer Kontaktaufnahme außerhalb von Rufbereitschaftszeiten und Dienstzeiten Gebrauch mache, wählt er nicht den zutreffenden Ansatz. Der Eingriff in das Persönlichkeitsrecht liegt nicht in der Kontaktaufnahme als solcher. Der Eingriff liegt bereits darin, dass die Mobiltelefonnummer erfasst wird und somit die Möglichkeit besteht, den Kläger jederzeit und an jedem Ort zu kontaktieren. Die Mobiltelefonnummer ist deshalb ein besonders sensibles Datum, weil jeder, der Kenntnis von dieser Nummer hat, grundsätzlich jederzeit in der Lage ist, den Nutzer zu erreichen. Hier ist auch zu beachten, dass der Beklagte die Nummer gerade und ausschließlich deshalb haben möchte, um den Kläger außerhalb der Dienstzeiten und außerhalb angeordneter Rufbereitschaft, mithin in seiner Freizeit, kontaktieren zu können. Freizeit zeichnet sich gerade dadurch aus, dass Arbeitnehmer in diesem Zeitraum den Arbeitgeber nicht zur Verfügung stehen müssen und selbstbestimmt entscheiden können, wie und wo sie diese Freizeit verbringen. In dieser Zeit müssen sie gerade nicht fremdnützig tätig sein und sind nicht Bestandteil einer fremdbestimmten arbeitsrechtlichen Organisationseinheit und fungieren nicht als Arbeitskraft. Es gehört zu den vornehmsten Persönlichkeitsrechten, dass ein Mensch selbst entscheidet, für wen er in dieser Zeit erreichbar sein will oder nicht. Erfasst ein Arbeitgeber die Mobiltelefonnummer gegen den Willen des Arbeitnehmers, so ist dieses Recht beeinträchtigt. Der Arbeitnehmer verfügt über seine Freizeit nicht mehr ausschließlich selbstbestimmt. Durch diese jederzeitige Verfügbarkeit reduziert der Arbeitgeber den Arbeitnehmer auf seine Funktion als Arbeitskraft. Abgesehen davon, dass damit der Kläger auf eine Funktion im Organisations- und Aufgabengefüge des Beklagten reduziert und damit seiner Subjektqualität beraubt und zum Objekt wird, was nach der Objektstheorie die Menschenwürde (dazu ErfK/Schmidt Art 1 GG Rn 6) betrifft, wäre dem Kläger jegliche Möglichkeit genommen, sich dem Zugriff seines Arbeitgebers zu entziehen ohne gleichzeitig auch allen anderen jegliche Kontaktmöglichkeit zu ihm zu entziehen. Der Kläger könnte nicht in seiner Freizeit tun und lassen, was er will. Er könnte nicht entscheiden, für einige Personen erreichbar sein zu wollen, aber für seinen Arbeitgeber nicht. Er könnte sein Mobiltelefon nur eingeschränkt nutzen, da er zum Beispiel auch für den Arbeitgeber erreichbar wäre, wenn er nur eine sportliche Betätigung tracken will. Er wäre tiefgreifend in seiner Lebensführung eingeschränkt. Wirkliche selbstbestimmte Freizeit könnte er nur erreichen, wenn er auf die Nutzung seines Mobiltelefons komplett verzichtete.

Die Einwendung des Beklagten, dass nur höchst selten, im Jahre 2017 in keinem Falle, von der Möglichkeit dieser Kontaktaufnahme während der Freizeit und damit der Beeinträchtigung der Lebensführung Gebrauch gemacht worden ist, trägt nicht. Die Beeinträchtigung liegt schließlich schon in der Möglichkeit kontaktiert zu werden, denn schon diese bedeutet, dass der Kläger in seiner Freizeit grundsätzlich als Arbeitnehmer zur Verfügung steht. Liegt der Eingriff in das Recht auf informationelle Selbstbestimmung damit allein schon in der Herausgabe der Mobiltelefonnummer und der dadurch geschaffenen abstrakten Möglichkeit der Kontaktaufnahme durch den Arbeitgeber, so kann es zur Rechtfertigung dieses Eingriffs nicht darauf ankommen, wie oft tatsächlich von der Möglichkeit der Kontaktaufnahme Gebrauch gemacht wird. Entscheidend ist, dass aus Sicht des Arbeitnehmers jederzeit und an jedem Ort mit einer Kontaktaufnahme gerechnet werden muss. Der Arbeitnehmer kann sich dem nicht in einer für ihn zumutbaren Weise entziehen.

…

Auch die Einwendung des Beklagten, der Kläger könne sich der Kontaktaufnahme entziehen, indem er das Handy nicht bei sich hat oder abschaltet, trägt nicht. Es ist gerade Sinn des Mobiltelefons, für diejenigen, für die man erreichbar sein möchte, auch außerhalb des häuslichen Bereichs und außerhalb üblicher Zeiten erreichbar zu sein. Denn der Kläger wäre auch in seinem Persönlichkeitsrecht beeinträchtigt, wenn er in Zeiten, in denen er von seinem Arbeitgeber nicht kontaktiert werden möchte, gezwungen wäre, auch für andere nicht über Mobiltelefon erreichbar zu sein.

Ebenso wenig verringert es die Eingriffsintensität, dass der Beklagte nach seinem Konzept die private Lebensführung in der Freizeit des Klägers deshalb nicht tangiert sieht, weil dieser nicht gezwungen sei, bei einer Kontaktaufnahme dem Wunsch zur Aufnahme der Arbeitsleistung nachzukommen, wenn er sich hierzu aus verschiedenen Gründen, etwa wegen zu weiter Entfernung zum Einsatzort oder aufgrund von „Unpässlichkeit“ hierzu nicht in der Lage fühle, so dass der Kläger in seiner Freizeit weiterhin tun und lassen könne, was er wolle. Er könne überall hinfahren und müsse keine Entfernungsgrenzen einhalten; er könne alkoholische Getränke zu sich nehmen usw. Die Beeinträchtigung liegt hier schon darin, dass der Kläger im Falle einer Kontaktaufnahme in die Lage gebracht wäre, sich für sein Freizeitverhalten zu rechtfertigen. Der Beklagte erwartet ausdrücklich, dass die Kontaktaufnahme nicht illoyal verhindert wird, indem die erkannte und gesendete Telefonnummer „weggedrückt“ wird oder der Kläger eine „Unpässlichkeit“ nur vorgibt. D.h., der Kläger sähe sich faktisch unter Druck gesetzt, eine Erklärung abzugeben, warum er im Falle einer erfolgreichen Kontaktaufnahme nicht zu Arbeitsleistung bereit wäre. Es besteht jedoch kein Anspruch des Beklagten als Arbeitgeber gegen den Kläger als Arbeitnehmer, dass dieser überhaupt Auskünfte über sein Freizeitverhalten gibt oder sich dafür rechtfertigt, wenn dies nicht unmittelbar Auswirkungen auf das Arbeitsverhältnis hat, was in diesem hier diskutierten Falle nicht gegeben ist.

Soweit der Beklagte meint, der Eingriff sei nicht so gravierend, weil er mit Wohnadresse und Festnetztelefonnummer den Kläger auch innerhalb seiner Freizeit erreichen könne, indem er ihn z.B. zu Hause aufsuche, unterstreicht er damit, dass die Bekanntgabe der Mobiltelefonnummer nicht erforderlich ist. Abgesehen davon passt dies nicht zum vom Beklagten vorgetragenen Konzept, denn danach soll eine Rettungsdienstleitstelle versuchen in den hier relevanten Zeiten, mithin zwischen 19:01 und 5:59 Uhr Kontakt aufzunehmen. Es ist recht unwahrscheinlich, dass dafür die Mitarbeiter die Rettungsdienstleistelle verlassen und Mitarbeiter des Beklagten zu Hause aufsuchen. Schließlich besteht der Unterschied auch darin, dass sich der Kläger einer Kontaktaufnahme an der Wohnanschrift und/oder der Festnetztelefonnummer dadurch entziehen kann, dass er sich schlicht nicht zu Hause aufhält.

Dem gegenüber haben die vom Beklagten geltend gemachten Belange nicht genügend Gewicht, um einen derart tiefgreifenden Eingriff zu rechtfertigen.

Der Beklagte trägt vor, dass er die Mobiltelefonnummer des Klägers benötigt, um in einem außerhalb von Dienstzeiten und eingerichteten Rufbereitschaftszeiten auftretenden Notfall im Bereich der Hygiene oder des Infektionsschutzes den Kläger kontaktieren zu können, um ihn zu Notfallarbeiten heranzuziehen.

Es ist schon nicht erkennbar, weshalb hierzu die Herausgabe der Mobiltelefonnummer des Klägers erforderlich ist, denn der Beklagte hat zunächst genügend andere Kontaktdaten zur Verfügung, so die Festnetztelefonnummer und die Wohnanschrift des Klägers, welche der Kläger bekannt gegeben hat. Ihm stehen auch Telefonnummern anderer Mitarbeiter der betreffenden Abteilung zur Verfügung, die grundsätzlich auch für diese Arbeiten geeignet sind. Der Beklagte will sich seiner eigenen Organisationentscheidung nach selbst nicht vorher festlegen, wen er zur Arbeitsleistung im Notfall heranziehen will, sondern dies dem Zufall überlassen. Es ist also nicht erkennbar, dass mit den bereits bei dem Beklagten vorhandenen Daten etwa auftretende Notfälle nicht abgedeckt werden können.

Es kann nicht bei der Abwägung der Belange unberücksichtigt bleiben, dass der Beklagte bewusst eine Arbeitsablauforganisation gewählt hat, welche das Risiko, dass er mit der Erfassung der Mobiltelefonnummer beseitigen will, überhaupt erst hervorruft. Mit der Abschaffung der umfassenden Rufbereitschaft schuf der Beklagte zeitliche Lücken, die er nun damit abzusichern versucht, dass er Arbeitnehmer gegebenenfalls jederzeit an jedem Ort auch in ihrer Freizeit über die Mobiltelefonnummer erreichen möchte. Diese selbstgeschaffene Situation darf der Beklagte nicht einseitig zulasten des Persönlichkeitsrechts des Klägers auflösen.

Grundsätzlich stehen dem Beklagten auch arbeitsrechtlich und datenschutzrechtlich zulässige Gestaltungsmittel zur Absicherung von Notfalleinsätzen zur Verfügung. Er kann von den Möglichkeiten der Anordnung besonderer Dienste nach § 6 Abs. 5 TVöD Gebrauch machen, wie er es bis zum 31.12.2016 erfolgreich praktiziert hat. Hieran ändert es auch nichts, dass der Beklagte meint, aus Gründen der von ihm zu verlangenden sparsamen und wirtschaftlichen Aufgabenerledigung zur Umorganisation der Rufbereitschaft und der Notfallbereitschaft gezwungen gewesen zu sein. Auch dieser Aspekt findet seine Grenze in den zu beachtenden Persönlichkeitsrechten des Klägers, welche bereits ausführlich beschrieben und erörtert sind. Der Wunsch nach Leistung (ständige Verfügbarkeit) ohne jegliche Gegenleistung ist insoweit nicht ganz widerspruchsfrei. Versucht der Beklagte aus Kostengründen, zeitweise ohne Bereitschafts- und Rufbereitschaftsdienste auszukommen, trägt er grundsätzlich das Risiko, dass er im Notfall Arbeitnehmer erreicht. Diese selbst geschaffene Situation erweitert nicht seine Eingriffsbefugnisse in die Persönlichkeitsrechte der Arbeitnehmer.

Schließlich kann nicht unberücksichtigt bleiben, dass die vom Beklagten bemühten „Notfälle" grundsätzlich Vorgänge sind, die nicht völlig überraschend, außergewöhnlich in dem Sinne sind, dass ihr Eintreten als unwahrscheinlich oder nahezu abwegig angesehen werden müsste. Vielmehr handelt es sich um Ereignisse im Rahmen des kommunalen Aufgabenspektrums, mithin grundsätzlich mögliche und damit einzukalkulierende Ereignisse, möge man auch auf deren Ausbleiben hoffen. Einsatznotwendigkeiten in diesen Fällen über Freizeitinanspruchnahme der Mitarbeiter abdecken zu wollen, schafft künstlich Bedarf an Informationen über die Arbeitnehmer, die – wie hier – zu weit in deren Persönlichkeitsrechte eingreifen. …

§ 6 Abs. 5 TVöD kommt als Anspruchsgrundlage schon deshalb nicht in Betracht, weil darin nur die besonderen Formen der Arbeit geregelt sind. Von diesen macht der Beklagte in dem hier interessierenden Fall gerade keinen Gebrauch, denn er ordnet die dort möglichen Arbeitsformen ausdrücklich nicht an.

Die Kammer kann auch nicht nachvollziehen, woraus die arbeitsvertragliche Nebenpflicht folgen soll, jederzeit an jedem Ort in der Freizeit für den Arbeitgeber erreichbar zu sein. Soweit der Beklagte darauf Bezug nimmt, dass Arbeitnehmer in Notfällen zur Arbeitsleistung herangezogen werden könnten, so bedeutet dies nicht, dass sie sich grundsätzlich darauf einzustellen, sich dauerhaft jederzeit bereit zu halten und erreichbar zu machen hätten. …

Der Beklagte hat gegen den Kläger unter diesem Gesichtspunkt auch keinen Anspruch auf Einwilligung des Klägers in die hier umstrittene Datenerhebung. …

Dieser ergibt sich auch nicht aus dem personalen Einschlag, den das Arbeitsverhältnis als Dauerschuldverhältnis mit personeller Bindung hat.

Auch unter dem Gesichtspunkt der gebotenen Rücksichtnahme auf die erkennbaren Interessen des Vertragspartners nach § 241 BGB ergibt sich nichts anderes. Das Austauschverhältnis im Arbeitsverhältnis erschöpft sich in der Regel darin, dass der Kläger die Arbeitsleistung erbringt und hierfür die Vergütung erhält. Dass er darüber hinaus in seiner Freizeit, mithin ständig, seinem Arbeitgeber zur Verfügung zu stehen hat, ergibt sich daraus gerade nicht. Auch hierbei ist wiederum beachtlich, dass der Beklagte es durch eigene Organisation der Arbeitsabläufe in der Hand hat, selbst dafür zu sorgen, dass er in dem von ihm als Notfälle bezeichneten Fällen seinen Aufgaben nachkommen kann.

Damit kommt es nicht mehr darauf an, dass nach dem Willen des Beklagten die Daten an einen Dritten, den die Rettungsleitstelle betreibenden Rettungsdienstzweckverband Ostthüringen, weiter gegeben werden sollten.

Umstellung auf automatisierte Personalaktenführung

(**Oberverwaltungsgericht Münster,** Beschluss vom 17. Dezember 2018 – 1 A 203/17 –)

1. Die Regelung des § 106 Abs. 1 Satz 3 BBG ermächtigt den Dienstherrn im Falle erfolgter Umstellung auf

eine vollständig automatisierte Führung der Personalakte (rein elektronische Personalakte), die Papierpersonalakte des Beamten zu vernichten, um eine – unzulässige – doppelte Aktenführung zu verhindern.

2. **Die nähere Ausgestaltung der Personalakten steht im Organisationsermessen des Dienstherrn, das grundsätzlich nur durch die einschlägigen personalaktenrechtlichen Vorgaben (§§ 106 ff. BGB) begrenzt wird.**

3. **Bei der Umwandlung einer Papierpersonalakte in eine rein elektronische Personalakte müssen alle in der Papierpersonalakte enthaltenen und materiell zur Personalakte gehörenden Unterlagen vollständig und in lesbarer Form übernommen werden. Das folgt aus dem in § 106 Abs. 1 Satz 4 BBG normierten Grundsatz der Vollständigkeit der Personalakte sowie dem in § 112 Abs. 1 Satz 1 Nr. 1 BBG zum Ausdruck gebrachten Grundsatz der Richtigkeit der Personalakte (Fortführung des Senatsbeschlusses vom 5. April 2016 – 1 B 203/16 –).**

Aus den Gründen:

a) Der Kläger wendet sich zunächst gegen die Einschätzung des Verwaltungsgerichts, § 106 Abs. 1 Satz 3 BBG enthalte für den Fall der erfolgten Umstellung auf eine vollständig elektronische Aktenführung die Ermächtigung zur Vernichtung der verbliebenen Papierakte. Er meint insoweit: Da die fragliche Vernichtung der Papierakte eine belastende Regelung darstelle, bedürfe es einer eindeutigen gesetzlichen Ermächtigung, die hier fehle. Dem Wortlaut der Norm könne eine solche Ermächtigung nicht entnommen werden. Der bloße Umkehrschluss aus der Erlaubnis zur Führung einer elektronischen Akte reiche insoweit nicht aus. Auch eine systematische Auslegung führe (zumindest) nicht auf ein klares Ergebnis. So gebe es Sonderregelungen – etwa in § 113 und 114 BBG – zu Aufbewahrungsfristen und zur automatisierten Bearbeitung, die die Voraussetzungen einer Vernichtung aufbewahrter Akten explizit regelten. Es hätte daher für den Gesetzgeber nahegelegen, eine entsprechende ausdrückliche Erlaubnis zur Vernichtung der Papierpersonalakte mit in § 106 Abs. 1 Satz 3 BBG aufzunehmen, wenn er sie gewollt hätte. Die Einschätzung des Verwaltungsgerichts lasse außerdem auch den Sinn und Zweck der Norm unberücksichtigt, eine effektive Personalaktenverwaltung sicherzustellen und zugleich die Persönlichkeitsrechte, insbesondere das Datenschutzrecht, des Beamten zu wahren.

Diese Argumentation greift ungeachtet der Frage, ob die beabsichtigte Vernichtung der Papierpersonalakte des Klägers diesen im vorliegenden Kontext überhaupt zu belasten vermag, nicht durch.

Nach § 106 Abs. 1 Satz 3 BBG kann die Akte in Teilen oder vollständig automatisiert – also als digitale bzw. elektronische Personalakte – geführt werden, wobei unter „Akte" die Personalakte zu verstehen ist (vgl. die amtliche Gesetzesüberschrift und den systematischen Zusammenhang der Vorschrift insbesondere mit § 106 Abs. 1 Satz 1 und Satz 4 bis 7 BBG). Diese Regelung ermächtigt den Dienstherrn im Falle erfolgter Umstellung auf eine vollständig automatisierte Führung der Personalakte, die Papierpersonalakte des Beamten zu vernichten, um eine – unzulässige – doppelte Aktenführung zu verhindern.

Zwar legt die Norm eine solche Befugnis nicht ausdrücklich fest. Sie setzt sie aber ohne weiteres voraus, indem sie dem Dienstherrn eine vollständig automatisierte Führung der jeweiligen Personalakte gestattet. Das ergibt sich im Einzelnen aus den folgenden Erwägungen: Ist bereits eine in Papierform geführte Personalakte vorhanden, so kann die Umstellung auf eine „vollständig" automatisierte Aktenführung nur erreicht werden, wenn die vorliegende Papierpersonalakte in eine elektronische Akte umgewandelt und vom Zeitpunkt der Umwandlung an auch als solche weitergeführt wird. Ohne die angesprochene Umwandlung läge nämlich der vom Gesetz gesondert genannte Fall einer (nur) „in Teilen" (hier: ab einem bestimmten Stichtag) automatisiert geführten Akte vor, also einer teils in elektronischer, teils in Papierform geführten sog. Hybridakte (zu diesem Begriff etwa Lemhöfer, in: Plog/Wiedow, BBG, Stand: November 2018, BBG 2009 § 106 Rn. 17, und die Gesetzesmaterialien zu dem – so Gesetz gewordenen – Entwurf des § 106 Abs. 1 Satz 3 BBG: Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Neuordnung und Modernisierung des Bundesdienstrechts (Dienstrechtsneuordnungsgesetz – DneuG), BT-Drs. 16/7076, 12. November 2007, S. 125).

Wählt der Dienstherr bei vorliegender Papierakte den Weg der Umstellung auf eine vollständig automatisierte Aktenführung (§ 106 Abs. 1 Satz 3 Fall 2 BBG), so hat er zu vermeiden, dass nach der Umstellung neben der nunmehr vollständig elektronischen Akte die Personalakte in Teilen zusätzlich noch in Papierform vorliegt (ebenso: Lemhöfer, in: Plog/Wiedow, BBG, Stand: November 2018, BBG 2009 § 106 Rn. 17, sowie Peters/Grunewald/Lösch, in: Lenders/Peters/Weber/Grunewald/Lösch, Das Dienstrecht des Bundes, 2. Aufl. 2013, Rn. 882 und 884; vgl. auch Kathke, in: Schütz/Maiwald, Beamtenrecht, Stand: Oktober 2018, LBG NRW § 84 Rn. 35b, wonach von dem Begriff der automatisierten Personalaktenführung (in der bis zum 30. Juni 2016 geltenden Parallelvorschrift des § 84 Abs. 1 Satz 2 LBG NRW a. F., nunmehr § 83 Abs. 1 Satz 2 LBG NRW) insbesondere auch „elektronische Registratursysteme" erfasst werden, „bei denen auf Papier erstellte Personalakten eingescannt werden, wobei die eigentliche Originalpapierakte anschließend vernichtet wird").

Dieses Verbot (teilweise) doppelter Aktenführung folgt bereits aus dem Wortlaut des § 106 Abs. 1 Satz 3 BBG, der von der (Personal-)Akte im Singular spricht und damit wie die übrigen Regelungen des § 106 Abs. 1 BBG zugrunde legt, dass für jeden Beamten nur eine Personalakte geführt werden darf (vgl. von Roetteken, in: von Roetteken/Rothländer, BeamtStG, Stand: November 2018, BeamtStG § 50 Rn. 28, m.w.N.; vgl. insoweit auch BT-Drs 16/7076, S. 125, wo der „Grundsatz der einen Personalakte" hervorgehoben und betont wird, dass jeder Zweifel an der Eindeutigkeit der Personalakte ausgeschlossen werden müsse).

Nachhaltig bestätigt wird dieser Befund in systematischer Hinsicht durch die Vorschrift des § 106 Abs. 2 Satz 3 BBG. Diese definiert Nebenakten als Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden, und knüpft die Zulässigkeit ihrer Führung an das Vorliegen besonderer Voraussetzungen. Damit aber will sie für den Regelfall, in dem diese besonderen Voraussetzungen nicht erfüllt sind, verhindern, dass identische Aktenbestandteile doppelt vorgehalten werden, und so die Einheitlichkeit und Klarheit der Personalakte sichern.

Bezogen auf die in Rede stehende Fallkonstellation bedeutet all dies, dass die nach der Umstellung auf vollständig elektroni-

sche Aktenführung noch vorhandene Papierakte, die Teile der Personalakte nunmehr doppelt vorhält, zu vernichten ist.

Bestätigt wird dieser Befund durch die bereits vom Verwaltungsgericht hervorgehobene Entstehungsgeschichte des § 106 Abs. 1 Nr. 3 BBG. In der oben zitierten Gesetzesbegründung zu dieser Norm ist u.a. ausgeführt, dass eine parallele Führung gleicher Aktenteile in Papierform und in elektronischer Form zu vermeiden sei, um Zweifel an der Eindeutigkeit der Personalakte zu vermeiden und um eine Einschränkung der Rechte der Beamtinnen und Beamten, insbesondere datenschutzrechtlicher Art, zu verhindern (BT-Drs 16/7076, S. 125).

Aus der zuletzt genannten – zutreffenden – Erwägung ergibt sich ohne weiteres, dass das dargelegte Gesetzesverständnis, § 106 Abs. 1 Satz 3 BBG ermächtige (bzw. zwinge) zur Vernichtung einer noch in Papierform vorhandenen Personalakte, soweit diese zugleich in elektronischer Weise vorhanden ist, entgegen dem Zulassungsvorbringen gerade dem Sinn und Zweck des § 106 Abs. 1 Satz 3 BBG entspricht. Mit Blick auf alles Vorstehende kann diesem Gesetzesverständnis auch nicht mit Erfolg das vom Kläger bemühte systematische Argument entgegengehalten werden, angesichts bestehender Sonderregelungen des Personalaktenrechts zu einer Vernichtung der Personalakte oder einzelner Bestandteile derselben hätte es im Rahmen des § 106 Abs. 1 Satz 3 BBG einer entsprechenden, aber nicht vorhandenen ausdrücklichen Regelung bedurft. Denn diese Regelungen betreffen keinen vergleichbaren Sachverhalt. Sie dienen nicht der Verhinderung doppelter und damit unklarer Aktenführung, sondern verfolgen andere Zwecke. Die Vorschrift des § 113 Abs. 4 BBG ordnet eine Vernichtung der Personalakte (Abs. 1) bzw. der Teilakten (Abs. 2 und 3) erst für einen Zeitpunkt an, zu dem diese endgültig nicht mehr benötigt werden. Die ferner nur noch in Betracht zu ziehenden, eine Vernichtung anordnenden Regelungen des § 112 Abs. 1 Satz 1 Nr. 1 bzw. Nr. 2 BBG betreffen nur einzelne Dokumente und schränken den Grundsatz der wertfreien, möglichst vollständigen Dokumentation der für das Beamtenverhältnis (auch: künftig) relevanten Umstände insoweit ein, um der Personalaktenwahrheit bzw. dem Resozialisierungsgedanken Rechnung zu tragen (vgl. etwa Lemhöfer, in: Plog/Wiedow, BBG, Stand: November 2018, BBG 2009 § 112, Rn. 4).

Welche Schlüsse insoweit die ferner ins Feld geführte Vorschrift des § 114 BBG erlauben oder gebieten soll, hat der Kläger schon nicht dargelegt.

b) Der Kläger macht ferner (sinngemäß) geltend, eine ordnungsgemäße Umwandlung der Papierpersonalakte in eine elektronische Akte und deren ordnungsgemäße Führung seien entgegen der Einschätzung des Verwaltungsgerichts nicht gewährleistet. Er bestreite schon, dass die technischen Voraussetzungen für die alleinige elektronische Aktenführung gegeben seien. Es sei ungeklärt, ob die elektronische Akte „vollständig elektronisch gesichert“ sei und wie die gesonderte Aufbewahrung ärztlicher Unterlagen sichergestellt werde. Es sei nicht dargelegt, wer im Falle des Klägers wann und wie genau die Identität der nachträglich erstellten elektronischen Akte mit der Papierpersonalakte überprüft habe („Validierungsprozess“). Auch seine Befürchtung, einzelne Schriftstücke aus der Papierakte könnten nicht (ordnungsgemäß) eingescannt worden sein, greife durch. Ihr könne nicht ihr spekulativer Charakter entgegengehalten werden, weil er selbst keine Prüfung der Vollständigkeit vornehmen könne. Hieran werde er durch die „fehlende Transparenz“ der wegen der Vergabe gleicher Namen für pdf-Dokumente (z.B. zweimal „Unterlagen zur Versetzung/Umsetzung“) nicht gut „durchzublätternden“ elektronischen Akte sowie dadurch gehindert, dass diese Akte nicht paginiert sei.

Auch dieser Vortrag greift nicht durch.

aa) Von vornherein nicht erfolgversprechend sind die Rügen des Klägers, soweit sie sich auf die konkrete – auch technische – Ausgestaltung des von der Beklagten gewählten Modells der elektronischen Akte nach erfolgter Umstellung beziehen. Das betrifft das Zulassungsvorbringen, das Vorliegen der technischen Voraussetzungen für die alleinige elektronische Aktenführung sei nicht dargetan, die elektronische Akte sei unübersichtlich, intransparent, nicht gut „durchzublättern“ und ermangele einer (am besten der Paginierung der Papierakte entsprechenden) Paginierung. Dieses Vorbringen verkennt nämlich, dass die nähere Ausgestaltung der Personalakten im Organisationsermessen des Dienstherrn steht, das grundsätzlich nur durch die – insoweit hier nicht betroffenen – einschlägigen personalaktenrechtlichen Vorgaben (§§ 106 ff. BBG) begrenzt wird (vgl. etwa Lemhöfer, in: Plog/Wiedow, BBG, Stand: November 2018, BBG 2009 vor § 106, Rn. 6, und von Roetteken, in: von Roetteken/Rothländer, BeamtStG, Stand: November 2018, BeamtStG § 50 Rn. 14 ff., m.w.N.).

Unabhängig davon könnte den Rügen des Klägers auch in der Sache nicht gefolgt werden. Dass die technischen Voraussetzungen für die alleinige elektronische Aktenführung nicht gegeben sein könnten, ist nicht ansatzweise ersichtlich. Im Gegenteil: Der am 8. Februar 2017 erstellte Ausdruck der Personalakte des Klägers, den die Beklagte am 10. Februar 2017 in dem Verfahren gleichen Rubrums mit dem Aktenzeichen 1 A 206/17 vorgelegt hat (dortige Beiakte Heft 2 bis 4 und 4a), belegt offenkundig eine erfolgreiche elektronische Aktenführung. Es ist auch nicht erkennbar, dass die von der Beklagten gewählte Ausgestaltung der elektronischen Personalakte den Zweck der Personalakte grundlegend verfehlen oder auch nur eine unzureichende Transparenz der Akte begründen würde. Vielmehr gewährleistet die hier etablierte thematische und hierarchische Ordnung der elektronischen Personalakte (vgl. die dem Ausdruck der Personalakte des Klägers vorangestellte Darstellung der Aktenstruktur; Beiakte Heft 2, Blatt 1 bis 3) ersichtlich eine hinreichende Transparenz, zumal dort eine Doppelung von Gliederungspunkten nicht erkennbar ist. Es ist auch nicht ersichtlich, dass eine – wie auch immer zu bewerkstelligende – „Paginierung“ bei dem gewählten Modell einer elektronischen Akte hilfreich geschweige denn zwingend erforderlich sein könnte.

bb) Auch das Zulassungsvorbringen, es sei nach wie vor unklar, wie sichergestellt sei, dass es bei der Umwandlung der Papierpersonalakte nicht zu einem Verlust von Daten komme, begründet keine ernstlichen Zweifel an der Ergebnisrichtigkeit der gegenteiligen Einschätzung des Verwaltungsgerichts.

Richtig ist zwar, dass bei einer Umwandlung einer Papierpersonalakte in eine rein elektronische Personalakte alle in der Papierpersonalakte enthaltenen und materiell zur Personalakte gehörenden Unterlagen vollständig und in lesbarer Form übernommen werden müssen, am Ende des Umwandlungsprozesses also ein zutreffendes Ergebnis stehen muss. Das folgt aus dem in § 106 Abs. 1 Satz 4 BBG normierten Grundsatz der Vollständigkeit der Personalakte sowie dem in § 112 Abs. 1 Satz 1 Nr. 1 BBG zum Ausdruck gebrachten Grundsatz der Richtigkeit der Personalakte (so schon OVG NRW, Beschluss vom 5. April 2016 – 1 B 203/16 –, juris, Rn. 3 bis 5; dem folgend Lemhöfer, in: Plog/Wiedow, BBG, Stand: November 2018, BBG 2009 § 106 Rn. 17 a. E., und Schrapper/Günther, LBG NRW, 2. Aufl. 2017, § 83 Rn. 1).

Dass diesem Erfordernis, dessen Einhaltung, was der Kläger zu verkennen scheint, übrigens auch im Interesse des Dienstherrn steht, bei der bereits 2007 abgeschlossenen Umwandlung der bis dahin geführten Papierpersonalakte des Klägers in eine elektronische Personalakte nicht genügt worden sein könnte, ergibt sich aus dem Zulassungsvorbringen aber nicht.

Die Beklagte hat bereits mit ihrem erstinstanzlich vorgelegten Schriftsatz vom 29. September 2016 das von der Deutschen Telekom AG gewählte Verfahren zur Erstellung der elektronischen Personalakten näher erläutert: Die Erstellung habe zentral im Scancenter P. in einer sicheren Umgebung stattgefunden. Alle Papierpersonalakten der Beamten seien zunächst für die Digitalisierung aufbereitet worden. Die Akten seien entheftet und entklammert worden, und Dokumente mit einem anderen Format als DIN-A 4 seien vor der Digitalisierung auf dieses Format vergrößert bzw. verkleinert worden. Aufgrund ihres Zustands nicht für das Scannen geeignete Dokumente seien z.B. durch Kontrastverstärkung angepasst worden. Vor der Digitalisierung sei ferner die Vollständigkeit und Lesbarkeit überprüft worden. Die Dokumente einer Papierpersonalakte seien sodann gescannt und mit der „Qualifizierten elektronischen Signatur" versehen worden. Das Scannen sei auf einem einzigen Scanner erfolgt, und zwar in Duplexscannung, bei der leere Rückseiten von einer Software automatisch entfernt worden seien. In einem (näher erläuterten) aufwendigen manuellen Validierungsprozess seien Lesbarkeit und Vollständigkeit aller eingescannten Dokumente geprüft worden. Das Verfahren der Deutschen Telekom AG zur Erstellung der elektronischen Personalakten sei von dem Bundesbeauftragten für den Datenschutz sowie dem Landesbeauftragten für Datenschutz und Informationsfreiheit für das Land Nordrhein-Westfalen geprüft und als ausreichend angesehen worden.

Diesem substantiierten Vortrag, der noch durch Angaben zum Umfang der Papierpersonalakte bei ihrem Abschluss und zur Zahl der daraus erstellten Dokumente angereichert worden ist, hat der Kläger auch mit seinem Zulassungsvorbringen nichts von Substanz entgegengestellt. Namentlich führt er keine konkreten Umstände dafür an, dass es bei der Umwandlung zu entsprechenden Datenverlusten gekommen ist. Ein entsprechender Vortrag wäre ihm, anders als er meint, aber möglich gewesen. Er hätte ohne weiteres über seinen Prozessbevollmächtigten Einsicht in die noch vorhandene Papierpersonalakte (vgl. den Senatsbeschluss vom 5. April 2016– 1 B 203/16 –, juris) nehmen können und sodann anhand der ihm zugänglichen (angeblich nicht „transparenten") elektronischen Personalakte oder des hier vorliegenden – transparenten – Ausdrucks derselben abgleichen können, ob sämtliche Dokumente aus der Papierpersonalakte Eingang in die elektronische Personalakte gefunden haben.

Auch die in diesem Zusammenhang noch erhobene Rüge, es sei unklar, wie eine gesonderte Aufbewahrung ärztlicher Bescheinigungen gesichert sei, genügt nicht den Anforderungen an eine hinreichende Darlegung. Der Kläger hat schon nicht vorgetragen, dass es in seinem Fall ärztlichen Äußerungen gegeben hat, die in der Papierpersonalakte in einem verschlossenen Umschlag aufzubewahren waren und nun auch elektronisch gesondert zu behandeln wären, vgl. insoweit allgemein: Schrapper/Günther, LBG NRW, 2. Aufl. 2017, § 83 Rn. 1, und ferner auch keine entsprechenden konkreten Fehler der Aktenführung in seiner elektronischen Personalakte aufgezeigt.

c) Ernstliche Zweifel an der Richtigkeit des angefochtenen Urteils ergeben sich auch nicht aus der behaupteten Abweichung des Urteils von dem auf der Grundlage einer nur summarischen Prüfung ergangenen und deshalb nicht divergenzfähigen – vgl. insoweit allgemein: Seibert, in: Sodan/Ziekow, VwGO, 5. Aufl. 2018, § 124 Rn. 168 – Senatsbeschluss vom 5. April 2016 – 1 B 203/16 –, juris. Der Senat hat seine seinerzeit geäußerten deutlichen Zweifel an der Vollständigkeit der erstellten elektronischen Personalakte im Kern damit begründet, dass die Beklagte dem Senat in verschiedenen Verfahren Ausdrucke von elektronischen Personalakten vorgelegt hatte, die zeitlich und thematisch völlig ungeordnet waren (OVG NRW, Beschluss vom 5. April 2016 – 1 B 203/16 –, juris, Rn. 6)).

Eine solche Sachlage ist heute – namentlich auch im Falle des Klägers – längst nicht mehr gegeben. Vielmehr zeigt gerade der vorgelegte Ausdruck der elektronischen Personalakte des Klägers vom 8. Februar 2017, dass diese Akte thematisch geordnet ist und dass deswegen auch einzelne Dokumente ohne größere Schwierigkeiten aufgefunden werden können. Vor diesem Hintergrund wäre, wie bereits ausgeführt, dem Kläger auch eine Vollständigkeitsprüfung möglich gewesen.

2. Die Berufung ist auch nicht wegen der vom Kläger geltend gemachten grundsätzlichen Bedeutung der Rechtssache i. S. d. § 124 Abs. 2 Nr. 3 VwGO zuzulassen.

Eine Rechtssache hat grundsätzliche Bedeutung im Sinne dieser Vorschrift, wenn sie eine konkrete noch nicht geklärte Rechts- oder Tatsachenfrage aufwirft, deren Beantwortung sowohl für die Entscheidung des Verwaltungsgerichts von Bedeutung war als auch für die Entscheidung im Berufungsverfahren erheblich sein wird, und die über den konkreten Fall hinaus wesentliche Bedeutung für die einheitliche Anwendung oder Weiterentwicklung des Rechts hat. Zur Darlegung des Zulassungsgrundes ist die Frage auszuformulieren und substantiiert auszuführen, warum sie für klärungsbedürftig und entscheidungserheblich gehalten und aus welchen Gründen ihr Bedeutung über den Einzelfall hinaus zugemessen wird. Ist die aufgeworfene Frage eine Rechtsfrage, so ist ihre Klärungsbedürftigkeit nicht schon allein deshalb zu bejahen, weil sie bislang nicht obergerichtlich oder höchstrichterlich entschieden ist. Nach der Zielsetzung des Zulassungsrechts ist vielmehr Voraussetzung, dass aus Gründen der Einheit oder Fortentwicklung des Rechts eine obergerichtliche oder höchstrichterliche Entscheidung geboten ist. Die Klärungsbedürftigkeit fehlt deshalb, wenn sich die als grundsätzlich bedeutsam bezeichnete Frage entweder schon auf der Grundlage des Gesetzeswortlauts nach allgemeinen Auslegungsmethoden oder aber (ggf. ergänzend) auf der Basis bereits vorliegender Rechtsprechung ohne weiteres beantworten lässt (vgl. OVG NRW, Beschlüsse vom 13. Februar 2018– 1 A 2517/16 –, juris, Rn. 32, und vom 13. Oktober 2011 – 1 A 1925/09 –, juris, Rn. 31, m.w.N.).

In Anwendung dieser Grundsätze liegen die Voraussetzungen für eine Zulassung der Berufung nicht vor.

a) Die vom Kläger zunächst als grundsätzlich bedeutsam aufgeworfene Rechtsfrage, „ob die Ermächtigung zur automatisierten Führung von Personalakten in § 106 Abs. 1 Satz 3 BBG über den Wortlaut hinaus auch eine Ermächtigung zur Vernichtung der dann durch elektronische Dokumente weitergeführten Papierpersonalakte enthält", versteht der Senat angesichts des hier entscheidungserheblichen Sachverhalts präzisierend dahin, dass es nicht lediglich um eine ab einem bestimmten Zeitpunkt greifende „Weiterführung" der Personalakte in elektronischer Form (Hybridakte), sondern um eine vollständig automatisierte Führung der Akte mit der Folge der Doppelung eines Aktenteils geht. Die so verstandene Rechtsfrage ist nicht klärungsbedürftig. Sie lässt sich vielmehr schon auf der Grundlage des Gesetzeswortlauts nach allgemeinen Auslegungsmethoden und im Übrigen auch in Ansehung des vorliegenden Schrifttums ohne

weiteres beantworten. Zur näheren Begründung wird auf die Ausführungen oben unter dem Gliederungspunkt 1. a) verwiesen.

b) Die ferner als grundsätzlich bedeutsam bezeichnete Frage, „ob die elektronische Akte eine mangelnde Transparenz aufweist und bejahendenfalls, ob Folge dieser mangelnden Transparenz und der damit einhergehenden fehlenden Kontrollmöglichkeit auf Vollständigkeit, ein Verbot der Vernichtung der Papierpersonalakte zur Folge hat," ist ebenfalls nicht klärungsbedürftig. Das gilt schon deshalb, weil die dieser Frage zugrunde liegende Grundannahme mangelnder Transparenz nicht zutrifft. Es ist bereits weiter oben dargelegt worden, dass die Entscheidung der Beklagten, wie sie die elektronische Personalakte im Einzelnen ausgestaltet, in ihr Organisationsermessen fällt, und dass die von ihr gewählte thematische und hierarchische Ordnung der elektronischen Personalakte im Übrigen auch eine hinreichende Transparenz gewährleistet.

c) Die schließlich noch als grundsätzlich bedeutsam aufgeworfene Rechtsfrage, „auf welche Weise der Dienstherr sicherstellen muss, dass die Daten der Papierakte in lesbarer und vollständiger Form übernommen werden, welche technischen Sicherungen und eventuell weitere Sicherungen hier notwendig sind, bevor die Papierakte vernichtet wird", ist in einem Berufungsverfahren nicht entscheidungserheblich. Die konkrete Organisation des Umwandlungsprozesses fällt nämlich ersichtlich in das hier insoweit nicht normativ eingeschränkte Organisationsermessen der Antragsgegnerin. Entscheidend ist insoweit – wie bereits ausgeführt – nur, dass am Ende des Umwandlungsprozesses ein zutreffendes Ergebnis steht.

3. Mit Blick auf die vorstehenden Ausführungen zu den Zulassungsgründen nach § 124 Abs. 2 Nr. 1 und 3 VwGO, mit denen auch bereits das dem Zulassungsgrund nach § 124 Abs. 2 Nr. 2 VwGO zugeordnete Zulassungsvorbringen gewürdigt worden ist, weist die Rechtssache auch keine tatsächlichen oder rechtlichen Schwierigkeiten i. S. d. § 124 Abs. 2 Nr. 2 VwGO auf. Insbesondere können die Erfolgsaussichten des angestrebten Rechtsmittels danach nicht schon als offen bezeichnet werden. Das gilt auch für den Vortrag, es sei rechtlich schwierig zu beantworten, ob im Kontext der Frage der Vernichtung inzidenter die Effektivität der elektronischen Akte zu überprüfen sei. Angesichts der obigen Ausführungen liegt es auf der Hand, dass die Vernichtung der Papierpersonalakte schon dann möglich und geboten ist, wenn die Umwandlung dazu geführt hat, dass alle in dieser Akte enthaltenen, materiell zur Personalakte gehörenden Dokumente in lesbarer Form Eingang in die elektronische Personalakte gefunden haben. Die Ausgestaltung der elektronischen Personalakte im Einzelnen (etwa: chronologische oder thematische Ordnung der Dokumente) und damit auch die Frage ihrer „Effektivität" fällt in das Organisationsermessen der Beklagten und kann sich ersichtlich nicht auf den hier in Rede stehenden Anspruch, die Vernichtung der Papierpersonalakte zu unterlassen, auswirken.

Einsicht eines Ratsmitglieds in Gewerbesteuerakten (Ls)

(**Oberverwaltungsgericht Münster**, Urteil vom 6. November 2018 – 15 A 2638/17 –)

1. **Offenbaren im Sinne von § 30 Abs. 2 AO ist die Offenlegung eines im Zeitpunkt der Offenlegung noch bestehenden Geheimnisses, das ein Dritter (noch) nicht, nicht in diesem Umfang, nicht in dieser Form oder nicht sicher kennt. Auch ein Ratsmitglied, das nach § 55 Abs. 4 Satz 1 GO NRW Einsicht in Gewerbesteuerakten nehmen soll, ist in diesem Verständnis ein „Dritter" (Aufgabe der bisherigen Rechtsprechung des Senats, Urteil vom 28. August 1997 – 15 A 3432/94 –, juris Rn. 32).**
2. **Es bemisst sich allein nach den eng begrenzten Ausnahmebestimmungen des § 30 Abs. 4 AO, ob die Weitergabe von Steuerdaten im Sinne von § 30 Abs. 2 AO befugt ist.**
3. **Ein zwingendes öffentliches Interesse nach § 30 Abs. 4 Nr. 5 AO ist gegeben, wenn bei Unterbleiben der Mitteilung die Gefahr bestünde, dass schwere Nachteile für das allgemeine Wohl eintreten.**

Zu den Voraussetzungen einer von einem Verstoß „betroffenen Person" i.S.d. Datenschutzgrundverordnung

(**Landgericht Wiesbaden**, Urteil vom 5. November 2018 – 5 O 214/18 –)

Ein Mitbewerber ist nach den §§ 3 Abs.1, 3a i.V.m. § 8 Abs. 3 Nr.1 UWG weder anspruchsberechtigt noch klagebefugt. Die Datenschutzgrundverordnung enthält in den Artikeln 77-84 eine die Ansprüche von Mitbewerbern abschließende und ausschließliche Regelung.

Sachverhalt:

Die Verfügungsklägerin ist ein im Jahr 2012 gegründetes Unternehmen, welches unter der Internetadresse ein Informationsportal betreibt. Auf diesem Informationsportal stellt die Verfügungsklägerin Verbrauchern Informationen zu unterschiedlichsten Auskunfteien in Deutschland bereit. Zu diesen Informationen gehört auch eine Aufklärung darüber, dass Betroffene auf Grundlage von § 34 BDSG bzw. Art. 15 DS-GVO einen gesetzlichen Auskunftsanspruch gegen die Auskunfteien haben, Auskunft über die zu ihrer Person gespeicherten personenbezogenen Daten zu erhalten. Zum Angebot der Verfügungsklägerin gehört es, dass der Nutzer der Internetseite einen entsprechenden Antrag auf Auskunft nach Art. 15 DS-GVO selbst ausfüllen und generieren kann. Diesen ausgefüllten Antrag kann der Nutzer anschließend herunterladen und ausdrucken und an die entsprechende Auskunftei bzw. an die Verfügungsbeklagte übersenden, um eine kostenfreie Auskunft nach Art. 15 DS-GVO zu erhalten. Daneben bietet die Verfügungsklägerin den Nutzer aber auch einen Versandservice an. Nehmen die Nutzer diesen in Anspruch, müssen sie den Antrag nach Art. 15 DS-GVO nicht selbst an die Auskunftei bzw. die Verfügungsbeklagte übersenden, sondern die Verfügungsklägerin übernimmt dies für sie und berechnete hierfür eine Servicepauschale von einmalig 9,95 € oder 14,90 € im Jahresabo.

Die Verfügungsbeklagte ist eine privatwirtschaftliche Wirtschaftsauskunftei in der Rechtsform einer Aktiengesellschaft. Ihr Geschäftszweck ist es, ihre Vertragspartner mit Informationen zur Bonität (Kreditwürdigkeit) Dritter zu versorgen. Die Verfügungsbeklagte erteilt ihren Kunden kostenpflichtig auf Basis unterschiedliche Geschäftsmodelle Auskunft. Ein Score bringt die Wahrscheinlichkeits-

einschätzung des Beklagten zum Ausdruck. Die Verfügungsbeklagte ermittelt für jede betroffene Person standardmäßig verschiedene Scores zu verschiedenen Lebenssachverhalten und Branchen. Daher errechnet die Verfügungsbeklagte unterschiedliche Branchenscores, wie den Basisscore, den tagesaktuellen SCHUFA Branchenscore und den historisch übermittelten SCHUFA Score, insoweit wird wegen der näheren Einzelheiten auf Seite 3 und 4 der Schutzschrift der Verfügungsbeklagten vom 7. September 2018 (Bl. 22 der Akte) Bezug genommen.

Vor dem Inkrafttreten der Datenschutzgrundverordnung (DS-GVO) war die Verfügungsbeklagte nach § 34 BDSG (BDSG) verpflichtet den Betroffenen einmal pro Jahr auf Aufforderung Auskunft über die zu seiner Person gespeicherten Daten zu erteilen („Selbstauskunft"). Unter der Geltung des §§ 34 BDSG hat die Verfügungsbeklagte umfassend Auskunft erteilt über die vorhandenen Daten, insbesondere sämtliche „Branchenscores", inklusive der jeweiligen Scorewerte, Ratingstufe, Erfüllungswahrscheinlichkeit und Risikobewertungen. Der Basisscore, der nicht an Dritte übermittelt wird, gibt die allgemeine Bonitätseinschätzung der Verfügungsbeklagten über die betroffene Person wieder. Der tagesaktuelle SCHUFA Branchenscore wird von der Verfügungsbeklagten nur auf eine konkrete Anfrage der betroffenen Person tagesaktuell – unabhängig davon, ob es eine konkrete Kreditwürdigkeitsprüfung gegeben hat – im Rahmen von Selbstauskunftsersuchen der betroffenen Person errechnet. Es handelt sich quasi um einen hypothetischen Wert, der nur im Rahmen von Selbstauskunftsersuchen errechnet wurde. Der historische übermittelte SCHUFA Score bezeichnet die anlassbezogenen im Rahmen einer Kreditwürdigkeitsprüfung an potenzielle Kreditgeber übermittelten Scores, die von der Verfügungsbeklagten gespeichert worden sind. Gespeicherte Informationen sind nicht tagesaktuell, sondern bleiben als historische Informationen der betroffenen Person verfügbar. Nach der alten Rechtslage unter dem Bundesdatenschutzgesetz enthielt die kostenlose Selbstauskunft nach § 34 BDSG alle 3 genannten Scorearten, da dies den Anforderungen des §§ 34 Abs. 4 BDSG entsprach.

Seit Geltung der DS-GVO vom 25. Mai 2018 wird der tagesaktuelle SCHUFA Branchenscore nicht mehr im Rahmen des gesetzlichen Selbstauskunftsanspruchs beauskunftet. Der Basisscore sowie die vorhandenen historisch übermittelten SCHUFA Scores sind noch Bestandteil der Auskunft. Die kostenlose Datenkopie nach Art. 15 DS-GVO wird von der Verfügungsbeklagten grundsätzlich schriftlich erteilt.

Die Verfügungsklägerin hat mit anwaltlichem Schreiben vom 3.9. 2018 die Verfügungsbeklagte aufgefordert, es ab sofort zu unterlassen, unvollständige Auskünfte nach Art. 15 Buchst. DS-GVO zu erteilen und die Auskünfte lediglich in Papierform anzubieten. Die Verfügungsbeklagte ließ mit anwaltlichem Schreiben vom 7.9.2018 mitteilen, dass sie keine Unterlassungsverpflichtungserklärung in dieser Sache abgeben wird, und wies die Ansprüche der Verfügungsklägerin zurück.

Die Verfügungsklägerin ist der Ansicht, dass durch die Datenschutzgrundverordnung der Auskunftsanspruch des Betroffenen in Art. 15 DS-GVO neu gefasst worden ist und die Verfügungsbeklagte als datenverarbeitende Stelle verpflichtet ist, sowohl den Betroffenen die Möglichkeit zu geben, ihren Antrag auf Auskunft elektronisch zu stellen, als auch auf elektronischem Wege eine Auskunft zu erteilen. Zudem müsse die Auskunft unverzüglich erfolgen. Schließlich könne ein Betroffener den Anspruch jederzeit geltend machen und nicht nur einmal jährlich.

Nunmehr erteile die Verfügungsbeklagte die Auskünfte nur noch teilweise, nämlich lediglich unter Angabe eines „Basisscores". Die einzelnen Branchenssores würden nicht mehr beauskunftet werden. Die Branchenscores halte die Verfügungsbeklagte weiterhin zum Abruf bereit, jedoch nur im Rahmen einer kostenpflichtigen Anfrage.

Im Übrigen halte die Verfügungsbeklagte die Auskünfte nach Art. 15 DS-GVO nur auf Papier bereit. Sie stelle die Information auch nicht in einem gängigen elektronischen Format zur Verfügung, wenn eine betroffene Person den Antrag elektronisch gestellt hat. Eine Identifizierung könnte anhand des Personalausweises erfolgen oder dadurch, dass die Verfügungsbeklagte einen Zugangscode per Post dem Verfügungskläger schickt und dass anhand dieses Verifizierungscodes er dann auf die Daten zugreifen könne. Der Gesetzestext sei eindeutig, so dass kein Spielraum für eine Auslegung eröffnet sei. Art. 15 DS-GVO sei zu Art. 12 DS-GVO lex specialis und gehe deshalb vor und beziehe sich nicht nur auf die Entgeltpflicht. Es sei eindeutig geregelt, dass eine elektronische Auskunft zu erfolgen habe. Art. 12 Abs. 6 DS-GVO sei eine Ausnahmeregelung für den Fall, dass nur bei berechtigten Zweifeln eine Identitätsprüfung vorzunehmen sei. Es bestünden keine unwägbare Risiken für die Verfügungsbeklagte, wenn ein Zivilgericht im Rahmen der Prüfung eines Unterlassungsanspruches eine andere Auffassung zu der Übermittlung der Daten auf elektronischem Weg gewinne als die Datenschutzkonferenz. Dies sei dem Prinzip der Gewaltenteilung schuldet. Es sei das Interesse der Verfügungsklägerin, dass die Auskunft ohne Medienbruch erfolge, da die elektronische Übermittlung der Daten die Verarbeitung und Abarbeitung durch die Verfügungsklägerin vereinfachen würde.

Die Verfügungsklägerin habe gegen die Verfügungsbeklagte einen Unterlassungsanspruch aus §§ 8, 3 Abs. 1, 3a UWG i.V.m. Art. 15 DS-GVO. Sie habe ein Recht auf eine umfassende Kopie der personenbezogenen Daten. Es komme nicht darauf an ob die Scorewerte bereits errechnet und gespeichert vorliegen oder aufgrund des Algorithmus und der gespeicherten personenbezogenen Daten jederzeit errechnet werden können. Die Art der Vorhaltung der Daten (Scores auf Anfrage) dürfe nicht zu einer Umgehung des Auskunftsrechtes führen. Der Betroffene muss auf seinen Antrag nach Art. 15 DS-GVO hin Auskunft erhalten, welche Daten die Verfügungsbeklagte gegebenenfalls auf Anfrage hinvorhält, denn diese sind Gegenstand der Verarbeitung. Die Verfügungsbeklagte habe über alle personenbezogenen Daten, die zum Zeitpunkt der Anfrage vorhanden sind, Auskunft zu erteilen. Durch die DS-GVO sei keine Absenkung des Schutzniveaus einhergegangen. In § 34 Abs. 2 S. 2 Nr. 1 und 2 BDSG sei ausdrücklich geregelt gewesen; dass Daten, deren Personenbezug erst bei der Berechnung hergestellt werden, ebenfalls zu beauskunften seien. Auch nach der neuen Rechtslage müsse eine Auskunft auf Basis von Art. 15 DS-GVO so ausgelegt werden. Aus den Erwägungsgründen zu 6, 9 und 10 der DS-GVO sei ersichtlich, dass ein hohes Schutzniveau von der Verordnung angestrebt werde. Einer besonderen Regelung hinsichtlich errechenbarer Scorewerte bedürfe es daher nicht. Es seien nicht nur die bei einer Stelle gespeicherten, sondern sämtliche von ihr irgendwie verarbeiteten Daten zu beauskunften, insoweit wird auf den Begriff der Verarbeitung gemäß Art. 4 Nr. 2 DS-GVO Bezug genommen.

Mit Art. 8 Abs. 1 Grundrechtscharta, Art. 16 Abs. 1 Buchst. a EU V, Art. 1 Abs. 2 DS-GVO wäre es nicht vereinbar, das Auskunftsrecht dahin auszulegen, dass bei der datenverarbeitenden Stelle bereits zum Abruf bereitgehaltene und damit vorhandene Daten nicht beauskunftet werden müssen.

Art. 15 Abs. 3 S. 3 Buchst. DS-GVO bestimme nach seinem eindeutigen Wortlaut, dass die Informationen in einem elektronischen Format zur Verfügung zu stellen sind.

Die Wiederholungsgefahr sei gegeben, da sich die Verfügungsbeklagte geweigert habe, eine Unterlassungsverpflichtungserklärung abzugeben.

Er habe keine Leistungsverfügung beantragt, sondern eine Unterlassungsverfügung, und demzufolge komme es nicht auf die Frage eines existenziellen Gläubigerinteresses an.

Der Verfügungsgrund ergebe sich aus § 12 Abs. 2 UWG. Der Geschäftsführer der Verfügungsklägerin hole eine Auskunft zu seiner eigenen Person auf seinen eigenen Namen regelmäßig bei der Verfügungsbeklagten ein. Als er dann die Auskunft bekommen habe, hätte er festgestellt, dass „ja die Hälfte" fehle und habe daraufhin recherchiert. Erst in diesem Zusammenhang habe er sich die Webseite der Verfügungsbeklagten angeschaut. In diesem Zusammenhang habe er auch gesehen, dass die Auskunft auf Papier erteilt werde und nicht, wie vom Gesetz vorgesehen, auf elektronischem Weg.

Die Verfügungsklägerin beantragt:

Der Antragsgegnerin wird im Wege der einstweiligen Verfügung bei Vermeidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu 250.000,00 EUR und für den Fall, dass dieses nicht beigetrieben werden kann, einer Ordnungshaft oder einer Ordnungshaft bis zu sechs Monaten, diese zu vollziehen an ihren gesetzlichen Vertretern,

- untersagt, im geschäftlichen Verkehr
- Auskünfte nach Art 15 DS-GVO zu erteilen, ohne über sämtliche Scores der jeweils betroffenen Person zu informieren, welche durch die Antragsgegnerin jederzeit auf Grundlage vorhandener Datensätze und eines vorhandenen Algorithmus generiert werden können, insbesondere wenn diese von ihr zur entgeltlichen Abfrage bereitgehalten werden;
- Auskünfte nach Art 15 DS-GVO lediglich in Papierform zu erteilen, soweit die betroffene Person den Antrag elektronisch stellt und nichts anderes angibt.

Die Verfügungsbeklagte beantragt:

Den Antrag auf Erlass einer einstweiligen Verfügung zurückzuweisen.

Die Verfügungsbeklagte ist der Ansicht, dass die Erteilung der Datenkopie nach Art. 15 DS-GVO in Schriftform zu erfolgen habe, da die Identität einer eine Datenkopie beantragenden Person nicht zweifelsfrei festgestellt werden könne. Durch den postalischen Versand stelle die Verfügungsbeklagte sicher, dass die sensiblen personenbezogenen Daten nur der betroffenen Person zur Verfügung gestellt werden, zu der sie in ihrem Datenbestand einen passenden Datensatz gefunden hat. Damit erhalte immer die betroffene Person die Selbstauskunft, deren Daten angegeben waren – auch in den Fällen, in denen dieses missbräuchlich durch einen Dritten geschehen sei. Die von der Verfügungsklägerin vorgelegte Anl. A8 belege, dass der Absender frei wählbar eingetragen werden könne, und damit eine verlässliche Identifizierung des Antragstellenden nicht möglich sei. Die Verfügungsbeklagte stünde in engem Kontakt zu der Datenschutzaufsichtsbehörde und mit dem hessischen Datenschutzbeauftragten und der Datenschutzkonferenz, insbesondere auch der Arbeitsgruppe Auskunfteien. Man habe sich bereits im Jahr 2016 über die Thematik der Sicherstellung einer sicheren Identifizierung des Betroffenen ausgetauscht und sei übereingekommen, dass in jedem Fall die sichere Identifizierung Vorrang haben müsse. Demzufolge sei die Übermittlung auf postalischem Wege die derzeit praktizierte Übermittlungsart, um sicherzustellen, dass nur die betroffene Person den Inhalt der so genannten Selbstauskunft erhält. Es bestehe keine Pflicht zur Erteilung einer Auskunft in einem elektronischen Format. Art. 12 Abs. 3 S. 4 DS-GVO formuliere selbst „nach Möglichkeit" auf elektronischem Weg. Eine Ausnahme von diesem Grundsatz sei dann möglich, wenn eine besondere Gefährdungslage eine postalische Zusendung erfordere. Eine ausschließlich elektronische Kommunikation sei unsicher, weil eine zweifelsfreie Identifizierung über den elektronischem Weg nicht möglich sei. Diese Ausnahme gelte insbesondere bei Wirtschaftsauskunftsgesellschaften, wie der Verfügungsbeklagten. Diese hätten in der Regel keinen unmittelbaren Kontakt zu der betroffenen Person, sondern erhielten ihre Daten über Dritte. Im Sinn der Sicherung der Vertraulichkeit sei es daher angemessen, Selbstauskünfte nach Art. 15 DS-GVO ausschließlich an postalische geprüfte Adressen zu versenden.

Im Rahmen der aktuellen Diskussion mit den beteiligten Datenschutzaufsichtsbehörden sei die Überlegung angestellt worden, dass man zukünftig eine „Postschleife" einbindet d.h. dass man den postalischen Versand beibehält, aber die Selbstauskunft mit einen Zugangscode versieht, der es dem Betroffenen ermöglicht, nachdem er die postalische Selbstauskunft erhalten hat, nochmals auf elektronischem Weg in den Datenbestand, der seine Person betreffe, Einsicht zu nehmen.

Die einstweilige Verfügung sei grundsätzlich ausgeschlossen, da die Verfügungsklägerin konkrete Handlungen im Wege der Leistungsverfügung von der Verfügungsbeklagten verlange, die eine Vorwegnahme der Hauptsache zur Folge hätten. Beide Anträge seien auf ein aktives Handeln der Verfügungsbeklagten gerichtet, und nicht auf ein Unterlassen. Ein Handlungsanspruch als Verfügungsanspruch komme nicht in Betracht, wenn damit nicht wieder gut zu machende Verhältnisse geschaffen werden und damit die Hauptsache vorweggenommen wird. Im Übrigen sei anerkannt, dass eine einstweilige Verfügung auf Erteilung von Auskunftsansprüchen ausgeschlossen sei (OLG Köln GRUR-RR 2003,296).

Im Rahmen der Interessenabwägung müsse berücksichtigt werden, dass die Schutzinteressen der Betroffenen bei der Abwägung einzustellen seien und nicht das Interesse der Verfügungsklägerin an einem reibungslosen Abarbeiten der ihr vorliegenden Anfragen ohne Medienbruch. Auch sei zu berücksichtigen, dass man der Verfügungsbeklagten im Falle des Erlasses der begehrten Leistungsverfügung ein Risiko aufbürden würde, sich gegenüber den Betroffenen schadenersatzpflichtig zu machen, wenn die verlässliche Identifizierung des Antragstellers entfiele. Der Erlass einer Leistungsverfügung würde die Verfügungsbeklagte in Widerspruch zu der mit den maßgeblichen Aufsichtsbehörden vereinbarten Vorgehensweise bei der Selbstauskunft setzen, da sie bei Befolgung einer etwaigen Leistungsverfügung sich in Widerspruch zu den in den einschlägigen Arbeitsgruppen vereinbarten Vorgehensweise setzen müsste.

Im Übrigen ergebe sich aus der Anlage A8, dass der Geschäftsführer der Verfügungsklägerin vom Inhalt der Webseite bereits zum Zeitpunkt der Antragstellung am 23.8.2018 Kenntnis hatte. Der Antrag auf Erlass der einstweiligen Verfügung beziehe sich auf die Auskunft, die auf der Webseite erteilt wird, und nicht die Auskunft, die als Folge der E-Mail vom 21.7.2018 von der Verfügungsbeklagten erteilt worden sei, insoweit wird wegen der näheren Einzelheiten auf Seite 10 der Antragsschrift Bezug genommen. Die Verfügungsbeklagte rügt die fehlende Glaubhaftmachung des Vortrages der Verfügungsklägerin, dass erstmals der Geschäftsführer der Verfügungsklägerin Kenntnis davon erlangt habe, dass die Auskunft auf Papier erteilt werde und nicht auf elektronischem Wege.

Es fehle an einem Wettbewerbsverstoß, da die von der Klägerin behaupteten Verstöße gegen Art. 15 DS-GVO nicht vorlägen. Streitig sei schon, ob Verstöße gegen die DS-GVO überhaupt den Rechtsbruchtatbestand des § 3 Buchst. a UWG erfüllen könnten.

Es fehle aber auch an einem Verstoß gegen die Vorschriften der DS-GVO. Die Auskunftsverpflichtung nach Art. 5 DS-GVO unterscheide sich von der ehemaligen Vorschrift des §§ 34 BDSG im Wesentlichen. Die Vorschrift des §§ 34 Abs. 4 BDSG sei durch die DS-GVO ersatzlos entfallen. Dementsprechend bedürfe es zur Erfüllung der gesetzlichen Auskunftsansprüche keiner Berechnung des tagesaktuellen SCHUFA Branchenscores. Dieser sei ein solcher tagesaktueller Score, der nach der Neuregelung der DS-GVO gerade nicht mehr bei der Auskunftserteilung extra berechnet werden müsse.

Die Auslegung der Datenschutzgrundverordnung dürfe sich nicht an der überholten deutschen Rechtslage zu § 34 BDSG orientieren, da mit der Datenschutzgrundverordnung ein einheitliches Datenschutzrecht für die gesamte EU geschaffen werden sollte. Dann

könne sich aber eine Auslegung dieser Datenschutzgrundverordnung nicht an dem Datenschutzniveau der Bundesrat Deutschland orientieren, sondern an den Maßstäben, die in sämtlichen EU-Ländern vorgelegen hätten. Bereits die Schaffung des § 34 Abs. 4 BDSG sei als nachträgliche Regelung umstritten gewesen, da sie teilweise als europarechtswidrig angesehen wurde. Die mit § 34 Abs. 4 BDSG vorgesehene Auskunft auf eine Berechnung sei als Fremdkörper im Datenschutzrecht angesehen worden. Diese Regelung habe auch nur für Auskunfteien gegolten. Demgegenüber habe Art. 15 DGSVO den Anspruch, für alle Bereiche zu gelten, bis hin in die öffentliche Verwaltung. Daraus folge, dass der europäische Verordnungsgeber sich von der nationalen Besonderheit des §§ 34 Abs. 4 BDSG gelöst habe. Nicht jede denkbare Konstellation könne für einen Branchenscore berechnet werden, da sich die Auskunftssituation je nach der Branche ändere.

Die Verfügungsbeklagte betreibt gegen die Verfügungsklägerin ein Verfahren im einstweiligen Rechtsschutz sowie ein Hauptsacheverfahren wegen marken- und wettbewerbsrechtlicher Verstöße auf der Internetseite, die jeweils vor dem Landgericht München I anhängig bzw. rechtshängig sind.

Wegen der näheren Einzelheiten des Sach- und Streitstandes wird auf die zwischen Parteien gewechselten Schriftsätze nebst Anlagen, die zur Gerichtsakte gereicht wurden, Bezug genommen.

Aus den Gründen:

Der Antrag auf Erlass einer Unterlassungsverfügung gerichtet darauf, dass der Verfügungsbeklagten untersagt wird im geschäftlichen Verkehr,

1. Auskunft nach Art. 15 DS-GVO zu erteilen, ohne über sämtliche Scores der jeweils betroffenen Person zu informieren, welche durch die Verfügungsbeklagte jederzeit auf Grundlage vorhandener Datensätze oder eines vorhandenen Algorithmus generiert werden können, insbesondere wenn diese ihr zu entgeltlichen Abfrage bereitgehalten werden;

2. Auskünfte nach Art. 15 Buchst. i SGB lediglich zu erteilen, soweit die betroffene Person den Antrag Elektronik stellt und nichts anderes angibt,

ist unbegründet.

Es kann offenbleiben, ob die von der Verfügungsklägerin beantragte einstweilige Verfügung als Leistungsverfügung oder als Unterlassungsverfügung zu qualifizieren ist und ob und inwieweit die besonderen Voraussetzungen einer Leistungsverfügung vorliegen müssen oder nicht. ...

Die aufgeworfenen Fragen können deshalb offenbleiben, weil der Verfügungsklägerin als Mitbewerberin nach den §§ 3 Abs. 1,3 a i.V.m. § 8 Abs. 3 Nr. 1 UWG weder anspruchsberechtigt noch klagebefugt ist.

Der Gesetzgeber hat in Kap. 8 (Rechtsbehelfe, Haftung und Sanktionen) der Datenschutzgrundverordnung eingehend geregelt, wie die Datenschutzbestimmungen durchzusetzen sind. Im Mittelpunkt steht dabei die von einem Verstoß „betroffene Person“. Sie kann sich mit einer Beschwerde an die zuständige Aufsichtsbehörde wenden (Art. 74, 78 DS-GVO), die dann ihrerseits tätig wird. Die betroffene Person hat aber auch nach Art. 79 DS-GVO selbst das „Recht auf einen wirksamen gerichtlichen Rechtsbehelf“, wenn sie der Ansicht ist, dass ihre Rechte aus der Datenschutzgrundverordnung verletzt worden sind. Die betroffene Person kann nach Art. 82 DGSVO Ersatz ihres materiellen und immateriellen Schadens verlangen. Nach Art. 80 Abs. 1 DS-GVO ist die betroffene Person ferner berechtigt, „Organisationen“ und „ähnlichen Einrichtungen, die bestimmte Anforderungen erfüllen“ zu beauftragen, in ihrem Namen ihre Rechte unter anderem aus Art. 79 DS-GVO wahrzunehmen. Art. 80 Abs. 2 DS-GVO enthält eine so genannte Öffnungsklausel zu Gunsten der Mitgliedstaaten. Sie können vorsehen, dass jede der in Art. 80 Abs. 1 DS-GVO genannten „Organisationen“ unabhängig von einem Auftrag der betroffenen Person das Recht hat, deren Rechte aus Art. 77-79 DS-GVO in Anspruch zu nehmen, wenn nach ihrer Ansicht deren Rechte verletzt worden sind. Diese Regelung ist nicht unumstritten, weil damit letztlich Dritte über das Persönlichkeitsrecht der betroffenen Personen verfügen. Von einer entsprechenden Befugnis der Mitbewerbers des Verletzers, die Rechte der betroffenen Person ohne deren Zustimmung wahrzunehmen, ist in Art. 80 Abs. 2 DS-GVO nicht die Rede.

Es wird die Frage diskutiert, ob die Durchsetzungsregelungen der DS-GVO eine abschließende unionsrechtliche Regelung darstellen oder ob im jeweils nationalen Recht Erweiterungen zulässig sind. Es geht darum, ob der nationale Gesetzgeber über die Öffnungsklausel des Art. 80 Abs. 2 DS-GVO hinaus zusätzliche Durchsetzungsregelungen aufstellen darf. Vor allem wird diskutiert, ob die Gerichte wegen eines Vorrangs des Unionsrechts daran gehindert sind, bestehende Regelungen des deutschen Rechtes anzuwenden, die zusätzliche Rechtsbehelfe gewähren könnten. Im Rahmen der Anwendung des §§ 3 Buchst. a UWG wird die Ansicht vertreten, die Vorschriften der Datenschutzgrundverordnung seien Marktverhaltensregelungen im Sinne von § 3 Buchst. a UWG, und dementsprechend seien auch Mitbewerber des Verletzers nach § 8 Abs. 1 und Abs. 3 Nr. 1 UWG berechtigt, gegen Verstöße vorzugehen (vergleiche Wolff ZD 2018, 248). Diese Ansicht verkennt, dass § 3 Buchst. a UWG dann nicht anwendbar ist, wenn die betreffende Regelung in der Datenschutzgrundverordnung die Rechtsfolgen eines Verstoßes abschließend regelt, was wiederum durch Auslegung festzustellen ist (vergleiche im Einzelnen Köhler ZD 2018, 337 ff.). Eine solche abschließende Regelung gegenüber § 3 Buchst. a UWG stellen, so Köhler und Barth (Köhler ZD 2018, 337 ff., Barth WRP 2018, 790) die Art. 70 ff. Datenschutz Grundverordnung dar. Diese Ansicht beruft sich auf den allgemeinen Grundsatz des Unionsrechts, dass Ausnahmeregelungen, wie hier Art. 80 Abs. 2 DS-GVO, eng auszulegen sind (ständige Rechtsprechung: EuGH WRP 2015, 1206, Rn. 54) und dementsprechend nicht über den Wortlaut hinaus erweitert werden dürfen. Die Autoren schließen aus dem Umstand, dass der Unionsgesetzgeber nicht schon jedem Verband ein Recht zur Wahrnehmung der Rechte einer betroffenen Person ohne deren Auftrag einräumt hat, sondern dafür ganz konkrete Anforderungen aufstellt, dass der Unionsgesetzgeber keine Erstreckung dieser Befugnis auf Mitbewerber des Verletzers zulassen wollte. Hätte der Unionsgesetzgeber, so die Autoren, dies gewollt, so hätte es nahegelegen, dass er eine dem Art. 11 Abs. 1 RL 2005/29/EG („einschließlich Mitbewerbern“) entsprechende Durchsetzungsregelungen eingeführt hätte. Köhler unterstreicht diese Argumentation durch die Herausarbeitung der unterschiedlichen Schutzzweckbestimmung der DS-GVO auf der einen Seite und dem UWG auf der anderen Seite. Die Datenschutzgrundverordnung schützt „die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten“, insoweit wird auf Art. 1 Abs. 2 DS-GVO Bezug genommen. Damit bringe die Datenschutzgrundverordnung klar zum Ausdruck, dass es um den Individualschutz der Betroffenen geht, vergleichbar dem Schutz des allgemeinen Persönlichkeitsrechtes nach den §§ 823 Abs. 1, 1004 Abs. 1 BGB analog. Demgegenüber stehe die Konzeption des UWG. Dieses Gesetz dient

„dem Schutz der Mitbewerber, der Verbraucherinnen und Verbraucher sowie der sonstigen Marktteilnehmer vor unlauteren geschäftlichen Handlungen“, insoweit wird auf § 1 S. 1 UWG Bezug genommen. Die gesetzliche Konzeption der Datenschutzgrundverordnung hat mit der dargestellten Regelung in Kap. VIII primär die Rechtsdurchsetzung bei den Aufsichtsbehörden angesiedelt, während § 8-10 UWG die Durchsetzung des Lauterkeitsrecht vollständig der privaten Initiative überlässt. Daraus folgt, dass einem Mitbewerber nach den §§ 3 Abs. 1,3 a UWG in Verbindung mit § 8 Abs. 3 Nr. 1 UWG die Klagebefugnis fehlt. Diese vornehmlich in der Literatur vertretene Ansicht findet ihre Bestätigung in der Entscheidung des Landgerichtes Bochum (Landgericht Bochum (12. Zivilkammer), Teil Versäumnis- und Schlussurteil vom 7.8.2018 – I – 12 O 85/18 zitiert nach Beck RS 2018, 25219). Das Landgericht Bochum hat ausgeführt, dass dem Verfügungskläger eine Klagebefugnis nicht zusteht, weil die Datenschutzgrundverordnung in den Artikeln 77-84 eine die Ansprüche von Mitbewerbern abschließende und ausschließende Regelung enthält. Das Landgericht Bochum hat sich der Ansicht von Köhler mit dem Argument angeschlossen, dass die Datenschutzgrundverordnung eine detaillierte Regelung des anspruchsberechtigten Personenkreises enthält. Danach steht nicht jedem Verband ein Recht zur Wahrnehmung der Rechte einer betroffenen Person zu, sondern nur bestimmten Einrichtungen, Organisationen und Vereinigungen ohne Gewinnerzielungsabsicht unter weiteren Voraussetzungen. Hieraus sei zu schließen, dass der Uniongesetzgeber eine Erstreckung auf Mitbewerber des Verletzers nicht zulassen wollte. Diese Ansicht überzeugt, da es keine Rechtsschutzlücke besteht. Vor dem Hintergrund, dass keine Rechtsschutzlücke im Bereich der Datenschutzgrundverordnung besteht, muss sie auch nicht durch eine Anwendung des §§ 3 Buchst. a UWG geschlossen werden. An diese Überlegungen knüpft die Bundesratsinitiative des Freistaats Bayern an, wonach zur Anpassung zivilrechtlicher Vorschriften an die Datenschutzgrundverordnung ein Gesetzesantrag in den Bundesrat eingebracht worden ist (Bundesratsdrucksache 304 18 vom 6. 20.6.2018) woraus sich ableiten lässt, dass eine Klagebefugnis eines angeblichen Mitbewerbers ausscheiden soll, da ihm bereits eine Abmahnungsmöglichkeit verwehrt wird.

Es ist streitig, ob die fehlende Anspruchsberechtigung und fehlende Klagebefugnis zur Abweisung der Klage als unzulässig oder als unbegründet führt, doch handelt es sich bei der Anspruchsberechtigung um eine Frage der Aktivlegitimation und damit um eine Prüfung im Rahmen der Begründetheit der Klage, so dass die Klage auf Erlass einer einstweiligen Verfügung als unbegründet abzuweisen war.

Prof. Golas neu konzipiertes Datenschutzbuch:
Unverzichtbar für alle, die mit Personaldaten arbeiten.
jetzt vorbestellen

PRAXISNAH
ausführliche Fallbeispiele und konkrete Lösungsansätze
ETABLIERT
8. aktualisierte und erweiterte Neuauflage
NÜTZLICH
ausgewertete Stellungnahmen der Aufsichtsbehörden
Handbuch Beschäftigtendatenschutz
8. aktualisierte Auflage 2019, ca. 700 Seiten
Hardcover, € 139,99 inkl. E-Book
ISBN 978-3-89577-801-8, erscheint Ende Mai 2019
Bestellen Sie direkt unter:
datakontext.com/handbuch
DATAKONTEXT

Berichte, Informationen, Sonstiges

Wirksamkeit eines Kopftuchverbots?

Vorabentscheidungsersuchen des BAG, Beschluss vom 30.01.2019 – 10 AZR 299/18 (A)

Das Verbot eines Unternehmens der Privatwirtschaft, auffällige großflächige Zeichen religiöser, politischer und sonstiger weltanschaulicher Überzeugungen am Arbeitsplatz zu tragen, wirft Fragen nach der Auslegung von Unionsrecht auf. Diese Fragen müssen im Zusammenhang mit Konventions- und Verfassungsrecht durch ein Vorabentscheidungsersuchen geklärt werden, das der Zehnte Senat des Bundesarbeitsgerichts an den Gerichtshof der Europäischen Union richtet.

Die Beklagte ist ein Unternehmen des Einzelhandels. Die Klägerin ist muslimischen Glaubens. Sie ist als Verkaufsberaterin und Kassiererin beschäftigt. Nach Rückkehr aus der Elternzeit trug die Klägerin – anders als zuvor – ein Kopftuch. Sie erfüllt damit ein islamisches Bedeckungsgebot, das sie als zwingend empfindet. Der Aufforderung der Beklagten, das Kopftuch am Arbeitsplatz abzulegen, kam die Klägerin nicht nach. Die Beklagte stützt sich zuletzt auf eine für alle Verkaufsfilialen geltende Kleiderordnung. Nach ihr ist das Tragen auffälliger großflächiger religiöser, politischer und sonstiger weltanschaulicher Zeichen am Arbeitsplatz verboten. Mit ihrer Klage will die Klägerin festgestellt wissen, dass die darauf beruhende Weisung der Beklagten unwirksam ist. Sie ist der Auffassung, die Weisung sei unwirksam, weil sie dadurch wegen ihrer Religion diskriminiert werde. Die Beklagte beruft sich auf ihre unternehmerische Freiheit und den Schutz der negativen Religionsfreiheit ihrer Kunden und Arbeitnehmer.

Die Vorinstanzen haben der Klage stattgegeben. Der Zehnte Senat des Bundesarbeitsgerichts ersucht den Gerichtshof der Europäischen Union, Fragen nach der Auslegung der Richtlinie 2000/78/EG und dem Verhältnis von primärem Unionsrecht und nationalem Verfassungsrecht zu beantworten. Ist eine allgemeine Anordnung in der Privatwirtschaft, die auch das Tragen auffälliger religiöser Zeichen verbietet, aufgrund der von Art. 16 der Charta der Grundrechte der Europäischen Union (GRC) geschützten unternehmerischen Freiheit diskriminierungsrechtlich stets gerechtfertigt? Oder kann die Religionsfreiheit der Arbeitnehmerin berücksichtigt werden, die von der GRC, der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) und dem Grundgesetz geschützt wird?

(Pressemitteilung des BAG Nr. 4/19)

Liebeskontakte per Internet

Jeder dritte Deutsche sucht Liebeskontakte im Internet, und dies mit Erfolg, denn jeder zweite Online-Dating-Nutzer hat im Internet schon einen festen Partner gefunden. Das ist das Ergebnis einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom im Vorfeld des Valentinstages 2019. Demnach haben 30 Prozent aller Befragten ab 16 Jahren schon einmal einen Online-Dating-Dienst genutzt. Bei den 16- bis 29-Jährigen sind bereits mehr als vier von zehn Befragten (41 Prozent) bei Online-Dating-Diensten aktiv. Bei den 30- bis 49-Jährigen und 50- bis 64-Jährigen ist es je gut jeder Dritte (36 Prozent bzw. 34 Prozent). In der Generation 65 plus hat mehr als jeder Zehnte (11 Prozent) schon einmal online nach der Liebe im Netz gesucht.

Online-Dating-Dienste werden überwiegend auf dem Smartphone genutzt – mit zunehmender Tendenz. Vor einem Jahr dateten 53 Prozent der Befragten auf ihrem Smartphone online, heute sind es bereits sechs von zehn Nutzem (60 Prozent). Auch das Tablet verzeichnet Zuwächse: Gebrauchten es vor einem Jahr noch 39 Prozent der Nutzer, sind es mittlerweile 47 Prozent.

Die Erfolgsbilanz der Nutzer fällt grundsätzlich positiv aus. Gut die Hälfte (52 Prozent) hat über Online-Dating-Dienste schon einmal einen festen Partner kennenglemt. Jeder Vierte (24 Prozent) ist mit dem Partner derzeit noch zusammen, bei jedem Dritten (32 Prozent) ist die Partnerschaft mittlerweile beendet. Jede Siebte der Verbindungen wurde per Messenger beendet Die Mehrzahl der hält es gegenüber dem Partner jedoch nicht für fair, eine Beziehung digital zu beenden. Mehr als acht von zehn Befragten (83 Prozent) sagen, dass sie es grundsätzlich nicht in Ordnung finden, eine Beziehung per SMS, Messenger oder Mail zu beenden. Jeder Siebte (15 Prozent) findet es dagegen legitim, per WhatsApp, Signal und Co. Schluss zu machen. Vor knapp zehn Jahren waren dies noch deutlich weniger: 2010 hatten in einer gleichlautenden Umfrage lediglich 3 Prozent angegeben, dass Schlussmachen per SMS in Ordnung sei. 92 Prozent waren damals dagegen.

Bei der Frage, ob das schriftliche Schlussmachen legitim ist oder nicht, sind sich Männer und Frauen einig. Allerdings gibt es deutliche Unterschiede je nach Alter..

Die meisten Beziehungen werden aber weiterhin in einem persönlichen Gespräch beendet. Zwei Drittel der Befragten (64 Prozent) geben an, so schon einmal Schluss gemacht zu haben. Auch hier unterscheiden sich die Einstellungen abhängig vom Alter: Bei den 16- bis 29-Jährigen sind es 57 Prozent, in der Generation 65 Plus 68 Prozent. Die zweithäufigste Methode, Schluss zu machen, ist per Anruf. Vier von zehn Befragten (41 Prozent) haben dies schon einmal gemacht. Es folgt das Schlussmachen per SMS oder Messenger, was jeder Fünfte (21 Prozent)

schon einmal gemacht hat. Bei den 16- bis 29-Jährigen haben 36 Prozent schon so eine Nachricht an den (Ex-) Partner gesendet. Auf den hinteren Plätzen rangiert das Beziehungs-Aus per Mail. Das haben 9 Prozent schon einmal gemacht. Auch über eine andere Person (9 Prozent), in einem Brief (8 Prozent) und durch Kontaktabbruch (5 Prozent) hat nur eine Minderheit schon einmal Schluss gemacht

(Bitkom, Pressemitteilung vom 11.02.2019 und 13.02.2019)

Literaturhinweise

Simitis, Spiros/Hornung, Gerrit/Spieker, Indra gen. Döhmann (Hrsg.) **Datenschutzrecht – DS-GVO und BDSG**, Großkommentar, Nomos-Verlag, Baden-Baden, 1. Aufl., 2019, 1474 S., 198,- €

Während die traditionellen BDSG-Kommentare – inzwischen als DS-GVO/BDSG Kommentierungen – und auch eine Reihe neuer Großkommentare zur DS-GVO bereits in zweiter Auflage vorliegen, ließ die Fortführung des „Simitis" auf sich warten. In erweiterter Herausgeberschaft liegt dies grundlegende Standardwerk zum Datenschutzrecht nun wieder vor. Die Mehrzahl der zwanzig Kommentatoren hatten auch an der BDSG-Kommentierung mitgewirkt, so dass die Tradition der Veröffentlichung gewahrt bleibt. Simitis hat seinen Beitrag auf Teile der Einleitung beschränkt. Gleichwohl wird das Buch für viele wohl noch lange der „Simitis" bleiben.

Vor dem Leser liegt ein Werk, das die einzelnen Vorschriften der DS-GVO bzw. des BDSG intensiv in enger Anlehnung an die Systematik und die Zielrichtung der nicht immer in gleiche Richtung agierenden Gesetzgeber betrachtet. Kritisch beleuchtet werden die in Nutzung der Öffnungsklauseln der DS-GVO ergangenen Vorschriften des BDSG und die in diesem Gesetz gleichzeitig vollzogene Umsetzung der JI-Richtlinie. Die europarechtlichen Bestimmungen werden jeweils mit den sie ergänzenden bzw. spezifizierenden nationalen Bestimmungen gemeinsam abgehandelt. Demgemäß findet sich die Erörterung des Arbeitnehmerdatenschutz mit seiner spezifischen Regelung in § 26 BDSG innerhalb der Kommentierung des Art. 88 DS-GVO wieder, wobei die von Seifert vorgelegten rund 80 Seiten bei einer etwas leserfreundlicheren Schriftgröße des Buches ein eigenes Handbuch hergeben würden.

Zu den besonders betrachteten neuen Einzelthemen gehören: die Rechte der Betroffenen einschließlich des „Rechts auf Vergessen"; das One-Stop-Shop-Prinzip; die Kohärenz der Datenschutzaufsicht und ihre neuen Möglichkeiten der Durchsetzung; die Neuregelung der Einwilligung und sonstige Erlaubnisse zur personenbezogenen Datenverarbeitungen; Datenschutzaudit und Zertifizierung; der Umgang mit statistischen Daten und Big Data und der Internetschutz.

Das Bestreben der Kommentierung ist dabei ausgerichtet auf

- die freiheitsrechtliche Auslegung der Vorschriften
- das Ausloten der verbleibenden Gestaltungsspielräume der Mitgliedsstaaten
- die Abgrenzung des Anwendungsbereich der Datenschutz-Grundverordnung
- und die Einflüsse der zunehmender Europäisierung (europarechtliche Interpretation des EuGH, faktische Einflüsse des Europäischen Datenschutzausschusses)

Der in der Tradition des BDSG-Kommentars von Simitis fortgeführte Datenschutz-Großkommentar wird wesentlich zur weiteren Meinungsbildung beitragen und wieder zu den unverzichtbaren Arbeitsmitteln von mit Datenschutzfragen Befassten zählen.

(Prof. Peter Gola, Königswinter)

Schmitt, Florian, **Die (unangekündigte) Datenschutzkontrolle des BfDI im Anwendungsbereich des BDSG und des TKG**, Beiträge zu Datenschutz und Informationsfreiheit Bd. 23, Verlag Dr. Kovac, Hamburg, 2019, 242 S., 88,90 €

Die Dissertation ist bei Prof. Dr. Ulrich M. Gassner, Institut für Öffentliches Recht, Universität Augsburg entstanden. Der Doktorvater ist vorwiegend auf dem Gebiet des Medizinprodukte- und eHealth-Rechts tätig und zugleich Datenschutzbeauftragter der Hochschule. Im ersten Kapitel skizziert Schmitt Ziel, Gang und Umfang der Untersuchung. Er begreift die effektive Datenschutzkontrolle als vom Überraschungsmoment sowie hoheitlichen Einsichts- und Zugriffsrechten bestimmt. Er stellt die Frage, ob ein vom „Symbiosegedanken" zwischen verantwortlicher Stelle und Aufsichtsbehörde getragenes BDSG (in der Fassung von 2016) einer „effizienten und pragmatischen Datenverarbeitungspraxis" gerecht werde (S. 3).

Der Verfasser setzt sich zum Ziel, die Aufgaben und Befugnisse des BfDI für den Bereich der öffentlichen Stellen des Bundes zu untersuchen und Voraus-

setzungen und Grenzen insbesondere von Vor-Ort-Kontrollen aufzuzeigen (S. 4). Im Rahmen des TKG soll dann die Rolle des BfDI in „ihrem tatsächlichen Ausmaß“ bestimmt werden (S. 4).

Das zweite Kapitel widmet sich der Datenschutzkontrolle im Anwendungsbereich des BDSG. Zunächst werden Geschichte, Wahlverfahren und -Voraussetzungen, Unabhängigkeit sowie die allgemeinen Aufgaben des BfDI dargelegt (S. 8-25). Danach untersucht SchmittAnlass, Gegenstand, Adressaten, Verfahren und nähere Umstände der Datenschutzkontrolle (S. 28-55). Breit wird sodann die Unterstützungspflicht des Kontrolladressaten diskutiert (S. 55-104). Dabei seien natürliche Personen im Rahmen der Unterstützungspflicht gegenüber der kontrollierten Behörde nicht ausreichend geschützt (S. 105 f.).

Der Verfasser plädiert u.a. für eine zwingende Ankündigung von unangekündigten Kontrollmaßnahmen beim BMI (S. 99 f.). Eine Unabhängigkeit des BfDI sei gar nicht gewährleistet, da es nach der BDSG-Novelle 2016 an effektiven Durchsetzungs- und Sanktionsbefugnissen fehle. Ausführungen zu den aufsichtsbehördlichen Befugnissen gem. Art. 58 Abs. 1 DS-GVO finden sich derweil auf gerade zwei halben Seiten (S. 65 f.)

Das dritte Kapitel hat die Datenschutzkontrolle im Anwendungsbereich des TKG zum Gegenstand. Zunächst gibt der Verfasser einen Überblick über die Geschichte, den Anwendungsbereich und konkrete Eigenheiten des Fernmeldegeheimnisses (S. 108-118). Die Abgrenzung des Fernmeldegeheimnisses zum Datenschutz fällt recht knapp aus. In einem Exkurs lehnt Schmitt die Tk-Provider-Eigenschaft von Arbeitgebern mit guten Gründen ab. Folgerichtig fehle auch die aufsichtsbehördliche Zuständigkeit des BfDI für jene Unternehmen (S. 124-137), welche die Behörde faktisch sowieso nie in Anspruch genommen habe.

Der Verfasser gelangt ferner zu der Ansicht, dass im Geltungsbereich des TKG keine anlassbezogene unangekündigte Kontrolle möglich sei, da diese die Qualität einer Durchsuchung besäße (S. 149 ff.). Da außerdem alle Anbieter von Universaldienstleistungen Aufgaben des Bundes übernähmen, seien sie per se als öffentliche Stellen des Bundes („Verwaltungsmittler“, S. 178) anzusehen. Der Verweis in § 115 Abs. 4TKG auf §24 BDSGa. F. sei daher funktionslos.

Rechtsprechung und Literatur wurden laut Schmitt bis einschließlich Januar 2018 berücksichtigt (S. 5 Fn. 13). Doch obschon die DS-GVO seit Mai 2016 und das neue BDSG seit April 2017 in ihrer jetzigen Gestalt feststehen, wird durchweg die alte Rechtslage untersucht. Verweise auf die neue BDSG-Rechtslage sind z.T. in Klammerzusätzen beigefügt, Fragen der Konformität mit höherrangigem Recht werden allerdings ausgeklammert. Leider sind essentielle Teile derArbeit schon bei Erscheinen vom Gesetzgebungsverfahren überholt und nurmehr rechtshistorisch interessant. Die Arbeit krankt darüber hinaus an ihrer vagen Fragestellung und der mäandernden Gliederung. Der vom Verfasser gehegte Wunsch, die Dissertation möge den BDSG- und TKG-Gesetzgeber motivieren und inspirieren (S. 4), wird sich auf dieser Grundlage schwerlich erfüllen.

(Dr. Lorenz Franck)

12. GDD
Sommer-Workshop
FÜR DATENSCHUTZBEAUFTRAGTE UND -BERATER SOWIE DATENSCHUTZDIENSTLEISTER
5. bis 7. August 2019
in
Timmendorfer Strand
Auszug aus der Themenliste:
- Gemeinsame Verantwortlichkeit in der Praxis
- Überwachungsauftrag des Datenschutzbeauftragten
- Web-Tracking und Retargeting unter der DS-GVO
- Password Leaks
- Maßnahmenkatalog zum Standard Datenschutzmodell – Inhalte und praktische Anwendung
DATAKONTEXT
Jetzt informieren und anmelden unter www.datakontext.com
DATAKONTEXT GmbH · Postfach 41 28 · 50217 Frechen · Tel.: 02234/98949-40 · Fax: 02234/98949-44 · E-Mail: tagungen@datakontext.com
GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

Neuerscheinungen

Aufsätze

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

Baumgartner, Ulrich/Hansch, Guido, **Der betriebliche Datenschutzbeauftragte,** ZD 2019, S. 99
Der Beitrag greift einige aktuelle offene Fragen rund um die Funktion des betrieblichen Datenschutzbeauftragten auf. Dabei geht es sowohl um die sachgerechte Strukturierung der Datenschutzorganisation und des „Datenschutzteams" als auch um die noch völlig ungeklärte Frage des Verhältnisses des DSB zum Betriebsrat. Die Beauftragung einer juristischen Person als DSB wird befürwortet.

Dausend, Tjorven, **Der Auskunftsanspruch in der Unternehmenspraxis,** ZD 2019, S. 103
Die Autorin gibt praxisnahe Beispiele zur Bearbeitung von Betroffenenanfragen und zur Reichweite des Auskunftsanspruchs unter Aufzeigen aktueller Rechtsprechung.

Gola, Peter/Klug, Christoph, **Die Entwicklung des Datenschutzrechts im 2. Halbjahr 2018,** NJW 2019, S. 639
Der Betrag setzt die seit Existenz des BDSG in der NJW stattfindende Berichterstattung aktuell fort. Schwergewichtig werden neben Anwendungsfragen der DS-GVO der Beschäftigten- und der Kundendatenschutz als bereichsspezifisch betrachtet.

Gausling, Tina, **Künstliche Intelligenz im Anwendungsbereich der Datenschutz-Grundverordnung,** PinG 2019, S. 61
Der Beitrag beleuchtet zunächst den Terminus der Künstlichen Intelligenz in praktischer und verständlicher Weise und an Hand der eigesetzten Technik. Sodann wird aufgezeigt, wie der Einsatz künstlicher Intelligenz, der regelmäßig auf Big Data und Algorithmen basiert, und die Anforderungen an eine DS-GVO-Compliance zum Ausgleich gebracht werden können.

Lensdorf, Lars, **Eine Orientierungshilfe für Unternehmen bei Auslagerungen an Cloud-Anbieter,** CR 2019, S. 8
Der Beitrag erörtert die Empfehlung der BaFin und der Deutschen Bundesbank für die Beschaffung von Clouddienstleistungen.

Raji, Behrang, **Auswirkungen der DS-GVO auf nationales Fotorecht,** ZD 2019, S. 61
Mit dem Untertitel seines Beitrags „ Das KUG im Zahnradmodell der DS-GVO" weist der Autor auf die derzeit teilweise völlig unberechtigten teilweise aber auch berechtigten Zweifel an dem Fortbestand der bisherigen Datenschutzregelungen bei der Herstellung und Veröffentlichung von Fotos hin, auf die der deutsche Gesetzgeber bislang nicht zu reagieren bereit ist und ihre Klärung damit der Rechtsprechung überlässt.

Schreiber, Kristina, **Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden,** ZD 2019, S. 55
Auch wenn das Institut der gemeinsamen Verantwortlichkeit nicht neu ist, sind eine Reihe von Fragen hinsichtlich der Erfüllung des Tatbestands selbst offen, und sodann wie eine notwendige Vereinbarung zu gestalten, wie der jeweilige Grad an Verantwortung zu bestimmen ist und welche Folgen eine nicht gleichwertige Verantwortung mehrerer hat. Ihre Klärung ist Gegenstand des Beitrags.

Söbbing, Thomas, **Deep Learning: Wenn künstliche Intelligenz lernt – kann das durchaus rechtliche Relevanz haben,** K&R 2019, S. 164
Eine der häufigsten Varianten der künstlichen Intelligenz (KI) ist die des maschinellen Lernens. Maschinelles Lernen ist ein selbstadaptiver Algorithmus, der darauf abzielt, Objekte, Sachverhalte und komplexe Systeme zu verstehen und einzuordnen. Die wichtigste Form des maschinellen Lernens ist Deep Learning, neben der Frage, wie die kostenintensive Herstellung eines Algorithmus für Deep Learning rechtlich abgesichert werden kann (was nicht Gegenstand dieses Artikels ist).

Wiencke, Jutta/Krüger, Stefan, **Bitte recht freundlich –Das Verhältnis zwischen KUG und DS-GVO,** MMR 2019, S. 76
Auch dieser Beitrag beleuchtet die zur Zeit strittige Rechtslag der weiteren Anwendung des KUG bei der Veröffentlichung von Fotos.

Auch die analoge Welt profitiert von digitalen Schutzmaßnahmen

Bares für den Datenschutz

Wer zum Bezahlen ein Bündel großer Geldscheine aus der Tasche zieht, der zeigt offen, was er hat. Ist dieser analoge Bezahlvorgang indiskret? Das kommt auf die Betrachtung an. Kassierer und die wenigen umstehenden Menschen bekommen den kaum oder nicht dokumentierten Vorgang mit. Insofern ist er diskret, auch wenn ihn jeder an der Kasse mitbekommt. Eine elektronische Zahlung bekommt zwar niemand mit, aber das bürgt noch lange nicht für Diskretion. Hier sind jedenfalls das verkaufende Unternehmen und die Bank involviert und der Vorgang wird mit der Konto- und gegebenenfalls der Kreditkartennummer auf den Käufer und den Kaufgegenstand bezogen gespeichert. Diese Informationen können vom Unternehmen und allen, die sie erhalten, ausgewertet werden. Bindet man die Zahldienste der Datenfresser auf den Smartphones, nämlich Google-Pay und Apple-Pay ein, dann wird die Datenspur des Kaufes potenziell uferlos. Sie ermöglicht eine intensive Auswertung des Zahlungsvorganges, die in der Zusammenschau mit zahlreichen weiteren Informationen, Profilbildungen und ein maschinelles Scoring zulässt, etwa vor dem Hintergrund individueller Preisbildung. Elektronisches Zahlen ist praktisch, aber bar zahlen kann es auch sein und es hat auch bei größeren Beträgen nichts Anrüchiges. Zahlungen über „Real Cash“ sind nicht nur diskreter als „Electronic Cash“ sondern oft auch schneller. Die Studie „Kosten der Bargeldzahlung im Einzelhandel (…) zur Ermittlung und Bewertung der Kosten, die durch die Bargeldzahlung im Einzelhandel verursacht werden“ der Deutschen Bundesbank in Zusammenarbeit mit dem Handelsinstitut EHI hat ergeben, dass eine durchschnittliche Barzahlung im Geschäft gut 22 Sekunden dauert und damit etwa sieben Sekunden schneller ist, als Kartenzahlungen mit PIN. Eine Zahlung mit Unterschrift dauert verglichen mit dem Barkauf sogar 16 Sekunden länger. „Time is Cash“ lautet eine alte Erkenntnis. Nun kommt eine weitere dazu: „Cash ist Datenschutz.“

SecuPedia

Das Portal für Sicherheits-Informationen

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

Diese Verbände und Unternehmen ermöglichen als Sponsoren die Sicherheitsplattform:

ZVEI: Die Elektroindustrie · ASW Bundesverband · VdS · BDSW · BDGW · BHE · security essen · itsa · BVSW

BDLS · GEUTEBRÜCK · tenable · ESSER by Honeywell · SALTO inspired access · VSW

dormakaba · NTT Security · secunet · WISAG

Mein Partner für Datenschutz und IT-Sicherheit

©Yuri Arcurs/Fotolia

DATAKONTEXT Kompetenz aus einer Hand

Bitte beachten Sie unser Seminarangebot unter **www.datakontext.com**