

Herausgegeben von

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

Aufsätze

SCHWARTMANN/JACQUEMAIN, Datenschutz in NRW –
exemplarische Probleme des DSGVO NRW

SCHÜTZ/SCHMITZ/IPPACH, Die elektronische Patientenakte –
Anforderungen aus Sicht des Datenschutzes

JASPERS/JACQUEMAIN, Künstliche Intelligenz und ihre
Auswirkungen auf den Beschäftigtendatenschutz

Kurzbeiträge

GOLA, Aus den aktuellen Berichten und Informationen der
Aufsichtsbehörden (43): Einzelfragen zur DSB-Benennungspflicht
im 1. TB DS-GVO des LfDI Thüringen

CLAUS/REIF, Praxisfälle zum Datenschutz I: Einführung in die
juristische Prüftechnik und Musterfalllösungen zum Auskunfts-
begehren von aktiven und ausgeschiedenen Mitarbeitern

RÜB, Der Nemo-tenetur-Grundsatz im BDSG im Lichte
der Kartellrechts-Judikatur des EuGH

Rechtsprechung Aus dem Inhalt

BAG, Auskunftsanspruch des Betriebsrats über sensitive
Beschäftigtendaten (Schwangerschaft einer Beschäftigten)
setzt Datensicherung voraus

BVERWG, Videoüberwachung privater Räume richtet sich
ausschließlich nach Unionsrecht

LAG BERLIN-BRANDENBURG, Tätowierung als Eignungsmangel
im öffentlichen Dienst (Ls)

LAG HESSEN, Sachvortragsverwertungsverbot bei Auswertung
privater E-Mails (Ls)

LAG HESSEN, Auskunft an den Betriebsrat über Sonderzahlungen

OVG LÜNEBURG, Kein Auskunftsanspruch des Insolvenzverwalters
gegenüber dem Finanzamt bzgl. personenbezogener Daten des
Insolvenzschuldners (Ls)

Ihr Dialog mit der Datenschutzaufsicht



**9. Dezember
2019
in Leipzig**

DS-GVO BDSG

AUS DEM INHALT

- **BLOCK 1:** Zulässigkeit
- **BLOCK 2:** Betroffenenrechte
- **BLOCK 3:** Datenschutzorganisation
- **BLOCK 4:** Praxis der Aufsichtsbehörde

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.

REFERENTEN



Dr. Stefan Brink



RA Andreas Jaspers



Thomas Kranig



Prof. Dr. Rolf Schwartmann

Jetzt informieren und anmelden unter datakontext.com

DATAKONTEXT GmbH

Postfach 41 28 · 50217 Frechen
Tel.: +49 22 34/989 49 -40 · Fax: + 49 22 34/989 49 -44
datakontext.com · tagungen@datakontext.com

DATAKONTEXT-Repräsentanz

Postfach 20 03 03 · 08003 Zwickau
Tel.: +49 375/29 17 28 · Fax: + 49 375/29 17 27
repraesentanz-zwickau@datakontext.com

Inhaltsverzeichnis

Editorial

217

Veranstaltungen

218

Aufsätze

Prof. Dr. Rolf SCHWARTMANN/
Dr. Tobias JACQUEMAIN, LL.M.
Datenschutz in NRW – exemplarische Probleme
des DSGVO NRW

219

Joachim SCHÜTZ/Sonja SCHMITZ/Jan IPPACH
Die elektronische Patientenakte –
Anforderungen aus Sicht des Datenschutzes

224

Andreas JASPERS/Dr. Tobias JACQUEMAIN, LL.M.
Künstliche Intelligenz und ihre Auswirkungen
auf den Beschäftigtendatenschutz

232

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten und Informationen
der Aufsichtsbehörden (43): Einzelfragen zur
DSB-Benennungspflicht im 1. TB DS-GVO des
LfDI Thüringen

236

Miriam CLAUS, LL.B./RAin Yvette REIF, LL.M.
Praxisfälle zum Datenschutz I: Einführung in
die juristische Prüftechnik und Musterfalllösungen
zum Auskunftsbegehren von aktiven und
ausgeschiedenen Mitarbeitern

238

Lennart RÜB
Der Nemo-tenetur-Grundsatz im BDSG im Lichte
der Kartellrechts-Judikatur des EuGH

246

Rechtsprechung

Auskunftsanspruch des Betriebsrats über
sensitive Beschäftigtendaten (Schwangerschaft
einer Beschäftigten) setzt Datensicherung voraus
(BAG, Beschluss vom 09.04.2019)

249

Videoüberwachung privater Räume richtet
sich ausschließlich nach Unionsrecht
(BVerwG, Urteil vom 27.03.2019)

254

Tätowierung als Eignungsmangel im öffentlichen Dienst (Ls)
(LAG Berlin-Brandenburg, Beschluss vom 25.04.2019)

255

Sachvortragsverwertungsverbot bei
Auswertung privater E-Mails (Ls)
(LAG Hessen, Urteil vom 21.09.2018)

255

Auskunft an den Betriebsrat über Sonderzahlungen
(LAG Hessen, Beschluss v. 10.12.2018)

255

Kein Auskunftsanspruch des Insolvenzverwalters
gegenüber dem Finanzamt bzgl. personenbezogener
Daten des Insolvenzschuldners (Ls)
(OVG Lüneburg, Urteil vom 20.06.2019)

256

Zur dienstlichen Beurteilung eines behördlichen
Beauftragten für Datenschutz und dem datenschutz-
rechtlichen Benachteiligungsverbot (Ls)
(OVG Berlin-Brandenburg, Beschluss vom 20.05.2019)

257

Schadensersatz wegen Verletzung der Informations-
pflichten über freie Vollzeitstellen nach angezeigtem
Wunsch auf Erhöhung der Arbeitszeit (Ls)
(ArbG Cottbus, Urteil vom 05.03.2019)

257

Zur Zulässigkeit der Übermittlung sozialer Auswahl-
daten unterlegener Mitbewerber an den Personalrat
(VerwGH München, Beschluss vom 21.05.2019)

257

Zwangsgeld (hier in Höhe von 5.000,- EUR)
wegen fehlender DS-GVO-Auskunft
(VerwG Mainz, Urteil vom 09.05.2019)

263

Berichte, Informationen, Sonstiges

Datenschutzbeauftragte stärken Unternehmen 268

EuGH: Zum Kontaktangebot von Onlinehändlern 268

Datenschutz für Grundschulen – überarbeitetes und
erweitertes Angebot der Berliner Beauftragten für
Datenschutz und Informationsfreiheit 269

Bitkom: Fast jeder Zweite teilt Urlaubsfotos in
sozialen Netzwerken 269

Literaturhinweise

Buchbesprechungen

Jan Heidtmann
Internet abschalten – Das Digitale frisst uns auf
(REDAKTION) 271

Martin Scheurer
Spielerisch selbstbestimmt (REDAKTION) 271

Lutz Bergmann/Roland Möhrle/Armin Herb
Datenschutzrecht: Bundesdatenschutzgesetz –
Europäische Datenschutzgrundverordnung (REDAKTION) 271

Philipp Reimer
Verwaltungsdatenschutzrecht – Das neue Recht für die
behördliche Praxis (PROF. DR. LORENZ FRANCK) 271

Stefan Weth/Maximilian Herberger/Michael Wächter/
Christoph Sorge (Hrsg.)
Datenschutz- und Persönlichkeitsschutz
im Arbeitsverhältnis (SCHRIFTFLEITUNG) 272

Neuerscheinungen

Aufsätze 273

Nachgefasst 274

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 LINNENKOHLE, 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. Irimi VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 5/2019; DATAKONTEXT, Frechen; C.H. Beck,
RDV-Sonderveröffentlichung

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 5
Seiten 217 – 274

RDV

Recht der Datenverarbeitung

35. Jahrgang · Oktober 2019 · Seiten 217 – 274

Editorial

Facebook im toten Winkel

Facebook-Fanpages und Plugins sind derzeit unter der Überschrift „Gemeinsame Verantwortung“ ein zentrales Thema des Datenschutzrechts. Während die Praxis sich bemüht, es in den Griff zu bekommen und die Konsequenzen der aktuellen EuGH-Rechtsprechung auf den betrieblichen Datenschutz herausarbeitet, erhebt Facebook weiter munter Daten, etwa mittels Gesichtserkennung. Weil es sich merkwürdig anfühlt, ohne Wissen auf Fotos abgebildet zu sein, die über Facebook verbreitet werden, bietet Facebook nun diesen „Service“ an. Damit man erfährt, ob das eigene Gesicht irgendwo bei Facebook auftaucht und, um dessen Veröffentlichung unterbinden zu können, kann man eine Gesichtserkennung aktivieren. Dann gleicht der Dienst das eigene Gesicht mit Fotos ab, die andere bei Facebook nutzen. Ergibt ein Vergleich der Bilder etwa, dass eine andere Person ein Bild von meinem Gesicht für ihr Profilbild nutzt, werde ich informiert. Das schützt einerseits meine Persönlichkeit. Andererseits wird sie durch denselben Vorgang aber beeinträchtigt, weil Facebook mein Bild nutzen kann, um es zum Gegenstand seiner stetig wachsenden Gesichtsdatabank zu machen. Gut ist, dass man Facebook das aktiv gestatten muss, indem man unter der Rubrik Gesichtserkennung den viel-sagenden Reiter „Lege fest, ob Facebook dich auf Fotos und in Videos erkennen darf“ aktivieren muss. Spätestens, wenn

man Facebook in dem Satz durch „Big Brother“ ersetzt, kann man ins Grübeln kommen. Wer dem Unternehmen eine so weitreichende und tiefgreifende Erlaubnis gibt, der muss ihm wirklich vertrauen. Er kann sich die Frage stellen, wodurch dieses Vertrauen sich rechtfertigt und welcher nahestehenden Person er dieses Recht einräumen würde. Falls es noch einen persönlichen toten Winkel im Netz gibt, in dem die Persönlichkeit geschützt ist, dann gestattet man Facebook so, ihn zu durchmessen.

Ein anderes Beispiel ist die Werbung. Der KI-Chef von Facebook pries die Leistungsfähigkeit des Dienstes kürzlich mit dem Hinweis darauf an, dass er täglich 200 Trillion Vorhersagen treffe. Das klingt nach intensiver Durchleuchtung der Nutzer. Auch wenn man nicht sicher sagen kann, wie viel davon personenbezogen ist, kann man mit Blick auf das auf Werbung gerichtete Geschäftsmodell von Facebook mit guten Gründen annehmen, dass ein Großteil der Vorhersagen nutzerbezogen ist.

Wer auf den Einsatz moderner Technik auf dem Weg zur künstlichen Intelligenz als Unternehmen oder als Privatperson aus guten Gründen nicht verzichten möchte, der sollte dringend die Risiken dieses Handelns bewerten und sich ihnen stellen. Anderenfalls besteht die Gefahr, dass wir unter die Räder der Technik und auch der Unternehmen kommen, die sie entwickeln, programmieren

und beherrschen. Noch jedenfalls trifft unseren Kenntnisstand über das was Datengiganten mit dem Wissen über uns anstellen, ein mahrender Vergleich von Albert Einstein. Er eröffnete die Funkausstellung 1930, als es um die Einführung der Funktechnik ging, mit der Bemerkung, dass sich alle schämen sollen, „die gedankenlos sich der Wunder von Wissenschaft und Technik bedienen und nicht mehr davon geistig erfasst haben, als die Kuh von der Botanik der Pflanzen, die sie mit Wohlbehagen frisst.“ Fast 90 Jahre später müssen wir aufpassen, dass die Pflanzen uns nicht fressen.

Prof. 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
04.11.2019	Basiswissen IT-Sicherheit	Berlin	GDD e.V. und DATAKONTEXT
04.-05.11.2019	Datenschutz-Management – Teil 3	Berlin	GDD e.V. und DATAKONTEXT
06.11.2019	Der neue Kundendatenschutz: Kunden datenschutzkonform gewinnen und binden	Bonn	GDD e.V. und DATAKONTEXT
07.11.2019	Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung?	Köln	GDD e.V. und DATAKONTEXT
12.11.2019	Datenschutz-Folgenabschätzung	Berlin	GDD e.V. und DATAKONTEXT
13.11.2019	Videoüberwachung nach BDSG 2018 und DS-GVO	Köln	GDD e.V. und DATAKONTEXT
14.11.2019	Datenschutz international	Berlin	GDD e.V. und DATAKONTEXT
19.11.2019	Löschen nach DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
20.11.2019	38. RDV-Forum	Köln	GDD e.V. und DATAKONTEXT
21.-22.11.2019	43. DAFTA	Köln	GDD e.V. und DATAKONTEXT
25.11.2019	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Köln	GDD e.V. und DATAKONTEXT
25.11.2019	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
26.11.2019	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
28.11.2019	Personalprozesse datenschutzkonform organisieren	Frankfurt/M.	GDD e.V. und DATAKONTEXT
25.-29.11.2019	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
03.12.2019	DS-GVO und künstliche Intelligenz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
02.-04.12.2019	SAP ERP für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
05.12.2019	Der Brexit und seine datenschutzrechtlichen Folgen	Köln	GDD e.V. und DATAKONTEXT
09.12.2019	Ihr Dialog mit der Datenschutzaufsicht	Leipzig	GDD e.V. und DATAKONTEXT
12.12.2019	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V. und DATAKONTEXT
12.12.2019	Datenschutzkonformer Fuhrpark	Frankfurt/M.	GDD e.V. und DATAKONTEXT
10.-14.02.2020	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
12.03.2020	Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung?	Berlin	GDD e.V. und DATAKONTEXT
10.-12.03.2020	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Köln	GDD e.V. und DATAKONTEXT
06.-07.04.2020	Datenschutz-Management – Teil 3	Köln	GDD e.V. und DATAKONTEXT
04.-08.05.2020	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT

Aufsätze

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

Datenschutz in NRW – exemplarische Probleme des DSGVO NRW

Wichtige Bereiche des öffentlichen Datenschutzes sind in den Landesdatenschutzgesetzen der Bundesländer geregelt. In diesem Beitrag werden Schlaglichter auf für die Praxis relevanten Fragen

und Herausforderungen geworfen, die sich mit dem Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) stellen.

I. EU-Recht verlangt Anpassungen und Umsetzungen auch im Landesrecht

1. DS-GVO und JI-Richtlinie

Am 17. Mai 2018 verabschiedete der nordrhein-westfälische Landtag das Datenschutz-Anpassungs- und Umsetzungsgesetz (NRWDSAnpUG-EU) für Nordrhein-Westfalen (NRW). Hauptergebnis des NRWDSAnpUG-EU ist das neue Datenschutzgesetz Nordrhein-Westfalen¹ (DSG NRW). Der legislative Akt erfolgte aufgrund der notwendigen Anpassung des Landesdatenschutzes an zwei Regelungsinstrumente der EU: Die Datenschutz-Grundverordnung (DS-GVO) und die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (JI-RL). Insbesondere die JI-Richtlinie verlangt aufgrund ihrer Rechtsnatur als umsetzbedürftige EU-Richtlinie eine Umsetzung im nationalen Recht.² Dies erstreckt sich in einem föderalen Gebilde wie der Bundesrepublik Deutschland (BRD), jedoch nicht allein auf dem Bund, der dieser Aufgabe im Bundesdatenschutzgesetz (BDSG) nachgekommen ist,³ sondern gleichermaßen auch auf die Länder. Analog zum Bund hat der Landesgesetzgeber in NRW im Rahmen seiner legislativen Umsetzungsfreiheit den Weg gewählt, die JI-RL im Landesdatenschutzgesetz NRW umzusetzen.⁴

Aber auch in Bezug auf die DS-GVO lässt sich festhalten, dass die Verordnung trotz ihres unmittelbar anwendbaren Charakters durch die vielfältigen nationalen Umsetzungspflichten und fakultativen Regelungsoptionen einem hybriden Status aus Richtlinie und Verordnung gleicht. Gerade die zahlreich in der DS-GVO vorhandenen Öffnungsklauseln eröffnen einen Gestaltungsspielraum für die nationalen Gesetzgeber zur Konkretisierung und Spezifizierung des Datenschutzes. Somit wird die Europarechtskonformität durch das Verhältnis von unmittelbar geltender DS-GVO in Verbindung mit den nationalen Regelungen determiniert. Das von der EU kodifizierte Schutzniveau für den Datenschutz in

Form der DS-GVO darf von den Mitgliedstaaten jedoch nicht geändert und schon gar nicht unterschritten werden, sondern muss vielmehr durch konkretisierende Normen ausgefüllt werden.

2. Regelungsbereich und -adressaten des Landesdatenschutzes

Aufgrund des BDSG als bereits existierendem nationalem Datenschutzrecht in Ergänzung und Umsetzung der DS-GVO stellt sich die Frage, warum auch die Länder neben dem Bund eine Gesetzgebungskompetenz im Bereich des Datenschutzes überhaupt besitzen. Die exakte Differenzierung zwischen den Bundes- und Landeskompetenzen für die Datenschutzgesetzgebung ist sehr komplex. Verkürzt lässt sich für den Datenschutz aus Sicht des Bundes eine Zuständigkeit im vom Art. 70 Abs. 1 GG normierten Umfang ausmachen.

Zur Abgrenzung zwischen Bundes- und Landeskompetenz ist auf den Regelungsinhalt der Landesdatenschutzgesetze hinzuweisen, der sich grundsätzlich nur auf Landesbehörden sowie Stellen bezieht, die der Aufsicht des Landes unterstellt sind. Demnach kann jedes Land für seine eigene Verwaltung Rechtssetzung betreiben. Die Gesetzgebungskompetenz für den Datenschutz in der Privatwirtschaft liegt allein beim Bund. Landesgesetzgeber haben somit keine Gesetzgebungskompetenz für den Datenschutz der nicht-öffentlichen Stellen, sondern ausschließlich der Bund.

Des Weiteren beurteilt sich der zulässige Gestaltungsspielraum nationaler Gesetzgeber nach dem Regelungsbereich der DS-GVO. Nicht abgeschlossene unionsrechtliche Vorschriften lassen dem nationalen Gesetzgeber Gestaltungsspielräume offen und erlauben eigene, individuelle

¹ Dazu ausführlich Schwartzmann/Pabst, Handkommentar zum Landesdatenschutzgesetz NRW (DSG NRW), Baden-Baden erscheint 2020. Der Beitrag greift exemplarische Praxisprobleme des LDG NRW heraus, die im derzeit erscheinenden Kommentar erörtert wurden. Die Zitate in den Randnummern stehen unter dem Vorbehalt der Endredaktion.

² Vgl. Art. 288 UAbs. 3 AEUV; Art. 63 JI-RL.

³ Vgl. §§ 45-84 BDSG.

⁴ Vgl. §§ 35-69 DSG NRW.

Vorgaben im einzelstaatlichen Recht vorzunehmen. Konkret betrifft dies bspw. den Gesundheits- oder Beschäftigtendatenschutz.⁵

Landesrechtliche Besonderheiten werden ausschließlich für die klassischen Landeskompetenzen im Bereich des Rundfunks oder des Polizei-, Kommunal- und Schulrechts und im Gesundheitswesen entstehen und verbleiben im Bereich der öffentlichen Stellen als grundsätzlich einzige Regelungsadressaten.

Regelungslücken und nicht mit dem Unionsrecht zu vereinbarende Vorschriften können in der Konsequenz aus einem unscharf gestalteten Umsetzungsspielraum zugunsten der Mitgliedstaaten erwachsen, der in föderalen Staaten auch noch von der konkurrierenden Gesetzgebung potenziert wird. Regulatorische Kollisionen sollte der Landesgesetzgeber vermeiden, um eine praktikable Rechtsanwendung zu gewährleisten und Rechtsunsicherheiten auszuschließen. Inwiefern dies tatsächlich erreicht wird, bleibt aufgrund der Vielschichtigkeit zwischen dem Mehrebenensystem von supranationaler Ebene, Bundesebene und Landesebene und der zusätzlichen Differenzierung zwischen allgemeinem und bereichsspezifischem Datenschutzrecht abzuwarten.

II. Ausgewählte Regelungsbereiche des DSGVO NRW

1. Pseudonymisierung (§ 4 DSGVO NRW)

§ 4 DSGVO NRW ergänzt die Begriffsbestimmungen der Art. 4 Nr. 1 und 5 DSGVO und enthält eine Definition des Begriffs Anonymisierung. Unter den Begriff fällt nach dem DSGVO NRW nun auch das Verändern personenbezogener Daten dergestalt, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.⁶

Die Norm steht in enger Verbindung mit den Definitionen zu „Personenbezogenen Daten“ (Art. 4 Nr. 1 DSGVO) und „Pseudonymisieren“ (Art. 4 Nr. 5 DSGVO) und kann nicht für sich allein betrachtet werden. Mit der Anonymisierung wollte der Landesgesetzgeber dem Schutz der personenbezogenen Daten sowie der Rechte und Freiheiten der betroffenen Person und als Maßnahme zur Gewährleistung einer rechtmäßig nach Treu und Glauben erfolgenden Datenverarbeitung Rechnung tragen. Der Zweck der Anonymisierung wird vom DSGVO NRW unmittelbar konturiert. So ergibt sich aus § 15 Nr. 5 DSGVO NRW, dass die Anonymisierung das Instrument zur Gewährleistung geeigneter Garantien zum Schutz personenbezogener Daten und anderer Grundrechte im Rahmen von Datenverarbeitungen ist. Auch in besonderen Verarbeitungssituationen wird die Anonymisierung zur Gewährleistung einer rechtmäßigen Datenverarbeitung herangezogen, etwa bei Datenverarbeitungen personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken (vgl. § 17 Abs. 1 bis 3 DSGVO NRW).⁷

Der Anwendungsbereich des DSGVO NRW steht in unmittelbarer Verbindung mit der Anonymisierung. So begrenzt § 5

DSGO NRW den Anwendungsbereich auf die Verarbeitung personenbezogener Daten durch die Stellen, die von den Normen genannt werden. Somit fallen die anonymen Daten auch aus dem Anwendungsbereich des DSGVO NRW. Dies überschneidet sich auch mit der DSGVO, die gem. ErwG 26 S. 5 und 6 DSGVO anonyme Daten vom Anwendungsbereich ebenfalls ausschließt.⁸

Relevanz erlangt der Begriff der Anonymisierung in den §§ 4, 15 Nr. 5, 17 Abs. 2 und 3, 36 Nr. 6 und 40 DSGVO NRW. Davon dienen die §§ 4, 15 Nr. 5 und 17 Abs. 2 und 3 DSGVO NRW der Umsetzung der DSGVO und §§ 36 Nr. 6 und 40 DSGVO NRW der Umsetzung der JI-RL.⁹

Aufgrund der umfänglichen Begriffsdefinitionen in Art. 4 DSGVO stellt sich die Frage nach der Regelungsbefugnis für weitere Legaldefinitionen im einzelstaatlichen Recht. Der Landesgesetzgeber beruft sich hierbei auf die Öffnungsklausel Art. 6 Abs. 2 und 3 DSGVO, wonach die Mitgliedstaaten Regelungen einführen oder beibehalten dürfen, die spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten. Aufgrund der Systematik des Art. 6 DSGVO kann die Öffnungsklausel für den Erlass von § 4 DSGVO NRW inhaltlich nicht bloß aus Art. 6 Abs. 2 und 3 DSGVO (wie in der Gesetzesbegründung angenommen)¹⁰ folgen, sondern ergibt sich aus einer Zusammenschau von Art. 6 Abs. 1 lit. e i.V.m. Abs. 2 und 3 DSGVO.¹¹

Im Wesentlichen wurde die bisherige Regelung der alten Fassung des DSGVO NRW¹² wortgleich in § 4 DSGVO NRW n.F. übernommen, wobei bezüglich der Prüfung der Unmöglichkeit bzw. Unverhältnismäßigkeit die Regelbeispiele in Anlehnung an ErwG 26 S. 5 DSGVO eingeführt wurden. Die früher vorhandenen Definitionen der Pseudonymisierung und des personenbezogenen Datums sind in der Neufassung nicht mehr enthalten. Schließlich wird die Pseudonymisierung nunmehr von Art. 4 Nr. 5 DSGVO definiert.¹³

Entscheidendes Merkmal der Begriffsdefinition des § 4 DSGVO NRW n.F. ist die Unmöglichkeit bzw. Unverhältnismäßigkeit der Identifizierung der natürlichen Person (§ 4 DSGVO

5 Vgl. Art. 88 DSGVO.

6 Vgl. Schwartzmann/Pabst-Schwartzmann/Mühlenbeck, § 4 DSGVO NRW, Rn. 1.

7 Vgl. Schwartzmann/Pabst-Schwartzmann/Mühlenbeck, § 4 DSGVO NRW, Rn. 1.

8 Vgl. Schwartzmann/Pabst-Schwartzmann/Mühlenbeck, § 4 DSGVO NRW, Rn. 2.

9 Vgl. Schwartzmann/Pabst-Schwartzmann/Mühlenbeck, § 4 DSGVO NRW, Rn. 3.

10 Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU – NRWDSAnpUG-EU) v. 20.02.2018, LT NRW-Drs. 17/1981, 134.

11 Dazu Rechtsgutachten Schwartzmann/Hermann/Mühlenbeck, Datenschutzrechtliche Zulässigkeit der Kenntlichmachung des Entzugs eines Doktorgrades in (Online-)Bibliothekskatalogen v. 26.09.2018, 20 ff. abrufbar unter http://www.ombudsman-fuer-die-wissenschaft.de/fileadmin/Ombudsman/Dokumente/Downloads/Schwartzmann_Gutachten_Ombudsman_26092018.pdf (zuletzt abgerufen: 14.03.2019); Kühling/Martini et. al. Die DSGVO und das nationale Recht, 2016, 27 ff. Vgl. Schwartzmann/Pabst-Schwartzmann/Mühlenbeck, § 4 DSGVO NRW, Rn. 5 f.

12 § 3 Abs. 7 DSGVO NRW a.F.

13 Vgl. Schwartzmann/Pabst-Schwartzmann/Mühlenbeck, § 4 DSGVO NRW, Rn. 10 ff.

NRW Alt. 1, 2). Diese bemisst sich jeweils durch eine Verhältnismäßigkeitsprüfung anhand der in § 4 DSGVO NRW genannten Regelbeispiele. Die Unmöglichkeit der Identifizierung einer natürlichen Person ist insbesondere einschlägig, wenn Informationen über eine betroffene Person derart verändert werden, dass Rückschlüsse auf die Identität der Person ausgeschlossen sind, etwa weil alle Identitätsdaten entfernt wurden. Beispielhaft wäre die alleinige Angabe von Geschlecht und Alter der betroffenen Person im Rahmen einer statistischen Auswertung.¹⁴

Die Unverhältnismäßigkeit der Identifizierung einer natürlichen Person ergibt sich, wenn die personenbezogenen Daten nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können. Diese Unverhältnismäßigkeit könnte bspw. vorliegen, wenn die Identifikation einer betroffenen Person für den Verantwortlichen zwar im Rahmen der technischen Möglichkeit liegt, dies aber faktisch ausgeschlossen ist, weil eine Abwägung hinsichtlich der erforderlichen Zeit, Kosten und Arbeitskraft ergeben, dass dieser eine Identifikation nicht vornehmen kann.¹⁵

2. Videoüberwachung (§ 20 DSGVO NRW)

In § 20 DSGVO NRW werden verschiedene Rechtfertigungstatbestände zur Videoüberwachung normiert. Dies geschieht der Gesetzesbegründung nach auf Grundlage des Art. 6 Abs. 1 lit. e DSGVO, welcher für das Vorliegen öffentlichen Interesses sowie der Ausübung öffentlicher Gewalt durch den Verantwortlichen Rechtfertigungsmöglichkeiten für die personenbezogene Datenverarbeitung vorsieht. Die Struktur der Norm ähnelt bis auf wenige Ausnahmen der Neufassung des § 4 BDSG. Allerdings normiert § 20 DSGVO NRW lediglich die Videoüberwachung für öffentliche Stellen, da nur hierfür die Ländergesetzgebungskompetenz gegeben ist. Ein öffentliches Interesse ist dem Gesetzgeber nach gegeben, da die Videoüberwachung für die Gewährleistung der Funktionsfähigkeit der betroffenen Behörden, Gerichte und der anderen öffentlichen Stellen bestimmt ist. Sowohl die Erhebung durch die Beobachtung als auch die Speicherung sind durch die weite Legaldefinition des Verarbeitungsbegriffs in Art. 4 Nr. 2 DSGVO umfasst, womit alle Verarbeitungsschritte zulässig sind.¹⁶

Bei § 20 DSGVO NRW und § 4 BDSG handelt es sich um selbstständige Regelungen eines bedeutenden Bereichs der Verarbeitung personenbezogener Daten. In der DSGVO selbst findet sich kein Verweis auf die Videoüberwachung, lediglich in ErwG 91 S. 3 DSGVO wird der Begriff der optoelektronischen Vorrichtungen erwähnt. Obwohl dieser Sachverhalt von der DSGVO nicht eigenständig geregelt wird, muss die nationale Regelung zur Videoüberwachung mit dem Primärrecht zum Schutz personenbezogener Daten im Allgemeinen und mit dem unmittelbar geltenden Sekundärrechtsakt im Besonderen vereinbar sein, damit sie unionsrechtskonform ist.¹⁷

Außerhalb des Anwendungsbereichs der DSGVO besteht kein Regelungsbedarf, § 20 DSGVO NRW an das Sekundärrecht anzupassen. Das Datenschutzrecht der EU ist nicht einschlä-

gig, solange die Videoüberwachung keinen Dritten innerhalb eines rein persönlichen oder familiären Bereichs berührt. Im Rahmen der DSGVO wird in zulässiger Weise von der Öffnungsklausel in Art. 6 Abs. 3 S. 3 DSGVO Gebrauch gemacht.¹⁸

Dem steht auch nicht die Rechtsprechung des Bundesverwaltungsgerichts (BVerwG) entgegen.¹⁹ Danach dürften nationale Gesetze aufgrund des Öffnungsklauseln des Art. 6 Abs. 2 und 3 DSGVO Videoüberwachungen privater Verantwortlicher nicht regeln.²⁰ Dem Anwendungsbereich des DSGVO NRW (§ 5) nach wird aber ebendiese Datenverarbeitung mit § 20 nicht geregelt, sondern dient lediglich öffentlichen Stellen als Erlaubnistatbestand.²¹

Zulässige Formen der Videoüberwachung sind nach § 20 DSGVO NRW zunächst solche, die mittels optisch-elektronischer Einrichtungen in öffentlich zugänglichen Bereichen personenbezogene Daten verarbeiten. Unter öffentlich zugänglichen Bereichen können Bereiche gefasst werden, die von einem unbestimmten und nur nach allgemeinen Merkmalen abgrenzbaren Personenkreis betreten und genutzt werden können und ihrem Zweck nach auch dazu bestimmt sind. Relevant sind hierbei die Zweckbestimmung und Nutzungsmöglichkeiten für die Allgemeinheit, nicht die Eigentumsverhältnisse.²²

Die von § 20 für die Zulässigkeit verlangte Verwendung optisch-elektronischer Einrichtungen kann als Legaldefinition für den Begriff Videoüberwachung angesehen werden. Die DSGVO selbst äußert sich hierzu aufgrund ihrer Technikneutralität nicht. Als optisch-elektronische Einrichtungen umfassen BDSG und DSGVO NRW solche Geräte jeder Art, die für derartige Beobachtungen geeignet sind, sofern sie Licht in elektrische Signale umwandeln können. Hierunter fallen klassische Kameras, Webcams oder Mobiltelefone mit integrierter Kamera, jedoch keine Attrappen, Spiegel oder auch Ferngläser.²³

Drei alternative Tatbestände werden normiert, die jeweils für die Zulässigkeit einer Videoüberwachung sorgen: zur Wahrnehmung des Hausrechts, zum Schutz des Lebens, der Gesundheit, des Eigentums oder Besitzes oder zur Kontrolle von Zugangsberechtigungen.²⁵ Das Hausrecht dient der Verhinderung von Straftaten und sonstigen Vergehen, womit das Hausrecht präventiv abgesichert werden soll.²⁶

Eine Einschränkung finden die Ausnahmetatbestände in der gesetzlich vorgeschriebenen Interessenabwägung mit

14 Vgl. Schwartzmann/Pabst-Schwartzmann/Mühlenbeck, § 4 DSGVO NRW, Rn. 19.

15 Vgl. Schwartzmann/Pabst-Schwartzmann/Mühlenbeck, § 4 DSGVO NRW, Rn. 20.

16 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 1-3.

17 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 4.

18 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 7 f.

19 BVerwG, Urteil v. 27.03.2019, 6 C 2.18.

20 BVerwG, Urteil v. 27.03.2019, 6 C 2.18, Rn. 47.

21 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 9.

22 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 10.

23 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 11.

24 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 12.

25 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 13.

26 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 14.

schutzwürdigen Interessen der Betroffenen. Hierbei muss insbesondere die Eingriffsintensität der Videoüberwachung berücksichtigt werden. Relevant sind hierbei die Art der erfassten Informationen (Informationsgehalt), Umfang der erfassten Informationen (Informationsdichte, zeitliches und räumliches Ausmaß), der betroffene Personenkreis, die Interessenlage der betroffenen Personengruppen, das Vorhandensein von Ausweichmöglichkeiten sowie Art und Umfang der Verwertung der erhobenen Daten. Dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen.²⁷ Vorzunehmen ist die Interessenabwägung auch für die etwaigen noch anschließenden Phasen der Verarbeitung: Die Speicherung oder eine noch zu erfolgende Auswertung. Die kurzfristige Speicherung einer üblichen Videoüberwachung ist von einer ausgesprochen geringen Eingriffsintensität gekennzeichnet.²⁸

Weitere Rechtfertigungen werden in Abs. 3 erwähnt. Der Zweckbindungsgrundsatz kann auch aufgehoben werden, „soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit, zur Verfolgung von Straftaten oder zur Geltendmachung von Rechtsansprüchen gegenüber betroffenen Personen erforderlich ist“. Insofern werden die Sicherheitsbehörden von den verfassungsrechtlichen Vorgaben zur Videoüberwachung durch öffentliche Stellen befreit.²⁹ Allerdings wird auch hier eine Erforderlichkeitsprüfung als zwingend vorgeschrieben und anlassbezogen eine Interessenabwägung mit den schutzwürdigen Interessen der betroffenen Personen verlangt.³⁰

Insofern stellt § 20 Abs. 3 eine Spezialnorm zu § 9 („Zulässigkeit der Datenverarbeitung im Hinblick auf die Zweckbindung“) dar. Durch das Wort „nur“ soll die gesetzlich abschließende Enumeration der zulässigen Zweckänderungsgründe für Datenverarbeitungen aus der Videoüberwachung zum Schutz der betroffenen Person beschränkt werden. Die Beweissicherungsfunktion kann sowohl im Strafprozess als auch der Durchsetzung zivilrechtlicher Ansprüche des Verantwortlichen und Dritter dienen.³¹

In Hinsicht auf die Transparenz geht der Gesetzgeber den einzig praktikablen Weg der gestuften Informationsgewährung. Er bewertet neben der Videoüberwachung selbst, die Angaben nach Art. 13 Abs. 1 lit. a (Verantwortlicher und Vertreter), lit. b (ggf. bestellter Datenschutzbeauftragter) und lit. c (Zwecke und Rechtsgrundlage) als Informationen der 1. Stufe. Bei dieser Regelung handelt es sich der Gesetzesbegründung nach nicht um eine denkbare Beschränkung der Informationspflicht nach Art. 23 DS-GVO, sondern um eine spezifische Bestimmung der Transparenz. Komplementär dazu ist darauf hinzuweisen, wo die betroffenen Personen die weiteren Informationen nach Art. 13 DS-GVO erhalten können, um den unionsrechtlichen Anforderungen zu entsprechen.³²

3. Professor*innen als eigene Verantwortliche (§ 17 DSGVO NRW)

Als Sonderfall für wissenschaftliche oder historische Forschungszwecke und statistische Zwecke ermöglicht § 17

DSG NRW die Verarbeitung personenbezogener Daten ohne Einwilligung der betroffenen Person. Stattdessen werden eine Erforderlichkeitsprüfung und eine Interessenabwägung mit den schutzwürdigen Belangen der betroffenen Person verlangt. Mit dieser Rechtfertigungsmöglichkeit wird der großen Bedeutung der Verarbeitung großer Datenmengen Rechnung getragen. Die unionsrechtliche Öffnungsklauseln bilden Art. 89 und 9 Abs. 2 lit. j DS-GVO, die es den Mitgliedsstaaten ermöglichen, eigene Regelungen in den geöffneten Bereichen zu treffen. Diese legte der Gesetzgeber bei der Schaffung des § 17 DSGVO NRW zugrunde.³³

Der § 17 DSGVO NRW n.F. stieß auf erhebliche Kritik der nordrhein-westfälischen Hochschulen. In einer Stellungnahme³⁴ an den federführend für das DSGVO NRW zuständige Hauptausschuss des Landtags bezogen sie Position. Demnach eigne sich § 17 DSGVO NRW nicht als Rechtsgrundlage für die wissenschaftliche Verarbeitung nicht-sensibler Daten. So handelte es sich bei § 28 DSGVO NRW a.F. um eine „klare, sachgerechte und praxisbewährte Ermächtigungsnorm“. Allerdings seien die „Rechtsslage sowie die Ausgestaltungsbefugnis der Mitgliedstaaten unter der DS-GVO im Bereich Forschung fragmentiert, oft unklar und teilweise mit Rechtsunsicherheit behaftet“. Nach Ansicht des Zusammenschlusses von Hochschulen und Hochschulleitungsorganen in NRW schlage sich dies auf die Genese des § 17 DSGVO NRW nieder. Insbesondere die Ansicht des Gesetzgebers wird kritisiert, der die Regelungsbefugnis auf Art. 6 Abs. 3 DS-GVO stütze und sich indirekt auf Art. 6 Abs. 1 S. 1 lit. e DS-GVO als Rechtsgrundlage für wissenschaftliche Forschung berufe. So sei nach Ansicht der Hochschulen zweifelhaft, ob die Hochschulen bei Forschungsvorhaben überhaupt Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO seien. Schließlich entschieden über die Zwecke und Mittel der Datenverarbeitung allein die Wissenschaftler. Dies geschehe auch in höchstpersönlicher Ausübung ihres Grundrechts auf Wissenschaftsfreiheit (Art. 5 Abs. 3 GG). Aufgrund dieser verfassungsrechtlichen Vorgabe haben die Hochschulen lediglich die freie Grundrechtsbetätigung zu ermöglichen, ohne inhaltlichen Einfluss zu nehmen (bspw. niedergelegt in § 4 HG NRW). Wenn man weiter damit rechnen muss, dass die allgemeine Aufgabenzuweisung in §§ 3, 4 HG NRW zu allgemein ist, um daraus die Erforderlichkeit der Verarbeitung personenbezogener Daten in einem konkreten Forschungsvorhaben ableiten zu können, scheidet Art. 6 Abs. 1 lit. e DS-GVO als Rechtsgrundlage aus. Als Konsequenz fordern

27 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 15.

28 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 25.

29 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 26.

30 Vgl. Schwartzmann/Pabst-Schwartzmann/Jacquemain, § 20 DSGVO NRW, Rn. 27.

31 GDD, Stellungnahme zum NRWDSAnpUG-EU v. 06.04.2018, Stellungnahme f. d. Hauptausschuss Nr. 17/488, 5.

32 Vgl. Schwartzmann/Pabst-Schwartzmann/Hermann, § 17 DSGVO NRW, Rn. 1.

33 Landesrektorenkonferenz des Landes Nordrhein-Westfalen u.a., Stellungnahme zum NRWDSAnpUG-EU v. 06.04.2018, Stellungnahme f. d. Hauptausschuss Nr. 17/507.

34 Landesrektorenkonferenz des Landes Nordrhein-Westfalen u.a., Stellungnahme zum NRWDSAnpUG-EU v. 06.04.2018, Stellungnahme f. d. Hauptausschuss Nr. 17/507, Anlage, 4 f.

die Hochschulen die Forschung, wie die nicht-öffentlichen Stellen, auf Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) zu stützen. Dessen Anwendungsverbot für Behörden sei auch überwindbar, weil die dienstliche Betätigung der höchstpersönlichen Wissenschaftsfreiheit gerade – anders als das verwaltungsrechtliche Hochschulhandeln – nicht von Art. 6 Abs. 1 S. 2 DSGVO gemeint sei.³⁵

Aus der Wissenschaftsfreiheit gem. Art. 5 Abs. 3 GG und seines einfachrechtlich konkretisierenden § 4 Abs. 1 HG NRW werden Land und Hochschulen dazu verpflichtet, jeder Aushöhlung der Freiheitsgarantien vorzubeugen. Für das einzelne Hochschulmitglied resultiert daraus kein originärer Leistungsanspruch, also auch kein Grundaussstattungsanspruch für die Ausübung der grundgesetzlichen Freiheiten aus Art. 5 Abs. 3 S. 1 GG. Es besteht nur ein Anspruch auf verhältnismäßige und am allgemeinen Gleichheitssatz orientierte Teilhabe an Leistungen und Einrichtungen, die vom Staat bereitzustellen sind. Werden diese Grundsätze auf das Datenschutzrecht übertragen, so ergibt sich, dass die jeweilige Hochschule für die in ihrem Rahmen durchgeführten wissenschaftlichen Forschungsvorhaben gem. Art. 4 Nr. 7 DSGVO verantwortlich ist, da sie die personellen, finanziellen und organisatorischen Mittel der in ihrem Verantwortungsbereich durchgeführten Forschungsvorhaben festlegt und verteilt werden, sodass die Hochschule dadurch zumindest mittelbar Einfluss auf die Datenverarbeitungszwecke nimmt.³⁶

In Betracht kommt auch eine gemeinsame Verantwortung von Hochschulen und Wissenschaftlern gem. Art. 26 DSGVO. Immerhin entscheiden neben den Hochschulen auch Wissenschaftler über die konkreten Zwecke und Mittel der Datenverarbeitung. Nach Ansicht des EuGH bedarf es dafür keiner Parität zwischen den Verantwortlichen, eine Beteiligung an der Entscheidung über die Zwecke und Mittel der Verarbeitung reicht für eine gemeinsame Verantwortung aus.³⁷

4. Möglichkeit der Stellvertretung für Datenschutzbeauftragte (§ 31 DSGVO NRW)

Der Gesetzgeber hat mit § 31 DSGVO NRW die Möglichkeit eröffnet neben der oder dem behördlichen Datenschutzbeauftragten auch Stellvertreter zu benennen. Dies folgt einem praktischen Verlangen, auch in Übergangsphasen eine Person in Stellen zu haben, die die Aufgaben eines Daten-

schutzbeauftragten wahrnimmt, ohne diese Person auch dauerhaft zum Datenbeauftragten zu ernennen.³⁸ Mit § 31 präzisiert und konkretisiert der Gesetzgeber Art. 37 und 39 DSGVO, welche die Stellung und Aufgaben des Datenschutzbeauftragten beschreiben.³⁹ Eröffnet wird die Möglichkeit der Stellvertretung in Art. 37 Abs. 1 DSGVO. Durch die Formulierung, der Verantwortliche habe „auf jeden Fall einen Datenschutzbeauftragten“ zu benennen, ist bei entsprechender Auslegung die Möglichkeit der Benennung mehrerer Datenschutzbeauftragter eröffnet. Bei der Benennung mehrerer Datenschutzbeauftragter ist insoweit eine klare Aufgabentrennung zu fordern, bspw. in die Bereiche Mitarbeiterdatenschutz und sonstigen Kontakt der Behörde nach außen mit Bürgern oder Lieferanten.⁴⁰



Prof. Dr. Rolf Schwartzmann

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)



Dr. Tobias Jacquemain (LL.M)

Er ist promovierter Datenschutzrechtler und als Wissenschaftlicher Referent bei der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) beschäftigt. Zudem ist er Lehrbeauftragter an der Universität zu Köln sowie an der Technischen Hochschule (TH) Köln.

35 Vgl. Schwartzmann/Pabst-Schwartzmann/Hermann, § 17 DSGVO NRW, Rn. 3.

36 Vgl. Schwartzmann/Pabst-Schwartzmann/Hermann, § 17 DSGVO NRW, Rn. 4 unter Verweis auf EuGH ZD 2018, 357 (359) Rn. 43 – Wirtschaftsakademie; U. v. 05.06.2018 – C-210/16 Rn. 34 ff. – Fanpages; U. v. 10.07.2018 – C-25/17 Rn. 69 – Zeugen Jehovas.

37 GDD, Stellungnahme zum NRWDSAnpUG-EU v. 06.04.2018, Stellungnahme f. d. Hauptausschuss Nr. 17/488, 6.

38 § 31 Rn. 1

39 § 31 Rn. 3

Joachim Schütz/Sonja Schmitz/Jan Ippach

Die elektronische Patientenakte – Anforderungen aus Sicht des Datenschutzes

I. Vorbemerkung

Die elektronische Patientenakte (ePA) soll eines der zentralen Elemente der vernetzten Gesundheitsversorgung und eine wichtige Zäsur bei der Entwicklung einer umfassenden Telematikinfrastruktur im Gesundheitswesen darstellen¹. Aktuell ist das Vorhaben abermals in die Kritik und damit ins Stocken geraten, da in dem bisher vorliegenden Gesetzentwurf² zur konkreten

Ausgestaltung notwendiger Bestimmungen zur Bereitstellung und Nutzung der ePA datenschutzrechtliche Mindestanforderungen nicht hinreichend abgebildet werden konnten³. An einem Gesetzentwurf, mit dem insbesondere die datenschutzrechtlichen Fragen rechtssicher gelöst werden sollen, wird aktuell gearbeitet. Welche Handlungsoptionen sich insoweit für den Gesetzgeber anbieten oder sogar aufdrängen, soll nachfolgend diskutiert werden.

II. Rechtsgrundlagen

Um beurteilen zu können, welche – weiteren – legislativen Maßnahmen für eine datenschutzrechtlich „saubere“ Ausgestaltung der ePA notwendig und – vor dem Hintergrund der DS-GVO – zulässig sind, soll zunächst die gegenwärtige Sach- und Rechtslage beschrieben werden:

Stand 8/2019 findet sich die zentrale Rechtsgrundlage für die Zurverfügungstellung und Nutzung der ePA in § 291 a Abs. 3 S. 1 Nr. 4 SGB V.

Danach ist die elektronische Patientenakte eine von mehreren Anwendungen der elektronischen Gesundheitskarte (eGK). Die ePA soll eine fall- und einrichtungsübergreifende Dokumentation über den Versicherten darstellen. Spätestens ab dem 01.01.2021 sind die gesetzlichen Krankenkassen verpflichtet, ihren Versicherten gemäß §§ 291a, 291 b SGB V eine von der Gesellschaft für Telematik nach § 291b Abs. 1a S. 1 zugelassene ePA zur Verfügung zu stellen (vgl. § 291a Abs. 5c S. 4 SGB V). Die ePA ist als freiwillige versichertengeführte Akte angelegt. Deren Inhalte sind Leistungserbringern nur mit Einwilligung des Versicherten zugänglich. Inhalte kann der Versicherte eigenständig löschen und auf sein ausdrückliches Verlangen kann er Inhalte von Leistungserbringern und seiner Krankenkasse einstellen lassen und/oder eigene Inhalte einstellen.

Die ePA ist kein Abbild der ärztlichen Dokumentation.⁴ Ziel ist es eher, ein von den Informationssystemen der Leistungserbringer unabhängiges Aktensystem des Patienten an die Primärsysteme der Leistungserbringer anzuschließen.⁵

Gesetzlich Versicherte haben einen Rechtsanspruch auf die Nutzung ihrer ePA; alle Leistungserbringer sind verpflichtet, ihren Patienten die Daten, die über diese erhoben wurden, in deren ePA bereitzustellen – wenn der Patient es wünscht.

1. Inhalte der ePA

In die ePA sollen gemäß § 291a Abs. 3 S. 1 Nr. 4 SGB V Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen aufgenommen werden können. Gemäß § 291a Abs. 5c S. 2 SGB V soll die ePA ferner geeignet sein, weitere medizinische Daten der Versicherten für deren Behandlung verfügbar zu machen, z.B. Daten aus fallbezogenen, einrichtungsübergreifenden Be-

handlungsdokumentationen, eines elektronischen Impf- oder Mutterpasses, Labor- oder radiologische Befunde und Daten aus Früherkennungsuntersuchungen. In die ePA werden lediglich ausgewählte „Kopien“ der in der Sphäre des jeweiligen Leistungserbringers verbleibenden Originale eingespeist, so dass keine Garantie auf Vollständigkeit besteht.⁶

Aktuell gilt das „Alles-oder-Nichts-Prinzip“: Eine differenzierte Freigabe einzelner Dokumente aus der ePA an den Leistungserbringer ist bis auf Weiteres nicht möglich.⁷ Sofern der Versicherte seine Einwilligung erteilt, kann der Leistungserbringer alle Daten des Versicherten sehen. Erst in der Weiterentwicklung der ePA-Spezifikationen sollen technischen Vorgaben und Details für ein differenziertes Berechtigungskonzept, nach dem auch einzelne ePA-Daten mit Leistungserbringern geteilt werden können, zur Verfügung gestellt werden.

2. Kreis der Zugriffsberechtigten

Zum Zwecke des Erhebens, Verarbeitens oder Nutzens mittels elektronischer Gesundheitskarte⁸ dürfen, soweit es zur Versorgung der Versicherten erforderlich ist, ausschließlich

1 Bales/Dierks et al., eGK, 2007, A, Rn. 3; Holland, in: Duttge/Dochow, eGK, 2009, S. 14; Dochow, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, S. 1021; vgl. auch Antwort des BMG vom 01.08.2019 auf die Kleine Anfrage der Abgeordneten Schulz, Cotar, Eschpiller und weiterer Abgeordneter und der Fraktion der AfD betreffend „Die Vereinbarkeit der elektronischen Patientenakte mit dem Datenschutz“, BT-Drs. 19/11756, S. 1.

2 Vgl. Referentenentwurf des BMG für ein Digitale Versorgung-Gesetz (DVG) vom 15.05.2019, hier: § 291h SGB V – E.

3 Berichterstattung in der Ärztezeitung („Spahn muss bei Patientenakte in die Warteschleife“ und „Spahn streicht Regelungen zur elektronischen Patientenakte“) vom 05.07.2019 sowie („Gesetz zur digitalen Versorgung auf dem Weg“) vom 10.07.2019. Interview Handelsblatt (vom BMG selbst veröffentlicht): „Das Prinzip lautet: Nicht App statt Arzt, sondern Arzt und App“ vom 11.07.2019 unter <http://www.bundesgesundheitsministerium.de/presse/interviews/interviews/handelsblatt-110719.html>.

4 Bales/Dierks et al., eGK, 2007, B I, § 291a, Rn. 43; Müller, DÄBL. 2008, A-571, A-752; Dochow, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, S. 1024.

5 Dochow, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, S. 1024.

6 Dochow, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, S. 1024 f.

7 So auch die Aussage der Gesellschaft für Telematik in einer Mitteilung vom 21.05.2019.

- Ärzte
 - Zahnärzte
 - Apotheker, Apothekerassistenten, Pharmazieingenieure, Apothekenassistenten
 - Berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf bei den zuvor genannten o. in einem Krankenhaus
 - Psychotherapeuten
auf Daten zugreifen (vgl. § 291a Abs.4 S.1 Nr.2 SGB V).
- Nach dem Entwurf zum DVG sollen zukünftig auch Angehörige der Pflegeberufe, Hebammen und Physiotherapeuten zugriffsberechtigt sein.⁹

3. Datenfluss – Kette der Datenverarbeitung

Nach dem Wortlaut des § 291a Abs. 5c S.4 SGB V sind die Krankenkassen verpflichtet, ihren Versicherten bis spätestens 01. Januar 2021 eine elektronische Patientenakte zur Verfügung zu stellen.¹⁰ Unklar bleibt, wie das „zur Verfügung stellen“ in rechtlicher Hinsicht umgesetzt werden soll, insbesondere, wenn man die beiden Varianten der ePA (mit und ohne eGK) betrachtet. Welche sozial-, zivil- und datenschutzrechtlichen (Leistungs-)beziehungen hier zwischen Versicherten – Krankenkassen – ePA-Anbieter (Betreiber) und Leistungserbringer entstehen, hängt von mehreren Umständen ab, insbesondere davon, ob die Krankenkasse selbst Anbieter der ePA ist oder hierfür ein externes Unternehmen beauftragt¹¹. Rechtlich unklar bleibt auch die Rolle der gematik. Letzteres wird der Regelfall sein.

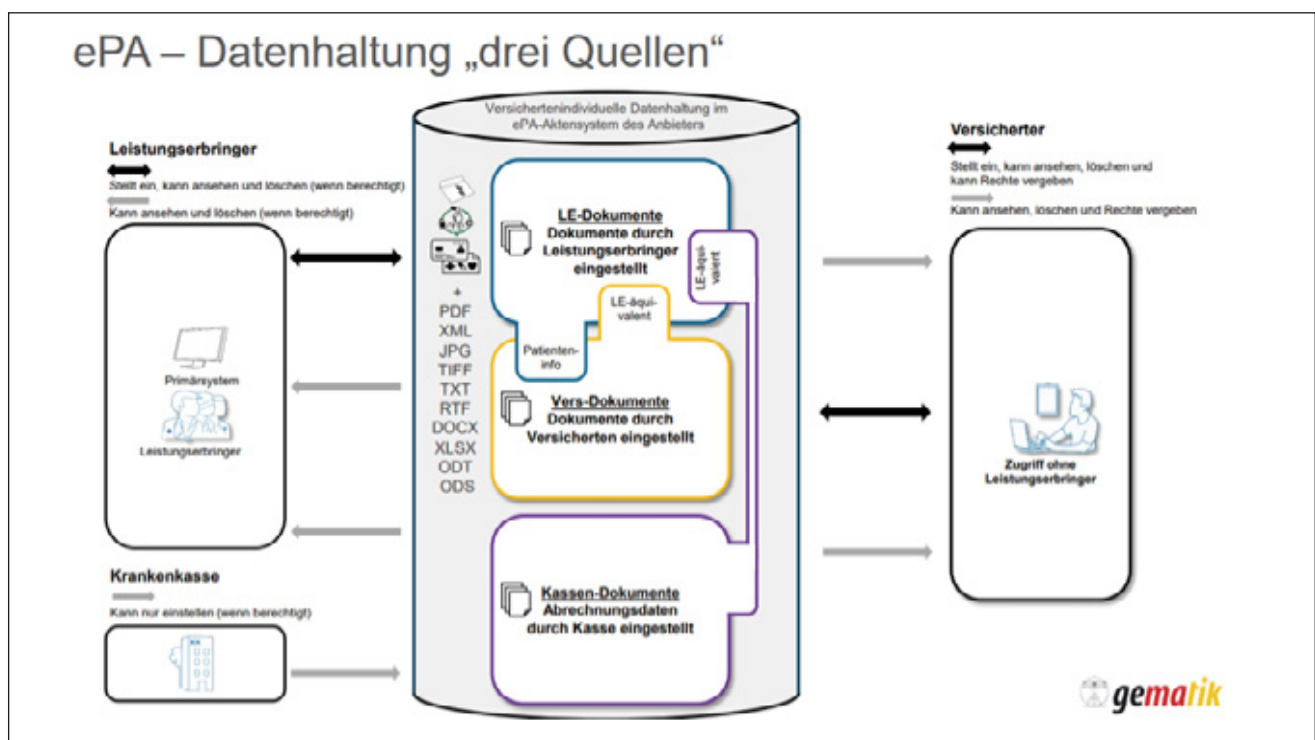
So hat die gematik Ende 2018 die Vorgaben und Zulassungsverfahren zur ePA bereitgestellt. Anhand dieser können Anbieter ihre Aktenlösungen nach § 291a SGB V implementieren und eine Zulassung durch die gematik beantragen¹². Dafür müssen sie nachweisen, dass ihre ePA die Anforderungen an Funktionalität und Sicherheit erfüllt. Das gewährleistet, dass die verschiedenen zugelassenen Aktenlösungen untereinander interoperabel sind, sodass Versi-

cherte ihren Anbieter wechseln können, ohne bereits in ihrer ePA gespeicherte Daten zu verlieren.

Die Wahl der Technologie, also die Frage, ob eine zentrale Speicherung erfolgt (zumeist auf nicht einem, sondern auf verteilten Servern) oder dezentrale Speichertechnologien zum Einsatz kommen, ist vom Gesetz her grundsätzlich offen. Nach dem aktuellen Stand werden die Daten der Versicherten patientenindividuell verschlüsselt auf dem Server des jeweiligen Betreibers gespeichert. Die entsprechenden Server müssen sich auf dem Gebiet eines Mitgliedstaates der Europäischen Union bzw. des Europäischen Wirtschaftsraums befinden. Für die Akte selbst, die Benutzerschnittstelle zu den Versicherten und den Konnektor, werden darüber hinaus Sicherheitsnachweise gefordert. Aufgrund der patientenindividuellen Verschlüsselung und weiterer Sicherheitsmaßnahmen wie einer vertrauenswürdigen Ausführungsumgebung für die Suche innerhalb der Metadaten und einer chipkartenbasierten Public-Key-Infrastruktur sollen die Daten vor Einsichtnahme sowohl durch den Anbieter bzw. Betreiber der elektronischen Patientenakte als auch durch Angreifer auf den Server und die Kommunikationswege geschützt werden.¹³

Für die Datenhaltung in der ePA selbst sind drei „Quellen“ vorgesehen: siehe Grafik

8 Gesetzlich nicht geregelt ist der Kreis der Zugriffsberechtigten bei Nutzung einer ePA ohne Einsatz der elektronischen Gesundheitskarte.
 9 Vgl. Referentenentwurf des BMG für ein Digitale Versorgung-Gesetz (DVG) vom 15.05.2019, hier: § 291a Abs. 4 Nr. 2 g) SGB V – E.
 10 § 291a Abs. 5c S. 4 SGB V.
 11 Vgl. hier die Ausführungen unter III.5.
 12 Vgl. Faktenblatt der Gematik vom Oktober 2018.
 13 Antwort des BMG vom 01.08.2019 auf die Kleine Anfrage der Abgeordneten Schulz, Cotar, Ependiller und weiterer Abgeordneter und der Fraktion der AfD betreffend „Die Vereinbarkeit der elektronischen Patientenakte mit dem Datenschutz“, BT-Drs. 19/11756, S. 5.



a) Der Versicherte und seine Einwilligung in die Datenverarbeitung

Gesetzlich Versicherte können – auf freiwilliger Basis – ihre gesundheitsbezogenen Dokumente mit einer ePA lebenslang verwalten. Die darin enthaltenen Informationen stehen ihnen selbst sowie ihren behandelnden Ärzten, Zahnärzten, Psychotherapeuten und Apothekern sowie weiteren Leistungserbringern zur Verfügung – sofern der Versicherte zuvor die jeweilige Praxis bzw. Apotheke bzw. anderweitigen Leistungserbringer dafür berechtigt hat. Der gesetzlich Versicherte selbst kann Daten einstellen, diese ansehen, löschen und Rechte vergeben. Je Versichertem kann maximal ein ePA-Aktenkonto existieren. Dem Versicherten soll ein einfacher Anbieterwechsel jederzeit möglich sein, und zwar bei vollem Datenerhalt.

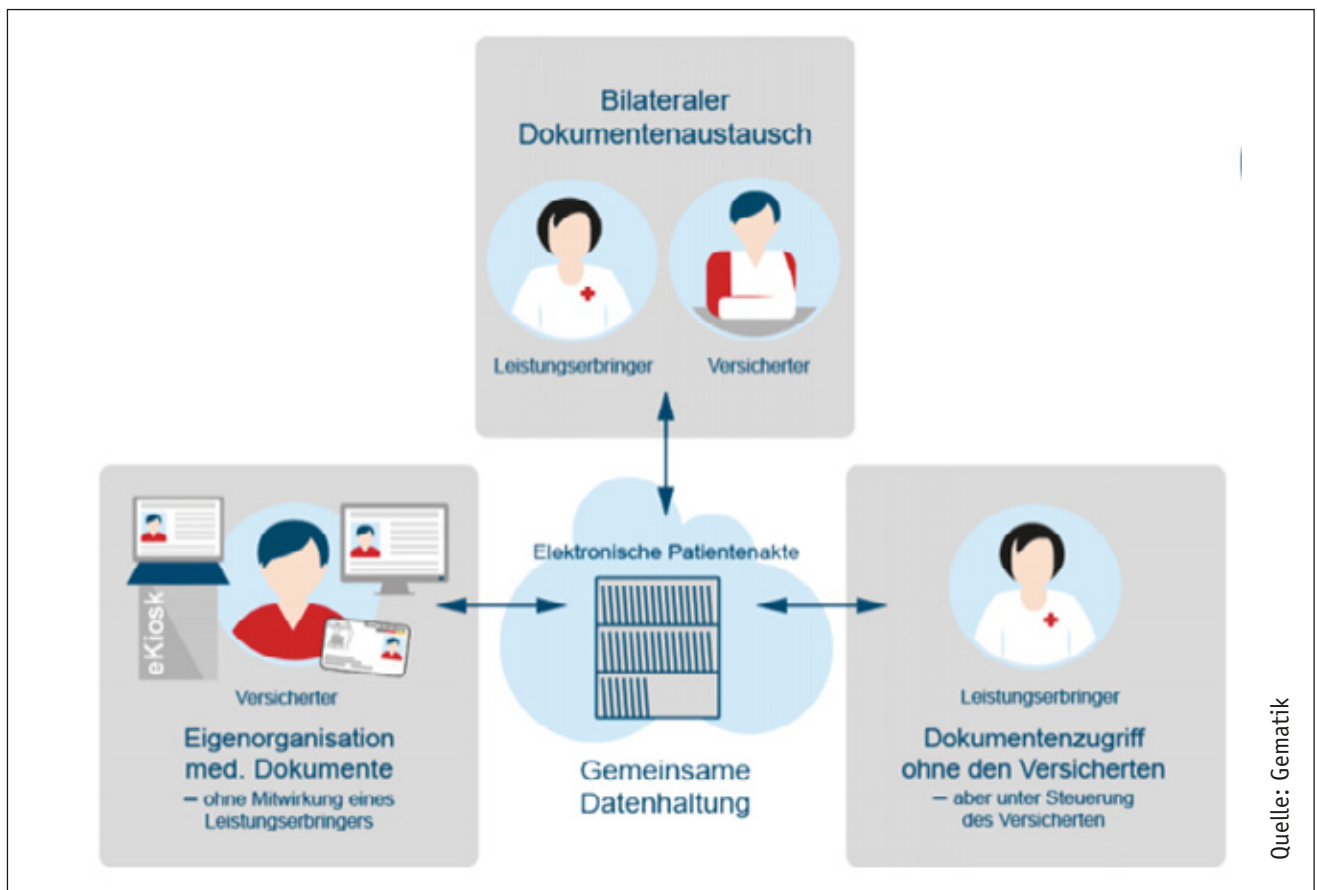
Gemäß § 291a Abs. 5 S. 7, 8 SGB V können Versicherte auf Daten der ePA auch zugreifen, wenn sie sich für den Zugriff durch ein geeignetes technisches Verfahren authentifizieren. Ein solcher Zugriff kann auch ohne Einsatz der elektronischen Gesundheitskarte erfolgen, wenn der Versicherte nach umfassender Information durch seine Krankenkasse gegenüber derselben schriftlich oder elektronisch erklärt hat, dieses Zugriffsverfahren zu nutzen. Entsprechend den Regelungen aus dem TSVG wird für die ePA somit zusätzlich ein alternatives Authentisierungsverfahren für die Versicherten ohne Einsatz der eGK am „ePA-Frontend des Versicherten“ ermöglicht. Dies vereinfacht den Zugriff auf die ePA mit mobilen Endgeräten (Smartphone und Tablets).

b) Der Leistungserbringer – Zugriff nur aufgrund der Einwilligung und mit HBA

Der Zugriff auf Daten mittels der elektronischen Gesundheitskarte darf nur in Verbindung mit einem elektronischen Heilberufsausweis bzw. einem entsprechenden Berufsausweis erfolgen (Vgl. § 291a Abs. 5, 5a SGB V). Leistungserbringer verwenden – wie gehabt – ihre bestehenden Informationssysteme. Nach Freigabe durch den Versicherten (Einwilligung) können sie von dort direkt auf die Dokumente des Versicherten zugreifen – unabhängig davon, welchen ePA-Anbieter der Versicherte gewählt hat. Unterstützt wird – neben eArztbrief, Notfalldatensatz und elektronischem Medikationsplan – eine Vielzahl der gängigen Dokumentformate, wie sie heute in der medizinischen Dokumentation zum Einsatz kommen (PDF, JPG, CDA etc.). Wie hier – zukünftig – mit dem Rechtsinstitut der Einwilligung umzugehen ist und wie die datenschutzrechtlichen Anforderungen hinreichend berücksichtigt werden können, wird unter III. behandelt.

Wenn der Patient es will, lädt der Arzt bestimmte Daten aus seinem Praxisverwaltungssystem (PVS) in die ePA hoch. Die Daten in der ePA sind nur Kopien der Daten aus dem PVS; die Primärdokumentation des Arztes in seinem PVS bleibt davon unberührt.¹⁴ Der Arzt stößt diesen Prozess bewusst selbst an; Daten werden nicht automatisch ohne Wis-

¹⁴ Dochow, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, S. 1021.



sen des Arztes übertragen. Die Betreiber der Patientenakten können nicht auf das PVS der Arztpraxis zugreifen. Ebenso soll es keiner zusätzlichen Hardware bedürfen (Konnektor wird nachgenutzt).

Damit Leistungserbringern ein einfacher Umgang mit der ePA möglich ist, müssen einheitliche Schnittstellen existieren, sodass Praxen unproblematisch mit Akten unterschiedlicher Anbieter arbeiten können. Diese Schnittstellen werden von der gematik spezifiziert. Ebenso bedarf es der Standardisierung der medizinischen Daten für die ePA, damit ein strukturierter Datentransfer der Niedergelassenen untereinander sowie zu Kliniken, zu Apotheken oder zu anderen medizinischen Fachberufen sinnvoll möglich ist. Unter der Bezeichnung medizinische Informationsobjekte (MIOs) werden bis Herbst 2020 erste Standards definiert, zum Beispiel für Labordaten, bestimmte medizinische Befunde oder den Impfpass.

c) Die Krankenkasse

Die Krankenkasse kann Daten nur einstellen, wenn sie hierzu durch den Versicherten berechtigt wird. Sie hat ihre Versicherten gemäß § 291a Abs. 5c) S. 5 SGB V spätestens bei der Zurverfügungstellung der ePA in allgemein verständlicher Form über deren Funktionsweise, einschließlich der Art der in ihr zu verarbeitenden Daten und über die Zugriffsrechte, zu informieren.

III. Legislative Handlungsoptionen – Anforderungen an eine rechtssichere ePA

Will der Gesetzgeber die ePA in datenschutzrechtlicher Hinsicht rechtssicher gestalten, muss zunächst betrachtet werden, welcher gesetzgeberische Rahmen sich hierfür anbietet und welche datenschutzrechtlichen Anforderungen in einem komplexen Zusammenwirken mehrerer Beteiligter zwingend geregelt werden müssen. Einer unbedingten Klärung bedarf aus datenschutzrechtlicher Sicht die Frage nach der Rollenzuordnung der Beteiligten im engeren Sinne – Versicherter, Leistungserbringer und Leistungsträger – und im erweiterten Kreis auch der beteiligten ePA-Anbieter.

Legislative Handlungsmöglichkeiten bestehen innerhalb des nationalen und unionsrechtlich vorgegebenen Rahmens. Der Sozialdatenschutz und das allgemeine Datenschutzrecht – welches Gesundheitsdaten als besonders sensible Daten einstuft – sind hier gleichermaßen von Bedeutung:¹⁵ Die Neufassung des § 35 SGB I in der seit dem 25.05.2018 geltenden Fassung statuiert eine abschließende Geltung der datenschutzrechtlichen Regelungen des Sozialdatenschutzes. Dies gilt gemäß § 35 Abs. 2 S. 1 SGB I jedoch nicht gegenüber den Bestimmungen der DS-GVO, die Anwendungsvorrang genießen.¹⁶

Welche der nachfolgend beschriebenen Handlungsoptionen der Gesetzgeber im Rahmen der Umsetzung des datenschutzrechtlichen Rahmens für die ePA nutzt, soll nachstehend offenbleiben:

Gesetzgeberischer Gestaltungsspielraum eröffnet sich zum einen dort, wo die Aufgaben der Krankenkassen neu definiert werden, denn Voraussetzung für die Anwendbar-

keit des Sozialdatenschutzes ist die Verarbeitung von Sozialdaten. Gemäß § 284 Abs. 1 SGB V dürfen die Krankenkassen Sozialdaten für Zwecke der Krankenversicherung nur erheben und speichern, soweit [...]. Laut der in § 67 Abs. 2 Satz 1 SGB X befindlichen Begriffsdefinition der Sozialdaten handelt es sich hierbei um personenbezogene Daten, die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben in diesem Gesetzbuch verarbeitet werden. Es muss sich also zwingend um Aufgaben der Krankenkassen handeln, die sich aus dem Sozialgesetzbuch selbst ergeben und von den Krankenkassen erfüllt werden.

Einen weiteren Anknüpfungspunkt für gesetzgeberischen Gestaltungsspielraum bietet sich in den seitens der DS-GVO bereitgehaltenen Öffnungsklauseln bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO, worunter auch Gesundheitsdaten als besonders sensible Daten fallen:

Nach der Legaldefinition von Gesundheitsdaten in Art. 4 Nr. 15 DS-GVO sind hierunter personenbezogene Daten zu verstehen, die sich auf den körperlichen oder geistigen Gesundheitszustand einer natürlichen Person, einschließlich der Erbringung von Gesundheitsleistungen, beziehen, und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Zentraler Anknüpfungspunkt stellt hierbei die Einwilligung nach Art. 9 Abs. 2 lit. a) DS-GVO als eine Rechtfertigungsmöglichkeit der Verarbeitung von Gesundheitsdaten als besonders sensible Daten dar. Art. 9 Abs. 2 lit. a) DS-GVO eröffnet den Mitgliedsstaaten hierbei konkret die Möglichkeit, im Rahmen einer „Rückausnahme“ die Verarbeitung von Daten trotz Vorliegens einer ausdrücklichen Einwilligung durch Gesetz zu untersagen. Unter Beachtung grundlegender Grenzen, insbesondere des Rechts auf informationelle Selbstbestimmung, sind die Mitgliedsstaaten insofern frei darin, von dieser Regelungsmöglichkeit Gebrauch zu machen, ebenso darin, das Anforderungsprofil der Einwilligung zu konkretisieren, so zum Beispiel nicht nur eine ausdrückliche, sondern eine schriftliche Einwilligung zu fordern. Lediglich angerissen werden kann in diesem Zusammenhang die Fragestellung, ob die Rechtsprechung des sechsten Senats des BSG¹⁷ unter den aktuell geltenden Rechtsnormen – weiterhin – Anwendung finden kann. Das BSG hatte – unter Anwendung der damaligen Normen – die Ansicht vertreten, dass im Geltungsbereich des SGB V die Weitergabe von Patientendaten durch Leistungserbringer nur dann und in dem Umfang erlaubt sei, in dem bereichsspezifische Regelungen über die Datenverarbeitung im SGB V dies gestatten; die allgemeinen Regelungen des Datenschutzes, die die Datenübermittlung bei Vorliegen einer Einwilligungserklärung gestatten, finden insoweit keine Anwendung. Das BSG wies in diesem Zusammenhang bei dem Punkt der Freiwilligkeit der Einwilligung im Verhältnis zwischen Versichertem zu Leistungserbringer darauf hin, dass nicht anzunehmen

15 Vgl. auch Buchner, Datenschutz im Gesundheitswesen (2. Auflage), A/2.2.1, S. 35.

16 Vgl. auch Wobbe, Datenschutz im Gesundheitswesen – Fragestellungen aus Sicht der Krankenkassen, MedR 2019, 625 ff. (626).

17 BSG, Urt. V. 10.12.2008 – B 6 KA 37/07 R.

sei, dass die Einwilligung freiwillig abgegeben werden könne.¹⁸ Mit Blick auf den Wortlaut des Art. 7 Abs. 1 DS-GVO, wonach Einwilligungen freiwillig sein müssen, und unter Heranziehung des Erwägungsgrundes 43¹⁹ der DS-GVO, wird sich die Frage stellen, ob sich der Anwendungsbereich für Einwilligungen im Hoheitsgebiet des SGB V möglicherweise entsprechend der BSG-Rechtsprechung reduziert.²⁰ Der Grad der Freiwilligkeit der Einwilligung der Versicherten bei Erteilung von Zugriffsberechtigungen auf die in seiner ePA hinterlegten Gesundheits- und ggf. Sozialdaten²¹ dürfte hier jedenfalls gänzlich anders zu bestimmen sein als bei der Einwilligung des Versicherten (Patienten) in die Weitergabe seiner Daten zum Zwecke der Leistungsabrechnung. Nachteile, die der Patient in dem zuletzt genannten Fall zu befürchten hat, also wenn er die Einwilligung nicht erteilt, werden bei der Verweigerung der Zugriffsberechtigung auf die ePA weniger schwerwiegend sein, was im Ergebnis für eine einwilligungsbasierte Lösung spricht; gleichzeitig wird dem Recht auf informelle Selbstbestimmung Rechnung getragen.

Weitere, umfassende Öffnungsklauseln für das Gesundheitswesen finden sich in Art. 9 Abs. 2 DS-GVO, wobei Art. 9 DS-GVO sog. fakultative Öffnungsklauseln gibt – es wird keine Konkretisierung vorgenommen, es werden lediglich Abweichungsmöglichkeiten eröffnet:²² diese erlauben die Verarbeitung von Gesundheitsdaten im Rahmen ihrer gesetzlich umschriebenen Voraussetzungen, enthalten Tatbestandsmerkmale wie etwa die Beschreibung des Zwecks (z.B. Diagnostik), zum Teil zusätzliche personelle Voraussetzungen (Art. 9 Abs. 3 DS-GVO) und das Merkmal der „Erforderlichkeit“ als Grenze für die Verarbeitungstätigkeit. Art. 9 Abs. 2 DS-GVO ist hierbei nicht bei allen dort aufgeführten Erlaubnisgründen die unmittelbar anwendbare Rechtsgrundlage. Die Vorschrift schafft vielmehr sog. Öffnungsklauseln für eine Gesetzgebung der EU-Mitgliedstaaten, und damit gesetzgeberischen Handlungsspielraum: Dem nationalen Gesetzgeber ist es möglich, Rechtsgrundlagen zu schaffen, die dann die eigentliche Erlaubnisnorm sind, so im Rahmen des Art. 9 Abs. 2 Buchst. h DS-GVO (insb. Gesundheitsvorsorge, medizinische Diagnostik, Versorgung oder Behandlung im Gesundheits- oder Sozialbereich), bei Art. 9 Abs. 2 Buchst. i DS-GVO (z.B. zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten), im Rahmen des Art. 9 Abs. 2 Buchst. j DS-GVO (für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke) oder im Rahmen des Art. 9 Abs. 2 Buchst. g DS-GVO (aus Gründen eines erheblichen öffentlichen Interesses).

Da das bisherige Konzept der ePA die freiwillige Einwilligung des Versicherten in den Fokus des Datenschutzkonzepts stellt, sind neben der Einwilligungserklärung als solcher, die inhaltliche und zeitliche Reichweite der Einwilligung (Umfang des Datenzugriffs und Dauer dieser Möglichkeit) und weitere datenschutzrechtlich relevante Punkte zu klären:

1. Informationspflichten gegenüber dem betroffenen Versicherten

Die Pflicht, den einzelnen Betroffenen über Art und Umfang der Verarbeitung seiner Daten zu informieren, ergibt sich unmittelbar aus Art. 13 bzw. Art. 14 DS-GVO.²³ Dies soll eine faire und transparente²⁴ Datenverarbeitung gewährleisten. Zu erteilen hat diese Information der datenschutzrechtlich Verantwortliche, also grundsätzlich bspw. auch der leistungserbringende Vertragsarzt. Ein nicht zu unterschätzendes Problem stellt sich derzeit aufgrund der Tatsache ein, dass keine allgemeingültige Aussage getroffen werden kann, wer für die ePA verantwortlich ist. Dies hängt entscheidend von der Frage ab, welche Stellen bei der jeweiligen ePA im Einzelfall zugriffsberechtigt sind. Hier ist der Gesetzgeber gefragt, eine Ausgestaltung zu wählen, die eine Zuordnung von Verarbeitungsvorgängen zu den Verantwortlichen ermöglicht. Andernfalls würde dies zu einer nicht hinnehmbaren Rechtsunsicherheit führen.

Zu überlegen ist, ob die Haltung der Bundesregierung etwas an dieser Einschätzung ändert, hat diese doch auf eine Anfrage erklärt, dass beabsichtigt sei, Informationspflichten der Krankenkassen über die ePA gesetzlich zu regeln.²⁵ Intention scheint es hierbei jedoch in erster Linie zu sein, das Bewusstsein der Versicherten für die ePA zu schärfen. Dies wird nicht zuletzt daran deutlich, dass die Beantwortung der Fragestellung mehr im Kontext einer etwaigen Informations- und Aufklärungskampagne zu stehen scheint.

Ohnehin ist die jeweilige Krankenkasse verpflichtet, über die ePA – einschließlich der Art der in ihr zu verarbeitenden Daten – zu informieren; dies gilt auch hinsichtlich der verschiedenen Zugriffsrechte und -wege.²⁶ Die Verpflichtung folgt aus der datenschutzrechtlichen Verantwortlichkeit der Krankenkassen gegenüber den Versicherten. Die Versicherten können nur dann von den ihnen zustehenden Rechten Gebrauch machen, wenn sie wissen, dass personenbezogenen Daten überhaupt, bzw. welche Daten zu welchen Zwecken,²⁷ verarbeitet werden. Nur so kann das Recht auf informationelle Selbstbestimmung bei der Datenerhebung und -verarbeitung sichergestellt werden. An diesem Grundsatz ist auch im Zusammenhang mit der ePA festzuhalten. Der

18 BSG, Urt. V. 10.12.2008 – B 6 KA 37/07 R – Rn. 37, 38.

19 Eine Einwilligung ist nicht als freiwillig anzusehen, wenn ein klares Ungleichgewicht zwischen betroffener Person und dem Verantwortlichen der Datenverarbeitung besteht.

20 Vgl. auch Wobbe, Datenschutz im Gesundheitswesen – Fragestellungen aus Sicht der Krankenkassen, MedR 2019, 625 ff. (629).

21 Vgl. hierzu Kühling, Datenschutz im Gesundheitswesen, MedR (2019) 37, S. 615, 616, wonach Patientendaten gleichzeitig Gesundheitsdaten und Sozialdaten sein können.

22 Vgl. auch Kühling, Datenschutz im Gesundheitswesen, MedR (2019) 37, S. 611 ff. (612); Greve, in: Auernhammer, DS-GVO/BDSG, Art. 9 DS-GVO Rn. 17.

23 Vgl. Eßer, in: Auernhammer, DS-GVO/BDSG, Art. 13 DS-GVO Rn. 3.

24 Vgl. Kingreen/Kühling, Gesundheitsdatenschutz, S. 76 mit Hinweis auf BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83.

25 BT-Drs. 19/3627, S. 5.

26 Vgl. hierzu auch unter III.4.

27 Schwartmann/Jaspers/Thüsing/Kugelman (Schneider), Heidelberger Kommentar Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 13 DS-GVO Rn. 38.

Umfang der Informationspflicht kann sich dabei nicht lediglich auf die freiwilligen Anwendungen der ePA beschränken, da nicht von vornherein feststeht, welche Anwendungen der Versicherte zu nutzen beabsichtigt. Mit anderen Worten: Um eine vollumfängliche Information zu erteilen, welche letztlich Grundlage der freiwilligen Einwilligung des Versicherten sein soll, muss sowohl über die Pflichtenwendungen als auch über freiwillige Anwendungen im Zusammenhang mit der eGK informiert werden.

Beachtlich ist, dass die Regelung des § 291a Abs. 2 S. 2 SGB V – immer noch – einen Verweis auf § 6c BDSG a.F. enthält, welcher im Zusammenhang mit der Novellierung des BDSG weggefallen ist. Der hinter der Regelung stehende Grundgedanke sollte indes weiter Anwendung finden können. Hiernach waren sowohl derjenige, der ein mobiles Speichermedium (also die eGK) ausgibt, als auch derjenige, der personenbezogene Daten auf ein solches Medium aufbringt oder ändert,²⁸ einer umfangreichen Informations- und Transparenzpflicht unterworfen.

2. Rechtsansprüche des Versicherten

Eine besondere Relevanz im Zusammenhang mit der ePA liegt darin, die Datenhoheit der Versicherten nachhaltig zu gewährleisten. Dies gilt insbesondere für den datenschutzrechtlichen Anspruch bestimmen zu können, wer Zugriff auf den Inhalt der ePA nehmen bzw. bereitgestellte Inhalte im Sinne eine Berichtigung ändern darf. Neben der Berichtigung wird den Versicherten zudem auch der Anspruch zugestanden werden, Inhalte der ePA (partiell) zu löschen bzw. löschen zu lassen.²⁹ Die sich hieraus unter Umständen ergebende Unvollständigkeit der ePA ist dem derzeitigen Konzept immanent, will man die datenschutzrechtlichen Ansprüche der Versicherten realisieren. Sich zwingend ergebende haftungsrechtliche Fragestellungen, die sich aufgrund dieser – bewusst oder unbewusst – herbeigeführten

Unvollständigkeit ergeben können, sollen nicht Gegenstand dieses Artikels sein. Dabei soll allerdings nicht unerwähnt bleiben, dass eine namenhafte Stelle sich bereits dahingehend positioniert hat, dass die ePA nicht die Kommunikation unter den Ärzten oder mit anderen Einrichtungen des Gesundheitswesens ersetze. Dies bedeutet im Umkehrschluss, der behandelnde Arzt darf sich nicht darauf verlassen, dass die ePA die vollständige Behandlungshistorie der Versicherten umfasst.

Besondere Bedeutung kommt auch der Datentransportabilität, also dem Recht der Versicherten auf Datenübertragbarkeit zu (Art. 20 DS-GVO), da die Datenverarbeitung im Zusammenhang mit der ePA regelmäßig aufgrund der Einwilligung der Versicherten erfolgen wird (Art. 20 Abs. 1 lit. a i.V. mit Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DS-GVO). Der Verantwortliche muss also sicherstellen, dass die ePA-Daten in einem strukturierten, gängigen und maschinenlesbaren Format³⁰ zur Verfügung stehen. Auch hier stellt sich wiederum das Problem der bisweilen ungeklärten Verantwortlichkeiten im Zusammenhang mit der ePA. Die Datentransportabilität soll gewährleisten, dass es jederzeit möglich ist, Daten auf eine andere (neue) ePA zu übertragen. Es kann somit zu einem „Zusammenspiel“ eines „alten“ mit einem „neuen“ Verantwortlichen kommen, soweit bspw. der Versicherte seine Krankenkasse wechselt.

In diesem Zusammenhang bleibt abzuwarten, in welche Richtung sich die ePA-Architektur entwickeln wird und der derzeitige Konsens zwischen GKV-SV, KZBV und KBV Bestand haben wird.

28 Vgl. hinsichtlich der Zugriffsberechtigten unter II. 2.

29 Wobei in datenschutzrechtlicher Hinsicht (Art. 17 Abs. 1 DS-GVO) hierbei entweder von einem teilweisen Einwilligungswiderruf oder aber eines Zweckwegfalls aufgrund Entscheidung des Patienten ausgegangen werden müsste; beides darf durchaus zur rechtlichen Diskussion gestellt werden.

30 Vgl. Schürmann, in: Auernhammer, DS-GVO/BDSG, Art.20 DS-GVO Rn. 7 ff.

Differenz der aktuellen Aktenmodelle und gemeinsamer Konsens für die 291a-Akte

Aktenmodelle heute aufgrund ihrer entscheidenden Dimensionen nicht vereinbar.		Dimension: Anbindung	
		Datenübergabe (Versicherte übergibt Daten an LE)	Berechtigung (Versicherte gibt LE Berechtigung)
Dimension: Datenhaltung	Zentral (auf der ePA des Versicherten)	TK / BITMARCK →	gematik
	Dezentral (in der Umgebung des LE als auch auf ePA des Versicherten)	-	↑ AOK
<p>Konsens: Gematik-Modell als gemeinsame Perspektive der ePA-Architektur (insb. beim Berechtigungskonzept). Eine Datenübermittlung erfolgt an die zentrale ePA-Umgebung des Versicherten nach dessen Zustimmung aus dem Primärsystem des Leistungserbringers. Dahinterliegende dezentrale Konzepte zur Datenhaltung obliegen dem ePA-Anbieter.</p>			

Quelle: KBV

Die Genannten einigten sich zuletzt darauf, dass das sog. „Gematik-Modell“ Grundlage der gemeinsamen Perspektive der ePA-Architektur sein soll. Dieses Modell umfasst unter anderem eine Datenübermittlung an eine zentrale ePA-Umgebung aus den Primärsystemen der verschiedenen Leistungserbringer. Die Datenhaltung hingegen soll dezentral stattfinden und den ePA-Anbietern – also den Krankenkassen – obliegen.³¹

3. Gewährleistung der allgemeinen Grundsätze: Zweckbindung, Datensparsamkeit etc.

Von nicht zu unterschätzender Bedeutung für eine rechtssichere Handhabung der ePA sind die in Art. 5 Abs. 1 DS-GVO aufgeführten Grundprinzipien der Datenverarbeitung, insbesondere der Zweckbindungsgrundsatz und der Grundsatz der Datenminimierung. Als bedeutsamstes Grundprinzip bei der Datenverarbeitung³² verlangt der Zweckbindungsgrundsatz in Art. 5 Abs. 1 lit. b DS-GVO, dass Gesundheitsdaten nur „für festgelegte, eindeutige und legitime Zwecke“ erhoben werden dürfen. Um dem Recht auf informationelle Selbstbestimmung Ausdruck zu verleihen, ist der verfolgte Zweck maßgeblich für die Frage der Rechtmäßigkeit der Datenverarbeitung.³³ Insofern ist es unverzichtbar, bei der gesetzlichen Ausgestaltung der Bestimmungen zur ePA festzulegen, wer wie lange zu welchem Zweck auf welche Daten und in welchem Umfang – lesen, herunterladen, schreiben, verändern oder löschen – zugreifen darf. Letztlich wird hieran die freiverantwortliche Einwilligung des Versicherten zu messen sein.

Entsprechend dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO), wonach die Verarbeitung personenbezogener Daten auf das für den Zweck erforderliche Maß beschränkt sein muss, ist zu fordern, dass die digitale Information über den Gesundheitszustand des Versicherten sowohl einzeln als auch zeitlich befristet zur Verfügung gestellt werden kann. Auch mit Blick auf die Gesundheitskompetenz des Versicherten wird man fordern müssen, den Zugriff auf die digitale Information in ihrem Umfang zu minimieren, damit auch der Versicherte abschätzen kann, welche Information er konkret mit welchen Folgen zur Verfügung stellt. Entgegen dem aktuell verankerten „Alles-Oder-Nichts-Prinzip“ muss dem Versicherten eine differenzierte Freigabe einzelner Dokumente aus der ePA ermöglicht werden. Ebenso muss der Kreis der Zugriffsberechtigten für den Versicherten frei bestimm- und einschränkbar sein (siehe unten).

4. Rechte der Zugriffsberechtigten – differenziert nach Inhalten

Um sich die Notwendigkeit differenzierter Zugriffsberechtigungen auf die in der ePA enthaltenen Daten zu vergegenwärtigen, bedarf es sowohl eines Blicks auf den Umfang der Daten, die der Versicherte per Einwilligung preisgibt als auch auf den Kreis derjenigen, die per Gesetz Zugriff auf diese nehmen können: In Erweiterung des aktuell in § 291a Abs. 4 S. 1 SGB V aufgeführten Kreises – Ärzte, Zahnärzte, Apotheker, Apothekerassistenten, Pharmazieingenieure, Apothekenassistenten, berufsmäßige Gehilfen oder zur Vor-

bereitung auf den Beruf bei den zuvor genannten oder in einem Krankenhaus, Psychotherapeuten – sollen nach dem aktuellen Gesetzesentwurf zum DVG auch Angehörige der Pflegeberufe, Hebammen und Physiotherapeuten mit Einwilligung des Patienten auf Daten zugreifen können.³⁴ Daten in einer ePA nach dem im Gesetzesentwurf geplanten § 291h SGB V neu sollen Befunddaten, vom Versicherten selbst zur Verfügung gestellte Daten, für den Versicherten zur Verfügung gestellte Daten sowie weitere Daten, die sich nicht ohne weiteres in die drei Alternativen des § 291a Abs. 2 Nr. 4 SGB V einordnen lassen, sein. Aus datenschutzrechtlicher und auch verbraucherpolitischer Sicht ist es gerade vor dem Hintergrund des Alles-oder-Nichts-Prinzips bei der per Einwilligung freigegebenen Datenmenge unerlässlich, eine – nach Inhalten – differenzierte Zugriffsberechtigung gesetzlich zu verankern: Als Minimum dürfte eine Unterscheidung zwischen Leistungserbringerdaten, Krankenkassendaten und vom Versicherten selbst zur Verfügung gestellten Daten zu treffen sein. In einem zweiten Schritt wäre ein gesetzliches Konzept von Zugriffsberechtigungen zu verankern, welches den Kreis derjenigen konkret zeichnet, die auf bestimmte Datenbereiche zugreifen dürfen und wie konkret sich der Zugriff gestaltet. Dies gilt gleichermaßen für Behandlungsdaten wie auch für Leistungsdaten. Der Versicherte muss hier jederzeit Herr seiner Daten sein und ausdifferenziert Berechtigungen erteilen und widerrufen können. Der Gesetzgeber wird dieses Recht nicht einschränken können.

5. Beschreibung der Rollen der Beteiligten (Versicherter, KK, Betreiber, LE)/Datenverantwortliche

Wie bereits an anderer Stelle angesprochen, werden die „Datenverantwortlichen“ (Betroffener, Verantwortlicher, gemeinsame Verantwortliche, Auftragsdatenverarbeiter, etc.) in Bezug auf die ePA im SGB V bislang nicht ausdrücklich benannt und lassen sich mangels ausdrücklicher gesetzlicher Beschreibung aus den §§ 291a ff. SGB V nicht rechtssicher identifizieren. Im engeren, organisatorischen Kern wird man im Gesundheitsdatenschutz grundsätzlich von einer Akteurstrias „Versicherter – Leistungserbringer – Leistungsträger bzw. Krankenkasse“³⁵ ausgehen können, wobei der von der Krankenkasse beauftragte Anbieter einer ePA hinzutreten kann. Der Versicherte als Empfänger gesundheitsbezogener Leistungen kann zweifelsohne als von der Datenverarbeitung Betroffener qualifiziert werden. Nach der Definition des Verantwortlichen i.S.d. Art. 4 Nr. 7 DS-GVO ist hierunter jede natürliche oder juristische Person, Be-

31 Vgl. Letter of Intent zwischen KZBV, KBV und GKV-Spitzenverband, abrufbar unter https://www.kbv.de/media/sp/LoI_ePA_final.pdf, zuletzt abgerufen am 22.08.2019

32 Herbst, in: Kühling/Buchner, Art. 5 DS-GVO, Rn. 5; Kramer, in: Auernhammer, Art. 5 DS-GVO Rn. 16.

33 Schwartmann/Jaspers/Thüsing/Kugelmann (Hermann), Heidelberger Kommentar Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 5 DS-GVO Rn. 40 ff.

34 Vgl. Referentenentwurf des BMG für ein Digitale Versorgung-Gesetz (DVG) vom 15.05.2019, hier: § 291a Abs. 4 Nr. 2 g) SGB V – E.

35 Vgl. Kühling, Datenschutz im Gesundheitswesen, MedR (2019) 37, S. 611 ff. (617).

hörde, Einrichtung oder andere Stelle zu verstehen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Hierunter könnten zum einen die Leistungsträger bzw. Krankenkassen zu fassen sein, die per gesetzlichen Auftrag in § 291a Abs. 5 c SGB V dazu verpflichtet sind, ihren Versicherten ab dem 01.01.2021 eine von der gematik nach § 291 b Abs. 1a S. 1 SGB V zugelassene ePA zur Verfügung zu stellen und/oder die gematik selbst, die konkret dafür zuständig ist, die erforderlichen Voraussetzungen dafür zu schaffen, dass den Versicherten Daten in einer ePA bereitgestellt werden können. Bei der gematik dürfte die Qualifikation als Verantwortliche im Ergebnis wohl zu verneinen sein, da sie selbst nicht konkret über die Zwecke und Mittel der Verarbeitung entscheidet, lediglich den „Rahmen“ für die Struktur der ePA „liefert“.

Gesetzlich unklar ist ferner die Rolle der ePA-Anbieter bzw. ePA-Betreiber, die die von der gematik aufgestellten Anforderungen zwecks Zulassung erfüllen müssen und seitens der Krankenkasse ausgewählt werden, um ihren Versicherten eine ePA-Lösung anzubieten: Handelt es sich bei den ePA-Anbietern um „Auftragsverarbeiter“ im Sinne des Art. 4 Nr. 8 DS-GVO – also um eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet? Nicht ausgeschlossen erscheint es an dieser Stelle auch, die Krankenkasse und den von dieser beauftragten ePA-Anbieter als gemeinsame Verantwortliche im Sinne des Art. 26 Abs. 1 DS-GVO, die als Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, zu qualifizieren.

Die bisherige Rechtslage rund um die ePA wirft eine Vielzahl von Fragen nach Rollen und Verantwortlichkeiten auf und zeichnet ein komplexes datenschutzrechtliches Zusammenspiel der Akteure. Die Vielzahl und das Nebeneinander unterschiedlicher gesetzlicher Normierungen tragen nicht zur Rechtssicherheit bei, eine Vereinfachung der Normenstruktur und Transparenz bleiben zu wünschen übrig.³⁶ Notwendig ist eine gesetzgeberische Klärung bzw. Klarstellung der Rechtsverhältnisse der unterschiedlichen Akteure im Zusammenhang mit der ePA, von der ausgehend sich die Fragen rund um die Einwilligung des Versicherten als Ausdruck der Datensouveränität sowie die Rollenverhältnisse und die Beachtung des Zweckbindungsgrundsatzes sodann klären lassen dürften.

IV. Ausblick

Wesentlich für eine rechtssichere Ausgestaltung der (bereichsspezifischen) Regelungen zum Angebot und zur Nutzung der ePA wird es sein, dass der Gesetzgeber in einer Art „Rollen – Rechte – Konzept“ die Zuständigkeiten und Verantwortlichkeiten der Beteiligten klar und möglichst abschließend regelt. Gemeint ist hier (noch) nicht das

Datenschutzrecht, sondern zunächst die eindeutige Beschreibung und Festlegung der sozial- und zivilrechtlichen Leistungsbeziehungen. Erst im Anschluss daran kann die Entscheidung getroffen werden, ob und, wenn ja, welche bereichsspezifischen Datenschutzregelungen notwendig sind, um die erforderliche Rechtssicherheit zu erreichen. Klar ist, dass jede – formal zulässige – Abweichung von den Vorgaben der DS-GVO das Risiko in sich birgt, dass Kollisionen zwischen nationalem Recht und Gemeinschaftsrecht die Folge sind, und sei es, dass diese Kollisionen erst aufgrund von nachgelagerten Entscheidungen des EuGH zu Tage treten.



Joachim Schütz

Herr Schütz ist Justiziar des Deutschen Hausärzterverbandes e.V. und Partner der Medizinrechtskanzlei Dr. HALBE in Köln. Für die Mitglieder im Deutschen Hausärzterverband hat Herr Schütz zur Umsetzung des neuen Datenschutzrechts umfassende Informationen und Arbeitshilfen erstellt sowie zahlreiche Veranstaltungen durchgeführt. Den Schwerpunkt hat Herr Schütz dabei auf die Themen gelegt, die in der täglichen Praxis besonders relevant sind.



Sonja Schmitz

Frau Schmitz ist Syndikusanwältin im Deutschen Hausärzterverband e.V. Für die Mitglieder im Deutschen Hausärzterverband erstellt Frau Schmitz umfassende Informationen und Arbeitshilfen. Der Schwerpunkt der Tätigkeit von Frau Schmitz liegt in den Gebieten des Datenschutz-, Sozial- und Vereinsrechts.



Jan Ippach, LL.M.

Rechtsanwalt in der ausschließlichen auf den Gebieten des Medizinrechts sowie des Wirtschaftsrechts im Gesundheitswesen bundesweit tätigen Kanzlei DR. HALBE RECHTSANWÄLTE mit Standorten in Köln und Berlin. Veröffentlichungen, Vorträge und Veranstaltungen zu medizin- und datenschutzrechtlichen Themen.

³⁶ Vgl. ähnlich Kühling, Datenschutz im Gesundheitswesen, MedR (2019) 37, S. 611 ff. (621).

Andreas Jaspers/Dr. Tobias Jacquemain, LL.M.

Künstliche Intelligenz und ihre Auswirkungen auf den Beschäftigtendatenschutz

Die bestehenden datenschutzrechtlichen Regelungen ermöglichen den Einsatz von Künstlicher Intelligenz im Rahmen des Beschäftigungsverhältnisses. Insbesondere im laufenden Beschäftigungsverhältnis darf bei Personalentscheidungen nicht

allein auf die Künstliche Intelligenz abgestellt werden. Die arbeitgeberseitige Fürsorgepflicht gebietet durch Künstliche Intelligenz erzeugte Entscheidungen zumindest eine Überprüfung durch einen entscheidungsbefugten Personalverantwortlichen.

I. Künstliche Intelligenz (KI) im Beschäftigungsverhältnis

1. Definition der KI durch die Datenethikkommission (DEK)

In einer Empfehlung für die Strategie Künstliche Intelligenz der Bundesregierung hat die Daten-ethikkommission (DEK) folgende Begriffsdefinition für Künstliche Intelligenz (KI) vorgenommen:

„Wir verstehen „Künstliche Intelligenz“ in diesem Zusammenhang als Sammelbegriff für diejenigen Technologien und ihre Anwendungen, die durch digitale Methoden auf der Grundlage potenziell sehr großer und heterogener Datensätze in einem komplexen und die menschliche Intelligenz gleichsam nachahmenden maschinellen Verarbeitungsprozess ein Ergebnis ermitteln, das ggf. automatisiert zur Anwendung gebracht wird. Die wichtigsten Grundlagen für KI als Teilgebiet der Informatik sind die subsymbolische Mustererkennung, das maschinelle Lernen, die computergerechte Wissensrepräsentation und die Wissensverarbeitung, welche Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung umfasst.“¹

Diese Begriffsdefinition ist sehr generisch. Eine effektive Regelungsfähigkeit des Einsatzes der KI im Beschäftigungsverhältnis setzt deutlich erkennbare Anwendungsszenarien und damit einhergehende tatsächliche Veränderungen für die Arbeitswelt voraus, um hierfür regulierende Rahmenbedingungen zu setzen.

2. Auswirkungen der KI auf Beschäftigungsverhältnisse

Da Anwendungen mit KI in alle Lebensbereiche eingreifen können und auch immer mehr menschliches Verhalten in immer breiteren Handlungsfeldern automatisieren und ersetzen sollen, wird sich auch die Arbeitswelt durch die KI verändern. KI-gesteuerte Systeme sind für ihr Funktionieren auf große Datenmengen angewiesen. „Die konkrete Funktionsweise ist zudem in besonderer Weise abhängig von der Auswahl und der Qualität der jeweils eingegebenen und/oder für die Entwicklung („Training“) genutzten Daten.“²

Sowohl Quantität als auch Qualität der Daten sind in der Konsequenz der Motor und der Kraftstoff für KI-Anwendungen. Im Beschäftigungsverhältnis muss somit der Beschäftigte selbst zum Datenlieferanten werden, damit die Tech-

nologie einen effektiven Nutzen entfalten kann. Ohne eine entsprechende Datengrundlage funktionieren die KI-Anwendung zugrundeliegenden Algorithmen nicht.

Mittels „trial and error“ wird der Beschäftigte als betroffene Person zum Datensubjekt, bei dem so lange zulässige Lösungsmöglichkeiten versucht werden, bis die gewünschte Lösung gefunden wurde. Die dabei beim Beschäftigten erhobenen Daten können den Algorithmen etwa zum Targeting oder zur Erkennung von Mustern oder strukturellen Prozessen dienen.

II. Rechtlicher Rahmen

Die Verarbeitung personenbezogener Daten und mithin ihre Erhebung ist grundsätzlich verboten, sofern dafür keine rechtliche Erlaubnis gegeben ist. Nur wenn einer der Erlaubnistatbestände erfüllt ist, dürfen Daten mit Personenbezug oder Personenbeziehbarkeit verarbeitet werden. Nach diesem Regelungskonzept ist grundsätzlich jede Verarbeitung personenbezogener Daten rechtfertigungsbedürftig, sofern sie in den sachlichen (Art. 2) und räumlichen (Art. 3) Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) fällt. Unter diesen regulatorischen Rahmen fallen auch die für KI-Systeme erforderlichen Daten von Beschäftigten und ihre Verarbeitung.

1. Entwicklung von KI bzw. Algorithmen

Eine Software mit KI muss mit riesigen Datenmengen versehen werden und daraus Muster erkennen. Zu vernachlässigen ist aber nicht, wie die Muster zustande kommen. In einem zweiten Schritt werden dafür von der programmierenden Person Regeln hinzugefügt. Man kann zum Beispiel festlegen, dass mehrjährige Beschäftigungspausen in einem Bewerbungsprozess nachteilig gewertet werden. Anschließend sucht die Software aus Millionen oder Milliarden Kombinationsmöglichkeiten die beste Lösung für ein Problem heraus. Die KI vermag frühzeitig zu erkennen, welche theoretischen Optionen effektiv wirken können und verwirft alle übrigen Optionen unverzüglich. Es wird deswegen stets Zeit in Anspruch nehmen, bis das Zusammenspiel so funktio-

¹ Datenethikkommission, Empfehlungen der Datenethikkommission für die Strategie Künstliche Intelligenz der Bundesregierung, 09.10.2018, 1.

² Datenethikkommission, Empfehlungen der Datenethikkommission für die Strategie Künstliche Intelligenz der Bundesregierung, 09.10.2018, 2.

niert, dass KI-Systeme Aufgaben übernehmen und mithin eigenständige Entscheidungen treffen können. Experten und Data Scientists müssen die Daten vorsortieren und die Software beherrschen.

Die den KI-Anwendungen zugrundeliegenden Algorithmen arbeiten zwar mit statistischen Methoden, fallen aber nur unter die Ausnahme für statistische Zwecke, wenn sie im öffentlichen Interesse durchgeführt werden.³ Für die Auswertung großer, aus einer Vielzahl unterschiedlicher Quellen stammender unstrukturierter Daten zum Zwecke der Erkennung von Gesetzmäßigkeiten, Korrelationen und Kausalitäten und der Generierung neuer Informationen (Kontextwissen) wird regelmäßig auf Art. 6 Abs. 4 DS-GVO als Rechtsgrundlage verwiesen.⁴ Bei der Auswertung vorhandener Daten bzw. unter Hinzuspeichern weiterer Daten zu einem bereits existierenden Datensatz werden neue, spezifischere Informationen zu einer bereits zuvor individualisierten natürlichen Person generiert, weswegen bei solchen Szenarien der zwingend erforderliche Einsatz von wirksamen Pseudonymisierungstechniken durch umfassende Transparenz und Betroffenenrechte, insbesondere durch ein Widerspruchsrecht, geboten ist.⁵ Unter dem Vorhandensein geeigneter Garantien erscheint die Entwicklung von KI bzw. von entsprechenden Algorithmen auf Grundlage des Art. 6 Abs. 4 DS-GVO denkbar. Eine Weiterverarbeitung i.S.d. Art. 6 Abs. 4 DS-GVO unter anderem für wissenschaftliche Forschungs- oder für statistische Zwecke gilt überdies nicht als unvereinbar mit den ursprünglichen Zwecken.⁶

Die Weiterverarbeitung personenbezogener Daten muss aber auch kollektivarbeitsrechtlich legitimiert sein. Hier bestehen gemäß § 87 Abs. 1 Nr. 6 BetrVG und gleichlautender Regelungen der Personalvertretungsgesetze umfassende Mitbestimmungsrechte der Mitarbeitervertretungen. Sofern die Mitarbeitervertretungen die Zustimmung der Datennutzung für die Generierung von KI verweigern, fehlt jedenfalls für Deutschland eine aussagekräftige Datenbasis für KI-Anwendungen. Diese müsste aus Ländern ohne arbeits- oder datenschutzrechtliche Restriktionen gewonnen werden. Deren Implikationen kultureller und rechtliche Art mit Blick auf die Nutzung in der deutschen Arbeitswelt sollte vorab untersucht werden.

2. Rechtmäßigkeit der Anwendung von KI bzw. Algorithmen

Nachdem die KI einsatzbereit zur Verfügung steht gilt es zu überprüfen, ob diese neue Technologie auch angewendet werden darf.

a) Beschäftigtendatenschutzrecht

Die Zulässigkeit der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses richtet sich nach der Erforderlichkeit

„für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung

*(Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten“.*⁷

Für alle Erlaubnistatbestände des § 26 Abs. 1 BDSG ist das Merkmal der Erforderlichkeit für die Zweckerreichung der zentrale Maßstab für die Zulässigkeit und Rechtmäßigkeit der Datenverarbeitung. Insoweit ist zu untersuchen, inwieweit der Einsatz von KI-Anwendungen als erforderlich qualifiziert werden kann.

aa) KI erforderlich für das Beschäftigungsverhältnis?

Für die Beurteilung der Erforderlichkeit kann auf die zu § 32 BDSG a.F. entwickelten Grundsätze zurückgegriffen werden, da der Gesetzgeber dieses Kriterium bewusst beibehalten hat.⁸ Erforderlich i.S.v. § 32 Abs. 1 S. 1 BDSG a.F. ist die Datenverarbeitung zur Informationsgewinnung nur, wenn ein berechtigtes, billigeswertes und schutzwürdiges Interesse des Arbeitgebers an der Beantwortung seiner Fragen bzw. der sonstigen Informationsbeschaffung besteht und das Interesse des Arbeitnehmers an der Geheimhaltung der Daten das Interesse der Arbeitgeber an ihrer Erhebung nicht überwiegt.⁹ Im Falle der Bewerbung eines Arbeitnehmers legt dieser im Bewerbungsprozess personenbezogene Daten offen, damit der Arbeitgeber sich einen Eindruck von der Person und ihren Qualifikationen verschaffen kann. Ein Geheimhaltungsinteresse lässt sich in diesem Beispiel verneinen, sodass aus dem weiten Verständnis der Erforderlichkeit kein Hindernis für den Einsatz von KI-Anwendungen resultiert; wie hier im Beispiel, um die Bewerbungen mit Hilfe von KI zu sichten und zu bewerten.

Problematischer dürfte die Erforderlichkeit der Nutzung von KI im laufenden Beschäftigungsverhältnis zu beurteilen sein. KI kann beispielsweise dazu genutzt werden, Teamstrukturen zu analysieren und zu optimieren (agiles Arbeiten). Durch den ggfls. nicht unerheblichen Eingriff in das Persönlichkeitsrecht der Beschäftigten ist die Zusammenstellung von Arbeitsteams unter Einsatz allein auf Effektivität ausgerichteter KI mit der arbeitgeberseitigen Fürsorgepflicht kritisch zu hinterfragen.

bb) Überwachungsdruck

Um erhebliche Datenmengen für das Funktionieren der Algorithmen zu generieren, droht der Beschäftigte in eine Totalüberwachung zu geraten. Die permanente Leistungsmessung vermag große Datensätze zu produzieren, die Aufschluss über Erfolgsmuster und effiziente Arbeitsweisen bieten können. Solche Daten sind für die funktionierende Anwendung von KI-System maßgeblich. Der Beschäftigte droht dadurch aber in eine permanente Beobachtung zu ge-

3 Simitis/Hornung/Spiecker gen. Döhmman-Roßnagel, Datenschutzrecht, 2019, Art. 6 Abs. 4 DS-GVO, Rn. 42.

4 Vgl. Gola-Schulz, DS-GVO, 2. Aufl., 2018, Art. 6 DS-GVO, Rn. 254.

5 Vgl. Gola-Schulz, DS-GVO, 2. Aufl., 2018, Art. 6 DS-GVO, Rn. 258.

6 Paal/Hennemann, Big Data im Recht, NJW 2017, 1697 (1700).

7 § 26 Abs. 1 S. 1 BDSG.

8 Paal/Pauly-Gräber/Nolden, 2. Aufl. 2018, § 26 BDSG, Rn. 14.

9 Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, 7. Aufl., 2016, Rn. 597.

raten. Auch wenn es keiner dauerhaften visuellen Kontrolle (Videoüberwachung) des Beschäftigten für die Datengenerierung bedarf, ist der Eingriff doch vergleichbar. Die Analogie zur Videoüberwachung bietet rechtliche Orientierung über die Zulässigkeit einer potenziellen Totalüberwachung. Schon die Möglichkeit der jederzeitigen Überwachung erzeugt einen mit dem Anspruch des Arbeitnehmers auf Wahrung seiner Persönlichkeitsrechte (§ 75 Abs. 2 BetrVG) regelmäßig nicht zu vereinbarenden Druck.¹⁰ Deswegen ist eine Dauerhebung beim Beschäftigten rechtlich nicht begründbar.

b) Interessenabwägung

Der § 26 BDSG regelt die Verarbeitung personenbezogener Daten von Beschäftigten nicht abschließend. Daher ist es zumindest denkbar, dass sich die rechtmäßige Verarbeitung von Beschäftigtendaten zur Anwendung von KI-Systemen alternativ auf Art. 6 Abs. 1 lit. f DS-GVO stützen kann. Lässt sich der Einsatz von KI-gestützten Anwendungen als berechtigtes Interesse qualifizieren, gilt es demgegenüber den Eingriff in die Rechte der Beschäftigten abzuwägen. Überwiegen die schutzbedürftigen Interessen der Beschäftigten, so kann Art. 6 Abs. 1 lit. f DS-GVO den Einsatz von KI nicht legitimieren. In Betracht kommen dafür sog. „beschäftigungsfremde“ Zwecke, die außerhalb der Zweckbestimmung „Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses“¹¹ liegen. Für solche Datenverarbeitung abseits des eigentlichen Beschäftigungszwecks relevant ist, ob der Beschäftigte vernünftigerweise erwarten kann oder konnte, dass möglicherweise eine Verarbeitung für diesen aus Sicht des Arbeitgebers berechtigten Zweck erfolgen wird bzw. erfolgt ist.¹² Davon wird im Falle des Einsatzes von KI regelmäßig nicht auszugehen sein.

c) Transparenzpflichten

Nach Art. 5 Abs. 1 lit. a DS-GVO muss eine Verarbeitung personenbezogener Daten nicht nur rechtmäßig, sondern auch transparent erfolgen. Die mit der DS-GVO stark erweiterten Informationspflichten nach Art. 13/14 DS-GVO stellen eine weitere Herausforderung für den Einsatz von KI-Systemen dar, sofern eine Rechtmäßigkeit gegeben ist.

Sofern der Einsatz von KI als Profiling i.S.d. Art. 4 Abs. 4 DS-GVO qualifiziert werden kann, ist dem Betroffenen dem Wortlaut nach und unter teleologischen Gesichtspunkten zwingend Kenntnis über involvierte Logik, Tragweite und angestrebte Auswirkungen zu verschaffen. Denn ohne zumindest ein grundlegendes Verständnis der Funktionsweise des hinter dem Profiling steckenden mathematischen Algorithmus ist es der betroffenen Person andernfalls regelmäßig nicht möglich, von außen etwaige Verstöße zu erkennen. Wie immer im Datenschutzrecht bedarf es auch hier einer Abwägung zwischen den Interessen der betroffenen Person und der verarbeitenden Stelle. Insbesondere soll dieses Recht Geschäftsgeheimnisse nicht beeinträchtigen. Um der betroffenen Person dennoch die geforderten Informationen zur Verfügung zu stellen, ist daher ein gewisser Abstraktionsgrad erforderlich, um einerseits den Schutz von

Geschäftsgeheimnissen zu wahren und andererseits die geforderte Transparenz der Verarbeitung herzustellen. Dabei wird der Verantwortliche die grundsätzliche Funktionsweise der automatisierten Entscheidungsfindung, die möglicherweise mit dem KI-Einsatz einhergeht, beschreiben müssen und die einfließenden Faktoren jedenfalls insoweit benennen, wie dies dem Schutz von Geschäftsgeheimnissen nicht entgegensteht. Nötigenfalls sind – auch wenn es sich hierbei nicht um Profiling handelt – die Faktoren abstrakt zu beschreiben oder in Gruppen zusammenzufassen. Eine allgemeine, verständliche Beschreibung der Berechnungsgrundlagen von Algorithmen und der Methodik dieser Berechnungen zur Erfüllung der Informationspflicht ist demnach ausreichend. Die Mitteilung des mathematischen Algorithmus selbst, der in aller Regel ein Geschäftsgeheimnis darstellen wird, ist hingegen nicht erforderlich, um die Informationspflicht zu erfüllen.¹³

d) Automatisierte Einzelentscheidung

Gelingt der KI eine wie von ihr beabsichtigte eigenständige Entscheidungsfindung, droht damit eine automatisierte Einzelentscheidung einherzugehen, die gem. Art. 22 DS-GVO regelmäßig untersagt ist. Aus einer ausschließlich automatisierten Bewertung einzelner Persönlichkeitsmerkmale dürfen demnach keine negativen Konsequenzen erwachsen. Fehlt es an einer für eine ausgeschriebenen Stelle erforderlichen Qualifikation und erfolgt aufgrund dessen eine Absage an den Bewerber, handelt es sich hierbei noch nicht um eine automatisierte Einzelentscheidung. Eine „ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende Entscheidung“¹⁴ ist nicht gegeben, wenn die mithilfe eines Systems gewonnenen Erkenntnisse nur die Grundlage einer nicht nur formalen menschlichen Letztentscheidung bilden. Fällt der Unternehmer aufgrund eines Rankings der Bewerberdaten durch ein System letztlich selbst die Entscheidung, welche Bewerber zum Vorstellungsgespräch eingeladen werden, so ist der Tatbestand des Art. 22 DS-GVO eben nicht erfüllt. Erfolgt hingegen eine vollautomatisierte Absage aufgrund einer KI-Anwendung, handelt es sich wegen der rechtlichen Wirkung dabei um eine automatisierte Einzelentscheidung, die gem. Art. 22 DS-GVO verboten ist. Die KI hat damit den Menschen erübrigt, der für die Rechtmäßigkeit einer solchen Handlung mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung gem. Art. 22 DS-GVO nötig ist.

Vielfach werden im laufenden Beschäftigungsverhältnis nur Entscheidungen aus dem Einsatz von KI resultieren, die nicht von der Regelung des Art. 22 DS-GVO erfasst sind, da sie keine unmittelbare Rechtswirkung entfalten oder den

10 Vgl. Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, 7. Aufl., 2016, Rn. 1200. Vgl. dazu BAG, RDV 1992, 179; ferner BAG, DB 1988, 403; ebenso LAG Frankfurt, BB 1990, 1280; ferner BVerwG, RDV 1989, 80.

11 Vgl. § 26 BDSG.

12 Vgl. Gola-Gola, DS-GVO, 2. Aufl., 2018, Art. 6 DS-GVO, Rn. 101.

13 Vgl. Schwartmann/Jaspers/Thüsing/Kugelmann-Schwartmann/Schneider, DS-GVO/BDSG, 1. Aufl., 2018, Art. 13 DS-GVO, Rn. 56, 58.

14 Art. 22 Abs. 1 DS-GVO.

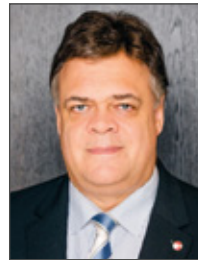
Grad der „erheblichen Beeinträchtigung“ nicht erreichen. Gleichwohl können diese Entscheidungen aber für die Persönlichkeitsrechte der Beschäftigten im Arbeitsverhältnis Auswirkungen haben. Aufgrund der arbeitgeberseitigen Fürsorgepflicht erscheint eine entsprechende Regelung i.S.d. Art. 22 DS-GVO für die durch KI getroffenen Entscheidungen mit Auswirkungen auf das Arbeitsverhältnis erwägenswert, insbesondere ein Recht auf menschliche Überprüfung und Letztentscheidung.

e) Diskriminierungsverbot, AGG

Bereits im Jahr 2014 hat Amazon in den USA eine Software entwickelt, die mittels KI ein Ranking der eingegangenen Bewerbungen erstellen sollte. Der Einsatz der Software führte dazu, dass Frauen diskriminiert wurden. Im Fall von Amazon bevorzugte das System vor allem technikaffine Bewerber. Da es in der IT-Branche mehr Männer gibt als Frauen, hat die KI geschlussfolgert, dass sich vor allem Männer für das Unternehmen interessieren und filterte Frauen eher heraus. In einem weiteren Fall in den USA erbrachte die KI, dass die Mitarbeiter, die weiter weg von der Arbeitsstelle wohnen, schneller ihre Stelle kündigen. Nicht berücksichtigt wurde allerdings, dass in den Außenbezirken oft Menschen wohnen, die einer ethnischen Minderheit angehören und damit unbeabsichtigt, aber faktisch im Auswahlverfahren diskriminiert wurden.¹⁵

Eine grundsätzliche geschlechtsbezogene oder ethnische Bevorzugung verstößt aber gegen das Allgemeine Gleichbehandlungsgesetz (AGG), das diskriminierende Datenverarbeitungen verbietet.¹⁶ Die Einsatz von KI im Beschäftigungsverhältnis bedarf also vor deren Nutzung der Erprobung, um diskriminierungsrelevante Auswirkungen zu ermitteln und auszuschließen.

keit aus, ein Beschäftigtendatenschutzgesetz zu erlassen. Die wiederholt von den jeweiligen Bundesregierungen der letzten Koalitionen geäußerte Absicht, den Datenschutz im Beschäftigungsverhältnis zu regulieren, hat sicherlich im Allgemeinen ihre Berechtigung, aber begründet sich nicht im Einzug von KI in die moderne Arbeitswelt.



Andreas Jaspers

Rechtsanwalt Andreas Jaspers ist Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD).



Dr. Tobias Jacquemain (LL.M)

Er ist promovierter Datenschutzrechtler und als Wissenschaftlicher Referent bei der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) beschäftigt. Zudem ist er Lehrbeauftragter an der Universität zu Köln sowie an der Technischen Hochschule (TH) Köln.

III. Fazit

Die KI wird zweifellos auch Auswirkungen auf Beschäftigungsverhältnisse haben. Zum jetzigen Zeitpunkt lösen die daraus erwachsenen Konsequenzen keine Notwendig-

15 Vgl. Wilke, Künstliche Intelligenz diskriminiert (noch), Zeit Online, 18.10.2018, online abrufbar unter: <https://www.zeit.de/arbeit/2018-10/bewerbungsroboter-kuenstliche-intelligenz-amazon-frauen-diskriminierung> (26.03.19).
 16 Vgl. Gola/Pötters/Wronka, Handbuch Arbeitnehmerdatenschutz, 7. Aufl., 2016, Rn. 789.

PrivacyConnect Kostenloser PrivacyConnect-Workshop
CCPA & GDPR Community by OneTrust in Ihrer Nähe

Themenschwerpunkte:


 DSGVO


 CCPA


 Vorfallsmanagement


 Cookie-Einwilligungen


 Lieferantenrisikomanagement

Wien | 13.11.19

Köln | 15.11.19

Berlin | 22.11.19

Hamburg | 28.11.19

Jetzt anmelden unter: www.privacyconnect.com/workshops

Kurzbeiträge

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (43): Einzelfragen zur DSB-Benennungspflicht im 1. TB DS-GVO des LfDI Thüringen

Zusammengestellt und erläutert von Prof. Peter Gola*

Der im Juni 2019 erschienene 1. Tätigkeitsbericht DS-GVO des LfDI Thüringen befasst sich umfangreich mit der Pflicht zur Benennung von Datenschutzbeauftragten (Ziff. 5.16 TB) und dabei auch mit Bestellung von Datenschutzbeauftragten bei Personalvertretungen (Ziff. 5.12 TB). U.a. wird ausgeführt:

I. Bestellpflicht bei Verarbeitungen „Besonderer Kategorien“ von Daten

Die Benennungsvoraussetzungen für Datenschutzbeauftragte finden sich in Art. 37 Abs. 1 der DS-GVO. Darüber hinaus hat sich der Gesetzgeber entschlossen, im Rahmen einer Öffnungsklausel nationale Regelungen zum DSB zu erlassen. Daher ist neben den Regelungen der DS-GVO bei der Beurteilung, ob eine Benennungspflicht besteht, auch § 38 BDSG zu beachten. Der Verantwortliche und der Auftragsverarbeiter müssen nach Art. 37 Abs. 1 Buchstabe b) und c) DS-GVO auf jeden Fall einen DSB benennen, wenn die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art.9 der DS-GVO besteht.

Zu den besonderen Kategorien von Daten zählen gemäß Art. 9 Abs. 1 der DS-GVO in Verbindung mit Art. 4 Nr. 15 der DS-GVO auch sensible bzw. sensitive Daten in Form von Gesundheitsdaten. Gemäß Art. 4 Nr. 15 der DS-GVO sind „Gesundheitsdaten personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“. Verantwortliche sowie Auftragsverarbeiter im Gesundheitsbereich (z.B. Ärzte oder Apotheker) müssen nach Art. 37 Abs. 1 Buchstabe c) der DS-GVO einen Datenschutzbeauftragten benennen, wenn „die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9“ besteht.

II. Die Verarbeitung (sensibler) personenbezogener Daten als Kerntätigkeit

Erwägungsgrund 97 Satz 2 stellt fest, dass sich der Begriff der Kerntätigkeit auf die Haupttätigkeit und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit bezieht. Nach allgemeiner Auffassung muss die Datenverarbeitung eine essentielle Maßnahme zum Erreichen der Ziele des Verantwortlichen bzw. Auftragsverarbeiters darstellen. Das Erstellen von Gehaltsabrechnungen und IT-Support sind oft häufige Beispiele für datenschutzrelevante Kerntätigkeiten oder Kerngeschäfte einer nicht-öffentlichen bzw. öffentlichen Einrichtung. Trotz ihrer Notwendigkeit oder Unverzichtbarkeit werden solche Tätigkeiten gemeinhin eher als Nebenfunktionen und nicht als eigentliche Kerntätigkeit betrachtet. Der Begriff der Kerntätigkeit steht in Wechselwirkung zum Umfang der Tätigkeit, sodass eine Gesamtbeurteilung vorgenommen werden muss. In der Literatur (Bergt/Kühling/Buchner, DS-GVO, Art. 37, Randnummer 24) wird beispielsweise bei der Bewertung der Tätigkeit von Ärzten als Kerntätigkeit folgendes vertreten: Ziel der Tätigkeit von Ärzten ist es, Menschen gesund zu machen. Um aber herauszufinden, wie das Leiden eines Patienten zu bekämpfen ist – oder ob, im Fall von Vorsorgeuntersuchungen, überhaupt ein Problem besteht –, ist eine umfassende Untersuchung und Beobachtung des Patienten erforderlich, typischerweise auch regelmäßig über einen längeren Zeitraum [...]. Die Kerntätigkeit von Ärzten liegt damit in der Verarbeitung sensibler Daten“. Diese Argumentation gilt analog auch für Apotheker, da auch hier die Diagnostik und Beratung über die Einnahme von Medikamenten im Vordergrund steht, sodass auch hier die Kerntätigkeit in der Verarbeitung sensibler Daten liegt (so auch der Beschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 26. April 2018 „Datenschutzbeauftragten-Bestellpflicht nach Art. 37 Abs. 1 Buchstabe c) Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs).

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

Maßgeblich bei der Bewertung der Erforderlichkeit eines Datenschutzbeauftragten ist, ob eine Verarbeitung sensibler personenbezogener Daten umfangreich im Sinne des Art. 37 Abs.1 Buchstabe c) der DS-GVO ist. In Erwägungsgrund 91 zur DS-GVO ist in Bezug auf die Datenschutz-Folgenabschätzung ebenfalls von einer „umfangreichen Verarbeitung“ die Rede. Darin heißt es: „Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogener Daten Patienten oder Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalts erfolgt“. Der Begriff „Gesundheitsberuf“ ist im Sinne der Aufzählung nach § 203 Abs.1 Strafgesetzbuch (StGB) ausulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

Am 26. April 2018 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die EntschlieÙung „Datenschutzbeauftragten-Bestellpflicht nach Art. 37 Abs. 2 Buchstabe c) DS-GVO bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs“ veröffentlicht: <https://www.tlfdi.de/tlfdi/datenschutz/datenschutzkonferenz/bundesund-laender/95/>. Darin wird ausdrücklich festgehalten: Soweit ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen betreibt und mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, besteht eine gesetzliche Verpflichtung zur Benennung eines DSB. Bei Angehörigen eines Gesundheitsberufs, die ihre Tätigkeit in einer Berufsgemeinschaft (Praxisgemeinschaft) ausüben und weitere Ärzte oder Apotheker beschäftigen, ist dann nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne des Art. 37 Abs. 2 Buchstabe c) DS-GVO auszugehen, wenn in einer Praxisgemeinschaft weniger als zehn Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind“.

Anmerkung: Es ist davon auszugehen, dass die von den Aufsichtsbehörden für die Konkretisierung des Begriffs der „umfangreichen Verarbeitung“ gewählte Zahl von hiermit Beschäftigten Bezüge zu der in der Regelung des § 38 Abs. 1 BDSG hat, was aber nicht die Übernahme der dort mit dem 2. DS-GVO AnpUG bewirkten Erhöhung auf 20 einschlägig Beschäftigte bedingt.

Zu beachten ist jedoch auch hier, dass, wenn bei der Verarbeitung personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zu erwarten ist, eine Datenschutz-Folgenabschätzung vorgeschrieben ist (Art. 35 Abs. 1 DS-GVO). Damit ist immer zwingend ein Datenschutzbeauftragter zu benennen, auch wenn weniger als zehn Personen mit der Verarbeitung personenbezogener Daten besonderer Kategorien beschäftigt sind“.

Im Zusammenhang mit den Benennungsvoraussetzungen äußert sich der LfDI u.a. dann auch ausführlich zur Frage von Inkompatibilitäten bei Nicht-Vollzeittätigkeit des DSB.

III. Anforderungen an den Datenschutzbeauftragten und Inkompatibilitäten

Ein Kandidat muss die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Bei der Einschätzung der Zuverlässigkeit sind sowohl subjektive Faktoren (persönliche Eigenschaften) als auch objektive Faktoren (mögliche Interessenskollisionen) zu berücksichtigen. Beide Kriterien sind bei der Benennung eines Datenschutzbeauftragten gleichgewichtig entscheidend. Eine Interessenskollision ist dann nicht gegeben, wenn zwischen dem Verantwortlichen und dem DSB eine klare Trennung besteht. Bei internen betrieblichen Datenschutzbeauftragten ist hierbei darauf zu achten, dass der Datenschutz mit der primären Verpflichtung vereinbar ist. Eine Vereinbarkeit ist immer dann zu verneinen, wenn die Haupttätigkeit eine Führungs- oder Leitungsposition im Unternehmen darstellt, mit der Verarbeitung personenbezogener Daten verbunden ist oder sich auf diese auswirkt. Insbesondere darf er als DSB in seiner Kontrollfunktion nicht in die Situation kommen sich selbst kontrollieren zu müssen.

Interessenkonflikte können immer dann auftreten, wenn der DSB gleichzeitig Aufgaben wahrnimmt in den Bereichen:

- Personal,
- Justitiariat/Recht,
- Automatisierte Datenverarbeitung (ADV)/ Informationstechnik (IT) oder
- Organisationseinheiten mit besonders umfangreicher oder sensibler Verarbeitung von personenbezogenen Daten wahrnimmt bzw.
- Geheimschutzbeauftragter oder
- Vorsitzender des Personalrats ist.

IV. Keine juristische Personen als Datenschutzbeauftragte

Ob und unter welchen Voraussetzungen juristische Personen als DSB benannt werden können, steht unter den Aufsichtsbehörden noch zur Diskussion. Nach dem ThürLfDI können jedoch juristische Personen nicht als externe DSB benannt werden. Bei der Benennung des Datenschutzbeauftragten liegt der Fokus auf den individuellen Fähigkeiten des DSB. Daher sei es zwar möglich, dass die Person des Datenschutzbeauftragten bei einer juristischen Person angestellt ist, jedoch sei eine Zuordnung einer bestimmten natürlichen Person zum jeweiligen betreuten Unternehmen notwendig, da eine wahllose Vertretung nicht der DS-GVO entspreche.

V. Bestellung eines Datenschutzbeauftragten beim Betriebs- und Personalrat

In Abschnitt 5. 12 befasst sich der ThürLfDI mit der Frage, ob der Personalrat einer öffentlichen Stellen oder der Betriebsrat eines Unternehmens einen eigenen Datenschutzbeauftragten bestellen müsse. Das neue Datenschutzrecht mache dazu keine Aussage. Die neue Rechtslage lege nicht

eindeutig fest, ob Betriebs- und Personalräte als eigenständige Verantwortliche im Sinne der DS-GVO anzusehen sind. Sowohl für die eigene Verantwortlichkeit im Sinne der DS-GVO als auch für die Betrachtung der Vertretung als Teil des Arbeitsgebers finden sich gute Argumente, denn nach der DS-GVO können auch „andere Stellen“ Verantwortliche sein.

Neben anderen Aufsichtsbehörden (z.B. Baden-Württemberg, RDV 2019, S. 75) ist – entgegen der bislang noch eindeutig überwiegend abweichenden Meinung der Literatur – auch der TLfDI nunmehr der Meinung, dass die Personalvertretung einer Dienststelle unter den Begriff des Verantwortlichen im Sinne von Art. 4 Nr. 7 der Datenschutz-Grundverordnung fällt und infolgedessen auch einen eigenen Datenschutzbeauftragten zu bestellen habe. Da der Personalrat insoweit als „Behörde“ einzustufen ist, kommt es auf seine Mitgliederzahl und darauf, wie viele Mitglieder personenbezogene Daten verarbeiten, nicht an. Der LfDI empfiehlt sodann, dass aus Praktikabilitäts- und wohl auch

Kostengründen der behördliche Datenschutzbeauftragte der Dienststelle in Personalunion auch das Amt des Datenschutzbeauftragten der Personalvertretung übernimmt, wenn dazu Einvernehmen zwischen Dienststelle und Personalvertretung besteht. Der Personalvertretung würden somit keine übermäßig rechtlichen oder tatsächlichen Hürden bei der Besetzung des Amtes ihres eigenen Datenschutzbeauftragten auferlegt werden. Dieser Auffassung folgte der Gesetzgeber durch Änderung des § 68 Abs. 1 ThürLPVG.

Für Betriebsräte sei die Situation grundsätzlich keine andere. Jedoch sei es erforderlich, dass es sich um einen Betrieb handelt mit mehr als 401 (demnächst) Arbeitnehmer handele, da dann der Betriebsrat aus 11 (demnächst 20) Mitgliedern bestehe. Dabei geht der LfDI wohl zutreffend davon aus, dass alle Mitglieder bei der Verarbeitung von – vornehmlich Beschäftigte betreffenden personenbezogenen Daten – involviert sind. Berücksichtigt werden muss zudem auch diesbezügliches Personal des Betriebsratsbüros.

Praxisfälle zum Datenschutz I: Einführung in die juristische Prüftechnik und Musterfalllösungen zum Auskunftsbegehren von aktiven und ausgeschiedenen Mitarbeitern

Miriam Claus, LL.B.*, RAin Yvette Reif, LL.M.*

I. Einführung in die juristische Prüftechnik¹

1. Grundlagen der Prüfung juristischer Sachverhalte

a) Rechtsquellen des Datenschutzrechts

Datenschutz-Grundverordnung

Die seit dem 25.05.2018 geltende europäische Datenschutz-Grundverordnung (DS-GVO) hat die 1995 in Kraft getretene Europäische Datenschutzrichtlinie (Richtlinie 95/46/EG) abgelöst. Dabei bleibt die DS-GVO dem dualistischen Ansatz der Datenschutzrichtlinie treu und schützt einerseits die natürliche Person bei der Verarbeitung ihrer personenbezogenen Daten, soll andererseits aber auch im Sinne der Funktionsfähigkeit des gemeinschaftlichen Binnenmarkts den freien Verkehr mit personenbezogenen Daten innerhalb der Gemeinschaft ermöglichen (Art. 1 DS-GVO). Mit der DS-GVO sollen das Datenschutzrecht in Europa vereinheitlicht sowie zugleich die Datenschutzrechte der Bürgerinnen und Bürger gestärkt werden.

Im Gegensatz zur Richtlinie 95/46/EG hat die DS-GVO gem. Art. 288 Abs. 2 AEUV unmittelbare Wirkung. Für die EU-Mitgliedstaaten heißt das, dass sie die Regelungen nicht mehr in ihr nationales Recht umsetzen müssen. Für die deutschen datenverarbeitenden Stellen bedeutet dies, dass sie sich im Hinblick auf ihre Datenverarbeitung unmittelbar an die europäischen Regelungen zu halten haben.

Für Fragen der Auslegung der DS-GVO muss der EuGH im Rahmen des sog. Vorabentscheidungsverfahrens gem. Art. 267 Abs. 1 Buchst. b) AEUV angerufen werden.²

Nationales Recht, insbesondere Bundesdatenschutzgesetz

Mit der DS-GVO wurde zwar das Ziel der Vollharmonisierung des europäischen Datenschutzrechts verfolgt. Gleichwohl hat der europäische Gesetzgeber an vielen Stellen sog. Öffnungsklauseln vorgesehen und so den nationalen Gesetzgebern die Möglichkeit gegeben, die Regelungen der DS-GVO für bestimmte Konstellationen zu präzisieren oder zu ergänzen. Solche die DS-GVO ergänzenden allgemeinen Regelungen finden sich in Deutschland für die Bundesverwaltung und die Privatwirtschaft in den Bestimmungen des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) – BDSG – und für die öffentliche Verwaltung der Länder inklusive der Kommunalverwaltung in den jeweiligen Landes-

* Miriam Claus, LL.B. ist Referentin bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. und schließt gerade ihr Masterstudium (LL.M.) an der TH Köln ab.

* RAin Yvette Reif, LL.M. ist stellvertretende Geschäftsführerin der GDD und Mitautorin des Werks Gola/Reif, Praxisfälle Datenschutzrecht, 2. Auflage 2016.

1 Dieser Abschnitt basiert auf den Ausführungen in Gola/Reif, Praxisfälle Datenschutzrecht, 2. Auflage 2016.

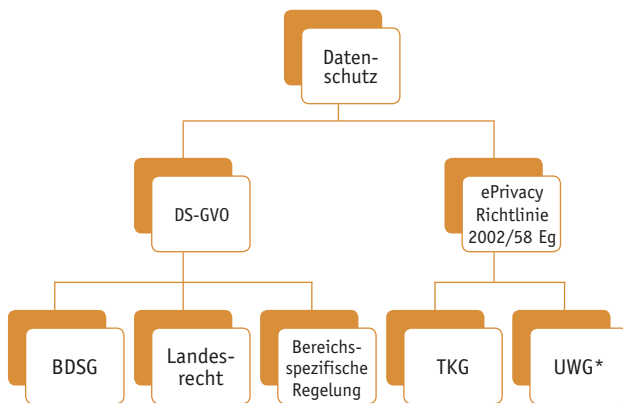
2 Vgl. Gola/Jaspers/Müthlein/Schwartzmann, Datenschutz-Grundverordnung im Überblick, S. 10.

datenschutzgesetzen. Ist eine bereichsspezifische Regelung vorhanden, so verdrängt diese die allgemeinen Datenschutzgesetze. Bei den allgemeinen Datenschutzgesetzen handelt es sich insofern um „Auffanggesetze“, welche nur subsidiär zur Anwendung kommen.

Beispiele:

Unter welchen Voraussetzungen ein Telekommunikationsanbieter Kundendaten zu Abrechnungs- und sonstigen Zwecken, z.B. für Werbezwecke, verwenden darf, bestimmt sich nicht nach der DS-GVO, sondern nach den insofern speziellen Regelungen des Telekommunikationsgesetzes (vgl. §§ 95 ff. TKG). Krankenkassen haben sich im Hinblick auf die Verarbeitung der Mitgliederdaten an § 284 Sozialgesetzbuch V (SGB V) zu orientieren.

Für die Verarbeitung von Beschäftigtendaten sind als „betriebsinternes“ Datenschutzrecht insbesondere bestehende Betriebsvereinbarungen zur Datenverarbeitung von Relevanz.



Quelle: Gola/Jaspers/Müthlein/Schwartzmann, Datenschutz-Grundverordnung im Überblick, 1. Auflage 2017, S. 27.

**Bei den Regelungen des UWG handelt es sich nicht um datenschutzrechtliche Vorgaben. Die Regelungen des UWG sind aber insbesondere für Datenverarbeitungen zu werblichen Zwecken von großer praktischer Relevanz. Zudem wirkt sich nach Auffassung der Aufsichtsbehörden eine bestehende wettbewerbsrechtliche Unzulässigkeit von Werbemaßnahmen auch auf die datenschutzrechtliche Wertung im Rahmen der Interessenabwägung (Art. 6 Abs. 1 Buchst. f) DS-GVO) aus.*

b) Das Verbot mit Erlaubnisvorbehalt

Jede Verarbeitung personenbezogener Daten berührt die Persönlichkeitsrechte der betroffenen Person. Daher stellt die DS-GVO die Verarbeitung personenbezogener Daten unter ein „Verbot mit Erlaubnisvorbehalt“ (ErwG 40). Damit die Verarbeitung rechtmäßig ist, müssen danach personenbezogene Daten mit Einwilligung der betroffenen Person oder auf Basis einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden.

Eine Verarbeitung personenbezogener Daten darf nach Art. 6 Abs. 1 DS-GVO nur erfolgen, wenn mindestens eine der nachfolgenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Für die Verarbeitungstätigkeiten von Behörden besteht die Möglichkeit der Interessenabwägung ausdrücklich nicht. Das Verbot mit Erlaubnisvorbehalt gilt u.a. auch für die Verarbeitung personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Diese besonderen Kategorien personenbezogener Daten werden auch als sensible oder sensitive Daten bezeichnet. Ausnahmen für das Verbot der Verarbeitung sieht insoweit Art. 9 Abs. 2 DS-GVO vor.

Spezielle bereichsspezifische Regelungen für die Verarbeitung von Beschäftigtendaten hat der deutsche Gesetzgeber in § 26 BDSG vorgesehen. Hierzu ist der nationale Gesetzgeber gemäß Art. 88 DS-GVO berechtigt. Nach § 26 Abs. 1 S. 1 BDSG ist die für Zwecke des Beschäftigungsverhältnisses gestattet, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigtenverhältnisses erforderlich ist. Die Verarbeitung besonderer Arten personenbezogener Daten durch den Arbeitgeber ist zulässig, soweit diese zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdige Interessen des Betroffenen am Ausschluss der Verarbeitung seiner personenbezogenen Daten überwiegen. Verarbeitungsvorgänge können auch im Beschäftigungskontext auf einer Einwilli-

gung des Betroffenen beruhen. In diesem Fall bedarf es jedoch einer besonderen Prüfung der Freiwilligkeit der Erklärung, und es gelten erhöhte Anforderungen an die Form der Erklärung (§ 26 Abs. 2 BDSG).

c) Zweckänderung

Sollen personenbezogene Daten zu anderen Zwecken verarbeitet werden, als zu denjenigen, zu denen sie ursprünglich erhoben wurden, und beruht die Weiterverarbeitung nicht auf einer Einwilligung oder Rechtsvorschrift der EU oder Deutschlands, so richtet sich die Zulässigkeit der Zweckänderung nach Art. 6 Abs. 4 DS-GVO. Demnach müssen der alte und der neue Zweck miteinander vereinbar bzw. „kompatibel“ sein. Daher wird im Zusammenhang mit Art. 6 Abs. 4 DS-GVO häufig von der „kompatiblen Weiterverarbeitung“ gesprochen. Mit dieser Regelung wird an den Zweckbindungsgrundsatz des Art. 5 Abs. 1 Buchst. b) DS-GVO angeknüpft. Für die Beurteilung, ob ein neuer Zweck mit dem vorangegangenen Zweck kompatibel ist, hat der europäische Gesetzgeber in Art. 6 Abs. 4 DS-GVO einen nicht abschließenden Kriterienkatalog aufgestellt, der in die Bewertung einfließen muss. Für die Beurteilung der Kompatibilität sind danach u.a. heranzuziehen:

- Jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO verarbeitet werden,
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können.

d) Aufsichtsbehördliche und sonstige Interpretationshilfen

Neben den reinen Gesetzestexten gibt es auch noch andere Dokumente, Orientierungshilfen, Praxishilfen etc., welche als Interpretationshilfen bei der Beurteilung datenschutzrechtlicher Sachverhalte herangezogen werden können.

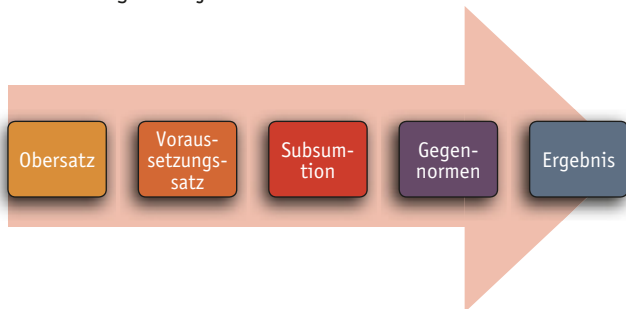
	<p>Der Europäische Datenschutzausschuss (EDSA) ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beitragen und die Zusammenarbeit zwischen den einzelnen EU-Datenschutzbehörden fördern soll. In dieser Funktion erarbeitet er Leitlinien, die das allgemeine Verständnis europäischer Datenschutzgesetze in der Europäischen Union und auch weltweit steigern sollen. https://edpb.europa.eu/edpb_de</p>
	<p>Die nationale Datenschutzkonferenz (DSK) besteht aus den Datenschutzbehörden des Bundes und der Länder und hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen und eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen. Dabei möchte sie auch für eine Fortentwicklung des Datenschutzrechts eintreten. Dazu gibt die DSK Entschlüsse, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen und Festlegungen heraus. https://www.datenschutzkonferenz-online.de/index.html</p>
	<p>Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert den Datenschutz bei den öffentlichen Stellen des Bundes sowie bei den Telekommunikations- und Postdienstunternehmen. Er veröffentlicht regelmäßig Tätigkeitsberichte. https://www.bfdi.bund.de/DE/Home/home_node.html</p>
<p>Aufsichtsbehörden in den einzelnen Bundesländern und den Stadtstaaten Deutschlands</p>	<p>Die Landesbeauftragten für den Datenschutz und die Beauftragten der drei Stadtstaaten sind zuständig für die Unternehmen und öffentlichen Stellen der Länder innerhalb ihres Gebietes. Ausgenommen sind kirchliche Stellen und der Rundfunk, welche ihre eigenen Datenschutzbeauftragten haben. Auf den jeweiligen Webseiten veröffentlichen die Aufsichtsbehörden regelmäßig ihre Tätigkeitsberichte, Stellungnahmen und Orientierungshilfen, welche zur Auslegung herangezogen werden können. Die Auffassungen der einzelnen Landesaufsichten können voneinander abweichen.</p>
	<p>Die GDD tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie unterstützt die datenverarbeitenden Stellen bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen. Die DS-GVO bietet u.a. umfangreiche Arbeits- und Praxishilfen sowie Informationen für Mitarbeiter an. https://www.gdd.de/gdd-arbeitshilfen</p>

e) Schrittweises Vorgehen bei der Prüfung juristischer Sachverhalte

Allgemeines

Wer mit juristischen Sachverhalten konfrontiert wird, von Hause aus aber kein Jurist ist, dem fällt es oft nicht leicht, diese systematisch zu prüfen. Der folgende Beitrag soll eine Hilfestellung für Nichtjuristen bieten und aufzeigen, wie man sich Schritt für Schritt dem Sachverhalt annähert und zu einer juristisch begründeten Lösung kommt.

Das nachfolgende Schema skizziert die Vorgehensweise bei der Prüfung eines juristischen Sachverhalts:



Obersatz

Unter dem Begriff „Obersatz“ versteht man die konkrete Fragestellung, die betrachtet werden soll. Der Obersatz bildet stets den Anfang eines jeden Rechtsgutachtens bzw. den Anfang eines ggf. nachfolgenden (Unter-)Abschnitts der Untersuchung. Im Obersatz werden die Normen/Rechtsgrundlagen aufgezeigt, die Regelungen für den zu prüfenden Anspruch oder die zu prüfende Maßnahme enthalten können.

Beispiele für die Formulierung von Obersätzen:

Als Anspruchsgrundlage für das von Herrn X erhobene Auskunftsbeghen kommt Art. 15 Abs. 1 DS-GVO in Betracht oder

Die Abberufung des Datenschutzbeauftragten durch die Unternehmensleitung könnte gem. Art. 38 Abs. 3 S. 2 DS-GVO unzulässig sein.

Es kann auch eine Verbotsnorm am Anfang der Untersuchung stehen, da diese der DS-GVO bzw. dem BDSG vorrangig sein kann.

Beispiel:

Der beabsichtigten Weitergabe der Patientendaten könnte die Schweigeverpflichtung aus § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) entgegenstehen.

Kommen mehrere Rechtsgrundlagen in Betracht, so müssen auch alle erörtert werden, selbst, wenn die erste Norm bereits zum gewünschten Ergebnis geführt hat. Eine Haftung z.B. kann sich neben den Regelungen der DS-GVO auch aus dem Zivilrecht (Bürgerliches Gesetzbuch – BGB) ergeben.

Voraussetzungssatz

Im Voraussetzungssatz, der dem Obersatz nachfolgt, werden die Voraussetzungen der im Obersatz genannten Norm aufgezählt. Handelt es sich bei diesen Voraussetzungen um

Rechtsbegriffe, müssen diese zunächst näher erläutert werden, damit der Sachverhalt anschließend darauf geprüft werden kann, ob die Begrifflichkeit erfüllt ist oder nicht.

Beispiel:

Nach Art. 15 Abs. 1 DS-GVO hat der Verantwortliche der betroffenen Person auf Verlangen Auskunft über die zu seiner Person verarbeiteten Daten zu erteilen.

Der Anspruch auf Auskunftserteilung nach dieser Regelung bezieht sich auf „personenbezogene Daten“, sofern diese vom Verantwortlichen „verarbeitet“ werden.

Nach Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird nach Art. 4 Nr. 1 DS-GVO eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Der Begriff der Verarbeitung ist in Art. 4 Nr. 2 DS-GVO definiert. Verarbeitung umfasst danach jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

In diesem Fall ist die Erläuterung der vom Gesetzgeber verwendeten Begrifflichkeiten einfach, da der Gesetzgeber selbst die Definitionen ins Gesetz geschrieben hat. Man spricht in solchen Fällen von einer sog. „Legaldefinition“.

Schwieriger ist die Begriffserklärung, wenn es sich um unbestimmte Rechtsbegriffe handelt. Ein unbestimmter Rechtsbegriff ist ein gesetzliches Tatbestandsmerkmal, das aus sprachlicher Sicht für sich betrachtet keinen eindeutigen Inhalt hat, also „unscharf“ ist (z.B. berechtigtes Interesse, gute Sitten, Erforderlichkeit). Diese Unschärfe ist dadurch zu beheben, dass der Begriff unter Berücksichtigung aller konkreten Umstände des Einzelfalls ausgelegt wird, wobei es in rechtlicher Sicht nur eine richtige Entscheidung gibt. Demgemäß unterliegt das Ergebnis der Auslegung der vollen rechtlichen Überprüfung.

Beispiel:

Eine Kündigung des Arbeitsverhältnisses des Datenschutzbeauftragten kommt gemäß §§ 38 Abs. 2; 6 Abs. 4 BDSG nur in Betracht, sofern Tatsachen vorliegen, welche die benennende Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen.

Der Begriff des „wichtigen Grundes“ ist ein unbestimmter Rechtsbegriff, welcher der Auslegung bedarf.

Subsumtion

Bei der Subsumtion wird geprüft, ob die in Frage stehende Norm tatsächlich auf den zu prüfenden Sachverhalt „passt“, d.h., die Voraussetzungen werden gegen den Sachverhalt abgeglichen.

Beispiel:

Nach Art. 15 Abs. 1 DS-GVO hat der Verantwortliche der betroffenen Person auf Verlangen Auskunft über die zu seiner Person verarbeiteten Daten zu erteilen.

Der Anspruch auf Auskunftserteilung nach dieser Regelung bezieht sich auf personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO, sofern sie vom Verantwortlichen verarbeitet werden.

Nach Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen... (siehe oben). Der Begriff der Verarbeitung ist in Art. 4 Nr. 2 DS-GVO definiert. Verarbeitung umfasst danach... (siehe oben).

Der Anspruch auf Auskunftserteilung wird von Herrn X und damit von einer natürlichen Person geltend gemacht. In der Kundendatenbank der in Anspruch genommenen Firma Z-GmbH (= Verantwortlicher) finden sich folgende Informationen zu seiner Person: Name, Adresse, Geburtsdatum und Vertragsdaten. Hierbei handelt es sich um personenbezogene Daten. Die Speicherung ist eine Verarbeitung im Sinne der Legaldefinition aus Art. 4 Nr. 2 DS-GVO.

Gegennorm

Für zahlreiche Normen gibt es Ausnahmeregelungen, daher ist ggf. in einem weiteren Schritt zu prüfen, ob der bislang gefundenen (Zwischen-)Lösung eine etwaige „Gegennorm“ entgegensteht. Selbst wenn die Gegennorm im Ergebnis nicht einschlägig ist, sollte dies kurz kenntlich gemacht werden, um zu signalisieren, dass eine entsprechende Prüfung vorgenommen wurde.

Beispiel:

Vorliegend könnte jedoch eine Ausnahme von der Auskunftspflicht gem. Art. 12 Abs. 5 S. 2 Buchst. b) DS-GVO eingreifen. (...)

oder

Ausnahmen von der Auskunftspflicht sind vorliegend nicht ersichtlich.

Ergebnis

Den Abschluss der Prüfung, respektive der Prüfung eines (Unter-)Abschnitts, bildet der Folgesatz, in dem das Ergebnis der vorangegangenen Überlegungen dargelegt wird.

Beispiel:

(...) Folglich steht X ein Auskunftsanspruch gem. Art. 15 Abs. 1 DS-GVO zu.

oder

Unternehmen X ist folglich gemäß Art. 16 DS-GVO zur Korrektur der zum Kunden K gespeicherten Bonitätsinformationen verpflichtet.

II. Musterfalllösungen zum Auskunftsbegehren von aktiven und ausgeschiedenen Mitarbeitern**Fall 1: Auskunftsbegehren eines aktiven Mitarbeiters**

Mitarbeiter M begehrt, dass ihm Einsicht in seine digital geführte Personalakte gewährt wird. Zudem verlangt er einen Ausdruck der Akte sowie einen Ausdruck sämtlicher von ihm über seinen Dienstaccount verfasster bzw. empfangener E-Mails. Stehen M die geltend gemachten Ansprüche zu? Berücksichtigen Sie neben den datenschutzrechtlichen Regelungen auch die Bestimmungen des Betriebsverfassungsgesetzes (BetrVG).

Anspruch aus § 83 Abs. 1 BetrVG

Obersatz M könnte einen Anspruch auf Einsicht in seine digitale Personalakte aus § 83 Abs. 1 S. 1 BetrVG haben.

Voraussetzungen Voraussetzung für das Recht auf Einsicht in die Personalakte gem. § 83 Abs. 1 S. 1 BetrVG ist, dass M Arbeitnehmer ist und eine Personalakte über ihn geführt wird.

Subsumtion M befindet sich gegenwärtig in einem Beschäftigungsverhältnis mit dem Anspruchsgegner. Der Anspruchsgegner führt über seine Mitarbeiter Personalakten in digitaler Form.

Gegennormen –

Ergebnis M hat einen Anspruch auf Einsicht in seine digitale Personalakte aus § 83 Abs. 1 S. 1 BetrVG. Der betriebsverfassungsrechtliche Anspruch ist auf die Möglichkeit der Einsichtnahme beschränkt, d.h., dem Mitarbeiter steht die Einsichtnahme in den Räumen des Arbeitgebers während der Arbeitszeit zu. Der Mitarbeiter hat nach § 83 Abs. 1 S. 1 BetrVG keinen Anspruch, Kopien der Personalakte zu erhalten, er darf sich lediglich Notizen über den Akteninhalt anfertigen.³

Auskunftsanspruch aus Art. 15 DS-GVO

Obersatz M könnte jedoch ein Recht auf Kopie seiner Personalakte sowie Kopien der versandten/empfangenen E-Mails aus Art. 15 Abs. 3 DS-GVO haben.

Voraussetzungen Voraussetzungen für das Recht auf eine „Datenkopie“ i.S.v. Art. 15 Abs. 3 DS-GVO sind, dass es sich bei den Daten um personenbezogene Daten handelt, die Gegenstand einer Verar-

³ Schulze/Ratzesberger, Einsicht in die Personalakte und die Hinzuziehung Dritter, ArbRAktuell 2017, S. 64.

beitungstätigkeit sind, und dass durch die betroffene Person ein Antrag gestellt wurde.

Subsumtion Bei den Daten in der digitalen Personalakte handelt es sich um personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO. Das Speichern von personenbezogenen Daten stellt nach Art. 4 Nr. 2 DS-GVO eine Form der Verarbeitung dar. In dem Begehren von M gegenüber seinem Arbeitgeber, eine Kopie der Personalakte zu erhalten, liegt ein ausreichender Antrag i.S.v. Art. 15 Abs. 3 DS-GVO. Insbesondere bestehen keine Formerfordernisse für einen Antrag auf „Datenkopie“. Ebenso sind in der E-Mail-Korrespondenz personenbezogene Daten des M enthalten.

Gegen-normen Dem Antrag des M auf Datenkopie müsste gem. Art. 15 Abs. 4 DS-GVO nicht entsprochen werden, wenn dadurch die Rechte und Freiheiten einer anderen Person beeinträchtigt werden. Mangels entsprechender Anhaltspunkte ist hier von einer Beeinträchtigung der Rechte und Freiheiten Dritter nicht auszugehen, insbesondere sofern es sich um die Personalakte von M selbst handelt. Im Hinblick auf die E-Mail-Korrespondenz könnten durch die Zurverfügungstellung der Datenkopie die Rechte und Freiheiten Dritter beeinträchtigt werden, denn zu diesen zählen auch Geschäftsgeheimnisse und der Schutz personenbezogener Daten Dritter. Ob dies tatsächlich der Fall ist, ist Frage des Einzelfalls. Ebenso könnte gem. Art. 12 Abs. 5 S. 2 Buchst. b) DS-GVO die Datenkopie verweigert werden, wenn M vorliegend unbegründet oder exzessiv von seinem Betroffenenrecht Gebrauch machen würde. Dafür enthält der Sachverhalt jedoch keine Anzeichen. Das Recht auf Auskunft aus Art. 15 DS-GVO besteht darüber hinaus nicht, sofern die Daten BDSG nur noch deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen (§ 34 Abs. 1 Nr. 2 Buchst. a) BDSG). M ist aber aktiver Mitarbeiter, seine digitale Personalakte wird aktiv gepflegt und nicht nur aufgrund von Aufbewahrungsfristen verwahrt.

Ergebnis M hat damit ein Recht auf „Datenkopie“ nach Art. 15 Abs. 3 DS-GVO. Insofern hat er jedenfalls Anspruch auf Kopien seiner Personalakte. Im übrigen ist umstritten, wie weit der Anspruch auf „Datenkopie“ nach Art. 15 Abs. 3 DS-GVO reicht. In der Praxis umstritten ist insbesondere, ob der Anspruch so weit geht,

dass Mitarbeiter Duplikate von allen Dokumenten, Dateien, E-Mails, Systemprotokollen etc. verlangen können, in denen Daten enthalten sind, die sich auf sie beziehen.

Ende 2018 hat sich das LAG Baden-Württemberg in seinem (nicht rechtskräftigen) Urteil vom 20.12.2018 – Az.: 17 Sa 11/18 – zum Umfang des Anspruchs auf Auskunft und Datenkopie aus Art. 15 DS-GVO geäußert. Das LAG hat die Beklagte, eine weltweit tätige Fahrzeugherstellerin, u.a. verurteilt, dem klagenden Beschäftigten eine Kopie seiner personenbezogenen Leistungs- und Verhaltensdaten, die Gegenstand der von der Beklagten vorgenommenen Verarbeitung sind, zur Verfügung zu stellen. Zugleich hat das Gericht festgestellt, dass jede einzelne vom Kläger im Rahmen seiner Tätigkeit geschriebene, gesendete oder empfangene E-Mail personenbezogene Daten enthält und auch eine Beschränkung des Anspruchs gemäß Art. 15 Abs. 4 DS-GVO aufgrund berechtigter Interessen eines Dritten im konkreten Fall abgelehnt. Das Urteil wird also so zu verstehen sein, dass sich der Anspruch auf Kopie nach Art. 15 DS-GVO auch auf die E-Mail-Korrespondenz bezieht, wenn auch der genaue Umfang der bereitzustellenden Informationen vom Gericht nicht näher konkretisiert wird.

Im Gegensatz dazu hat das LG Köln in einem (ebenfalls nicht rechtskräftigen) (Teil-)Urteil vom 18.03.2019 – 26 O 25/18 – die Auffassung vertreten, dass sich der Auskunftsanspruch der betroffenen Person nicht auf sämtliche internen Vorgänge beim Verantwortlichen bezieht, wie z.B. Vermerke, oder darauf, dass die betreffende Person sämtlichen gewechselten Schriftverkehr, der Person bereits bekannt ist, erneut ausgedruckt und übersendet erhalten kann. Der Anspruch aus Art. 15 DS-GVO diene nicht der vereinfachten Buchführung des Betroffenen, sondern solle sicherstellen, dass der Betroffene den Umfang und Inhalt der gespeicherten personenbezogenen Daten beurteilen kann, so das LG Köln. Auch das Bayerische Landesamt für Datenschutzaufsicht hat in seinem 8. Tätigkeitsbericht eine eher praxisbezogene Haltung eingenommen und festgestellt, dass der datenschutzrechtliche Auskunftsanspruch „nicht regelmäßig die Herausgabe von allen Dokumenten, E-Mails etc., in denen z.B. der Name der betroffenen Person und eventuelle

4 8. Tätigkeitsbericht des Bay LDA abrufbar unter https://www.lida.bayern.de/media/baylda_report_08.pdf.

weitere Informationen über diese Person erhalten sind,“ erfordert.⁴

Auch in der Literatur werden der Umfang des Auskunftsanspruchs aus Art. 15 DS-GVO und insbesondere Möglichkeiten für eine sinnvolle Auslegung der Regelung in der Unternehmenspraxis rege diskutiert.⁵ Zum Teil wird vertreten, dass es sich bei dem Recht auf Kopie aus Art. 15 Abs. 3 DS-GVO lediglich um einen Hilfsanspruch zu Art. 15 Abs. 1 DS-GVO handele und dieser daher nicht über die Pflichtangaben des Abs. 1 hinausragen könne.⁶ Art. 15 Abs. 3 S. 1 DS-GVO spricht nach seinem Wortlaut allerdings wohl eher dafür, dass die Daten so zur Verfügung zu stellen sind, wie sie „Gegenstand der Verarbeitung“ sind, und insofern ggf. auch über Art. 15 Abs. 1 DS-GVO hinausgehende Informationen gegeben werden müssen.

Ein Vorschlag zur Beschränkung des Anspruchs auf eine „Datenkopie“ besteht darin, Art. 15 Abs. 3 S. 1 DS-GVO teleologisch zu reduzieren und einen hinreichenden Personenbezug bei E-Mails, Protokollen und ähnlichen Dokumenten nur dann zu bejahen, wenn das Dokument aussagekräftige Informationen zur Person des Betroffenen enthält und der Bezug zu dessen Person nicht nur zufällig, beiläufig oder beliebig ist.⁷ Eine andere Stimme⁸ geht davon aus, dass solche personenbezogenen Daten, die nicht Gegenstand der Verarbeitung sind, weil ihre Aufbewahrung z.B. lediglich zu Datenschutz- oder Datensicherungszwecken erfolgt, nicht preisgegeben werden müssen. Anzunehmen sei, dass dem Betroffenen zwar einzelne Stammdaten zur Verfügung gestellt werden müssten, nicht jedoch etwa die Gesamtheit der mit der betroffenen Person geführten E-Mail-Korrespondenz oder Kopien sämtlicher mit der betroffenen Person getätigter geschäftlicher Vorgänge.

Ein vermittelnder Vorschlag⁹ für die Praxis besteht darin, die Auskunft nach Art. 15 DS-GVO in einem gestaffelten Prozess umsetzen. Hierbei erhalten Mitarbeiter nach dem Stellen eines Auskunftsantrags zunächst die in Art. 15 Abs. 1 DS-GVO genannten Angaben. Zudem stellt ihnen das Unternehmen eine Kopie mit einer Art „erweitertem Stammdatensatz“ mit den wesentlichen relevanten Informationen, „die Gegenstand der Verarbeitung sind“, zur Verfügung. In der Praxis hat sich insoweit bewährt, den Mitarbeitern Zugang zu Informationssystemen zu geben, aus denen sie selbst solche Daten nach ihren Bedürfnissen abrufen können (sog. Self-Service-Zugänge).

Wie Unternehmen mit Auskunftersuchen praktisch umgehen, insbesondere wie weitreichend Datenkopien zur Verfügung gestellt werden, ist nach alledem letztlich auch eine Frage der unternehmerischen Risikobewertung. Wichtig ist in jedem Fall, proaktiv einen entsprechenden Prozess aufzusetzen, mit dem auf entsprechende Betroffenenbegehren reagiert werden kann.

Fall 2: Auskunftsbegehren eines ausgeschiedenen Mitarbeiters

Der kürzlich ausgeschiedene Mitarbeiter A begehrt, dass ihm Einsicht in die digital geführte (qualifizierte) Personalakte gewährt wird, die bis zu seinem Ausscheiden über ihn geführt wurde. Auch verlangt er einen Ausdruck der Akte sowie einen Ausdruck sämtlicher von ihm über seinen Dienstaccount verfasster bzw. empfangener E-Mails. Bestehen die geltend gemachten Ansprüche?

Anspruch aus § 83 Abs. 1 BetrVG

Obersatz A könnte einen Anspruch auf Einsicht in seine Personalakte aus § 83 Abs. 1 S. 1 BetrVG haben.

Voraussetzungen Voraussetzung für das Recht auf Einsicht in die Personalakte gem. § 83 Abs. 1 S. 1 BetrVG ist, dass A Arbeitnehmer ist und eine Personalakte über ihn geführt wird.

Subsumtion A ist kürzlich aus dem Unternehmen ausgeschieden und befindet sich demnach gegenwärtig nicht in einem Beschäftigungsverhältnis mit dem Anspruchsgegner.

Gegennormen –

Ergebnis A hat keinen Anspruch auf Einsicht in seine Personalakte aus § 83 Abs. 1 S. 1 BetrVG.

Auskunftsanspruch aus Art. 15 DS-GVO

Obersatz A könnte jedoch ein Recht auf Kopie seiner Personalakte sowie Kopien der versandten/empfangenen E-Mails aus Art. 15 Abs. 3 DS-GVO haben.

⁵ Vgl. etwa Wybitul/Brams, Welche Reichweite hat das Recht auf Auskunft und auf eine Kopie nach Art. 15 I DS-GVO?, NZA 2019, 672 ff.; Härtling, Was ist eigentlich eine „Kopie“?, CR 2019, 219 ff.; Fuhlrott, Anmerkungen zum Urteil des LAG Baden-Württemberg vom 20.12.2018 – Az.: 17 Sa 11/18, NZA-RR 2019, 242 ff.

⁶ Paal/Pauly/Paal, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, Art. 15 DS-GVO, Rn. 33; Plath/Kamlah, DS-GVO/BDSG, 3. Aufl. 2018, Art. 15, Rn. 16.

⁷ Härtling, CR 2019, 219 ff., 225.

⁸ So Dag (<https://www.pingdigital.de/blog/2018/11/21/das-auskunftsersuchen-nach-der-datenschutzgrundverordnung-was-versteht-man-unter-einer-kopie-im-sinne-des-art-15-ds-gvo/1487>).

⁹ <https://www.linkedin.com/pulse/erstes-urteil-zur-reichweite-des-rechts-auf-kopie-nach-tim-wybitul>.

Voraussetzungen Voraussetzungen für das Recht auf eine „Datenkopie“ i.S.v. Art. 15 Abs. 3 DS-GVO sind, dass es sich bei den Daten um personenbezogene Daten handelt, die Gegenstand einer Verarbeitungstätigkeit sind, und dass durch die betroffene Person ein Antrag gestellt wurde.

Subsumtion Bei den Daten in der digitalen Personalakte handelt es sich um personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO. Das Speichern von personenbezogenen Daten stellt nach Art. 4 Nr. 2 DS-GVO eine Form der Verarbeitung dar. In dem Begehren von A gegenüber seinem ehemaligen Arbeitgeber, eine Kopie der Personalakte zu erhalten, liegt ein ausreichender Antrag i.S.v. Art. 15 Abs. 3 DS-GVO. Insbesondere bestehen keine Formerfordernisse für einen Antrag auf „Datenkopie“. Ebenso sind in der E-Mail-Korrespondenz personenbezogene Daten des A enthalten.

Gegennormen Dem Antrag des A auf Datenkopie müsste gem. Art. 15 Abs. 4 DS-GVO nicht entsprochen werden, wenn dadurch die Rechte und Freiheiten einer anderen Person beeinträchtigt werden. Vgl. dazu die entsprechenden Ausführungen zu Fall 1.

Ebenso könnte gem. Art. 12 Abs. 5 S. 2 Buchst. b) DS-GVO die Datenkopie verweigert werden, wenn A vorliegend unbegründet oder exzessiv von seinem Betroffenenrecht Gebrauch machen würde. Dafür enthält der Sachverhalt keine Anzeichen.

Das Recht auf Auskunft aus Art. 15 DS-GVO besteht darüber hinaus gem. § 34 Abs. 1 Nr. 2 BDSG nicht, sofern personenbezogene Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen (Buchst. a), oder die Daten ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen (Buchst. b) und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Die beiden letztgenannten Voraussetzungen für eine Ausnahme von der Auskunftspflicht beziehen sich sowohl auf die Ausnahme nach Buchst. a) als auch auf die Ausnahme nach Buchst. b).

Eine Ausnahme von der Auskunftspflicht könnte sich danach vorliegend ergeben, wenn die E-Mail-Korrespondenz von A in den Produktivsystemen des Anspruchsgegners nicht mehr vorgehalten wird, sondern diese zwecks Wahrung gesetzlicher Aufbewahrungspflichten oder zur Datensicherung in entspre-

chende Archivierungs-/Sicherungssysteme verschoben wurde. Eine Ausnahme ergibt sich aber auch in diesen Fällen nur dann, wenn die übrigen in § 34 Abs. 1 Nr. 2 BDSG genannten Voraussetzungen erfüllt sind, also ein unverhältnismäßiger Aufwand vorliegt und technisch-organisatorische Maßnahmen zur Gewährleistung der Zweckbindung der archivierten/gesicherten Daten ergriffen worden sind. Ob tatsächlich ein Ausnahmetatbestand gegeben ist, kann nicht abstrakt beurteilt werden. Maßgeblich sind die konkreten Gegebenheiten beim Arbeitgeber.

Ergebnis

Bezüglich des von A geltend gemachten Anspruchs auf Kopien der Personalakte gelten die zu Fall 1 gemachten Ausführungen entsprechend, d.h., A kommt ein solcher Anspruch zu.

Soweit die Korrespondenz des A noch im E-Mail-System des früheren Arbeitgebers vorhanden ist, kann auf die Ausführungen zu Fall 1 verwiesen werden. Sollten die Mails bereits archiviert sein, kann – je nach den tatsächlichen Gegebenheiten – eine Ausnahme von der Auskunftspflicht nach § 34 Abs. 1 Nr. 2 BDSG in Betracht kommen.

Anspruch aus allgemeinen persönlichkeitsrechtlichen Gesichtspunkten

Obersatz

Der ausgeschiedene Mitarbeiter A könnte einen Anspruch auf Einsichtnahme in die Personalakte aus allgemeinen persönlichkeitsrechtlichen Gesichtspunkten haben. Rechtseinbußen im Zusammenhang mit der Führung qualifizierter Personalunterlagen können unabhängig davon eintreten, ob die Person, über die die Akten geführt wurden, noch bei dem betroffenen Unternehmen beschäftigt ist. So könnten ggf. etwa Auskünfte aus der Akte an zukünftige Arbeitgeber erteilt werden. Ein individualrechtlicher Einsichtsanspruch steht daher nach Ansicht des Bundesarbeitsgerichts¹⁰ unabhängig davon, ob dieser gesetzlich explizit verankert ist, jedem zu, über den qualifizierte Unterlagen im Zusammenhang mit einem Beschäftigungsverhältnis geführt werden. Auch solchen Personen, die nicht mehr in einem Beschäftigungsverhältnis stehen, könne eine zur Wahrung ihres informationellen Selbstbestimmungsrechts erforderliche Einsicht nicht generell verwehrt werden. Dieses Recht kann aus der auch über das Ende des Beschäftigungsverhältnisses hinauswirkenden und unter Berücksichtigung des Grundrechts auf

10 BAG, 16.11.2010 – 9 AZR 573/09.

informationelle Selbstbestimmung zu interpretierenden arbeitsrechtlichen Schutz- und Rücksichtnahmepflicht des Arbeitgebers (§ 241 Abs. 2 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG) abgeleitet werden. Der nachvertragliche Anspruch setzt nach Ansicht des Bundesarbeitsgerichts auch nicht voraus, dass der Arbeitnehmer ein konkretes berechtigtes Interesse nachweist. Zur Begründung hierzu wird insbesondere aufgeführt, dass der Betroffene seine fortbestehenden Ansprüche auf Korrektur der Akte nur geltend machen kann, wenn er auch von dem Inhalt Kenntnis hat.

Voraussetzungen	A steht ein Anspruch auf Einsichtnahme zu, sofern der Anspruchsgegner qualifizierte Unterlagen im Zusammenhang mit einem Beschäftigungsverhältnis über ihn geführt hat.
Subsumtion	Dies ist vorliegend der Fall.
Gegennormen	–
Ergebnis	A steht damit ein Anspruch auf Einsichtnahme in die Personalakte aus allgemeinen persönlichkeitsrechtlichen Gesichtspunkten zu.

Der Nemo-tenetur-Grundsatz im BDSG im Lichte der Kartellrechts-Judikatur des EuGH

Lennart Rüb*

Der Nemo-tenetur-Grundsatz stellt eine wichtige Privilegierung im Falle von umfassenden Meldungen von Datenpannen dar. Der EuGH hat sich hiermit im Zusammenhang mit kartellrechtlichen Sanktionen befasst. Was bedeutet das für den Datenschutz?

I. Der Fall Qualcomm

Am 09.04.2019 wies das EuG im Rechtsstreit Qualcomm Inc. dessen Vorwurf gegen die Europäische Kommission zurück, sie habe es in seinem Recht auf Selbstbelastungsfreiheit verletzt.¹ Die europäischen Wettbewerbsbehörden hatten Qualcomm wettbewerbswidriger Absprachen verdächtigt und im Rahmen der Ermittlungen Auskünfte von dem Unternehmen verlangt. Das Gericht urteilte, dass Auskunftsverlangen der Kommission, deren Antworten lediglich faktischer Natur sind, das Recht des Unternehmens auf Selbstbelastungsfreiheit nicht verletzen. Damit bestätigt das Gericht die sehr enge Auslegung des Nemo-tenetur-Grundsatzes in europäischen Kartellrechtsverfahren durch die europäischen Gerichte, die vor 30 Jahren im Orkem-Urteil des EUGH ihren Ausgangspunkt nahm.² In diesem Urteil im Streit zwischen einem französischen Chemie-Konzern und der Europäischen Kommission entwickelte das Gericht den Grundsatz, dass lediglich Aussagen, die unmittelbar einem Schuldeingeständnis entsprechen, vom Recht auf Selbstbelastungsfreiheit erfasst würden.

II. Bedeutung der Entscheidung für das Datenschutzrecht

Fraglich ist, inwieweit die §§ 42 Abs. 4, 43 Abs. 4 BDSG vor diesem Hintergrund mit der europäischen Judikatur vereinbar sind.³ In diesen Vorschriften hat der deutsche Gesetzge-

ber nämlich, im Rahmen seiner Ermächtigung aus Art. 83 Abs. 8 DS-GVO „angemessene Verfahrensgarantien“ zu schaffen, ein Recht auf Selbstbelastungsfreiheit normiert. Dieses kommt dem Verantwortlichen zugute, der nach Art. 33 DS-GVO nach einer Datenschutzverletzung binnen 72 Stunden eine Meldung an die Aufsichtsbehörde machen muss. Die §§ 42 Abs. 4, 43 Abs. 4 BDSG sehen vor, dass der Verantwortliche seine Zustimmung erteilen muss, damit die in der Meldung übermittelten Informationen in einem Straf- oder Bußgeldverfahren gegen ihn verwendet werden dürfen. Gemäß Art. 33 Abs. 3 DS-GVO enthält die Benachrichtigung Informationen wie die Art der Datenschutz-Verletzung, die Zahl der betroffenen Personen und Datensätze und die durch den Verantwortlichen ergriffenen Maßnahmen. Solche Informationen könnten durchaus als lediglich faktischer Natur angesehen werden und mithin nicht den Ansprüchen des EUGH genügen, um durch ein Recht auf Selbstbelastungsfreiheit privilegiert zu werden.

Dennoch ist der Nemo-tenetur-Grundsatz im BDSG in einem anderen Licht zu betrachten. Zum einen lässt sich nämlich die Frage stellen, inwieweit der EUGH mit seiner Limitierung des Rechts auf Selbstbelastungsfreiheit noch den europäischen Grundrechtskanon im Blick hat.⁴ In seiner grundlegenden Orkem-Rechtsprechung erörtert er bspw. ex-

* Lennart Rüb ist Student im Fach Wirtschaftsrecht (LL.B.) an der TH Köln. Seine Schwerpunkte sind Internationales Wirtschaftsrecht und Recht der Finanzdienstleistungen.

1 EuG Urte. v. 09.04.2019 – T-371/17, BeckRS 2019, 5395, EU:T:2019:232.

2 EuGH Urte. v. 18.10.1989 – 374/87, BeckRS 2004, 71022, EU:C:1989:387. Dazu bereits Spittka, RDV 2019, 167, 169.

3 Diese Frage wirft bspw. der Datenschutzbeauftragte des Landes Baden-Württemberg in seinem Tätigkeitsbericht der Jahre 2016/17 auf.

4 Jarass GrCh EU-Grundrechte-Charta Art. 48 Rn. 32.

plizit, ob aus Art. 6 der Europäischen Menschenrechtskonvention (EMRK) ein Recht auf Selbstbelastungsfreiheit erwachsen kann, und kommt zu einem negativen Ergebnis.⁵ In der Tat regelt dieser Artikel zwar das Recht der Grundrechtsträger auf ein faires Verfahren, benennt aber nicht explizit den Nemo-tenetur-Grundsatz. Gleichwohl hat aber der Europäische Gerichtshof für Menschenrechte, der über die Einhaltung der EMRK wacht, inzwischen mehrfach bestätigt, dass aus Art. 6 der Konvention ein umfassendes Recht auf Selbstbelastungsfreiheit hervorgeht, das jegliche Form von Äußerungen beinhaltet, die geeignet sind, direkt oder indirekt straf- und verwaltungsrechtlich gegen den Betroffenen verwendet zu werden.⁶ Zwar ist die EU entgegen Art. 6 Abs. 2 EUV der EMRK immer noch nicht beigetreten. Laut Art 6 Abs. 3 EUV sind aber die Grundrechte der Konvention zumindest als allgemeine Grundsätze Teil des Unionsrechts. Spätestens durch Art. 48 der Charta der Grundrechte der Europäischen Union, die Grundrechtsträgern die Achtung ihrer Verteidigungsrechte garantiert und alle EU-Organe unmittelbar bindet,⁷ besteht eine gewichtige grundrechtliche Legitimationsgrundlage für den Gesetzgeber, den Nemo-tenetur-Grundsatz weiter auszulegen, als es die europäischen Gerichte tun.

Zum andern ist fraglich, ob aus praktischen Erwägungen die Rechtsgedanken aus der europäischen Kartellrechtsprechung ohne weiteres auf die fraglichen BDSG-Vorschriften übertragbar sind. Einerseits war eine wesentliche Begründung des EUGH dafür, dass er den Nemo-tenetur-Grundsatz in seinen Urteilen stark beschränkt, dass die Effektivität der kartellrechtlichen Ermittlungen gewahrt werden müsse.⁸ Dies erscheint in Teilen nachvollziehbar. Der Natur der Sache nach sind wettbewerbswidrige Absprachen konspirativ und schwer nachweisbar und die Beweisführung kompliziert. Ob die Aufsichtsbehörden, welche auf Grundlage der DS-GVO arbeiten, jedoch im gleichen Maße Schützenhilfe durch die Rechtsprechung brauchen, darf bezweifelt werden. Art. 58 Abs. 1 DS-GVO sieht eine ganze Reihe von Untersuchungsbefugnissen der Aufsichtsbehörden vor. Wenn der Verdacht gegen ein Unternehmen besteht, Datenschutzrecht gebrochen zu haben, kann die Behörde Auskünfte und Informationen einholen, Zugang zu personenbezogenen Daten verlangen, Datenschutz-Audits durchführen und sich im Rahmen von Verhältnismäßigkeit und Verfahrensrecht sogar Zugang zu Räumlichkeiten und Computern verschaffen. Verstöße gegen das Datenschutzrecht, wie ein prominenter Fall, bei dem ein Chat-Portal entgegen seinen Pflich-

ten aus Art. 32 DS-GVO Userdaten unverschlüsselt speicherte,⁹ sind verhältnismäßig einfach festzustellen und zu beweisen.

Andererseits führen auch teleologische Erwägungen zu einer anderen Beurteilung des Privilegierung selbstbelastender Aussagen im Datenschutzrecht als im Kartellrecht. In Fällen, in denen die EU-Kommission gegen Unternehmen wegen Verdacht auf wettbewerbswidriges Verhalten ermittelt und Auskunftsverlangen einholt, tut sie das aufgrund von Hinweisen durch andere Unternehmen, oder weil sie selbst Anhaltspunkte dafür sieht.¹⁰ Art. 33 DS-GVO sieht hingegen vor, dass jemand, in dessen Verantwortung sich eine Datenschutzverletzung ereignet hat, diese proaktiv an die zuständige Behörde meldet. Lieferte derjenige zeitgleich die Grundlage für ein Straf- oder Bußgeldverfahren gegen sich an die Behörde, wäre aus Sicht des Verantwortlichen ein starker Anreiz geschaffen, eine solche Meldung erst gar nicht zu machen. Das ist ein bedeutendes Argument für den Nemo-tenetur-Grundsatz im Datenschutzrecht, der im Kartellrecht keine Berücksichtigung finden konnte.

III. Fazit

Mithin kann man die Rechtsprechung des EUGH zum Recht auf Selbstbelastungsfreiheit im kartellrechtlichen Ermittlungsverfahren mit Blick auf die Grundrechte kritisch hinterfragen. Es ist richtig, im Datenschutzrecht einen anderen Weg zu gehen. Außerdem sprechen auch praktische Erwägungen für die Berechtigung der Privilegierung dieser Meldung gem. §§ 42 Abs. 4, 43 Abs. 4 BDSG durch den deutschen Gesetzgeber, insbesondere der Anreiz für Verantwortliche, eine Datenschutzpanne auch wirklich zu melden.

5 EuGH, Urt. v. 18.10.1989 – 374/87, BeckRS 2004, 71022, EU:C:1989:387, Rn. 30.

6 EGMR, Urt. v. 25.02.1993 – 10828/84, CE:ECHR:1993:0225JUD001082884. Dazu MüKoStPO/Gaede EMRK Art. 6 Rn. 318; Schubert, Legal privilege und Nemo tenetur im reformierten europäischen Kartellermittlungsverfahren der VO 1/2003, S. 508.

7 Art. 52 Abs. 3 der GRCh verweist seinerseits für den Gehalt gemeinsamer Grundrechte explizit auf die EMRK.

8 Schubert, Legal privilege und Nemo tenetur im reformierten europäischen Kartellermittlungsverfahren der VO 1/2003, S. 472.

9 <https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/>

10 Laut Art. 7 Abs. 1 der 1/2003 VO kann die Kommission von Amts wegen oder aufgrund einer Beschwerde eine Zuwiderhandlung gegen Wettbewerbsrecht feststellen.

Prof. Golas neu konzipiertes Datenschutzbuch:

Unverzichtbar für alle, die mit Personaldaten arbeiten.



**jetzt
bestellen**

PRAXISNAH

- ausführliche Fallbeispiele
und konkrete Lösungsansätze

ETABLIERT

- 8. aktualisierte und
erweiterte Neuauflage

NÜTZLICH

- ausgewertete Stellungnahmen
der Aufsichtsbehörden

Handbuch Beschäftigtendatenschutz
8. völlig neu bearbeitete Auflage 2019
726 Seiten / Hardcover / € 139,99 inkl. E-Book
ISBN 978-3-89577-801-8

Bestellen Sie direkt unter:
datakontext.com/handbuch

Rechtsprechung

Auskunftsanspruch des Betriebsrats über sensitive Beschäftigtendaten (Schwangerschaft einer Beschäftigten) setzt Datensicherung voraus

(Bundesarbeitsgericht, Beschluss vom 9. April 2019 – 1 ABR 51/17 –)

Umfasst ein allgemeiner Auskunftsanspruch des Betriebsrats nach § 80 Abs. 2 Satz 1 BetrVG eine besondere Kategorie personenbezogener Daten (sensitive Daten im datenschutzrechtlichen Sinn), ist Anspruchsvoraussetzung, dass der Betriebsrat zur Wahrung der Interessen der von der Datenverarbeitung betroffenen Arbeitnehmer angemessene und spezifische Schutzmaßnahmen trifft.

Sachverhalt:

A. Die Beteiligten streiten über einen Auskunftsanspruch.

Die Arbeitgeberin ist ein Luft- und Raumfahrtunternehmen, in deren Betrieb in M der antragstellende Betriebsrat gewählt ist. Diesen informierte die Arbeitgeberin in der Vergangenheit darüber, welche Arbeitnehmerin ihre Schwangerschaft angezeigt hat. Seit Mitte 2015 räumt sie der schwangeren Arbeitnehmerin die Möglichkeit ein, der Weitergabe dieser Information an den Betriebsrat fristgebunden zu widersprechen.

3 Der Betriebsrat hat die Ansicht vertreten, die Arbeitgeberin habe ihm jede von einer Arbeitnehmerin angezeigte Schwangerschaft mitzuteilen. Er habe als Gremium darüber zu wachen, dass die zugunsten der Arbeitnehmerin geltenden Gesetze, darunter das Mutterschutzgesetz (MuSchG), von der Arbeitgeberin durchgeführt würden. Seine Informations- und Kontrollrechte seien gegenüber dem Vertraulichkeitsinteresse einer widersprechenden Arbeitnehmerin vorrangig.

Aus den Gründen:

B. Die zulässige Rechtsbeschwerde der Arbeitgeberin ist begründet. Sie führt zur Aufhebung des angefochtenen Beschlusses und zur Zurückverweisung der Sache an das Landesarbeitsgericht. Mit der vom Landesarbeitsgericht gegebenen Begründung kann dem Begehren des Betriebsrats nicht entsprochen werden. Der Senat kann aufgrund der bislang getroffenen Feststellungen nicht abschließend beurteilen, ob der zulässige Antrag begründet oder unbegründet ist.

I. Der Antrag des Betriebsrats ist – in seiner gebotenen Auslegung – zulässig.

1. Er bezieht sich, anders als es sein Wortlaut nahelegt, ausschließlich auf die Fallgestaltung, in der eine Arbeitnehmerin der Information des Betriebsrats über ihre Schwangerschaft widerspricht. Äußert sich die Arbeitnehmerin nicht dahingehend, unterrichtet die Arbeitgeberin den Betriebsrat über die ihr angezeigte Schwangerschaft. Entsprechend streiten die Beteiligten nicht über diese Konstellation. Im Übrigen geht es dem Betriebsrat lediglich um die Nennung der Namen derjenigen Arbeitnehmerinnen, die ihre Schwangerschaften der Arbeitgeberin mitgeteilt haben, nicht um eine Unterrichtung über die weiteren Daten eine Anzeige iSd. § 15 MuSchG.

2. In diesem Verständnis begegnen dem Antrag keine Zulässigkeitsbedenken; insbesondere ist er hinreichend bestimmt iSv. § 253 Abs. 2 Nr. 2 ZPO.

II. Das bisherige Vorbringen des Betriebsrats trägt den Anspruch auf die streitbefangene Auskunft nicht. Das hat das Landesarbeitsgericht verkannt.

1. Nach § 80 Abs. 2 Satz 1 BetrVG hat der Arbeitgeber den Betriebsrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten. Hieraus folgt ein entsprechender Anspruch des Betriebsrats, soweit die begehrte Information zur Aufgabenwahrnehmung erforderlich ist. Anspruchsvoraussetzung ist damit zum einen, dass überhaupt eine Aufgabe des Betriebsrats gegeben ist, und zum anderen, dass im Einzelfall die begehrte Information zur Wahrnehmung der Aufgabe erforderlich ist. Dies hat der Betriebsrat darzulegen. Erst anhand dieser Angaben können der Arbeitgeber und im Streitfall das Arbeitsgericht prüfen, ob die Voraussetzungen einer Auskunftspflicht sowie eines damit korrespondierenden Auskunftsanspruchs vorliegen (vgl. BAG 24. April 2018 – 1 ABR 6/16 – Rn. 22; 7. Februar 2012 – 1 ABR 46/10 – Rn. 7, BAGE 140, 350). Es ist nicht Aufgabe des Gerichts, ohne solche Angaben von Amts wegen zu prüfen, welche Aufgabe den Auskunftsanspruch stützen und aus welchen Gründen die verlangte Information für die Durchführung dieser Aufgabe benötigt werden könnte (vgl. BAG 20. März 2018 – 1 ABR 15/17 – Rn. 18).

2. Das gilt auch, wenn sich der Betriebsrat – wie vorliegend – zur Begründung seines Auskunftsanspruchs auf seine Aufgabe zur Überwachung der zugunsten der Arbeitnehmer geltenden Gesetze iSv. konkreten Ge- oder Verboten (vgl. BAG 20. März 2018 – 1 ABR 15/17 – Rn. 16 mwN) nach § 80 Abs. 1 Nr. 1 BetrVG stützt. Mit einem allgemein gehaltenen Verweis auf jegliche gesetzliche (Schutz-)Pflichten des Arbeitgebers gegenüber Arbeitnehmern und der Belegschaft genügt der Betriebsrat seiner Vortragslast regelmäßig nicht. Eine solche Antragsbegründung vernachlässigt, dass der Informationsanspruch als solcher – ebenso wie der darauf bezogene Anspruch auf Vorlage von Unterlagen (§ 80 Abs. 2 Satz 2 Halbs. 1 BetrVG) – strikt aufgabengebunden und in seiner Reichweite durch das Erforderlichkeitsprinzip bestimmt ist. Daher muss der Betriebsrat die konkrete normative (Arbeitsschutz-)Vorgabe, deren Durchführung er zu überwachen hat und die sein Auskunftsverlangen tragen soll, aufzeigen. Dies gilt insbesondere, wenn er sich auf ein Gesetz mit mehreren und unterschiedlichen (Schutz-)Bestimmungen bezieht. Kann der Schutz nur im Hinblick auf konkrete betriebliche Gegebenheiten greifen, sind diese gleichfalls anzugeben. Nur bei einem so gehaltenen Tatsachenvortrag und einer so aufgezeigten Aufgabe kann eine Prüfung erfolgen, ob die beanspruchte Auskunft für deren Wahrnehmung erforderlich ist.

3. Hiervon ausgehend ist die Begründung des Landesarbeitsgerichts für den von ihm angenommenen Unterrichtsanspruch des Betriebsrats nicht frei von Rechtsfehlern.

a) Das Landesarbeitsgericht ist davon ausgegangen, die streitbefangene Informationspflicht der Arbeitgeberin bestehe „insbesondere zur Überwachung der Einhaltung von Arbeitsschutzvorschriften, wie etwa des Mutterschutzgesetzes und der in diesem Zusammenhang ergangenen Verordnungen ... auch im Zusammenhang mit den Aufgaben nach § 89 BetrVG“; der entspre-

chende Aufgabenbezug sei zwischen den Beteiligten „unstreitig“.

b) Diese – auf dem insoweit nicht weitergehenden und allgemein gehaltenen Vorbringen des Betriebsrats beruhende – Annahme verkennt, dass sich der Betriebsrat für die erstrebte Unterrichtung nicht mit einem bloßen Hinweis auf die Überwachung von nicht näher bezeichneten, zugunsten schwangerer Arbeitnehmerinnen geltenden mutterschutzrechtlichen Pflichten der Arbeitgeberin berufen kann (anders noch – allerdings vor Inkrafttreten des BDSG und zu § 54 BetrVG 1952 iVm. den damals geltenden mutterschutzrechtlichen Vorschriften – BAG 27. Februar 1968 – 1 ABR 6/67 – BAGE 20, 333).

aa) Die seinen Unterrichtsanspruch nach § 80 Abs. 2 Satz 1 BetrVG begründende Überwachungsaufgabe iSv. § 80 Abs. 1 Nr. 1 BetrVG muss genau benannt worden sein. Der generelle Verweis auf den beschäftigungsspezifischen Schutznormkomplex für schwangere Frauen, der seinerseits eine Vielzahl von Pflichten für den Arbeitgeber begründet, ermöglicht keine Prüfung, welches zugunsten der Arbeitnehmerinnen konkret geltende Ge- oder Verbot der Betriebsrat hinsichtlich seiner Durchführung oder Einhaltung zu überwachen beabsichtigt und inwieweit er dafür die Unterrichtung über jede einzelne der Arbeitgeberin angezeigte Schwangerschaft unter Namensnennung der mittelenden Arbeitnehmerin benötigt. Dies gilt umso mehr, weil bestimmte mutterschutzspezifische Pflichten – wie etwa das grundsätzliche Verbot der Nachtarbeit für schwangere Frauen – nur bei entsprechenden betrieblichen Gegebenheiten greifen (Nachtarbeit im Betrieb) und auch nur dann eine entsprechende Überwachungsaufgabe auszulösen vermögen.

bb) Der Bezug der verlangten Auskunft zu einer – hier nicht einmal konkret aufgezeigten – Aufgabe kann auch nicht als „unstreitig“ angesehen oder von den Beteiligten „unstreitig gestellt“ werden. Für die weitergehende Annahme des Beschwerdegerichts, die Aufgabe folge ebenso aus „dem Zusammenhang mit § 89 BetrVG“, fehlt es – außer der Nennung der betriebsverfassungsrechtlichen Vorschrift – gleichfalls an jeglichem Vorbringen des Betriebsrats, für was genau er sich einsetzen will (§ 89 Abs. 1 Satz 1 BetrVG) oder hinsichtlich welcher Fragen er sein Hinzuziehungsrecht (§ 89 Abs. 2 Satz 1 BetrVG) oder andere in der Vorschrift geregelten Aufgaben und Berechtigungen geltend macht.

III. Der Rechtsfehler führt zur Aufhebung der angefochtenen Entscheidung und zur Zurückverweisung der Sache an das Landesarbeitsgericht. Das Verfahren ist nicht im Sinn einer Antragsabweisung zur Endentscheidung reif (§ 563 Abs. 3 ZPO).

1. Bevor der Antrag mangels hinreichenden Vorbringens des Betriebsrats abgewiesen werden kann, ist ein Hinweis des Gerichts erforderlich, das ihm Gelegenheit gibt, diesen Antragsmangel zu beseitigen. Dies gebietet der Anspruch auf rechtliches Gehör der Beteiligten, nachdem beide Vorinstanzen das Begehren des Betriebsrats trotz dessen nicht hinreichender Darlegung einer Aufgabe und der darauf bezogenen Erforderlichkeit der beanspruchten Auskunft für die Wahrnehmung der Aufgabe als begründet angesehen haben und auch die Arbeitgeberin insoweit keine Beanstandungen erhoben hat. Das entsprechende Vorbringen vermag der Betriebsrat im Rechtsbeschwerdeverfahren nicht nachzuholen, da es bezüglich ggf. vorliegender betrieblicher Spezifika neuen Tatsachenvortrag umfassen kann. Zudem muss sich das Vorbringen des Betriebsrats angesichts seines gegenwarts- und zukunftsbezogenen Auskunftsverlangens nunmehr an der gegenüber dem Zeitpunkt der letzten Anhörung in der Tatsacheninstanz (27. September 2017) geänderten Rechtslage – und damit ua. an den Bestimmungen des MuSchG in der seit 1. Januar 2018 geltenden Fassung vom 23.

Mai 2017 (BGBl. I S. 1228) – ausrichten (vgl. zB BAG 30. September 2014 – 1 ABR 79/12 – Rn. 17). Hierzu ist ihm – ebenso wie der Arbeitgeberin zur Erwidern – Gelegenheit zu geben.

2. Der Auskunftspflicht der Arbeitgeberin gegenüber dem Betriebsrat steht nicht der mit einem Widerspruch der schwangeren Arbeitgeberin geäußerte Wille, der Betriebsrat möge in Bezug auf ihre Person keine sie schützenden Aufgaben wahrnehmen, entgegen. Die Erfüllung der dem Betriebsrat von Gesetzes wegen zugewiesenen Aufgaben ist nicht von einer vorherigen Einwilligung der Arbeitnehmer abhängig und steht nach der betriebsverfassungsrechtlichen Konzeption nicht zu deren Disposition (vgl. auch BAG 7. Februar 2012 – 1 ABR 46/10 – Rn. 17, BAGE 140, 350).

3. Der Antrag ist nicht von vornherein in Ansehung der seit dem 25. Mai 2018 geltenden Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DS-GVO) und dem durch das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 geänderten Bundesdatenschutzgesetzes – BDSG – (BGBl. I S. 2097) unbegründet. Ob dem streitbefangenen Unterrichtsverlangen datenschutzrechtliche Gründe entgegenstehen, ist offen. Das Landesarbeitsgericht wird dies zu prüfen und auch in diesem Zusammenhang dem Betriebsrat Gelegenheit zu ergänzendem Vorbringen – sowie der Arbeitgeberin zur Erwidern – zu geben haben. Hierfür gelten folgende Maßgaben:

a) Die datenschutzrechtliche Zulässigkeit der streitbefangenen Auskunftserteilung folgt nicht ohne weiteres aus § 26 Abs. 6 BDSG. Zwar bleiben nach dieser Vorschrift im Hinblick auf die in § 26 BDSG geregelte Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses die Beteiligungsrechte der Interessenvertretungen der Beschäftigten „unberührt“. Dieser Norm, welche § 32 Abs. 3 BDSG in der bis zum 24. Mai 2018 geltenden Fassung (aF) im Sinn einer klarstellenden Funktion übernommen hat (BT-Drs. 18/11325 S. 97), kommt indes kein Regelungsgehalt als die Datenverarbeitung durch Arbeitgeber oder Betriebsrat eigenständig erlaubender Tatbestand zu. Mit ihr ist vielmehr ausgedrückt, dass sich der Beschäftigtendatenschutz nach § 26 BDSG und der im kollektiven Arbeitsrecht durch die Beteiligungsrechte der Interessenvertretungen der Beschäftigten flankierte Beschäftigtendatenschutz ergänzen (zu § 32 Abs. 3 BDSG aF vgl. Seifert, in: Simitis, BDSG 8. Aufl. § 32 Rn. 144 ff.). Die kollektiven Beteiligungsrechte werden nicht eingeschränkt, aber auch nicht erweitert (Däubler, in: Däubler/Wedde/Weichert/Sommer, EU-Datenschutzgrundverordnung und BDSG-neu, BDSG § 26 Rn. 272). Die Ausübung von Beteiligungsrechten ist damit einerseits datenschutzrechtlich nicht von vornherein unzulässig, weil sie mit der Verarbeitung personenbezogener Daten einhergeht; andererseits müssen in solch einem Fall aber auch von den Betriebsparteien die Anforderungen des Datenschutzes beachtet werden (Gräber/Nolden, in: Paal/Pauly Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., § 26 BDSG Rn. 54).

b) Der Inhalt der streitbefangenen Auskunft ist auf die Verarbeitung einer besonderen Kategorie personenbezogener Daten im Beschäftigtenkontext gerichtet. Das ist bei Vorliegen der Voraussetzungen des § 26 Abs. 3 BDSG erlaubt.

aa) Nach § 26 Abs. 3 Satz 1 BDSG ist – abweichend von Art. 9 Abs. 1 DS-GVO – die Verarbeitung besonderer Kategorien

personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Entsprechend § 22 Abs. 2 BDSG sind hierfür angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 26 Abs. 3 Satz 3 BDSG).

bb) Mit der Regelung des § 26 Abs. 3 BDSG hat der Gesetzgeber in zulässiger Weise von der Öffnungsklausel in Art. 9 Abs. 2 Buchst. b DS-GVO der gemäß Art. 288 AEUV in allen ihren Teilen verbindlichen und unmittelbar in jedem Mitgliedstaat geltenden DS-GVO Gebrauch gemacht.

(1) Nach Art. 9 Abs. 1 DS-GVO ist die Verarbeitung der in der Vorschrift benannten besonderen Kategorien von personenbezogenen Daten grundsätzlich untersagt. Hierzu zählen Gesundheitsdaten. Gemäß der Legaldefinition des Art. 4 Nr. 15 DS-GVO handelt es sich dabei um Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Das Verarbeitungsverbot nach Art. 9 Abs. 1 DS-GVO gilt allerdings nicht, wenn einer der gesondert in Art. 9 Abs. 2 DS-GVO aufgeführten Erlaubnistatbestände gegeben ist. Gemäß Art. 9 Abs. 2 Buchst. b DS-GVO kann die Verarbeitung sensibler Daten nach dem Recht der Mitgliedstaaten ua. dann zulässig sein, wenn sie erforderlich ist, damit der Verantwortliche die ihm aus dem Arbeitsrecht erwachsenden Rechte ausüben und seinen diesbezüglichen Pflichten nachkommen kann, wobei das nationale Recht geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen muss. Damit gewährt die Norm den Mitgliedstaaten die Möglichkeit, unter den in ihr genannten Voraussetzungen die Verarbeitung besonderer Kategorien personenbezogener Daten zu erlauben. Mit § 26 Abs. 3 Satz 1 und Satz 3 BDSG hat der Gesetzgeber hiervon Gebrauch gemacht (vgl. BT-Drs. 18/11325 S. 98 f.).

2) Die Regelung entspricht den Vorgaben der Öffnungsklausel des Art. 9 Abs. 2 Buchst. b DS-GVO (ebenso Schaffland/Holthaus, in: DS-GVO/BDSG § 26 BDSG Rn. 118; Schiff in: Ehmann/Selmayr, Datenschutz-Grundverordnung 2. Aufl. Art. 9 Rn. 79). Der Ausnahmetatbestand des Art. 9 Abs. 2 Buchst. b Halbs. 1 DS-GVO ist in Satz 1 von § 26 Abs. 3 BDSG inhaltsgleich übernommen (Seifert, in: Simitis/Hornung/Spieker, Datenschutzrecht, Art. 88 DS-GVO Rn. 221). Das widerspricht nicht dem unionsrechtlichen Umsetzungs- oder Normwiederholungsverbot (vgl. dazu zB Selmayr/Ehmann, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl., Einführung Rn. 80 ff.), was angesichts der im Erwägungsgrund (8) zur DS-GVO ausgedrückten Möglichkeit für die Mitgliedstaaten, unter näheren Voraussetzungen Teile der DS-GVO in ihr nationales Recht aufzunehmen, auf der Hand liegt. Zudem sieht das nationale Recht für die Verarbeitung besonderer Kategorien personenbezogener Daten geeignete Garantien für die Grundrechte und die Interessen der betroffenen Personen vor. Die Zulässigkeit der Verarbeitung derartiger Daten erfordert nach § 26 Abs. 3 Satz 1 BDSG ausdrücklich, dass kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Die entsprechende Geltungsanordnung von § 22 Abs. 2 BDSG nach § 26 Abs. 3 Satz 3 BDSG stellt den Schutz der Grundrechte und die Wahrung der Interessen der Betroffenen sicher. Danach sind bei der Verar-

beitung besonderer Kategorien personenbezogener Daten angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen.

(3) Zur Frage der generellen Vereinbarkeit von § 26 Abs. 3 Satz 1 und Satz 3 BDSG mit den Anforderungen der Öffnungsklausel des Art. 9 Abs. 2 Buchst. b DS-GVO ist ein Vorabentscheidungsverfahren durch den Gerichtshof der Europäischen Union nach Art. 267 AEUV nicht veranlasst. Dem Verständnis des Art. 9 Abs. 2 Buchst. b DS-GVO als Öffnungsklausel begegnen ebenso wenig Bedenken wie der Annahme, dass der deutsche Gesetzgeber bei ihrer Umsetzung mit § 26 Abs. 3 Satz 1 und Satz 3 BDSG die unionsrechtlichen Vorgaben beachtet hat. Die Erwägungen des Senats hierzu ergeben sich ohne weiteres aus dem Wortlaut der zitierten Normen der DS-GVO und des BDSG; die richtige Anwendung des Unionsrechts ist mithin derart offenkundig, dass für vernünftige Zweifel kein Raum bleibt (acte clair, vgl. dazu zB EuGH 15. September 2005 – C-495/03 – [Intermodal Transports] Rn. 33).

cc) Der – unter Rückgriff auf die in der DS-GVO sowie im BDSG verwandten Begriffe zu bestimmende – Anwendungsbereich des § 26 Abs. 3 BDSG ist hinsichtlich der verfahrensgegenständlichen Auskunft eröffnet.

(1) Die vom Betriebsrat erstrebte Unterrichtung unterfällt dem Geltungsbereich der DS-GVO nach deren Art. 2 Abs. 1 und Art. 3 Abs. 1 sowie dem des BDSG nach dessen § 1 Abs. 1 Satz 2.

(a) Die Mitteilung der Schwangerschaft unter Namensnennung einer Arbeitnehmerin an den Betriebsrat durch die Arbeitgeberin stellt eine Verarbeitung sich auf eine bestimmte natürliche Person beziehender und damit personenbezogener Daten nach Art. 4 Nr. 1 und Nr. 2 DS-GVO dar. Der Begriff der Verarbeitung bezeichnet nach Art. 4 Nr. 2 DS-GVO ua. jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten. Hierzu zählt die Offenlegung durch Übermittlung, also die gezielte Weitergabe von Daten an einen Empfänger, der – was seinerseits aus Art. 4 Nr. 9 DS-GVO folgt – kein Dritter sein muss (Roßnagel, in: Simitis/Hornung/Spieker, Datenschutzrecht, Art. 4 Nr. 2 DS-GVO Rn. 26 mwN; vgl. auch Herbst, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl., Art. 4 Nr. 2 DS-GVO Rn. 29; ebenso Schaffland/Wiltfang DS-GVO/BDSG Art. 4 DS-GVO Rn. 85; wohl aA Weichert, in: Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 4 DS-GVO Rn. 47 und Rn. 94). Damit ist es für die Annahme einer Datenverarbeitung – anders als bei § 3 Abs. 4 Nr. 3 BDSG in seiner vom 28. August 2002 bis zum 24. Mai 2018 geltenden Fassung (aF), wonach es sich nur bei der Bekanntgabe von Daten gegenüber Dritten um eine Datenübermittlung gehandelt hat – nicht ausschlaggebend, ob der Betriebsrat Dritter iSv. Art. 4 Nr. 10 DS-GVO ist.

(b) Angesichts des von der Arbeitgeberin durchgeführten Verfahrens nach der Anzeige der Schwangerschaft durch eine Arbeitnehmerin (Musterbrieferstellung, Datenweitergabe) handelt es sich um eine nicht automatisierte Verarbeitung von personenbezogenen Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DS-GVO, § 1 Abs. 1 Satz 2 BDSG). Diese erfolgt durch die Arbeitgeberin und damit – vorliegend – durch eine nichtöffentliche Stelle iSv. § 1 Abs. 1 Satz 2 iVm. § 2 Abs. 4 Satz 1 BDSG.

(2) Die Erfüllung der vom Betriebsrat begehrten Auskunft stellt eine betriebsinterne Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses dar. Die verlangte Information bezieht sich auf die Daten von Arbeitnehmerinnen und damit Beschäftigten iSv. § 26 Abs. 8 Satz 1 Nr. 1 BDSG. Da der Betriebsrat geltend macht, diese für die Wahrnehmung einer

gesetzlichen Aufgabe zu benötigen, liegt mit der Weitergabe der Namen der ihre Schwangerschaft iSv. § 15 Abs. 1 Satz 1 MuSchG mitteilenden Arbeitnehmerinnen eine Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses vor. Eine solche ist – wie § 26 Abs. 1 Satz 1 BDSG zeigt – auch gegeben, wenn die Verarbeitung dazu dient, sich aus dem Gesetz ergebende Pflichten der Interessenvertretung der Beschäftigten zu erfüllen.

(3) Das Verlangen des Betriebsrats betrifft die Verarbeitung von Gesundheitsdaten als eine der besonderen Kategorien personenbezogener Daten iSv. Art. 9 Abs. 1 DS-GVO.

(a) Nach Art. 4 Nr. 15 DS-GVO sind Gesundheitsdaten diejenigen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

(b) Das meint auch positive oder neutrale Informationen zur körperlichen Verfasstheit. Nach der Wertung in Erwägungsgrund (35) zur DS-GVO gilt ein weiter Gesundheitsdatenbegriff, der beispielsweise Informationen, die von der Prüfung einer körpereigenen Substanz oder aus biologischen Proben abgeleitet wurden, ebenso einschließt wie Informationen über den physiologischen oder biomedizinischen Zustand einer Person unabhängig von der Herkunft der Daten (vgl. zu einem weiten Verständnis des bereits in Art. 8 Abs. 1 der aufgehobenen Richtlinie 95/46/EG verwandten Begriffs „Daten über die Gesundheit“ auch EuGH 6. November 2003 – C-101/01 – [Lindqvist] Rn. 50). Entsprechend ist die Schwangerschaft ein Gesundheitsdatum im datenschutzrechtlichen Sinn (ebenso Petri, in: Simitis/Hornung/Spieker, Datenschutzrecht, Art. 4 Nr. 15 DS-GVO Rn. 3; Kircher, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, S. 27).

dd) Hat der Betriebsrat nach § 80 Abs. 2 Satz 1 BetrVG einen Anspruch darauf, dass ihm die Arbeitgeberin nach einer Anzeige iSd. § 15 Abs. 1 MuSchG den Namen der schwangeren Arbeitnehmerin mitteilt, ist die damit verbundene Datenverarbeitung iSv. § 26 Abs. 3 Satz 1 BDSG zur Erfüllung einer rechtlichen Pflicht aus dem Arbeitsrecht erforderlich. Für den Fall des Vorliegens von Schutzmaßnahmen iSv. § 26 Abs. 3 Satz 3 iVm. § 22 Abs. 2 BDSG besteht auch kein Grund zu der Annahme, dass schutzwürdige Interessen der betroffenen Arbeitnehmerinnen an dem Ausschluss der Verarbeitung überwiegt.

(1) Mit dem Kriterium der Erforderlichkeit der Datenverarbeitung nach § 26 Abs. 3 Satz 1 BDSG ist – ebenso wie bei § 26 Abs. 1 Satz 1 BDSG – sichergestellt, dass ein an sich legitimes Datenverarbeitungsziel nicht zum Anlass genommen wird, überschneidend personenbezogene (sensitive) Daten zu verarbeiten (Petri, in: Simitis/Hornung/Spieker, Datenschutzrecht, Art. 9 DS-GVO Rn. 42). Bei einer auf Beschäftigtendaten bezogenen datenverarbeitenden Maßnahme des Arbeitgebers bedingt dies entsprechend der Bekundung des Gesetzgebers – welcher hierbei an die bis 24. Mai 2018 geltenden datenschutzrechtlichen Bestimmungen und die hierzu ergangene höchstrichterliche Rechtsprechung anknüpft (vgl. BT-Drs. 18/11325 S. 97) – eine Abwägung widerstreitender Grundrechtspositionen im Wege praktischer Konkordanz sowie eine Verhältnismäßigkeitsprüfung (ausf. dazu – unter Hinzuziehung der Gesetzeshistorie und -begründung – zB Stamer/Kuhnke, in: Plath, BDSG/DS-GVO, 3. Aufl., § 26 BDSG Rn. 16 ff.). Diesen Anforderungen ist genügt, wenn die Verarbeitung personenbezogener Daten zur Erfüllung eines sich aus dem Gesetz ergebenden Rechts der Interessenvertretung der Beschäftigten – und damit einer „aus dem Arbeitsrecht“ iSv. § 26 Abs. 3 Satz 1 BDSG resultierenden Pflicht des Arbeitgebers – erforderlich ist. Das hat der Gesetzgeber

durch den entsprechenden Erlaubnistatbestand in § 26 Abs. 1 Satz 1 BDSG klargestellt (vgl. BT-Drs. 18/11325 S. 97).

(2) Soweit § 26 Abs. 3 Satz 1 BDSG bei der Verarbeitung sensibler Daten – ebenso wie § 28 Abs. 6 BDSG aF (dazu BAG 7. Februar 2012 – 1 ABR 46/10 – Rn. 40 ff., BAGE 140, 350) – darüber hinaus verlangt, dass kein Grund zu der Annahme des Überwiegens typischer schutzwürdiger Interessen von Betroffenen gegenüber den Interessen an der Verarbeitung bestehen darf (BT-Drs. 18/11325 S. 98), ist diesem Erfordernis im Zusammenhang mit der Erfüllung einer sich aus dem Gesetz ergebenden Aufgabe des Betriebsrats durch die von § 26 Abs. 3 Satz 3 BDSG angeordnete entsprechende Anwendung von § 22 Abs. 2 BDSG Rechnung getragen. Danach sind zur Wahrung der Interessen Betroffener angemessene und spezifische Maßnahmen vorzusehen. Sind solche vorhanden, ist davon auszugehen, dass schutzwürdige Interessen der Beschäftigten der Datenverarbeitung nicht entgegenstehen. Fehlt es hieran, ist die Verarbeitung sensibler Daten unzulässig.

(3) Steht dem Betriebsrat ein Anspruch auf die streitbefangene Information nach § 80 Abs. 2 Satz 1 BetrVG zu, ist die von § 26 Abs. 3 Satz 1 BDSG verlangte Erforderlichkeit der Datenverarbeitung gegeben.

(a) Dies ergibt sich – ebenso wie bei § 26 Abs. 1 Satz 1 BDSG – aus der strikten Bindung der Unterrichtsverpflichtung des Arbeitgebers an eine dem Betriebsrat obliegende Aufgabe, für dessen Wahrnehmung dieser das verlangte Datum benötigt. Der bloße Bezug der vom Betriebsrat verlangten Information zu einer von ihm wahrzunehmenden Aufgabe reicht nicht aus, um den betriebsverfassungsrechtlichen Auskunftsanspruch hinsichtlich personenbezogener oder gar sensibler Daten zu begründen (dies vernachlässigend und daher in der Konsequenz eine Diskrepanz zwischen betriebsverfassungsrechtlicher und datenschutzrechtlicher Erforderlichkeit annehmend vgl. Stamer/Kuhnke, in: Plath, BDSG/DS-GVO, 3. Aufl. § 26 BDSG Rn. 156; ähnlich Wybitul, NZA 2017, 413, 416). Es bedarf vielmehr der Feststellung, dass die verlangte Information – vorliegend: das sensitive Datum – unerlässlich ist, um sich der Aufgabe überhaupt annehmen zu können. Vermag der Betriebsrat dies nicht aufzuzeigen, scheiden sein Auskunftsanspruch und die damit verbundene Datenverarbeitung bereits aus diesem Grund aus. Diese Kopplung des Inhalts und Umfangs vom Betriebsrat verlangter Daten an den Aufgabenbezug bei einem auf den allgemeinen Unterrichtsanspruch des § 80 Abs. 2 Satz 1 BetrVG gestützten Anspruch (vgl. anschaulich dazu BAG 12. März 2019 – 1 ABR 48/17 – Rn. 22 ff.) rechtfertigt die Annahme, dass im Fall einer auf personenbezogene Daten gerichteten Auskunftsverpflichtung des Arbeitgebers gegenüber dem Betriebsrat die darin liegende Datenverarbeitung regelmäßig auch datenschutzrechtlich erforderlich ist (zur datenschutzkonformen Auslegung des betriebsverfassungsrechtlichen Erforderlichkeitsbegriffs beim allgemeinen Auskunftsanspruch vgl. bei Gola BB 2017, 1462, 1465; Lelley/Bruck/Yildiz BB 2018, 2164, 2172). Das gilt jedenfalls dann, wenn sich der Betriebsrat zur Begründung des Auskunftsbegehrens auf die Wahrnehmung einer gesetzlichen Aufgabe beruft.

(b) Dem steht nicht der Umstand entgegen, dass der allgemeine Auskunftsanspruch des § 80 Abs. 2 Satz 1 BetrVG greifenbezogen ausgestaltet ist. Eine solche Art und Weise der Datenverarbeitung ist grundsätzlich von der Tatbestandsvoraussetzung der Erforderlichkeit des § 26 Abs. 3 Satz 1 BDSG (Erfüllung einer Pflicht „aus dem Arbeitsrecht“) erfasst.

(c) Die Annahme, dass mit dem auf ein (sensitives) personenbezogenes Datum gerichteten Unterrichtsverlangen des

Betriebsrats bei Erfüllung der Anspruchsvoraussetzungen des § 80 Abs. 2 Satz 1 BetrVG regelmäßig eine datenschutzrechtlich erforderliche Datenverarbeitung verbunden ist, verbietet sich nicht aus unionsrechtlichen Gründen. Ausweislich der Erwägungsgründe (51) und (52) zur DS-GVO, auf deren Art. 9 Abs. 2 Buchst. b DS-GVO die nationale Erlaubnisnorm beruht, unterliegt die Verarbeitung von personenbezogenen Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, zwar einerseits einem besonderen Schutz; andererseits sollen aber Ausnahmen vom Verbot der Verarbeitung dieser besonderen Kategorie von personenbezogenen Daten auch erlaubt sein, wenn das – vorbehaltlich angemessener Schutzgarantien – „insbesondere für die Verarbeitung von personenbezogenen Daten auf dem Gebiet des Arbeitsrechts“ gerechtfertigt ist.

(d) Vorstehendes gilt bei dem konkret streitbefangenen Datum des Namens einer Arbeitnehmerin, welche der Arbeitgeberin ihre Schwangerschaft mitgeteilt hat, auch unter Berücksichtigung des aus Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG abgeleiteten allgemeinen Persönlichkeitsrechts der schwangeren Beschäftigten und ihres in Art. 6 Abs. 4 GG verankerten Schutz- und Fürsorgeanspruchs. Eine Arbeitnehmerin ist gegenüber dem Arbeitgeber nicht verpflichtet, das Bestehen ihrer Schwangerschaft mitzuteilen; nach § 15 Abs. 1 Satz 1 MuSchG „soll“ eine entsprechende Information erfolgen. Die gesetzliche Fassung als Sollvorschrift beruht auf der Achtung des Persönlichkeitsrechts der Frau und ihren grundrechtlichen Gewährleistungen. Obwohl die Gesundheit von Mutter und Kind eine frühzeitige Unterrichtung des Arbeitgebers nahelegt, sind Arbeitnehmerinnen damit nicht zur Offenbarung einer Schwangerschaft gezwungen. Hiervon ist die höchstrichterliche Rechtsprechung zur Vorgängervorschrift nach § 5 Abs. 1 Satz 1 MuSchG aF ausgegangen (BAG 18. Januar 2000 – 9 AZR 932/98 – BAGE 93, 179; 13. Juni 1996 – 2 AZR 736/95 – BAGE 83, 195), dessen Regelungsgehalt mit § 15 Abs. 1 Satz 1 MuSchG unverändert geblieben und lediglich redaktionell überarbeitet worden ist (vgl. BT-Drs. 18/8963 S. 86 f.). Wird die Schwangerschaft iSv. § 15 Abs. 1 Satz 1 MuSchG mitgeteilt, beeinflusst dies die Rechtsbeziehung zum Arbeitgeber. Er hat nunmehr diverse mutterschutzrechtliche Ge- und Verbote zu beachten, deren Durchführungsüberwachung wiederum nach § 80 Abs. 1 Nr. 1 BetrVG kraft Gesetzes dem Betriebsrat obliegt. Kann dieser seine gesetzlich geregelte Überwachungsaufgabe nur wahrnehmen, wenn er weiß, welche Arbeitnehmerin ihre Schwangerschaft angezeigt hat, ist die Annahme schutzwürdiger Interessen der von der Datenverarbeitung Betroffenen an einem Verarbeitungsausschluss nicht veranlasst.

(4) Im Hinblick auf das Vorliegen von Maßnahmen nach § 26 Abs. 3 Satz 3 iVm. § 22 Abs. 2 BDSG als aus datenschutzrechtlichen Gründen weiterer Zulässigkeitsvoraussetzung für die erstrebte, ein sensibles Datum umfassende Auskunft bedürfte es hingegen noch weiteren Vorbringens des Betriebsrats und einer hierauf gerichteten Würdigung des Landesarbeitsgerichts.

(a) Bei der Weitergabe sensibler Daten an den Betriebsrat hat der Arbeitgeber die Beachtung des in § 26 Abs. 3 Satz 3 iVm. § 22 Abs. 2 BDSG geregelten Gebots angemessener und spezifischer Schutzmaßnahmen nicht in der Hand. Ihm sind hierauf bezogene Vorgaben an den Betriebsrat aufgrund dessen Unabhängigkeit als Strukturprinzip der Betriebsverfassung verwehrt (vgl. ausf. BAG 11. November 1997 – 1 ABR 21/97 – zu B III 2 c aa der Gründe, BAGE 87, 64). Daher hat der Betriebsrat bei der Geltendmachung eines auf sensitive Daten gerichteten Auskunftsbegehrens das Vorhalten von Maßnahmen darzulegen,

welche die berechtigten Interessen der betroffenen Arbeitnehmer – vorliegend der ihre Schwangerschaft mitteilenden Arbeitnehmerinnen – wahren. Den Betriebsrat trifft insoweit, unabhängig davon, ob er iSv. Art. 4 Nr. 7 DS-GVO Teil der verantwortlichen Stelle (so zB Bonanni/Niklas ArbRB 2018, 371; Gola/Pötters DS-GVO Art. 88 Rn. 38; Gola/Gola DS-GVO Art. 4 Rn. 56) oder gar Verantwortlicher (so zB Kurzböck/Weinbeck BB 2018, 1652, 1655; Kleinebrink DB 2018, 2566; Wybitul NZA 2017, 413 f.) ist, eine spezifische Schutzpflicht.

(b) Dabei ist zu berücksichtigen, dass § 22 Abs. 2 BDSG die möglichen Maßnahmen nur beispielhaft („insbesondere“) aufzählt. Deshalb muss es sich bei den vom Betriebsrat zu treffenden und bei einem auf sensitive Daten gerichteten Auskunftsverlangen darzulegenden Schutzvorkehrungen nicht um die ausdrücklich in § 22 Abs. 2 Satz 2 Nr. 1 bis Nr. 10 BDSG genannten Maßnahmen handeln, zumal bei einzelnen dieser Maßnahmen zweifelhaft ist, ob sie der Betriebsrat überhaupt ergreifen könnte. Es ist aber zu gewährleisten, dass er bei einer Verarbeitung sensibler Daten – hier: des Namens schwangerer Arbeitnehmerinnen – das Vertraulichkeitsinteresse der Betroffenen strikt achtet und Vorkehrungen trifft, die bei wertender Betrachtung den in § 22 Abs. 2 Satz 2 BDSG aufgelisteten Kriterien entsprechen. Hierzu können Maßnahmen zur Datensicherheit wie das zuverlässige Sicherstellen des Verschlusses der Daten, die Gewähr begrenzter Zugriffsmöglichkeiten oder deren Beschränkung auf einzelne Betriebsratsmitglieder sowie die Datenlöschung nach Beendigung der Überwachungsaufgabe gehören. Ein Fehlen solcher Schutzmaßnahmen oder ihre Unzulänglichkeit – was der Würdigung des Tatsachengerichts unterliegt – schließt den streitbefangenen Anspruch aus.

c) Der bloße Umstand, dass die betroffenen Arbeitnehmerinnen der Information des Betriebsrats über ihre Schwangerschaft widersprochen haben, steht der verlangten Datenübermittlung hingegen nicht entgegen. Zwar gewährt Art. 18 Abs. 1 Buchst. d DS-GVO den von einer Datenverarbeitung betroffenen Personen unter bestimmten Voraussetzungen das Recht, die Einschränkung der Verarbeitung zu verlangen, wenn sie hiergegen nach Art. 21 Abs. 1 DS-GVO Widerspruch eingelegt haben. Die Voraussetzungen des Widerspruchsrechts nach Art. 21 Abs. 1 DS-GVO sind vorliegend aber schon deshalb nicht erfüllt, weil die Offenlegung der Daten gegenüber dem Betriebsrat nicht auf der Grundlage von Art. 6 Abs. 1 Buchst. e oder f DS-GVO, sondern von Art. 9 Abs. 2 Buchst. b DS-GVO iVm. § 26 Abs. 3 BDSG erfolgen würde.

4. Sollten für die vom Betriebsrat begehrte Auskunft die Voraussetzungen des allgemeinen Unterrichtsanspruchs nach § 80 Abs. 2 Satz 1 BetrVG erfüllt und – im Fall ausreichender Schutzmaßnahmen des Betriebsrats iSv. § 26 Abs. 3 Satz 3 iVm. § 22 Abs. 2 BDSG – damit die in der Auskunftserteilung liegende Datenverarbeitung nach § 26 Abs. 3 Satz 1 und Satz 3 BDSG zulässig sein, stünden dem Begehren entgegen der Auffassung der Arbeitgeberin keine verfassungsrechtlichen Gründe entgegen.

a) Ist eine Datenverarbeitung nach den Vorschriften des BDSG (iVm. der DS-GVO) zulässig, ist das Recht des von der Datenverarbeitung betroffenen Arbeitnehmers auf informationelle Selbstbestimmung gewahrt (vgl. – zum BDSG aF – BAG 27. Juli 2017 – 2 AZR 681/16 – Rn. 17, BAGE 159, 380). Dem durch Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG gewährleisteten allgemeinen Persönlichkeitsrecht der Arbeitnehmer, das die Befugnis jedes Einzelnen umfasst, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen (Recht auf informatio-

nelle Selbstbestimmung; BVerfG 11. März 2008 – 1 BvR 2074/05 ua. – Rn. 67, BVerfGE 120, 378) – wobei sich der Begriff der persönlichen Daten mit dem datenschutzrechtlichen Begriff personenbezogener Daten deckt (vgl. BVerfG 27. Juni 2018 – 2 BvR 1562/17 – Rn. 44 mwN) – ist im Rahmen der datenschutzrechtlichen Erwägungen Rechnung getragen.

b) Gleiches gilt vorliegend für Art. 6 Abs. 4 GG als Ausdruck der für den gesamten Bereich des privaten und des öffentlichen Rechts verbindlichen verfassungsrechtlichen Wertentscheidung (dazu BVerfG 25. Januar 1972 – 1 BvL 3/70 – BVerfGE 32, 273), dass jede, insbesondere jede werdende, Mutter Anspruch auf den Schutz und die Fürsorge der staatlichen Gemeinschaft hat (BVerfG 24. Mai 2005 – 1 BvR 906/04 – zu II 1 a der Gründe). Darin liegt ein besonderer Belang der von der Datenverarbeitung betroffenen schwangeren Frauen, der jedoch die gesetzliche Unterrichtspflicht des Arbeitgebers nach § 80 Abs. 2 Satz 1 BetrVG sowie die damit verbundene zulässige Datenverarbeitung nicht auszuschließen vermag. Insoweit gilt nichts anderes als bei der gesetzlichen Pflicht des Arbeitgebers, unverzüglich die Aufsichtsbehörde zu benachrichtigen, wenn eine Frau ihm mitgeteilt hat, dass sie schwanger ist (§ 27 Abs. 1 Satz 1 Nr. 1 Buchst. a MuSchG).

IV. Auf die im Verfahren und im angefochtenen Beschluss problematisierte Entscheidung des Bundesverwaltungsgerichts vom 29. August 1990 (– 6 P 30.87 –) zu einem personalvertretungsrechtlichen Auskunftsanspruch und auf die insoweit geltend gemachte Abweichung der Rechtsprechung des erkennenden Senats zu Unterrichtsverlangen des Betriebsrats nach § 80 Abs. 2 Satz 1 iVm. Abs. 1 Nr. 1 BetrVG, wonach es keines besonderen Anlasses für den auf eine Überwachungsaufgabe gestützten Auskunftsanspruch des Betriebsrats bedarf, kommt es nicht an. Allerdings ist darauf hinzuweisen, dass nach der aktuellen Rechtsprechung des Bundesverwaltungsgerichts ein zur Wahrnehmung allgemeiner Überwachungsaufgaben geltend gemachter Informationsanspruch des Personalrats nicht notwendig daran gebunden ist, dass sich die Personalvertretung gegenüber dem Dienststellenleiter auf einen besonderen Anlass – wie etwa einen bekannt gewordenen oder zu besorgenden Rechtsverstoß der Dienststelle – berufen kann (vgl. zu § 69 Abs. 2 Satz 1 LPersVG RP BVerwG 19. Dezember 2018 – 5 P 6.17 – Rn. 39 ff.).

Videüberwachung privater Räume richtet sich ausschließlich nach Unionsrecht

(Bundesverwaltungsgericht, Urteil vom 27. März 2019 – 6 C 2.18 –)

- 1. Die Rechtmäßigkeit von Anordnungen zur Beseitigung datenschutzrechtlicher Verstöße nach § 38 Abs. 5 Satz 1 BDSG a.F. ist nach der Rechtslage zu beurteilen, die zum Zeitpunkt der letzten behördlichen Entscheidung gilt. Nachträgliche Rechtsänderungen sind nicht zu berücksichtigen.**
- 2. Die Zulässigkeit einer Videüberwachung im Sinne von § 6b Abs. 1 BDSG a.F. zu privaten Zwecken setzt voraus, dass der Verantwortliche plausibel Gründe darlegt, aus denen sich die Erforderlichkeit der Maßnahme ergibt.**

3. Die Videüberwachung ist zur Verhinderung von Straftaten erforderlich, wenn in Bezug auf die beobachteten Räume eine erheblich über das allgemeine Lebensrisiko hinausgehende Gefährdungslage besteht.

4. Die Datenschutz-Grundverordnung der Europäischen Union gilt nicht für die Beurteilung der Rechtmäßigkeit von Anordnungen zur Beseitigung datenschutzrechtlicher Verstöße, die die Behörden vor deren Geltungsbeginn auf der Grundlage des nationalen Rechts getroffen haben.

5. Die Zulässigkeit von Videüberwachungen zu privaten Zwecken richtet sich nunmehr nach Art. 6 Abs. 1 UnterAbs. 1 Buchst. f DS-GVO.

Aus den Gründen:

b) Die Zulässigkeitsvoraussetzungen für die Verarbeitung sind in Art. 6 Abs. 1 DS-GVO abschließend geregelt, wobei die Absätze 2 und 3 begrenzte Öffnungsklauseln zugunsten der Mitgliedstaaten enthalten. Haben die Betroffenen wie im vorliegenden Fall nicht rechtswirksam in die Verarbeitung ihrer personenbezogenen Daten eingewilligt (Art. 6 Abs. 1 UnterAbs. 1 Buchst. a i.V.m. Art. 4 Nr. 11 DS-GVO), sind Verarbeitungsvorgänge nur rechtmäßig, wenn sie auf mindestens einen Erlaubnistatbestand des Art. 6 Abs. 1 DS-GVO gestützt werden können.

45 Datenverarbeitungen durch Privatpersonen wie die Videoüberwachung der Klägerin können von vornherein nicht auf Art. 6 Abs. 1 UnterAbs. 1 Buchst. e DS-GVO gestützt werden. Danach muss die Datenverarbeitung erforderlich für die Wahrnehmung einer Aufgabe sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Eine zusätzliche Abwägung mit den Interessen der Betroffenen ist nicht vorgesehen. Dies lässt sich in Anbetracht des hohen Stellenwerts des informationellen Selbstbestimmungsrechts der Betroffenen nur rechtfertigen, wenn der Anwendungsbereich des Tatbestands entsprechend seinem Wortlaut auf behördliche oder staatlich veranlasste Verarbeitungsvorgänge beschränkt wird. Die Verarbeitung personenbezogener Daten unterfällt dem Schutzbereich der Grundrechte auf Privatleben nach Art. 7 und auf Schutz der eigenen Daten nach Art. 8 der Grundrechtecharta der Europäischen Union (EuGH, Urteil vom 11. Dezember 2014 – C-212/13 – Rn. 28).

46 Dementsprechend erfasst Art. 6 Abs. 1 UnterAbs. 1 Buchst. e DS-GVO Datenverarbeitungen durch Behörden, die diese in Erfüllung ihrer Aufgaben vornehmen. Privatpersonen können sich darauf nur berufen, wenn ihnen die Befugnis, auf personenbezogene Daten zuzugreifen, im öffentlichen Interesse oder als Ausübung öffentlicher Gewalt übertragen ist. Sie müssen anstelle einer Behörde tätig werden. Dies setzt einen wie auch immer gestalteten staatlichen Übertragungsakt voraus. Eine Privatperson kann sich nicht selbst zum Sachwalter des öffentlichen Interesses erklären. Insbesondere ist sie nicht neben oder gar anstelle der Ordnungsbehörden zum Schutz der öffentlichen Sicherheit berufen. Beim Schutz individueller Rechtsgüter, seien es ihre eigenen oder diejenigen Dritter, verfolgt sie keine öffentlichen, sondern private Interessen (Buchner/Petri, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 111 ff.; Kramer, in: Auernhammer, DS-GVO/BDSG, 5. Aufl. 2017, Art. 6 Rn. 24 f.; Pabst, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 2018, Art. 6 DS-

GVO Rn. 95; Wedde, in: Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, DS-GVO Art. 6 Rn. 87 und 89). Somit kann dahingestellt bleiben, ob es sich bei Art. 6 Abs. 1 UnterAbs. 1 Buchst. e DS-GVO um einen eigenständigen Erlaubnistatbestand handelt oder die Bestimmung durch unionsrechtliche oder nationale Bestimmungen über behördliche Datenverarbeitungen im öffentlichen Interesse ausgefüllt werden muss (vgl. Schulz, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 48 und 197).

47 Daraus folgt, dass die Öffnungsklauseln des Art. 6 Abs. 2 und 3 DS-GVO für Verarbeitungen nach Art. 6 Abs. 1 UnterAbs. 1 Buchst. e DS-GVO Videoüberwachungen privater Verantwortlicher nicht erfassen. Aufgrund dessen ist kein Raum für eine künftige Anwendung des § 4 Abs. 1 Satz 1 des seit 25. Mai 2018 geltenden Bundesdatenschutzgesetzes in der Fassung von Art. 1 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097) – BDSG n.F. – als wortgleicher Nachfolgeregelung des § 6b Abs. 1 BDSG a.F. auf Videoüberwachungen privater Verantwortlicher. Diese sind an Art. 6 Abs. 1 UnterAbs. 1 Buchst. f DS-GVO zu messen. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Das zweistufige Prüfprogramm dieser Bestimmung entspricht demjenigen des § 6b Abs. 1 BDSG a.F. Die Verarbeitung ist erforderlich, wenn der Verantwortliche zur Wahrung berechtigter, d.h. schutzwürdiger und objektiv begründbarer Interessen darauf angewiesen ist. Eine nach diesem Maßstab erforderliche Verarbeitung ist zulässig, wenn die Abwägung in dem jeweiligen Einzelfall ergibt, dass berechnete Interessen des Verantwortlichen höher zu veranschlagen sind als das informationelle Selbstbestimmungsrecht der Betroffenen. Hierfür ist nach Erwägungsgrund 47 zur Datenschutz-Grundverordnung unter anderem bedeutsam, ob die Datenverarbeitung für die Verhinderung von Straftaten unbedingt erforderlich ist, ob sie absehbar, d.h. branchenüblich ist, oder ob die Betroffenen in der konkreten Situation vernünftigerweise damit rechnen müssen, dass ihre Daten verarbeitet werden.

48 Danach wäre die Videoüberwachung des öffentlich zugänglichen Bereichs der Zahnarztpraxis der Klägerin auch nach Maßgabe des Art. 6 Abs. 1 UnterAbs. 1 Buchst. f DS-GVO unzulässig, weil sie nicht erforderlich ist, um berechnete Interessen der Klägerin zu wahren. Insoweit kann auf die Ausführungen zur Erforderlichkeit nach § 6b Abs. 1 BDSG a.F. unter 3.b) verwiesen werden.

Tätowierung als Eignungsmangel im öffentlichen Dienst (Ls)

(Landesarbeitsgericht Berlin-Brandenburg, Beschluss vom 25. April 2019 – 5 Ta 730/19 –)

1. Tätowierungen können dann einen im Auswahlverfahren bei der Besetzung von Stellen im Objektschutz der Berliner Polizei zu berücksichtigenden Eignungsmangel begründen, wenn sich aus ihrem Inhalt eine Straftat ergibt oder ihr Inhalt für den Bürger als Betrachter direkt (und nicht als Folge einer nur als möglich angesehenen und damit dem Regelungsvorbehalt des Gesetzgebers überlassenen Wirkung in der Bevölkerung) Zweifel an der geforderten Gewähr des Einstellungs-

bewerbers begründen, jederzeit für die freiheitliche demokratische Grundordnung im Sinne des Grundgesetzes einzutreten.

2. Die zweitgenannte Alternative ist gegeben, wenn der Bewerber zumindest beim Tragen sommerlicher Dienstkleidung sichtbare Tätowierungen trägt, die das Wort "omerta", Revolverpatronen und Totenköpfe abbilden.

Sachvortragsverwertungsverbot bei Auswertung privater E-Mails (Ls)

(Landesarbeitsgericht Hessen, Urteil vom 21. September 2018 – 10 Sa 601/18 –)

- 1. Ist der Sendevorgang abgeschlossen, kommt ein Verwertungsverbot von E-Mails nach § 88 Abs. 3 TKG jedenfalls dann nicht in Betracht, wenn die E-Mails auf einem Ordner abgelegt sind, auf den der Arbeitgeber ohne Zugriff auf das Internet zugreifen kann.**
- 2. Es stellt eine unverhältnismäßige Kontrollmaßnahme nach § 32 Abs. 1 Satz 1 BDSG a.F. dar, wenn der Arbeitgeber auf einen vagen Hinweis, der Arbeitnehmer hätte sich geschäftsschädigend über den Arbeitgeber geäußert, den privaten E-Mail-Verkehr eines Arbeitnehmers in einem Zeitraum von einem Jahr auswertet. Im anderen Falle kann die Datenverarbeitung zwecks der Klärung der Berechtigung zur Beendigung des Arbeitsverhältnisses für einen angemessenen Zeitraum erforderlich sein.**
- 3. Dieser Verstoß gegen Datenschutzrecht führt nach einer Abwägung zwischen Art. 103 Abs. 1 GG und dem Recht auf informationelle Selbstbestimmung nach Art. 1, 2 Abs. 1 GG zu einem „Sachvortragsverwertungsverbot“.**
- 4. Der Arbeitgeber kann grundsätzlich die Arbeitnehmer anhalten, private E-Mails in einem separaten Ordner abzuspeichern oder nach Kenntnisnahme zu löschen. Allerdings müssen diese Vorgaben selbst dem aus Art. 1, 2 Abs. 1 GG abzuleitenden Verhältnismäßigkeitsgrundsatz entsprechen. Dies bedeutet, dass die Vorgaben transparent und erforderlich sein müssen, um die vom Arbeitgeber verfolgten Zwecke zu wahren.**

Auskunft an den Betriebsrat über Sonderzahlungen

(Landesarbeitsgericht Hessen, Beschluss vom 10. Dezember 2018 – 16 TaBV 130/18 –)

Es bestehen keine datenschutzrechtlichen Bedenken, den Arbeitgeber für verpflichtet zu halten, dem Betriebsrat Auskunft darüber zu erteilen, an welche Arbeitnehmer mit Ausnahme leitender Angestellter Sonderzahlungen geleistet wurden.

Sachverhalt:

Die Beteiligten streiten über die Verpflichtung des Arbeitgebers zur Auskunftserteilung gegenüber dem Betriebsrat, an welche Arbeitnehmer, in welcher Höhe, auf welcher Grundlage und nach welchen Kriterien Zulagen, Prämien, Gratifikationen, Provisionen oder sonstige Sonderzahlungen ab 1. September 2016 gezahlt wurden.

Das Arbeitsgericht hat dem Antrag stattgegeben und sich der Entscheidung des Hessischen Landesarbeitsgerichts vom 4. Mai 2015 -16 TaBV 175/14- angeschlossen.

Aus den Gründen:

1. Die Beschwerde ist statthaft, aber nicht begründet.

Wie das Arbeitsgericht zutreffend erkannt hat, wird der allgemeine Unterrichtsanspruch des § 80 Abs. 2 S. 1 BetrVG nicht durch den Anspruch auf Einsicht in die Bruttoentgeltlisten nach § 80 Abs. 2 S. 2 BetrVG verdrängt.....

Wie das Arbeitsgericht weiter zutreffend erkannt hat, kann sich der Betriebsrat für sein Begehren auch auf § 80 Abs. 1 Nr. 1 BetrVG berufen, weil er darüber zu wachen hat, dass die zugunsten der Arbeitnehmer geltenden Gesetze und Tarifverträge durchgeführt werden...(wird ausgeführt)

Entgegen der Auffassung der Arbeitgeberseite bestehen hinsichtlich der Weitergabe der im Antrag genannten Daten an den Betriebsrat keine datenschutzrechtlichen Bedenken. Hinsichtlich der Rechtslage vor dem 25. Mai 2018 wird insoweit zunächst auf die Entscheidung des Bundesarbeitsgerichts vom 14. Januar 2014 – 1 ABR 54/12 – Rn. 27ff Bezug genommen.

Für die Zeit ab 25. Mai 2018 ergibt sich nichts anderes. .. (wird ausgeführt). Dies folgt aus § 26 Abs. 1 BDSG. Wie § 26 Abs. 6 BDSG ausdrücklich klarstellt, bleiben die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt. Hieraus folgt, dass der Arbeitgeber berechtigt und verpflichtet ist (auch gegen den Willen der betreffenden Beschäftigten) deren personenbezogene Daten im Rahmen der dem Betriebsrat obliegenden Aufgaben an den Betriebsrat weiterzuleiten. Zur Wahrnehmung der ihm obliegenden Aufgaben (Ausübung des Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 10 BetrVG sowie des Überwachungsrechts nach § 80 Abs. 1 Nr. 1 BetrVG) benötigt der Betriebsrat die im Antrag genannten personenbezogenen Daten der Beschäftigten.

Mit dem Grundsatz der Datensparsamkeit kann nicht gerechtfertigt werden, dem Betriebsrat die von diesem für die Wahrnehmung seiner Aufgaben benötigten personenbezogenen Daten der Beschäftigten vorzuenthalten. Gegen die Erhebung dieser Daten durch den Arbeitgeber bestehen daher auch unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit keine Bedenken. Benötigt der Betriebsrat diese Daten zur Wahrnehmung seiner gesetzlichen Aufgaben, sind sie ihm vom Arbeitgeber zur Verfügung zu stellen. Dies ergibt sich aus § 26 Abs. 6 BDSG, was Lelley/Bruck/Yildiz, BB 18, 2164, 2172 nicht hinreichend berücksichtigen. Eine gesonderte Prüfung einer „datenschutzrechtlichen Erforderlichkeit“, die Lelley/Bruck/Yildiz (a.a.O.) vornehmen und hierzu ein dreistufiges Prüfprogramm entwickeln, erübrigt sich daher. Soweit § 80 Abs. 2 Satz 2 BetrVG den Anspruch auf die erforderlichen Unterlagen beschränkt, ist dies seit jeher (also auch vor Inkrafttreten der Datenschutzgrundverordnung und des neuen BDSG) der Fall. Der Prüfungsmaßstab hat sich insoweit nicht geändert. Auch Kort (NZA 18, 1097, 1103) räumt ein, dass die betriebsverfassungsrechtliche Rolle des Betriebsrats auch unter Geltung der Datenschutzgrundverordnung und des (neuen) BDSG im Grundsatz erhalten bleibt. Dies betone § 26 Abs. 6 BDSG. Der Betriebsrat verfüge daher nach wie vor über das (aufgabenbezo-

gene) Informationsrecht nach § 80 BetrVG sowie über die Beteiligungsrechte nach § 87 BetrVG, ohne dass (neue) datenschutzrechtliche Bestimmungen diesen Beteiligungsrechten entgegen stehen..... (wird weiter ausgeführt)

Im Übrigen bestehen datenschutzrechtliche Bedenken auch deshalb nicht, weil der Betriebsrat selbst Teil der verantwortlichen Stelle im Sinne von Art. 4 Nr. 7 Datenschutz-Grundverordnung ist. (wird ausgeführt). Dies hat zur Folge, dass die von den Beschäftigten erteilte Einwilligung gemäß Art. 6 Abs. 1a Datenschutzgrundverordnung zu der Verarbeitung der sie betreffenden personenbezogenen Daten, die bei Aufnahme des Arbeitsverhältnisses regelmäßig gegenüber dem Arbeitgeber erteilt wird, die Weitergabe derselben an den Betriebsrat im Rahmen der diesem obliegenden gesetzlichen Aufgaben – beginnend mit der Mitbestimmung bei der Einstellung nach § 99 BetrVG und sodann für sämtliche weiteren vom Betriebsrat wahrzunehmenden Aufgaben bis hin zu einer Anhörung des Betriebsrats nach § 102 BetrVG – ebenfalls umfasst.

Kein Auskunftsanspruch des Insolvenzverwalters gegenüber dem Finanzamt bzgl. personenbezogener Daten des Insolvenzschuldners (Ls)

(Oberverwaltungsgericht Lüneburg, Urteil vom 20. Juni 2019 – 11 LC 121/17 –)

1. Betroffene Person i.S.v. Art. 15 Abs. 1 DS-GVO ist diejenige Person, die davor zu schützen ist, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird.
2. Ein Insolvenzverwalter ist hinsichtlich der beim Finanzamt gespeicherten personenbezogenen Daten des Insolvenzschuldners nicht „Betroffener“ i.S.v. Art. 15 Abs. 1 DS-GVO.
3. Das datenschutzrechtliche Auskunftsrecht des Betroffenen nach Art. 15 Abs. 1 DS-GVO geht nicht durch die Eröffnung des Insolvenzverfahrens auf den Insolvenzverwalter über, weil es sich bei diesem Auskunftsrecht um ein höchstpersönliches Recht handelt, welches nicht zur Insolvenzmasse gehört.
4. Für die Frage, ob der Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO höchstpersönlicher Natur ist, kommt es nicht auf den Inhalt der mit dem Auskunftsanspruch begehrten Informationen an, sondern ausschließlich auf den Rechtscharakter des Auskunftsanspruchs an sich. Dieser Rechtscharakter lässt sich nur einheitlich und damit unabhängig vom Inhalt der personenbezogenen Daten bestimmen.
5. Steht einem von einem Insolvenzverwalter geltend gemachten Auskunftsanspruch entgegen, dass er nicht „Betroffener“ i.S.v. Art. 15 Abs. 1 DS-GVO ist, kann er sein Auskunftsbegehren in Niedersachsen auch nicht mit Erfolg auf andere – geschriebene oder ungeschriebene – nationale Regelungen stützen.

Zur dienstlichen Beurteilung eines behördlichen Beauftragten für Datenschutz und dem datenschutzrechtlichen Benachteiligungsverbot (Ls)

(Oberverwaltungsgericht Berlin-Brandenburg, Beschluss vom 20. Mai 2019 – 10 S 34.18 –)

1. § 4 f Abs. 3 S. 3 BDSG a.F. (vgl. nun Art. 38 Abs. 3 Satz 2 DS-GVO, § 6 Abs. 3 Satz 3 BDSG n.F.) enthält das Verbot, den Datenschutzbeauftragten wegen der Erfüllung seiner Aufgaben zu benachteiligen. Das Benachteiligungsverbot bezweckt den Schutz sowohl der Funktion des Datenschutzbeauftragten, der in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei ist (§ 4 f Abs. 3 S. 2 BDSG a.F.; vgl. § 6 Abs. 3 Satz 1 BDSG) als auch der bestellten Person, und soll gewährleisten, dass Beauftragte für den Datenschutz ihre Aufgaben unbeeinflusst von der Furcht vor Benachteiligungen erfüllen kann.
2. Der Datenschutzbeauftragte kann nur dann seinen Aufgaben ordnungsgemäß nachkommen, wenn er der ihn benennenden Stelle, ggf. auch zum Schutz der informationellen Selbstbestimmung, „lästig“ werden kann, ohne Sanktionen befürchten zu müssen (vgl. Kühling/Buchner/Bergt, BDSG, 2. Aufl. 2018, § 6 Rn. 7; Gola, DS-GVO, 2. Aufl. 2018, Art. 38 Rn. 10).
3. Dieses Benachteiligungsverbot ist auch bei der Beurteilung eines Beauftragten für Datenschutz einer öffentlichen Stelle als Grundlage der nach Art. 33 Abs. 2 GG zu treffenden Auswahlentscheidung zu beachten. Es führt dazu, dass die Beurteilung in besonderer Weise auf den weisungsfreien Anteil der Tätigkeit der Beamtin oder des Beamten bei der Erfüllung seiner Aufgaben als Datenschutzbeauftragter Rücksicht zu nehmen hat und er wegen der Erfüllung dieser Aufgaben bei der dienstlichen Beurteilung nicht benachteiligt werden darf.

(Nicht amtliche Leitsätze)

Schadensersatz wegen Verletzung der Informationspflichten über freie Vollzeitstellen nach angezeigtem Wunsch auf Erhöhung der Arbeitszeit (Ls)

(Arbeitsgericht Cottbus, Urteil vom 5. März 2019 – 3 CA 608/18 –)

1. Bei der Informationspflicht nach § 7 Abs. 2 TzBfG muss der Arbeitgeber den Arbeitnehmer, der ihm den Wunsch auf Erhöhung der Arbeitszeit angezeigt hat, individuell über freie oder frei werdende entsprechende Vollzeitstellen informieren.

2. Bei der Informationspflicht handelt es sich um eine Dauerverpflichtung des Arbeitgebers, die erst endet, wenn der geäußerte Arbeitszeitwunsch des Arbeitnehmers erfüllt ist.
3. Eine zeitliche Beschränkung der Informationspflicht kann dem Wortlaut und dem Sinn und Zweck von § 7 Abs. 2 TzBfG nicht entnommen werden.
4. Krankheitsbedingte Fehlzeiten oder Minderleistungen des Arbeitnehmers können dringende betriebliche Gründe darstellen, die einem Arbeitszeitveränderungswunsch entgegenstehen. Sie müssen aber ein Ausmaß erreichen das geeignet wäre, hypothetisch eine Kündigung oder Änderungskündigung zu rechtfertigen.

Zur Zulässigkeit der Übermittlung sozialer Auswahldaten unterlegener Mitbewerber an den Personalrat

(Verwaltungsgerichtshof München, Beschluss vom 21. Mai 2019 – 17 P 18.2581 –)

Im Rahmen der Mitbestimmung der Personalvertretung über Arbeitnehmersetzungen ohne Bestenauslese kann die namentliche Übermittlung sozialer Auswahldaten über Beschäftigte, die eine Versetzung beantragen, aber nicht zum Zuge kommen, einen gravierenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG) bzw. das Grundrecht auf Schutz personenbezogener Daten (Art. 8 GRCh) darstellen, im Vergleich zu dem der Informationsanspruch der Personalvertretung nach bayerischem Landesrecht nicht pauschal überwiegt, was einem generellen Anspruch der Personalvertretung auf eine nicht anonymisierte Preisgabe dieser Auswahldaten entgegensteht.

Sachverhalt:

Das Verfahren betrifft Datenschutzfragen zur Unterrichtung der Personalvertretung durch die Dienststelle bei der Mitbestimmung anlässlich der Versetzung von Arbeitnehmern (nicht von Beamten) ohne Bestenauslese. Im Kern geht es um die Frage, ob der Personalvertretung auch hinsichtlich solcher Arbeitnehmer, die für Versetzungen zur Auswahl stehen, aber von der Dienststelle gerade nicht ausgewählt werden, Angaben unter Nennung des Namens zu übermitteln sind oder ob insoweit anonymisierte Daten ausreichen.

Aus den Gründen:

Die Beschwerde des Antragstellers ist zwar zulässig, hat aber in der Sache keinen Erfolg. Das Verwaltungsgericht hat den Antrag festzustellen, dass die Dienststelle bei der Unterrichtung zu Versetzungen von Arbeitnehmern nach Art. 75 Abs. 1 Satz 1 Nr. 6 BayPVG auch die Namen der nicht zum Zuge gekommenen Bewerber mit Nennung der Beschäftigungsbehörde mitzuteilen hat, im Ergebnis zu Recht abgelehnt.

1. Der abstrakte Feststellungsantrag betrifft seiner Tragweite nach nicht allein die Übermittlung der Namen unterlegener Versetzungsbewerber nebst deren Beschäftigungsbehörde.

Zwar ist im Wortlaut der Antragsformulierung nur von den Namen der unterlegenen Versetzungsbewerber (einschließlich der Beschäftigungsbehörde) die Rede. Das Begehren der Namenspreisgabe ist aber vor dem Hintergrund der zur Prüfung der Sozialauswahl (vgl. Art. 75 Abs. 2 Nr. 1-3 BayPVG) bislang anonymisiert übermittelten Angaben zu sehen, die dem Antragsteller nicht genügen. Es geht der Personalvertretung vorliegend darum, zusätzlich zu den bislang von der Dienststelle anonymisiert übermittelten Informationen der nicht zum Zuge kommenden Versetzungsbewerber auch den jeweils zugehörigen Namen (einschließlich Beschäftigungsbehörde) zu erfahren. Je nach dem Inhalt der (bisher anonymisierten) Angaben kann eine solche Namenspreisgabe zu Datensätzen ganz unterschiedlicher Sensibilität führen – wie etwa der Angabe des Wohnorts und seiner Entfernung zum bisherigen bzw. zukünftigen Dienstort oder des Alters der Versetzungsbewerber bis hin zu intimen Angaben betreffend Erkrankungen oder Behinderungen – und außerdem auch den Rechtskreis dritter Personen, beispielsweise die Namen von Kindern, Ehegatten oder Verwandten, deren Alter, Erkrankungen, Behinderungen oder etwaige Pflegebedürftigkeiten, betreffen. Deshalb ist der Feststellungsantrag inhaltlich weitgehender, als es seine Formulierung nahelegt.

2. Ein Anspruch der Personalvertretung auf Preisgabe derartiger namensbezogener Informationen ergibt sich nicht aus Art. 69 Abs. 2 Satz 3 BayPVG.

2.1. Zwar würde diese Vorschrift von ihrer Rechtsfolge her – dass nämlich die Personalvertretung auch die zur Erfüllung ihrer Aufgaben erforderliche Vorlage von Bewerbungsunterlagen verlangen kann – auch die vorliegend begehrte Übermittlung nicht anonymisierter Angaben erfassen.

2.2. Allerdings liegen schon vom Wortlaut des Art. 69 Abs. 2 Satz 3 BayPVG her die tatbestandlichen Voraussetzungen dieser Norm nicht vor, weil dort die Vorlage von Unterlagen nur für Bewerber bei Einstellungen, Beförderungen oder bei der Übertragung von Dienstposten mit höherem Endgrundgehalt, gerade nicht aber auch für Versetzungen vorgesehen ist.

2.3. Dabei ist kein Grund ersichtlich, Art. 69 Abs. 2 Satz 3 BayPVG über seinen Wortlaut hinaus auch auf Versetzungen zu erstrecken. Insbesondere spricht die historische Auslegung gegen ein solches erweiterndes Verständnis.

2.3.1. Die historische Auslegung spricht gegen eine erweiternde Interpretation des Art. 69 Abs. 2 Satz 3 BayPVG und für einen Umkehrschluss dahingehend, dass jedenfalls hinsichtlich der außerhalb der dort genannten Fallgruppen (Einstellung, Beförderung, Übertragung höherwertiger Dienstposten) liegenden Versetzungsmittelbestimmung die Übermittlung der begehrten sozialen Daten von vornherein ausgeschlossen ist. Art. 69 Abs. 2 Satz 3 BayPVG wurde eingeführt durch § 1 Nr. 20 Buchst. a Doppelbuchst. aa des Änderungsgesetzes vom 10. April 2007 (GVBl S. 276). Die Gesetz gewordene Fassung geht zurück auf eine Beschlussempfehlung des seinerzeit federführenden Ausschusses für Fragen des öffentlichen Dienstes (LT-Drs. 15/7705) und stellt bereits gegenüber dem ursprünglichen Gesetzentwurf der Staatsregierung (LT-Drs. 15/6238 S. 6, 16) eine nicht unerhebliche Erweiterung dar. Während nämlich der ursprüngliche Gesetzentwurf der Staatsregierung die Vorlage von Bewerbungsunterlagen nur für die Fallgruppe der Einstellung vorsah, hat die Gesetz gewordene Fassung die Unterlagenübermittlung zusätzlich auch bei Beförderungen und Übertragungen höherwertiger Dienstposten vorgesehen. Weil es sich aber somit um eine

klare Erweiterung des Tatbestands gehandelt hat, kann nicht von einem Redaktionsversehen, sondern muss von einer gezielten Entscheidung des Gesetzgebers ausgegangen werden. Hinzu kommt die Besonderheit, dass gerade auch der Mitbestimmungstatbestand der Versetzung (Art. 75 Abs. 1 Satz 1 Nr. 6 BayPVG) im selben Änderungsgesetz vom 10. April 2007 (dort § 1 Nr. 22 Buchst. a Doppelbuchst. bb) die noch heute geltende Erweiterung erfahren hat, dass – anders als nach der früheren Fassung – die Personalvertretung nunmehr auch bei Versetzungen mit Einverständnis mitzubestimmen haben soll. Dabei ging auch diese – im seinerzeitigen Gesetzentwurf der Staatsregierung gerade abgelehnte (LT-Drs. 15/6238 S. 16) – Änderung wiederum auf die besagte Beschlussempfehlung des seinerzeit federführenden Ausschusses zurück (LT-Drs. 15/7705 S. 2). Im Ergebnis spricht gerade diese Vorgehensweise des historischen Gesetzgebers gegen eine noch weitergehende Erstreckung des Art. 69 Abs. 2 Satz 3 BayPVG auch auf den Bereich der Versetzungsmittelbestimmung nach Art. 75 Abs. 1 Satz 1 Nr. 6 BayPVG.

2.3.2. Auch die verfassungskonforme Auslegung spricht im Hinblick auf das Gewicht des Grundrechts auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG), das von Datenübermittlungen an die Personalvertretung betroffen wird, gegen eine erweiternde Auslegung des Art. 69 Abs. 2 Satz 3 BayPVG über dessen Wortlaut hinaus. Es ist zu sehen, dass sowohl in der personalvertretungsrechtlichen (BVerwG, B.v. 19.3.2014 – 6 P 1.13 – NZA-RR 2014, 387 Rn. 39 ff.) als auch in der arbeitsgerichtlichen Rechtsprechung (LAG Berlin-Bbg, B.v. 4.5.2016 – 14 TaBV 2163/15 – juris Rn. 151 f.) betont wird, dass – im Hinblick auf die unmittelbare Grundrechtsbindung im Bereich staatlicher Verwaltung – für die Auskunftserteilung der Dienststelle an den Personalrat andere, strengere Grundsätze gelten als für die Auskunftserteilung des Arbeitgebers an den Betriebsrat.

2.4. Die vom Antragsteller als Beleg für die Pflicht zur vollständigen und nicht anonymisierten Datenübermittlung auch bei der Versetzungsmittelbestimmung benannten Fundstellen gebieten keine abweichende Auslegung des Art. 69 Abs. 2 Satz 3 BayPVG.

Die seitens der Personalvertretung zitierte Literaturstelle (Gräfl, in: Richardi/Dörner/Weber, Personalvertretungsrecht, 4. Aufl. 2012, § 68 BPersVG Rn. 64) geht auf die besagten Besonderheiten des bayerischen Landesrechts nicht ein, weswegen daraus kein entscheidender Schluss für eine von Wortlaut und Gesetzgebungsgeschichte abweichende Auslegung des Art. 69 Abs. 2 Satz 3 BayPVG zu ziehen ist.

Die zitierte Rechtsprechung des Landesarbeitsgerichts Hamm (LAG NW, B.v. 17.4.2008 – 13 TaBV 130/07 – juris Rn. 42) bezieht sich nicht auf Art. 69 Abs. 2 BayPVG, sondern auf § 99 BetrVG. Gänzlich abweichend von Art. 69 Abs. 2 Satz 3 BayPVG wird in § 99 Abs. 1 Satz 1 BetrVG aber explizit die Vorlage gerade auch von Bewerbungsunterlagen für den Fall der „Versetzung“ vorgeschrieben. Hierin liegt ein offenkundiger Unterschied der betriebsverfassungsrechtlichen zur bayerischen personalvertretungsrechtlichen Regelung. Schon dieser Umstand spricht gegen einen Rückgriff auf die Entscheidung des Landesarbeitsgerichts Nordrhein-Westfalen im Kontext einer Versetzungsmittelbestimmung nach bayerischem Personalvertretungsrecht. Hinzu kommt die bereits dargestellte (siehe 2.3.2.), im Vergleich zu privaten Arbeitgebern, auf die sich das Betriebsverfassungsgesetz bezieht, strengere Grundrechtsbindung staatlicher Dienststellen im Bereich des Personalvertretungsrechts.

Auch die seitens der Personalvertretung zitierten Beschlüsse des Bundesverwaltungsgerichts vom 11. Februar 1981 – 6 P

44.79 – (BVerwGE 61, 325) und des Verwaltungsgerichts Köln vom 16. Februar 2017 – 33 K 7012/15.PVB – (juris Rn. 17 ff.) sind nicht geeignet, den geltend gemachten Anspruch zu untermauern. Denn in diesen Entscheidungen ging es gerade nicht um eine Versetzung, sondern jeweils um Einstellungen.

Der zusätzlich herangezogene Beschluss des Bundesverwaltungsgerichts vom 26. Januar 1994 – 6 P 21.92 – (BVerwGE 95, 73) betraf eine hier nicht einschlägige Konstellation, in der es um ausgeschriebene Dienstposten ging, die – anders als vorliegend – gerade im Wege der Bestenauslese besetzt werden sollten.

Der außerdem in Bezug genommene Beschluss des Oberverwaltungsgerichts Niedersachsen vom 24. Februar 1993 – 18 L 8484/91 – (PersR 1993, 460) betraf keine Versetzung, sondern die Frage von Höhergruppierungen und ist schon deshalb mit der vorliegenden Konstellation im Hinblick auf Art. 69 Abs. 2 BayPVG nicht vergleichbar.

3. Der Anspruch ergibt sich auch nicht aus Art. 69 Abs. 2 Satz 1 und 2 BayPVG. Die vorliegend beantragte nicht anonymisierte Datenübermittlung ist unter Berücksichtigung des Gewichts der informationellen Selbstbestimmung der von der Datenübermittlung betroffenen Personen nicht nach Art. 69 Abs. 2 Satz 1 und 2 BayPVG zu rechtfertigen, und zwar auch nicht im Hinblick auf Art. 75 Abs. 2 Nr. 1-3 BayPVG.

3.1. Art. 69 Abs. 2 Satz 1 und 2 BayPVG ist auch im Kontext konkreter Mitbestimmungstatbestände neben Art. 70 Abs. 2 BayPVG anwendbar. Art. 69 Abs. 2 BayPVG ist eine bereichsspezifische Gesamtregelung für den Bereich des Arbeitnehmerdatenschutzes im bayerischen Personalvertretungsrecht mit Art. 69 Abs. 2 Satz 1 und 2 BayPVG als generalklauselartigen Bestimmungen (BayVG, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 49). Für eine Anwendbarkeit auch im Bereich der Mitbestimmung spricht dabei nicht zuletzt auch Art. 69 Abs. 2 Satz 3 BayPVG, der spezielle Regelungen für gerade mitbestimmungspflichtige Fallgruppen (Einstellung, Beförderung, Übertragung höherwertiger Dienstposten) vorsieht.

3.2. Wie gezeigt (siehe 2.3.1.) spricht insbesondere die historische Auslegung gegen eine erweiternde Auslegung des Art. 69 Abs. 2 Satz 3 BayPVG und infolge dessen für einen Umkehrschluss dahin, dass für die in dieser Norm gerade nicht genannten Versetzungen eine namentliche Datenübermittlung nicht in Betracht kommt.

3.3. Unabhängig davon sind aber selbst dann, wenn ein solcher Umkehrschluss nicht gezogen und im Kontext der Versetzungsmitbestimmung nur Art. 69 Abs. 2 Satz 1 und 2 BayPVG in den Blick genommen wird, die Voraussetzungen für eine nicht anonymisierte Übermittlung von Sozialauswahldaten nach Art. 69 Abs. 2 Satz 1 und 2 BayPVG nicht gegeben.

Nach dem Wortlaut des Art. 69 Abs. 2 Satz 2 BayPVG sind der Personalvertretung nur die zur Durchführung ihrer Aufgaben „erforderlichen“ Unterlagen zur Verfügung zu stellen, so dass die in Art. 69 Abs. 2 Satz 1 und 2 BayPVG vorgesehene Unterrichtungspflicht streng aufgabenbezogen zu interpretieren ist (stRspr, vgl. BVerwG, B.v. 20.3.2002 – 6 P 6.01 – PersV 2002, 405/410 f. zum inhaltsgleichen § 68 Abs. 2 Satz 1 und 2 BPersVG; BayVG, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 21 m.w.N.). Was in diesem Sinn „erforderlich“ ist, lässt sich nicht rein begrifflich klären, sondern setzt als Korrektiv eine wertende Betrachtung voraus, in die neben einer Bewertung des Aufgabenbezugs selbst auch grundrechtliche Wertungen im Hinblick auf die von Art. 2 Abs. 1 GG geschützte informationelle Selbstbestimmung (vgl. BVerwG, B.v. 4.9.2012 – 6 P 5.11 – BVerwGE 144, 156 Rn. 26 ff.; BayVG, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 49) einzufließen haben,

wobei personalvertretungsrechtliche Datenübermittlungen auch nicht gegen unionsrechtliche Datenschutzvorgaben verstoßen dürfen (siehe 3.4.).

3.3.1. Die für die Personalvertretung bei der Versetzungsmitbestimmung (Art. 75 Abs. 1 Satz 1 Nr. 6 BayPVG) maßgeblichen Kriterien (Art. 75 Abs. 2 BayPVG) können auch auf der Basis bloß anonymisierter Daten weitgehend überprüft werden. Eine darüber hinausgehende Datenübermittlung ist in der beantragten Tragweite nicht erforderlich. Der Unterscheidung zwischen namentlichen und anonymisierten Daten kommt für die Frage der Erforderlichkeit große Bedeutung zu (vgl. BVerwG, B.v. 19.12.2018 – 5 P 6.17 – juris Rn. 11, 50, 54 zu einem Fall, in dem die Personalvertretung lediglich anonymisierte Daten begehrte).

3.3.1.1. Im Anwendungsbereich spezieller Mitbestimmungstatbestände ist auf das dort gesetzlich vorgesehene – gegenüber den allgemeinen Aufgaben der Personalvertretung (Art. 69 Abs. 1 BayPVG) speziellere – Prüfprogramm (Art. 75 Abs. 2 BayPVG) abzustellen (vgl. BVerwG, B.v. 20.3.2002 – 6 P 6.01 – PersV 2002, 405/412). Dabei erstreckt sich die Prüfung der Personalvertretung im vorliegenden Kontext auf die Frage etwaiger Verstöße gegen versetzungsbezogene Gesetze, Verordnungen, Tarifverträge, gerichtliche Entscheidungen oder Richtlinien (Art. 75 Abs. 2 Nr. 1 BayPVG), die Frage einer begründeten Besorgnis ungerechtfertigter Benachteiligungen (Art. 75 Abs. 2 Nr. 2 BayPVG) sowie die Frage der Besorgnis einer etwaigen Störung des Friedens in der Dienststelle durch einen Beschäftigten (Art. 75 Abs. 2 Nr. 3 BayPVG).

3.3.1.2. Im Prinzip kann die Personalvertretung auch aus der Mitteilung anonymisierter Daten die Auswahl anhand der genannten Maßstäbe des Art. 75 Abs. 2 BayPVG überprüfen. Das gilt insbesondere auch im Hinblick auf die für Art. 75 Abs. 2 Nr. 2 BayPVG maßgeblichen Sozialauswahlkriterien hinsichtlich erfolgloser Mitbewerber. Aufgrund anonymisierter Angaben kann hinsichtlich der zwischen der Personalvertretung und der Dienststelle abgestimmten Sozialauswahlkriterien eine Differenzierung (Ranking) vorgenommen werden, etwa im Hinblick auf den gesundheitlichen Zustand der jeweiligen Bewerber und ihrer Angehörigen, die etwaige Anzahl und Betreuungsbedürftigkeit von Angehörigen, die Distanz zwischen Wohn- und Dienstort, das Alter oder die Dauer der Dienstzugehörigkeit oder des Wartens auf die gewünschte Versetzung.

3.3.1.3. Zwar kann die Möglichkeit, dass der Dienststelle bei der Erstellung der anonymisierten Datensätze Fehler unterlaufen, ebenso wenig ausgeschlossen werden wie Konstellationen, in denen die Übermittlung namentlicher Daten zu einer größeren Kontrolldichte seitens der Personalvertretung führt. Der mit einer pauschalen Namensnennung möglicherweise verbundene Vorteil bei der Kontrolle möglicher Fehler ist aber gerade im Hinblick auf Sozialauswahlaspekte nicht hoch zu veranschlagen, weil bei der Versetzungsmitbestimmung auch anonymisierte Daten im Regelfall als tragfähige Rückschlussbasis angesehen werden können (siehe 3.3.1.3.1.). Infolge dessen rechtfertigt der allgemeine Aspekt einer etwaigen durch eine Pflicht zur Übermittlung namentlicher Daten denkbaren Erhöhung von Sorgfalt und Transparenz hinsichtlich der Prüfung der in Art. 75 Abs. 2 BayPVG vorgegebenen Kriterien es – auch mit Blick auf eine etwaige, vom Antragsteller im Versetzungskontext vertretene Ausübungskontrolle hinsichtlich des in § 106 GewO vorgesehenen Weisungsrechts des Arbeitgebers – nicht, die versetzungsrelevanten Sozialauswahldaten pauschal unter Namensnennung mitzuteilen (siehe 3.3.1.3.2.).

3.3.1.3.1. Auch anonymisierte Sozialauswahldaten können bei der Versetzungsmitbestimmung eine geeignete Rückschluss-

basis sein, um die in Art. 75 Abs. 2 BayPVG genannten Kriterien zu prüfen.

Es ist davon auszugehen, dass die bei Versetzungswünschen relevanten Sozialauswahlkriterien der einzelnen Beschäftigten in einer Behörde und insbesondere deren Personalvertretung (bzw. der Stufenvertretung) keineswegs allgemein bekannt sind und deshalb der (zuständigen) Personalvertretung – außerhalb der Unterrichtung durch die Dienststelle – vor allem dann bekannt werden, wenn sich einzelne Versetzungsbewerber direkt an diese wenden. Geschieht dies und teilen die Versetzungsbewerber der Personalvertretung dabei diejenigen Informationen mit, die sie auch der Dienststelle bei ihrem jeweiligen Versetzungsgesuch vorgetragen haben, so darf davon ausgegangen werden, dass die Personalvertretung die von der Dienststelle übermittelten anonymisierten Sozialauswahldaten hinreichend mit den ihr vorliegenden namentlichen (von den Bewerbern direkt der Personalvertretung offenbarten) Daten vergleichen und eventuelle Fehler seitens der Dienststelle feststellen kann. Ein solcher Vergleich ist dabei etwa denkbar, wenn die Dienststelle einen Versetzungsbewerber komplett übersehen und deshalb in dem anonymisierten Datensatz vollständig unberücksichtigt gelassen haben sollte. Aber auch für den Fall, dass die Dienststelle bei Versetzungsbewerbern einzelne Sozialauswahlumstände in der anonymisierten Darstellung unberücksichtigt gelassen haben sollte, wäre der Personalvertretung ein Vergleich mit den ihr parallel von Beschäftigten offenbarten Daten durchaus möglich, je nachdem wie sich die Daten der Bewerber voneinander unterscheiden. Dabei ist zu sehen, dass es in erster Linie eine Obliegenheit der Arbeitnehmer ist, bei Versetzungsgesuchen dem Dienstherrn, der nur ihm bekannte soziale Daten bei seiner Auswahlentscheidung berücksichtigen kann, vollständige Angaben zu machen, die auch im anonymisierten Zustand einen Vergleich mit den gegebenenfalls der Personalvertretung offenbarten Angaben erlauben. Insgesamt stellen vor diesem Hintergrund auch anonymisierte Sozialauswahldaten eine im Grundsatz tragfähige Rückschlussbasis für die Prüfung der in Art. 75 Abs. 2 Nr. 1-3 BayPVG vorgesehenen Kriterien dar. Grundsätzlich besteht die Möglichkeit, etwaige erkannte Unstimmigkeiten zum Anlass für Nachfragen zu nehmen und gegebenenfalls weitere Datenübermittlungen seitens der Dienststelle zu veranlassen.

3.3.1.3.2. Eine pauschale namentliche Datenübermittlung ist nicht erforderlich i.S.v. Art. 69 Abs. 2 Satz 1 und 2 BayPVG, weil sie im Vergleich zu einer anonymisierten nicht wesentlich besser geeignet ist, um Art. 75 Abs. 2 BayPVG bei Versetzungen zu prüfen (s.o.), gleichzeitig aber im Vergleich zu anonymisierten Datenübermittlungen deutlich intensiver in die informationelle Selbstbestimmung (Art. 2 Abs. 1 GG) eingreift.

Es kann dabei offenbleiben, inwieweit der im Kontext des betrieblichen Eingliederungsmanagements nach dem Neunten Teil des Sozialgesetzbuchs (SGB IX) – und der diesbezüglichen Aufgabe der Personalvertretung, zu kontrollieren, ob alle betroffenen Beschäftigten in das Eingliederungsmanagement einbezogen worden sind (vgl. § 167 Abs. 2 Satz 3 und 6 SGB IX; zuvor § 84 Abs. Satz 3 und 6 SGB IX a.F.) – relevante Aspekt einer durch Namenspreisgabe möglichen Erhöhung von Sorgfalt und Transparenz (vgl. BVerwG, B.v. 4.9.2012 – 6 P 5.11 – BVerwGE 144, 156 Rn. 17) auf das in Art. 75 Abs. 2 Nr. 1-3 BayPVG hinsichtlich der Mitbestimmung vorgesehene Prüfprogramm überhaupt übertragbar ist (vgl. etwa BVerwG, B.v. 29.8.1990 – 6 P 30.87 – NJW 1993, 373; B.v. 28.6.2013 – 6 PB 8.13 – PersV 2013, 377 Rn. 10 zu den Grenzen des Unterrichtsanspruchs außerhalb der Mitbestimmung). Denn selbst wenn man den Ge-

danken der abstrakt gesehen möglichen Erhöhung von Sorgfalt und Transparenz auch auf die in Art. 75 Abs. 2 BayPVG vorgesehenen Kriterien vom Ansatz her überträgt, rechtfertigt dieser Aspekt jedenfalls im Kontext der Versetzungsmitbestimmung eine pauschale namentliche Übermittlung der Sozialauswahldaten nicht.

Zunächst spricht gegen die Erforderlichkeit einer pauschalen Übermittlung namentlicher Sozialauswahldaten im Hinblick auf eine Erhöhung von Sorgfalt und Transparenz der Umstand, dass die bei Versetzungen übermittelten Sozialauswahldaten im Regelfall auch in anonymisierter Form geeignet sind, die besonderen Umstände der Lebenssituation jeweils betroffener Versetzungsbewerber zu beschreiben, und deshalb auch ohne Namenspreisgabe – wie gezeigt – eine tragfähige Rückschlussbasis jedenfalls dann bieten können, wenn der Personalvertretung die namentlichen Daten von Versetzungsbewerbern offenbart worden sind. Insoweit unterscheidet sich die Situation deutlich von der beim betrieblichen Eingliederungsmanagement, wo es nur darum geht, dass alle Beschäftigten in das Eingliederungsmanagement einbezogen werden und deshalb nur wenig spezifische Daten (Name, Privatanschrift, Überschreiten des Grenzwerts der Arbeitsunfähigkeitsdauer) namentlich mitzuteilen sind (BayVG, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 30, 54), aus denen bei nicht anonymisierter Übermittlung kaum Rückschlüsse auf einzelne Beschäftigte gezogen werden könnten. Für den Fall, dass bei der Auswahlentscheidung Bewerber übersehen werden, die der Personalvertretung nicht bekannt sind, kann diese einen solchen Fehler auch dann nicht erkennen, wenn ihr die Namen der nicht übersehenen Mitbewerber mitgeteilt werden. Ein derartiger Kontrollnachteil beruht dann aber jedenfalls auch auf der Entscheidung der betroffenen Arbeitnehmer als Träger des Grundrechts der informationellen Selbstbestimmung, sich nicht an die Personalvertretung zu wenden, was sich typischer Weise zu Lasten der Schutzfunktion der Personalvertretung auswirkt. Der in einer namentlichen Sozialdatenübermittlung liegende Vorteil einer Erhöhung von Sorgfalt und Transparenz erscheint bei der Versetzungsmitbestimmung im Vergleich zum betrieblichen Eingliederungsmanagement relativ gering.

Gegen die Erforderlichkeit einer pauschalen namentlichen Sozialdatenübermittlung spricht bei der Versetzungsmitbestimmung aber auch der Umstand, dass die für eine Versetzung relevanten Sozialauswahldaten der Personalvertretung – anders als etwa beim betrieblichen Eingliederungsmanagement – regelmäßig nicht ohnehin bereits bekannt sind und eine Datenübermittlung unter Namenspreisgabe insoweit einen relativ stark belastenden Eingriff in die Persönlichkeitsrechte der Versetzungsbewerber darstellen kann. Bei der Versetzungsmitbestimmung ist der Unterschied zwischen einer namentlichen Übermittlung von Sozialauswahldaten und einer diesbezüglichen anonymisierten Datenübermittlung signifikant größer als etwa zwischen einer namentlichen oder anonymisierten Datenübermittlung im Rahmen des betrieblichen Eingliederungsmanagements. So ist beim betrieblichen Eingliederungsmanagement generell davon auszugehen, dass die Personalvertretung schon wegen der mit längeren Arbeitsunfähigkeitszeiträumen verbundenen Vertretungsfälle und daraus regelmäßig resultierender Beschwerden durch solche Vertretungen mehrbelasteter Beschäftigter über eine Reihe von Beschäftigten mit Abwesenheitszeiten unterrichtet ist (BVerwG, B.v. 4.9.2012 – 6 P 5.11 – BVerwGE 144, 156 Rn. 16 f.). Gerade aus dieser ohnehin anzunehmenden Informationsbasis der Personalvertretung verbunden mit dem Umstand, dass es dort um weniger spezifische

Daten (Name, Privatanschrift, Überschreiten des Grenzwerts der Arbeitsunfähigkeitsdauer) geht (BVerwG, B.v. 4.9.2012 a.a.O.), wurde dort abgeleitet, dass der Aspekt der Erhöhung von Sorgfalt und Transparenz eine namentliche Datenübermittlung rechtfertigt, wobei beim betrieblichen Eingliederungsmanagement eine Rückschlussmöglichkeit aus anonymisierten Daten praktisch ausgeschlossen ist. Dagegen sind bei der Versetzungsmitbestimmung Versetzungswünsche von Beschäftigten und die diesbezüglichen sozialen Gründe für die Personalvertretung keineswegs offenkundig, wenn sich nicht einzelne Versetzungsbewerber aktiv an die Personalvertretung wenden und dieser ihre Sozialauswahldaten offenbaren.

Insgesamt spricht der Umstand, dass bei der Versetzungsmitbestimmung die namentliche Datenübermittlung im Vergleich zur anonymisierten relativ gesehen stark in Persönlichkeitsrechte der nicht zum Zuge kommenden Mitbewerber eingreifen kann, zusammen mit dem Umstand, dass eine namentliche Datenübermittlung im Vergleich zu einer anonymisierten Datenübermittlung relativ gesehen nur vergleichsweise kleine Vorteile erwarten lässt, gegen die Erforderlichkeit der vorliegend begehrten pauschalen namentlichen Sozialauswahldatenübermittlung.

Zwar können auch im Kontext der Versetzungsmitbestimmung Konstellationen, in denen sich die Sozialdaten der Versetzungsbewerber stark ähneln und deshalb etwaige Fehler nicht eindeutig zu entdecken sind, nicht ausgeschlossen werden. Dabei handelt es sich aber nicht um eine stets und pauschal zu erwartende Situation, so dass damit eine pauschale namentliche Übermittlung von Sozialauswahldaten nicht als stets erforderlich gerechtfertigt werden kann.

3.4. Auch das mit 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 Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DS-GVO – ABl 2016 L 119 vom 4.5.2016 S. 1) zum 25. Mai 2018 unionsrechtlich geregelte Datenschutzrecht spricht im Hinblick auf den mit der Datenübermittlung verbundenen Eingriff in das unionsrechtliche Grundrecht auf Schutz personenbezogener Daten (Art. 8 i.V.m. Art. 51 Abs. 1 Satz 1 GRCh) gegen die vorliegend von der Personalvertretung begehrte pauschale Übermittlung namentlicher Sozialauswahldaten.

3.4.1. Die Datenschutz-Grundverordnung erfasst unmittelbar auch die vorliegend streitgegenständliche Datenübermittlung im Rahmen des Arbeitnehmerdatenschutzes. Ungeachtet des Umstands, dass Art. 69 Abs. 2 BayPVG als bereichsspezifische Gesamtregelung dem Bayerischen Datenschutzgesetz vorgeht (vgl. BayVG, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 49; vgl. auch BVerwG, B.v. 19.12.2018 – 5 P 6.17 – juris Rn. 52), erfasst die direkt anwendbare Datenschutz-Grundverordnung im Hinblick auf den Anwendungsvorrang des Unionsrechts unmittelbar auch den Beschäftigtendatenschutz (siehe 3.4.1.1. bis 3.4.1.2.), wobei das bayerische Landesrecht – anders als etwa § 26 des Bundesdatenschutzgesetzes (BDSG) – für den Bereich des Beschäftigtendatenschutzes die Ausnahmemöglichkeit des Art. 88 DS-GVO nicht ausgeschöpft hat (siehe 3.4.1.3. bis 3.4.1.6.).

3.4.1.1. Die Datenschutz-Grundverordnung ist vorliegend als Unionsrecht unmittelbar und nicht erst aufgrund des ergänzenden bayerischen Normanwendungsbefehls in Art. 2 BayDSG anwendbar.

Die von der Personalvertretung begehrte namensbezogene Übermittlung der sozialen Auswahlgründe bei Versetzungen ist begrifflich eine Verarbeitung personenbezogener Daten i.S.v.

Art. 2 Abs. 1 i. V. m. Art. 4 Nr. 1 und 2 DS-GVO, und zwar zumindest in Form der Verwendung durch Zurverfügungstellung an die Personalvertretung (vgl. Klabunde, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 4 DS-GVO Rn. 23), wobei unerheblich ist, ob gerade diese Verwendung automatisiert erfolgt oder nicht (Art. 4 Nr. 2 DS-GVO).

Dabei geht schon aus der erstinstanzlich vom Beteiligten vorgelegten Tabelle hervor, dass die bei der Versetzung relevanten Personaldaten i.S.v. Art. 2 Abs. 1 DS-GVO „in einem Dateisystem gespeichert“ werden, wobei ein „Dateisystem“ auch bei nichtautomatisierten (manuellen) Verarbeitungen möglich ist, solange nur eine strukturierte Sammlung personenbezogener Daten vorliegt, die nach bestimmten Kriterien zugänglich sind (Zerdick, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 2 DS-GVO Rn. 3 m.w.N.).

Für die Frage der „Datenverarbeitung“ unerheblich ist, ob „Verantwortlicher“ i.S.v. Art. 4 Nr. 7 DS-GVO beim Umgang mit diesen Daten durch die Personalvertretung die Dienststelle ist (deren Teil die Personalvertretung ist) oder ob die Personalvertretung eine eigene Verantwortlichkeit hat (vgl. etwa Kurzböck/Weinbeck, BB 2018, 1652; Hitzelberger-Kijima, öAT 2018, 136/138).

3.4.1.2. Eine Ausnahme vom Anwendungsbereich gemäß Art. 2 Abs. 2 DS-GVO liegt nicht vor. Insbesondere fällt die Datenübermittlung im Zusammenhang mit der Beteiligung einer Personalvertretung nicht i.S.v. Art. 2 Abs. 2 Buchst. a DS-GVO aus dem Anwendungsbereich des Unionsrechts heraus. Denn nach der insoweit gebotenen abstrakten Betrachtung (vgl. Bäcker, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand: 1.8.2018, Art. 2 DS-GVO Rn. 7 m.w.N.) ist von einschlägigen Rechtsetzungskompetenzen der Europäischen Union auszugehen. Anders als etwa der Bereich des auswärtigen Handelns der Union und der gemeinsamen Außen- und Sicherheitspolitik der Union (Titel V EUV) oder der nationalen Sicherheit (Art. 4 Abs. 2 Satz 3 EUV; vgl. etwa EuGH, U.v. 30.5.2006 – C-317/04 u.a. – ECLI:EU:C:2006:346 Rn. 54 ff.; BVerfG, U.v. 24.4.2013 – 1 BvR 1215/07 – BVerfGE 133, 277 Rn. 88 ff.) kann die Rechtsetzungskompetenz der Europäischen Union durchaus auch den Bereich des Arbeitsrechts und der diesbezüglichen Mitarbeitervertretung (hier: Personalvertretung) betreffen, was etwa durch Art. 2 Buchst. f, Art. 4 Abs. 4, Art. 6 Abs. 1 Satz 1 oder Abs. 7 der Richtlinie 2002/14/EG des Europäischen Parlaments und des Rates vom 11. März 2002 zur Festlegung eines allgemeinen Rahmens für die Unterrichtung und Anhörung der Arbeitnehmer in der Europäischen Gemeinschaft (ABl. L 80 vom 23.3.2002 S. 29) belegt wird.

3.4.1.3. Auch ergibt sich aus Art. 88 DS-GVO keine Ausnahme vom Geltungsbereich der Datenschutz-Grundverordnung für den Beschäftigtendatenschutz an sich. Hiergegen spricht schon der Wortlaut des Art. 88 Abs. 1 DS-GVO, wo von „spezifischeren Vorschriften“ die Rede ist. Die Verwendung des Komparativs (spezifischerer) ist ein deutlicher Hinweis darauf, dass es sich insoweit nicht um eine vollständige Geltungsbereichsausnahme, sondern vielmehr um eine Öffnungsklausel handelt, die den Mitgliedstaaten die Möglichkeit gibt, die im Ausgangspunkt einschlägigen Regelungen der Datenschutz-Grundverordnung durch spezifischere nationale Vorschriften zu präzisieren (vgl. Art. 88 Abs. 2 DS-GVO; Franzen, in: Franzen/Gallner/Oetker, Kommentar zum europäischen Arbeitsrecht, 2. Aufl. 2018, Art. 88 DS-GVO Rn. 5 f. m.w.N.).

3.4.1.4. Der im Bereich des Bundes erlassene § 26 BDSG, insbesondere § 26 Abs. 6 BDSG, der Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt lässt, ist vorlie-

gend nicht einschlägig, weil die Voraussetzungen des § 1 Abs. 1 Satz 1 Nr. 2 i.V.m. § 2 Abs. 2 BDSG nicht vorliegen.

3.4.1.5. Das infolgedessen für den Beschäftigtendatenschutz im Hinblick auf Art. 88 DS-GVO maßgebliche bayerische Landesrecht sieht im Zusammenhang mit der vorliegend streitgegenständlichen Versetzungsmittelbestimmung und der diesbezüglichen Datenübermittlung an die Personalvertretung aber gerade keine „spezifischere“ Regelung vor.

Es bestehen keinerlei Anhaltspunkte dafür, dass der bayerische Landesgesetzgeber für den Bereich der Datenübermittlung bei Versetzungsmittelbestimmung gegenüber Art. 88 DS-GVO spezifischere Vorschriften als die genannten Bestimmungen der Datenschutz-Grundverordnung erlassen hat. Während nämlich Art. 69 Abs. 2 Satz 3 BayPVG einen im Vergleich zur Datenschutz-Grundverordnung höheren Konkretisierungsgrad aufweist und insofern eine „besondere“ landesgesetzgeberische Maßnahme i.S.v. Art. 88 Abs. 2 DS-GVO darstellt, weist Art. 69 Abs. 2 Satz 1 und 2 BayPVG im Vergleich zu Art. 88 DS-GVO und zu Art. 5, 6 und 9 DS-GVO keine höhere Spezifizierung auf – insbesondere auch nicht hinsichtlich der in Art. 88 DS-GVO betonten Grundrechte der jeweils betroffenen Personen –, wobei das bayerische Landesrecht bislang auch keine dem § 26 Abs. 6 BDSG vergleichbare explizite Vorschrift kennt. Vielmehr handelt es sich bei Art. 69 Abs. 2 Satz 1 und 2 BayPVG um generalklauselartige Bestimmungen (BayVGh, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 49).

Deshalb bleibt es derzeit im Bereich des bayerischen Personalvertretungsrechts bei der unmittelbaren Anwendbarkeit der Datenschutz-Grundverordnung, und damit insbesondere auch der dort (Art. 6 DS-GVO) vorgesehenen Rechtmäßigkeitsvoraussetzungen für Datenverarbeitungen (vgl. Gola, ZD 2018, 448; Hitzelberger-Kijima, öAT 2018, 136/138; Kremer, CR 2017, 367/370).

3.4.1.6. Weil aber – wie gezeigt – die Datenschutz-Grundverordnung unmittelbar als Unionsrecht und nicht erst aufgrund des ergänzenden Normenwendungsgebefehls in Art. 2 BayDSG gilt, ist ihre Auslegung im Lichte des primären Unionsrechts und insbesondere der Unionsgrundrechte vorzunehmen (vgl. Art. 51 Abs. 1 Satz 1 der Charta der Grundrechte der Europäischen Union – Grundrechtecharta, GRCh). Besondere Bedeutung erlangt insofern Art. 8 GRCh (Schutz personenbezogener Daten).

3.4.2. Innerhalb der somit maßgeblichen und im Licht der Unionsgrundrechte auszulegenden Datenschutz-Grundverordnung ist der vorliegende Fall insbesondere zu messen an Art. 6 Abs. 1, Art. 5 Abs. 1 Buchst. c sowie Art. 9 Abs. 2 Buchst. b DS-GVO.

3.4.2.1. Dabei ist hinsichtlich der streitgegenständlichen Datenübermittlung bei Versetzungsmittelbestimmung gerade für Arbeitnehmer auch keine gegenüber Art. 88 DS-GVO spezifischere Kollektivvereinbarung ersichtlich. Zwar besteht im Bereich des Oberlandesgerichts München die Übung, sich im Arbeitnehmerbereich an die für den Beamtenbereich vereinbarten Richtlinien anzulehnen. Allerdings wurde für den Arbeitnehmerbereich nicht von einer eigenständigen verbindlichen Regelung berichtet. Auch wurde übereinstimmend darauf hingewiesen, dass im Bereich der Arbeitnehmer die örtlichen Dienststellen Einstellungen vornehmen können, was bei Versetzungsentscheidungen im Arbeitnehmerbereich zu berücksichtigen ist, so dass eine unterschiedslose Übertragung der Beamtenregeln auf den Arbeitnehmerbereich im Zusammenhang mit Versetzungsmittelbestimmung und diesbezüglicher Datenübermittlung nicht möglich ist. Der Frage, ob sich das Fehlen einer dem § 26 Abs. 6 BDSG entsprechenden Vorschrift im bayerischen Landesrecht auf die Anforderungen an Kollektivvereinbarungen i.S.v. Art. 88 DS-GVO auswirkt, ist deshalb im vorliegenden Fall nicht nachzugehen.

3.4.2.2. Eine Rechtfertigung der streitgegenständlichen Datenübermittlung an die Personalvertretung ergibt sich nicht aus Art. 6 Abs. 1 UnterAbs. 1 Buchst. a DS-GVO. Insbesondere kann in der bloßen Äußerung eines Versetzungswunsches – auch wenn sie sich auf behördenintern bekannt gegebene, zu besetzende Dienstposten bezieht – noch keine i.S.v. Art. 6 Abs. 1 UnterAbs. 1 Buchst. a DS-GVO hinreichende Einwilligung in eine Datenübermittlung der Dienststelle an die Personalvertretung gesehen werden. Hinsichtlich eventueller namensbezogener Gesundheitsdaten ergibt sich dies schon aus Art. 9 Abs. 2 Buchst. a DS-GVO, der eine ausdrückliche Einwilligung verlangt. Im Übrigen reicht die bloße Äußerung eines Versetzungswunsches aber auch nicht hin, um i.S.v. Art. 7 Abs. 1 DS-GVO „nachzuweisen“, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten in Form der Übermittlung ihrer sozialen Auswahldaten an die Personalvertretung eingewilligt hat.

3.4.2.3. Aber auch Art. 6 Abs. 1 UnterAbs. 1 Buchst. c DS-GVO rechtfertigt die begehrte Datenübermittlung vorliegend nicht, weil sie bei einer Auslegung im Licht des Art. 8 GRCh für die Erfüllung der rechtlichen Pflichten der Dienststelle nicht „erforderlich“ ist. Nicht anders als bei der verfassungskonformen Auslegung (vgl. BayVGh, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 49) kommt auch die unionsrechtskonforme Auslegung unter Berücksichtigung des Rechts auf Schutz der personenbezogenen Daten (Art. 8 GRCh) als Korrektiv dort zum Zuge, wo sich die typisierende gesetzliche Abwägung des Art. 69 Abs. 2 Satz 1 und 2 BayPVG im Einzelfall als unverhältnismäßig erweist. Der Unterscheidung zwischen namentlichen und anonymisierten Daten kommt auch aus Sicht des unionsrechtlichen Datenschutzes große Bedeutung zu (vgl. BVerwG, B.v. 19.12.2018 – 5 P 6.17 – juris Rn. 54, 50, 11).

Vorliegend spricht die abstrakt gesehen mögliche Sensibilität der gewünschten namensbezogenen Datenübermittlung – angesichts der wie gezeigt ohnehin auch bei anonymisierten Daten bestehenden Rückschlussmöglichkeiten (siehe 3.3.1.3.) – gegen die Erforderlichkeit der von der Personalvertretung abstrakt und generell begehrten namensbezogenen Übermittlung der sozialen Auswahlinformationen im Hinblick auf den bei der Auslegung des Art. 6 Abs. 1 UnterAbs. 1 Buchst. c DS-GVO wie gezeigt (siehe 3.4.1.6.) heranzuziehenden Art. 8 (i.V.m. Art. 51 Abs. 1 Satz 1) GRCh.

Die vorliegend von der Personalvertretung begehrten namentlichen Angaben zu den sozialen Auswahlkriterien der Dienststelle bei Versetzungen können gerade in intime private und gesundheitliche Themen hineinreichen und nicht nur die Daten betroffener Beschäftigter, sondern auch die Daten Dritter – insbesondere von Kindern, Ehegatten oder pflegebedürftigen Verwandten – betreffen. Schon von daher ist die begehrte Datenübermittlung sozialer Auswahlinformationen unter Namenspreisgabe geeignet, einen schwerwiegenden Eingriff in Art. 8 GRCh hervorzurufen, was sich auf die erforderliche Abwägung zwischen dem Informationsanspruch der Personalvertretung einerseits und den grundrechtlich geschützten Interessen der betroffenen Beschäftigten andererseits entscheidend auswirkt.

Damit kann der mit der begehrten Datenübermittlung verbundene Grundrechtseingriff weit über die Eingriffsintensität bei den in der ersten Phase des betrieblichen Eingliederungsmanagements zu übermittelnden Daten hinausgehen, weswegen sich entgegen der Ansicht der Personalvertretung aus der Pflicht der Dienststelle zur Namenspreisgabe beim betrieblichen Eingliederungsmanagement aufgrund des Neunten Teils des Sozialgesetzbuchs (vgl. BayVGh, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 26 ff.) im vorliegenden Kontext keine

Rückschlüsse auf die Problematik der Datenübermittlung nicht zum Zuge kommender Versetzungsbewerber ziehen lassen. Denn es bestehen zwischen dem Inhalt der in beiden Fallgruppen betroffenen Daten ganz erhebliche Unterschiede. Beim betrieblichen Eingliederungsmanagement erstreckt sich der Kreis der zu übermittelnden Daten auf einen von vornherein überschaubaren und weniger intimen Datensatz, nämlich auf den jeweiligen Namen – ggf. mit Privatanschriften (vgl. BVerwG, B.v. 4.9.2012 – 6 P 5.11 – BVerwGE 144, 156 Rn. 35) – und den Umstand eines länger als sechs Wochen im Jahr dauernden Arbeitsunfähigkeitszeitraums. Für die auch beim betrieblichen Eingliederungsmanagement erforderliche Abwägung der Datenschutzinteressen der betroffenen Beschäftigten einerseits und des Informationsanspruchs der Personalvertretung andererseits ist entscheidend, dass sich die Datenübermittlungspflicht der Dienststelle allein auf die erste Phase des betrieblichen Eingliederungsmanagements erstreckt, in der lediglich die genannten Informationen übermittelt werden, während intimere Daten erst in der zweiten Phase des betrieblichen Eingliederungsmanagements erhoben werden, bei denen eine Einbindung der Personalvertretung ohne Zustimmung des Betroffenen gerade nicht vorgesehen ist (§ 167 Abs. 2 Satz 1 SGB IX; zuvor § 84 Abs. 2 Satz 1 SGB IX a.F.; vgl. BayVGh, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 54 m.w.N.). Hinzu kommt, dass die Rechtsprechung den Datenzugriff bei der Personalvertretung auf eine Person begrenzt (BayVGh, B.v. 15.3.2016 a.a.O. Rn. 56 f. m.w.N.). Hinsichtlich aller weitergehenden Informationen in der zweiten Phase des betrieblichen Eingliederungsmanagements räumt das Gesetz dem Gewicht der Datenschutzinteressen der betroffenen Beschäftigten den Vorrang ein (vgl. BVerwG, B.v. 23.6.2010 – 6 P 8.09 – BVerwGE 137, 148 Rn. 54 ff.; B.v. 4.9.2012 – 6 P 5.11 – BVerwGE 144, 156 Rn. 13).

Von der Sensibilität der betroffenen Daten her ist die vorliegend streitgegenständliche Übermittlung sozialer Auswahlkriterien bei Versetzungsmittelbestimmung viel eher mit der zweiten als mit der ersten Phase des betrieblichen Eingliederungsmanagements vergleichbar. Hinzu kommt, dass die sozialen Auswahlkriterien bei der Versetzungsmittelbestimmung sich gerade auch aus Daten Dritter ergeben können, etwa bei erkrankten oder behinderten Kindern, Ehegatten oder sonstigen Angehörigen. Abgesehen davon, dass schon fraglich ist, inwieweit Art. 88 DS-GVO hinsichtlich der Daten Dritter überhaupt Erleichterungen ermöglicht, führt diese besondere Problematik – abstrakt gesehen – jedenfalls zu einer erheblichen Schwere des mit dem Ansinnen der Personalvertretung vorliegend verbundenen Eingriffs in Art. 8 GRCh hinsichtlich eventuell betroffener Dritter.

Es mag sein, dass Fälle nicht ausgeschlossen werden können, in denen mittels einer namentlichen Übermittlung der Sozialauswahlkriterien das in Art. 75 Abs. 2 BayPVG für Mitbestimmungsfälle (hier Art. 75 Abs. 1 Satz 1 Nr. 6 BayPVG) vorgesehene Prüfprogramm von der Personalvertretung mit einem noch höheren Maß an Gewissheit geprüft und noch weitergehend sichergestellt werden kann, dass die Auswahlentscheidung tatsächlich allen gesetzlichen Anforderungen entspricht (siehe 3.3.1.2.; vgl. BayVGh, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 30, 38 m.w.N.). Allerdings ist auch insoweit zu sehen, dass – wie gezeigt – auch anonymisierte Sozialauswahlkriterien der Personalvertretung eine deutlich tragfähigere Rückschlussbasis verschaffen, als es beim betrieblichen Eingliederungsmanagement die dort zu übermittelnden unspezifischeren Basisdaten (Name, Privatanschrift, Überschreiten des Arbeitsunfähigkeitsgrenzwerts) vermöchten (siehe 3.3.1.2. und 3.3.1.3.). Vor diesem Hintergrund verbietet das Gewicht des

von Art. 8 GRCh vermittelten Grundrechtsschutzes es, schon aus diesem weniger schwer wiegenden Kontrollvorteil für die Personalvertretung die Zulässigkeit der Datenübermittlung zu folgern. Vielmehr ist – im Prinzip nicht anders als beim betrieblichen Eingliederungsmanagement (vgl. BayVGh, B.v. 15.3.2016 – 17 P 14.2689 – PersV 2016, 266 Rn. 53 ff.) – gerade auch in Kenntnis der der Personalvertretung gemäß Art. 75 Abs. 2 BayPVG obliegenden Prüfung eine Abwägung erforderlich zwischen dem Informationsanspruch der Personalvertretung einerseits und dem Gewicht des Rechts der betroffenen Personen auf Schutz ihrer sozialen Daten. Da aber – wie gezeigt – der mit einer Übermittlung der für eine Versetzungsauswahl erforderlichen sozialen Daten verbundene Grundrechtseingriff erheblich schwerwiegender ist als der mit der Übermittlung der in der ersten Phase des betrieblichen Eingliederungsmanagements sozialen Daten (s.o.), fällt die Abwägung im Kontext der Datenübermittlung bei Versetzungsmittelbestimmung jedenfalls hinsichtlich der abstrakten Weite der vorliegend pauschal begehrten namensbezogenen Datenübermittlung zugunsten des Datenschutzes der betroffenen Beschäftigten aus. Im Ergebnis führt Art. 6 Abs. 1 UnterAbs. 1 Buchst. c DS-GVO damit vorliegend zu keinem anderen Ergebnis als das bislang gültige Personalvertretungsrecht.

3.4.2.4. Andere Rechtfertigungsgründe i.S.v. Art. 6 DS-GVO kommen vorliegend nicht in Betracht. Insbesondere ergibt sich nichts anderes aus Art. 6 Abs. 1 UnterAbs. 1 Buchst. f DS-GVO. Denn ungeachtet der Frage, ob eine Geltung dieser Vorschrift im Zusammenhang mit personalvertretungsrechtlicher Aufgabenerfüllung nicht schon gemäß Art. 6 Abs. 1 UnterAbs. 2 DS-GVO ausgeschlossen ist, kann jedenfalls die in Art. 6 Abs. 1 UnterAbs. 1 Buchst. f DS-GVO vorgeschriebene Interessenabwägung im Hinblick auf den von Art. 8 GRCh vermittelten Grundrechtsschutz nicht anders ausfallen als die Erforderlichkeitsprüfung bei Art. 6 Abs. 1 UnterAbs. 1 Buchst. c DS-GVO (siehe 3.4.2.3.).

3.4.2.5. Weil der mit der – ohne Rücksicht auf etwaige Besonderheiten des Einzelfalls generell – pauschal begehrten Datenübermittlung verbundene Grundrechtseingriff auch mit Art. 8 GRCh nicht zu vereinbaren ist (s.o.), ist auch der Frage nicht weiter nachzugehen, ob Konstellationen denkbar sind, in denen wegen konkreter objektiver Anhaltspunkte für einen Versagungsgrund i.S.v. Art. 75 Abs. 2 BayPVG – nach Übermittlung der zunächst anonymisierten Angaben – eine Namenspreisgabe erforderlich werden kann wegen Unstimmigkeiten oder Hinweisen auf besondere Fallgestaltungen (vgl. BVerwG, B.v. 19.3.2014 – 6 P 1.13 – NZA-RR 2014, 387 Rn. 11 und Rn. 32 f. zur elektronischen Arbeitszeiterfassung).

Zwangsgeld (hier in Höhe von 5.000,- EUR) wegen fehlender DS-GVO-Auskunft

(Verwaltungsgericht Mainz, Urteil vom 9. Mai 2019 – 1 K 760/18.MZ –)

Verzögerte Auskunftserteilung gegenüber dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz rechtfertigt ein Zwangsgeld iHv. 5.000,- EUR.

Sachverhalt:

Die Klägerin wendet sich gegen die Auferlegung eines Zwangsgeldes durch den Beklagten.

Die Klägerin betreibt das Tanzlokal „N.“ in A. Neben erotischen Tanzvorführungen werden in den Separees der Gaststätte auch andere sexuelle Dienstleistungen erbracht. An der Außenfassade der Gaststätte sowie im Innenraum und den Separees installierte die Klägerin Videokameras zur Erfassung von Kundinnen und Kunden sowie ihren Mitarbeiterinnen und Mitarbeitern.

Aufgrund einer Eingabe der Staatsanwaltschaft A. (aufgrund eines Ermittlungsverfahrens wegen § 201a StGB) begehrte der Beklagte von der Klägerin mit Schreiben vom 24. März 2017 Auskunft in Form eines Fragenkataloges, der insgesamt 16 Fragen umfasst, insbesondere hinsichtlich des Umfangs der von der Klägerin eingesetzten Videoüberwachungstechnik. Eine Stellungnahme der Klägerin erfolgte innerhalb der bis zum 1. Mai 2017 gesetzten Frist nicht.

Mit Schreiben vom 4. Mai 2017 wandte sich das Rechts- und Ordnungsamt der Stadtverwaltung A. an die Beklagte mit dem Hinweis, dass in der streitgegenständlichen Gaststätte Überwachungskameras installiert seien, mit denen der angrenzende Gehweg überwacht werden könne. Dies sei bei einer Kontrolle am 21. April 2017 festgestellt worden. Hinweise auf eine Videoüberwachung seien keine angebracht.

Mit Schreiben vom 10. August 2017 forderte der Beklagte die Klägerin erneut zur Beantwortung des Fragenkatalogs auf. Dabei wurde darauf hingewiesen, dass es Eingaben zu einer Videoüberwachung in Bezug auf die „Separees“ im Innenbereich und den Außenbereich der Gaststätte gegeben habe. Der Klägerin wurde eine Frist zur Stellungnahme bis zum 15. September 2017 gesetzt. Eine Beantwortung dieses Schreibens erfolgte nicht.

Der Beklagte forderte die Klägerin mit Schreiben vom 25. September 2017 erneut zur Stellungnahme bis zum 15. Oktober 2017 auf. Auch diese Frist ließ die Klägerin verstreichen.

Mit Bescheid vom 16. November 2017 forderte der Beklagte die Klägerin auf, das ihr mit Schreiben vom 10. August 2017 übersandte Auskunftersuchen hinsichtlich der Überwachungstechnik in und an ihrer Gaststätte zu beantworten. Er setzte dazu eine Frist bis zum 15. Dezember 2017 und drohte für den Fall der nicht fristgerechten Erteilung der Auskünfte die Auferlegung eines Zwangsgeldes in Höhe von 500,00 € an. Dem Schreiben war eine Rechtsbehelfsbelehrung mit dem Hinweis auf die Möglichkeit einer Klageerhebung bei dem Verwaltungsgericht Mainz angefügt.

Mit zwei Schreiben vom 15. Dezember 2017 (Eingang am 18. Dezember 2017 per Fax) teilte der Prozessbevollmächtigte der Klägerin unter Bezugnahme auf das Schreiben vom 25. September 2017 mit, dass „die Kameras, die den öffentlichen Raum erfassen, derzeit nicht in Betrieb sind“. Diese würden auch entfernt und die Klägerin habe bereits entsprechende Maßnahmen eingeleitet. Weitere Ausführungen, insbesondere zum Innenbereich der Gaststätte enthielt das Schreiben nicht.

Der Beklagte teilte der Klägerin mit Schreiben vom 3. April 2018 mit, dass bisher nur auf die Außenkameras eingegangen worden sei, die inzwischen entfernt worden seien. Die Eingabe der Staatsanwaltschaft A. betreffe allerdings den Innenraum der Gaststätte. Für das Verfahren sei insbesondere von Belang, ob diese Innenkameras weiterhin in Betrieb bzw. installiert seien. Es werde um Mitteilung gebeten, auf welche Rechtsgrundlage sich die Klägerin dafür stütze. Außerdem wurde wieder um die Beantwortung des Fragenkatalogs gebeten und der Klägerin hierfür eine Frist bis zum 1. Mai 2018 gesetzt.

Mit Bescheid vom 14. Juni 2018 (abgesendet am 14. Juni 2018 mit einfacher Post) forderte der Beklagte die Klägerin auf, dem Auskunftsverlangen vom 3. April 2018 bis zum 29. Juni 2018 nachzukommen. Rechtsgrundlage sei Art. 58 Abs. 1 lit. a der Daten-

schutz-Grundverordnung (DS-GVO). Der Beklagte drohte für den Fall der nicht fristgerechten Erteilung der Auskünfte die Auferlegung eines Zwangsgeldes in Höhe von 5.000,00 € an. Es wurde darauf hingewiesen, dass der Klägerin ein Auskunftsverweigerungsrecht zustehen könne. Die angefügte Rechtsbehelfsbelehrung wies auf die Möglichkeit einer verwaltungsgerichtlichen Klage bei dem Verwaltungsgericht Mainz hin.

Mit Schreiben vom 25. Juni 2018 legte die Klägerin bei dem Beklagten durch ihren Prozessbevollmächtigten Widerspruch ein. Die Frist sei so kurz bemessen, dass die Auskünfte nicht fristgerecht erteilt werden könnten.

Mit Bescheid vom 2. Juli 2018 (Zustellung per PZU am 4. Juli 2018) verwarf der Beklagte den Widerspruch als unzulässig, da es sich gemäß § 68 Abs. 1 Satz 2 Nr. 2 der Verwaltungsgerichtsordnung (VwGO) bei dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit um eine oberste Landesbehörde handele und daher ein Vorverfahren unstatthaft sei. Darüber hinaus setzte der Beklagte letztmalig eine Frist zur Beantwortung des mit Bescheid vom 14. Juni 2018 gestellten Informationsersuchens bis zum 10. Juli 2018. Dem Bescheid war eine Rechtsbehelfsbelehrung mit dem Hinweis auf eine mögliche verwaltungsgerichtliche Klage bei dem Verwaltungsgericht Mainz angefügt.

Der Prozessbevollmächtigte der Klägerin führte mit Schreiben vom 4. Juli 2018 (Zugang 4. Juli 2018) aus, dass er den Bescheid vom 2. Juli 2018 erhalten habe. Aufgrund der Sommerferien sei es ihm nicht möglich, bis zum 10. Juli 2018 zu antworten. Es werde darum gebeten, die Frist „stillschweigend“ bis zum 17. Oktober 2018 zu verlängern.

Mit Bescheid vom 10. August 2018 (Zustellung per PZU am 11. August 2018) setzte der Beklagte ein Zwangsgeld in Höhe von 5.000,00 € fest und erlegte der Klägerin die Kosten der Postzustellung in Höhe von 6,90 € auf. Der Klägerin wurde eine Frist zur Zahlung von zwei Wochen nach Eintritt der Rechtskraft des Bescheides gesetzt. Die Informationsersuchen vom 3. April und 14. Juni 2018 seien innerhalb der gesetzten Fristen „teilweise unbeantwortet“ geblieben. Ferner wurde der Klägerin eine weitere Frist zur Beantwortung des Informationsersuchens zum 15. September 2018 gesetzt. Der Bescheid enthielt eine Rechtsbehelfsbelehrung mit dem Hinweis auf eine mögliche Klage bei dem Verwaltungsgericht Mainz.

Die Klägerin hat am 5. September 2018 Klage gegen den Bescheid vom 10. August 2018 erhoben. Sie trägt zur Begründung vor, es bestehe kein Grund zur Auferlegung eines Zwangsgeldes durch den Beklagten. Sie sei der Aufforderung des Beklagten, die Kameras im Außenbereich der Gaststätte zu entfernen, nachgekommen. In Bezug auf die Kameras im Innenraum der Gaststätte seien deren Einsatz deutlich mit Hinweisschildern gekennzeichnet, sodass Mitarbeiter und Gäste hierüber in Kenntnis gesetzt würden. Die Überwachungstechnik sei auch notwendig und rechtmäßig, da es in der Vergangenheit immer wieder zu strafrechtlich relevanten Handlungen innerhalb der Gaststätte gekommen sei. Die erhobenen Daten würden nach kurzer Zeit gelöscht und dienen dem Schutz der Klägerin und ihrer Kunden.

Aus den Gründen:

Die zulässige Klage hat keinen Erfolg, da sie unbegründet ist.

I. Die Klage ist als Anfechtungsklage auch ohne erfolglos durchgeführtes Vorverfahren zulässig. Die Klägerin wendet sich gegen die Zwangsgeldfestsetzung mit Bescheid vom 10. August 2018. Dabei handelt es sich um einen Verwaltungsakt, der selbstständig mit einer Anfechtungsklage angegriffen werden kann (vgl. OVG RP, Urteil vom 18. März 1993 – 1 A 10570/92. OVG –, NVwZ 1994, 715). Das Vorverfahren ist gemäß § 68 Abs. 1 Satz 2 Nr. 1 VwGO unstatthaft, da es sich bei dem Be-

klagten um eine oberste Landesbehörde handelt (vgl. § 15 Abs. 4 Satz 1 des Landesdatenschutzgesetzes in der Fassung vom 8. Mai 2018 – LDSG –). Damit war eine unmittelbare Klageerhebung möglich. Auch die übrigen Zulässigkeitsvoraussetzungen sind gegeben.

II.

Die Klage ist allerdings unbegründet. Die Festsetzung des Zwangsgeldes ist rechtmäßig und verletzt die Klägerin nicht in ihren Rechten (§ 113 Abs. 1 Satz 1 VwGO).

1. Die Ermächtigungsgrundlage für die Festsetzung des Zwangsgeldes durch den Beklagten in Höhe von 5.000,00 € gegen die Klägerin ergibt sich aus §§ 2 Nr. 1, 61 Abs. 1, 62 Abs. 1 Nr. 2, 64 des Landesverwaltungsvollstreckungsgesetzes (LVwVG). Im Rahmen des gestreckten Verwaltungsvollstreckungsverfahrens können Verwaltungsakte, die auf Herausgabe einer Sache oder auf eine Handlung, Duldung oder Unterlassung gerichtet sind, durch Anwendung von Zwangsmitteln vollstreckt werden.

2. Die Festsetzung des Zwangsgeldes ist formell rechtmäßig erfolgt.

a) Nach dem sog. Grundsatz der Selbstvollstreckung ist der Beklagte gemäß § 4 Abs. 2 Satz 1 LVwVG als Erlassbehörde für die Vollstreckung der durch ihn erlassenen Verwaltungsakte zuständig. Verfahrens- und Formfehler sind nicht ersichtlich. Einer Anhörung der Klägerin bedurfte es gemäß § 28 Abs. 2 Nr. 5 des Verwaltungsverfahrensgesetzes (VwVfG) in Verbindung mit § 1 Abs. 1 des Landesverwaltungsverfahrensgesetzes (LVwVfG) nicht, da es sich bei der Festsetzung eines Zwangsmittels um eine Maßnahme in der Verwaltungsvollstreckung handelt. Das Zwangsgeld wurde gemäß § 64 Abs. 2 Satz 1 LVwVG schriftlich festgesetzt.

b) Ferner wurde der Klägerin auch die Festsetzung eines Zwangsgeldes in der nunmehr festgesetzten Höhe von 5.000,00 € schriftlich im Bescheid vom 14. Juni 2018 gemeinsam mit der Grundverfügung angedroht (§ 66 Abs. 1 Satz 1, Abs. 2 Satz 1 LVwVG). Zwar wurde die schriftliche Zwangsgeldandrohung nicht gemäß § 66 Abs. 6 LVwVG i.V.m. § 1 Abs. 1 des Landesverwaltungszustellungsgesetzes (LVwZG) i.V.m. § 1 ff. des Verwaltungszustellungsgesetzes (VwZG) förmlich zugestellt. Allerdings ist der Bescheid vom 14. Juni 2018, der dort unter Ziffer 2 auch die Zwangsgeldandrohung enthält, dem Prozessbevollmächtigten – wie sich dessen „Widerspruch“ mittelbar entnehmen lässt – spätestens am 25. Juni 2018 tatsächlich zugegangen, sodass der Bescheid gemäß § 8 VwZG jedenfalls zu diesem Zeitpunkt als zugestellt gilt.

Der Beklagte hat der Klägerin allerdings keine gemäß § 66 Abs. 1 Satz 3 LVwVG erforderliche angemessene Frist gesetzt, sodass die – bestandskräftige – Zwangsgeldandrohung als rechtswidrig einzustufen wäre. Die Frist wurde mit Bescheid vom 14. Juni 2018 ursprünglich auf den 29. Juni 2018 gesetzt und mit Bescheid vom 2. Juli 2018 (zugestellt mit PZU am 4. Juli 2018) auf den 10. Juli 2018 verlängert. Damit bezog sich der Fristablauf (auch nach Fristverlängerung) auf einen Zeitpunkt, der noch innerhalb der Rechtsbehelfsfrist des § 74 Abs. 1 VwGO lag und zu dem der Grundverwaltungsakt in Form des Auskunftersuchens allerdings weder kraft Gesetzes sofort vollziehbar war (§ 80 Abs. 2 Satz 1 Nr. 1 bis 3, Satz 2 VwGO) noch die sofortige Vollziehung besonders durch den Beklagten angeordnet worden ist (§ 80 Abs. 2 Satz 1 Nr. 4, Abs. 3 VwGO). Da damit zum Zeitpunkt des Fristablaufs die Vollstreckungsvoraussetzungen des § 2 LVwVG hinsichtlich des Grundverwaltungsaktes (noch) nicht vorlagen, wäre die Androhung als rechtswidrig einzuordnen (vgl. OVG Berlin-Brandenburg, Urteil

vom 22. April 2010 – 11 B 9/09 –, NVwZ-RR 2010, 748 [749]; Beckmann/Stollenwerk, in: PdK Rheinland-Pfalz, A 19 RhPf, Stand: August 2012, Erläuterungen zu § 66 Abs. 1 LVwVG; Lemke, in: Danker/Lemke, Verwaltungs-Vollstreckungsgesetz, 1. Auflage 2012, § 13, Rn. 12).

Allerdings ist die Zwangsgeldandrohung, die einen Verwaltungsakt darstellt (vgl. nur BVerwG, Gerichtsbescheid vom 26. Juni 1997 – 1 A 10/95 –, NVwZ 1998, 393), wirksam und auch (gemeinsam mit dem Grundverwaltungsakt) bestandskräftig geworden, sodass sie trotz rechtswidriger Fristsetzung grundsätzlich eine hinreichende Grundlage für die Festsetzung des Zwangsgelds sein kann (vgl. VGH BW, Urteil vom 17. August 1995 – 5 S 71/95 –, NVwZ-RR 1996, 612 [613]). Die vorgenannte zu kurze Fristsetzung stellt auch keinen derart schwerwiegenden Fehler dar, der ein Abweichen von diesem Grundsatz rechtfertigen würde. Eine solche Ausnahme käme nur bei Nichtigkeit gemäß § 44 VwVfG in Verbindung mit § 1 Abs. 1 LVwVfG in Betracht (anders bei der fehlenden Bestimmtheit der Zwangsmittelandrohung: VGH BW, a.a.O.). Dies ist hier allerdings – insbesondere vor dem Hintergrund der mehrmaligen Aufforderungen zur Auskunftserteilung vor der Androhung – nicht anzunehmen (vgl. für eine gänzlich fehlende Frist: Troidl, in: Engelhardt/App/Schlatmann, VwVG VwZG, 11. Auflage 2017, § 13 VwVG, Rn. 3). Denn spätestens mit der Bestandskraft des Grundverwaltungsaktes musste die Klägerin erkennen, dass sie nunmehr die dort enthaltene Verpflichtung erfüllen muss. Damit kann sie weiter ihre Wirkung dahingehend entfalten, die Klägerin zur Vornahme der begehrten Handlung anzuhalten. Infolgedessen kann hier auch eine zu kurz bemessene Frist keinen derart erheblichen Fehler darstellen, der die Androhung als nichtig erscheinen lässt.

3. Die Festsetzung des Zwangsgeldes erfolgte auch materiell rechtmäßig.

a) Mit Bescheid vom 14. Juni 2018 hat der Beklagte einen nach § 61 Abs. 1 LVwVG erforderlichen, wirksamen Grundverwaltungsakt erlassen. Dieser ist gemäß § 2 Nr. 1 LVwVG auch vollstreckbar, da er bereits im Zeitpunkt der Festsetzung des Zwangsgeldes unanfechtbar und damit in Bestandskraft erwachsen war. Die Einlegung eines (unstatthaften) Widerspruchs hemmt die Bestandskraft nicht. Eine insoweit erforderliche verwaltungsgerichtliche Klage gegen den Bescheid hat die Klägerin – trotz diesbezüglicher Rechtsbehelfsbelehrung – binnen der Klagefrist des § 74 Abs. 1 VwGO nicht erhoben.

b) Die Rechtmäßigkeit des Bescheides vom 14. Juni 2018 als Grundverwaltungsakt ist nach dem Wortlaut des § 61 Abs. 1 LVwVG bei der Überprüfung der Rechtmäßigkeit einer Vollstreckungsmaßnahme grundsätzlich nicht erforderlich (vgl. BVerwG, Urteil vom 25. September 2008 – 7 C 5/08 –, NVwZ 2009, 122, Rn. 12). Da für den Betroffenen insoweit auch eine Rechtsschutzmöglichkeit gegen den Grundverwaltungsakt gegeben war, ist dies auch im Hinblick auf Art. 19 Abs. 4 GG unbedenklich (vgl. BVerwG, a.a.O., Rn. 14). Einwände der Klägerin gegen die Rechtmäßigkeit des mit Bescheid vom 14. Juni 2018 gestellten – hinreichend bestimmten – Informationsersuchens verfangen daher von vornherein nicht. Sie wären vielmehr in einer Klage gegen den Bescheid vom 14. Juni 2018 geltend zu machen gewesen; von dieser Möglichkeit hat die Klägerin allerdings (innerhalb der Klagefrist) keinen Gebrauch gemacht.

Sofern die – anwaltlich vertretene – Klägerin in diesem Klageverfahren jedoch vorträgt, dass die Videoüberwachung im Innenraum ihrer Gaststätte rechtmäßig sei, so verkennt sie grundlegend den Streitgegenstand. Überdies hätten die Ausführungen ihres Prozessbevollmächtigten weder Entscheidungsrele-

vanz in diesem Klageverfahren noch im Rahmen einer – nunmehr längst verfristeten – Klage gegen den Grundverwaltungsakt (das Informationersuchen mit Bescheid vom 14. Juni 2018). Eine Bewertung der Rechtmäßigkeit der Videoüberwachung im Innenraum der Gaststätte wurde seitens des Beklagten noch überhaupt nicht vorgenommen, sondern sollte offenbar erst auf Grundlage der Antworten der Klägerin auf das Informationersuchen erfolgen. Dies hätte sich auch bei sorgfältiger Lektüre der Bescheide und Schreiben der Beklagten für die Klägerin bzw. ihren Prozessbevollmächtigten aufdrängen müssen.

Überdies dürften auch hinsichtlich der Rechtmäßigkeit des Informationersuchens keine Bedenken bestehen. Der Beklagte ist zunächst zuständige Aufsichtsbehörde für die Überwachung von nichtöffentlichen Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen. Insoweit weist Art. 51 Abs. 1 DS-GVO die Mitgliedstaaten der europäischen Union an, eine unabhängige Behörde für die Überwachung der Anwendung der Verordnung zu schaffen. Aufgrund dieser Regelung hat der Bundesgesetzgeber mit Wirkung zum 25. Mai 2018 § 40 Abs. 1 BDSG neu gefasst und den Ländern die Überwachung des Anwendungsbereiches der DS-GVO für nichtöffentliche Stellen übertragen (vgl. Art. 1 und 8 Datenschutz-Anpassungs- und -Umsetzungsgesetz EU vom 30. Juni 2017; BGBl. I 2017, S. 2097). Der rheinland-pfälzische Gesetzgeber hat die Wahrnehmung dieser Aufgaben in § 15 Abs. 2 LDSG (in der Fassung vom 8. Mai 2018; vgl. GVBl. 2018, 93) dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit überantwortet.

Mit Art. 58 DS-GVO verfügt die Aufsichtsbehörde über sämtliche Untersuchungsbefugnisse, die es ihr gestatten, die Klägerin anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben nach Art. 57 DS-GVO erforderlich sind. Als Aufgabe kommt hier insbesondere die Überwachung und Durchsetzung der Anwendung der DS-GVO nach Art. 57 Abs. 1 lit. a DS-GVO bzw. die Durchführung von Untersuchungen über die Anwendung der DS-GVO nach Art. 57 Abs. 1 lit. h DS-GVO in Betracht. Den Aufsichtsbehörden steht in diesem Rahmen gemäß Art. 58 Abs. 1 lit. a DS-GVO auch ein Auskunftsanspruch zu, dem die Klägerin als datenschutzrechtlich Verantwortliche grundsätzlich nachkommen muss (vgl. Lachenmann/Leibold, Prüfkataloge der Aufsichtsbehörden zur Umsetzung der DS-GVO-Vorgaben, ZD-Aktuell 2019, 06419). Demnach darf die Aufsichtsbehörde den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Dies hat der Bundesgesetzgeber auch in § 40 Abs. 4 Satz 1 BDSG (entspricht § 38 Abs. 3 BDSG a.F.) im nationalen Recht insbesondere dahingehend konkretisiert, dass Auskunftspflichtige die Beantwortung der Fragen des Beklagten mit Rücksicht auf ein Auskunftsverweigerungsrecht ablehnen können (§ 40 Abs. 4 Satz 2 BDSG). Ihr kommt insoweit auch die Befugnis zu, durch Verwaltungsakt zu handeln (sog. VA-Befugnis), was bereits im Wortlaut der Vorschrift („anzuweisen“) zum Ausdruck kommt. Zudem steht es auch grundsätzlich im Ermessen einer Behörde, eine bestehende Handlungsverpflichtung (hier die Auskunftspflicht der Klägerin) durch Verwaltungsakt zu konkretisieren und dann auch im Wege des Verwaltungszwanges durchzusetzen (vgl. zu Auskunftsverlangen nach § 52 MessEG: Ambs, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, Werkstand: 223. EL Januar 2019, § 52 MessEG, Rn. 12 ff.).

Die Ausgestaltung der Fragebögen obliegt weitestgehend dem Ermessen der Aufsichtsbehörde (vgl. Lachenmann/Leibold, Prüfkataloge der Aufsichtsbehörden zur Umsetzung der DS-GVO-

Vorgaben, ZD-Aktuell 2019, 06419). Hier bestehen keine Anhaltspunkte dafür, dass die Beklagte insoweit ihren Ermessensspielraum überschritten haben könnte. Insbesondere sind die Fragen gerade nicht willkürlich gewählt, sondern dienen erkennbar dazu, die von der Klägerin durchgeführte Videoüberwachung umfassend datenschutzrechtlich zu bewerten. Gemäß § 4 Abs. 1 Satz 1 Nr. 2 und 3 BDSG ist die Beobachtung – wie hier – öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen für nichtöffentliche Stellen nur zulässig, soweit sie zur Wahrung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dabei zielen etwa die Fragen 1 bis 4, 7, 8 und 10 auf den Umfang der Videoüberwachung ab, die bei der Gewichtung der Interessen der Klägerin gegenüber den Rechten der beobachteten Personen (Recht am eigenen Bild bzw. informationelle Selbstbestimmung) eine wesentliche Rolle spielt. Auch die übrigen Fragen dienen der Information über die Einhaltung besonderer Datenschutzvorschriften oder enthalten weitere wesentliche Aspekte für die Zulässigkeit der Videoüberwachung.

c) Auch im Übrigen bestehen keine Bedenken gegen die Zwangsgeldfestsetzung.

aa) Die Auswahl des Zwangsmittels ist nicht zu beanstanden. Durch die Festsetzung eines Zwangsgelds kann der Beklagte die Klägerin auch zur Vornahme einer unvertretbaren Handlung, vorliegend die Auskunftserteilung, veranlassen und auf diese Weise die im Grundverwaltungsakt vom 14. Juni 2018 enthaltene Verpflichtung vollstrecken (vgl. Deusch/Burr, in: BeckOK VwVfG, 42. Edition, Stand: 1. Januar 2018, § 11 VwVfG, Rn. 1). Die Ersatzvornahme nach §§ 62 Abs. 1 Nr. 1, 63 LVwVG wäre hier von vornherein unstatthaft, da sie an eine vertretbare Handlung anknüpft. Die Anwendung unmittelbaren Zwanges nach §§ 62 Abs. 1 Nr. 3, 65 LVwVG wäre nur als letztes Mittel der Verwaltungsvollstreckung anzuwenden und musste vorliegend ohnehin außer Betracht bleiben, da dieser für die Erzwingung einer aktiven Auskunftserteilung offensichtlich ausgeschlossen ist. Die Duldung einer sonstigen Informationsbeschaffung – etwa mittels Durchsuchung der Geschäftsräume – ist hier nicht streitgegenständlich.

bb) Die Pflicht zur Auskunftserteilung bestand im Zeitpunkt der Festsetzung des Zwangsgeldes fort, worauf die Klägerin auch im Zuge dessen gemäß § 62 Abs. 4 LVwVG hingewiesen wurde. Sie dauerte auch noch im Zeitpunkt der mündlichen Verhandlung an, ohne dass zwischenzeitlich eine hinreichend konkrete und vor allem vollständige Beantwortung des betreffenden Informationersuchens erfolgt wäre. Die Behauptung der Einstellung der Überwachungsmaßnahmen ersetzt die Erfüllung des Auskunftsersuchens nicht. Der Beklagte hat der Klägerin eine nach § 64 Abs. 2 Satz 4 LVwVG angemessene Frist zur Zahlung des Zwangsgeldes gesetzt, indem er diese auf zwei Wochen nach dem Eintritt der Rechtskraft des Bescheides festlegte. Aufgrund der mehrmaligen gleichartigen Auskunftsersuchen im Vorfeld des Bescheids war eine Beantwortung in diesem Zeitraum auch ohne weiteres zumutbar.

cc) Die Rechtsfolgenseite der Ermächtigungsgrundlage eröffnet dem Beklagten gemäß § 64 Abs. 1 und 2 LVwVG einen Ermessensspielraum. Demnach kann die Vollstreckungsbehörde den Vollstreckungsschuldner durch ein Zwangsgeld zur Erfüllung seiner Pflichten anhalten und dabei einen Betrag zwischen mindestens fünf und höchstens fünfzigtausend Euro festsetzen. Bei der Bemessung sind einerseits die wirtschaftlichen Vorteile, die mit der Nichtbefolgung des Verwaltungsaktes verbunden sind,

zu berücksichtigen, andererseits muss das Zwangsmittel nach § 62 Abs. 2 LVwVG in einem angemessenen Verhältnis zu seinem Zweck stehen. Der Beklagte hat sein Ermessen vollständig und entsprechend dem Zweck der Ermächtigungsgrundlage ausgeübt sowie die gesetzlichen Grenzen des Ermessens eingehalten (§ 114 Satz 1 VwGO).

Zunächst bestehen hinsichtlich des Entschließungsermessens keine rechtlichen Bedenken. Dem Beklagten steht es grundsätzlich frei, ob er zur Durchsetzung seines Grundverwaltungsaktes, hier in Gestalt des Bescheides vom 14. Juni 2018, überhaupt Zwangsmittel androht bzw. später festsetzt. Insoweit gilt allerdings, dass es in der Regel sachgerecht ist, eine erlassene Grundverfügung mit Mitteln des Verwaltungszwangs durchzusetzen (vgl. Deusch/Burr, in: BeckOK VwVfG, 42. Edition, Stand: 1. Januar 2018, § 6 VwVG, Rn. 2). Bereits die Androhung des Zwangsgeldes soll dem Anliegen des Beklagten Nachdruck verleihen und der Klägerin aufzeigen, dass sie den Forderungen des Beklagten nachzukommen hat. Die Anwendung von Verwaltungszwang dient hier auch der Effektivität der Verwaltung und der Durchsetzung der Rechtsordnung. Sie dient hier erkennbar der Willensbeugung und hat keinen Sanktionscharakter. Dies gilt insbesondere vor dem Hintergrund, dass das Auskunftersuchen für die Vorbereitung weiterer Maßnahmen aus Sicht des Beklagten erforderlich ist.

Eine Beantwortung des detaillierten Fragenkatalogs ist bisher – wenn überhaupt – nur sehr rudimentär in dem Sinne erfolgt, dass innerhalb der gesetzten Fristen pauschal auf die Außenkameras und deren zwischenzeitliche Entfernung hingewiesen worden ist. Insbesondere fehlen jegliche Aussagen zu den Kameras im Innenraum der Gaststätte. Auch dazu hat der Beklagte mehrmals (ausdrücklich) aufgefordert. Die Aussage, dass die Kameras im Innenraum nunmehr abgeschaltet seien, hat die Klägerin weder substantiiert dargetan oder belegt. Überdies entbindet sie dies auch nicht rückwirkend von ihrer Verpflichtung zur Beantwortung des Fragenkatalogs. Anders, als die Klägerin zu meinen scheint, hat der Beklagte sie stets nur zur Beantwortung des Fragenkatalogs aufgefordert, eine ausdrückliche Anordnung zur Entfernung der Kameras im Außen- oder Innenbereich ist bisher durch die Beklagte nicht erfolgt. Dieser prüft – wie es nach dessen Ausführungen in der mündlichen Verhandlung anzunehmen ist – die Rechtmäßigkeit des Kameraeinsatzes zunächst anhand der Auskünfte der Betroffenen; erst dann ergeht gegebenenfalls ein Bescheid über weitergehende Maßnahmen. Insoweit erfüllen auch die Ausführungen im gerichtlichen Verfahren die Anforderungen an eine vollständige Erfüllung des Informationsersuchens nicht, sondern erschöpfen sich wiederum ausschließlich in allgemein gehaltenen Aussagen, denen es auch an einer näheren Substantiierung mangelt.

Die Festsetzung des Zwangsgeldes in Höhe von 5.000,00 € ist auch verhältnismäßig. Das angewandte Zwangsmittel ist vorliegend geeignet, die Klägerin anzuhalten die ihr obliegenden Pflichten zu erfüllen, da es zur Durchsetzung des Grundverwaltungsaktes zumindest förderlich ist. Ob ein von der Klägerin im gerichtlichen Verfahren angebotener Vor-Ort-Besuch zweckmäßiger wäre, ist gerichtlich nicht zu überprüfen. Dies kann ggf. zu einer außergerichtlichen Einigung bis hin zu einer Reduzierung des Zwangsgeldes führen, was hier indessen nicht streitgegenständlich ist.

Das Zwangsgeld ist auch erforderlich. Dies ist dann der Fall, wenn es unter mehreren gleich geeigneten Mitteln das relativ Mildeste darstellt und die Klägerin am wenigsten beeinträchtigt. Hierbei ist nicht nur auf das Zwangsmittel abzustellen, sondern der Beklagte hat zu prüfen, ob der angestrebte Zweck

sich auch mit anderen Maßnahmen verwirklichen lässt (vgl. Deusch/Burr, in: BeckOK VwVfG, 42. Edition, Stand: 1. Januar 2018, § 9 VwVG, Rn. 8). Der Beklagte hat bereits im März 2017 mit der Klägerin Kontakt aufgenommen und ihr den für seine Prüfungen erforderlichen Fragenkatalog übersandt, dies erfolgte durch einfaches Schreiben. Der Einsatz eines Fragebogens ist bereits das mildeste Mittel, insbesondere eingriffssärmer als eine (erzwungene) persönliche Kontrolle durch den Beklagten im Rahmen eines Ortstermins. Hinsichtlich der Auswahl des Zwangsmittels bestehen keine rechtlichen Bedenken, denn der Gesetzgeber hat die möglichen Zwangsmittel in § 62 LVwVG abschließend geregelt. Wie oben bereits festgestellt, waren sowohl die Ersatzvornahme als auch der unmittelbare Zwang vorliegend unzulässig.

Auch der Höhe nach ist die Festsetzung nicht zu beanstanden. Die Klägerin reagierte – bereits nach mehrmaliger Aufforderung – auf die Androhung eines Zwangsgeldes in Höhe von 500,00 € nicht. Die weitere beharrliche Weigerung der Klägerin, die an sie gestellten Fragen zum Einsatz der Videokameras insbesondere im Innenraum der Gaststätte zu beantworten, führte letztlich zur Androhung und Festsetzung des Zwangsgeldes in Höhe von 5.000,00 €. Es wurde damit zunächst über einen beträchtlichen Zeitraum hinweg mit mildereren Mitteln vergeblich versucht, die Klägerin zur Beantwortung des ihr übersandten Fragenkatalogs zu bewegen.

Die Festsetzung des Zwangsgeldes in Höhe von 5.000,00 € ist auch angemessen im Hinblick auf den angestrebten Erfolg der Beantwortung des Fragenkatalogs bzw. des Informationsersuchens. Den Vollstreckungsinteressen des Beklagten zur Durchsetzung datenschutzrechtlicher Bestimmungen ist vorliegend Vorrang vor den Interessen der Klägerin zu gewähren.

Der Gesetzgeber hat dem Beklagten einen weiten Spielraum bei der möglichen Höhe des Zwangsgeldes eingeräumt. Gemäß § 64 Abs. 2 Satz 2 LVwVG kann er ein Zwangsgeld zwischen fünf und fünfzigtausend Euro festsetzen. Die Höhe des Zwangsgeldes ist im Einzelfall und anhand der Dringlichkeit und Bedeutung der Angelegenheit und des bisherigen Verhaltens der Klägerin zu bestimmen. Die Wichtigkeit des vom Beklagten verfolgten Zwecks und die Intensität des von der Klägerin geleisteten Widerstandes gegen die Erfüllung der Verpflichtung sind ebenso von Bedeutung (vgl. Deusch/Burr, in: BeckOK VwVfG, 42. Edition, Stand: 1. Januar 2018, § 11 VwVG, Rn. 13). Hierbei kann der Beklagte das Zwangsgeld auch steigern, wenn sich die Klägerin – wie hier – beharrlich weigert, der ihr auferlegten Verpflichtung nachzukommen. Die Beantwortung der Fragen weist besondere Dringlichkeit und Bedeutung auf, denn es besteht besondere datenschutzrechtliche Relevanz hinsichtlich der von der Klägerin angefertigten Aufnahmen sogar aus der Privat- bzw. Intimsphäre ihrer Kunden und Mitarbeiterinnen. Dabei ist es hier auch unerheblich, ob insoweit etwa in einem Separee nur eine erotische Tanzvorführung stattfindet oder weitere sexuelle Handlungen erfolgen. Es handelt sich in beiden Fällen um besonders sensible Daten (vgl. Art. 9 Abs. 1 DS-GVO).

Zu beachten ist hier, dass sich die Klägerin über einen erheblichen Zeitraum weigerte, die ihr übersandten Fragen zu beantworten. Diesem Umstand durfte der Beklagte Rechnung tragen, indem er die Zwangsandrohung deutlich erhöhte. Vorliegend sind nicht nur die Kosten einer möglichen Demontage der Kameras anzulegen, sondern insbesondere ist auch die erhebliche datenschutzrechtliche Relevanz bei Videoaufzeichnungen von sexuellen Handlungen zu beachten, wie sich aus den in der in der staatsanwaltlichen Ermittlungsakte befindlichen „Screenshots“ ergibt. Der Vortrag des Prozessbevoll-

mächtigen der Klägerin in der mündlichen Verhandlung, dass Prostitution arbeitsvertraglich für die Mitarbeiterinnen untersagt sei, ist wiederum weder hinreichend substantiiert noch ansatzweise belegt. Überdies dürfte dies auch zu keiner anderen Beurteilung führen, da offenbar faktisch sexuelle Handlungen vollzogen werden und es nicht auszuschließen ist, dass dies insoweit von der Klägerin geduldet wird. Jedenfalls würde auch alleine die Videoüberwachung von erotischen Tanzvorstellungen, bei denen sich jedenfalls die Tänzerinnen unter Umständen vollständig entkleiden, datenschutzrechtlich als besonders sensibler Bereich einzuordnen (vgl. Art. 9 Abs. 1 DS-GVO: „Daten zum Sexualleben oder der sexuellen Orientierung“) und im Übrigen auch arbeitsrechtlich bedenklich sein.

Darüber hinaus handelt es sich bei der Klägerin nicht um eine natürliche Person, sondern um eine gewinnorientiert arbeitende GmbH. Der vom Gesetzgeber in § 64 Abs. 2 Satz 1 LVwVG eingeräumte Ermessensspielraum soll gerade auch eine Orientierung an der wirtschaftlichen Leistungsfähigkeit der Klägerin ermöglichen. Diese ist ohne gegenteilige Anhaltspunkte bei Gewerbetreibenden in aller Regel höher einzuschätzen als bei Privatpersonen. Das Zwangsgeld kann gerade nur dann seine willensbeugende Wirkung erreichen, wenn es in seiner Höhe auch ausreichend ist, um bei der Klägerin die angestrebte Auskunft zu erwirken (vgl. zur Zulässigkeit eines Zwangsgeldes in dieser Höhe auch: SächsOVG, Beschluss vom 17. Juli 2013 – 3 B

470/12 –, BeckRS 2014, 45288; VG Darmstadt, Beschluss vom 21. Mai 2013 – 5 L 304/13.DA –, juris, Rn. 59). Die von dem Prozessbevollmächtigten der Klägerin in der mündlichen Verhandlung zur Akte gereichte „Gewinn- und Verlustrechnung“ für das Jahr 2017 rechtfertigt insoweit keine andere Einschätzung. Vielmehr lässt dies keine hinreichend schlüssige Prognose hinsichtlich der allgemeinen wirtschaftlichen Leistungsfähigkeit der Klägerin zu, sondern stellt vielmehr nur eine Momentaufnahme dar, aus der sich entnehmen lässt, dass die Klägerin in den Jahren 2016 und 2017 erhebliche Gewinnschwankungen hatte. Eine niedrigere Bemessung des Zwangsgeldes wäre bei diesem – ohnehin erst nachträglich eingebrachten – Aspekt daher von vornherein nicht zwingend angezeigt gewesen.

Sofern die Klägerin vorträgt, sie habe ein berechtigtes Interesse an der Videoüberwachung im Innenraum und den Separees ihrer Gaststätte und weise darauf auch ausreichend hin, so betrifft dieser Vortrag nicht die Frage der Festsetzung des Zwangsgeldes. Dies ist in dem vom Beklagten übersandten Fragebogen anzubringen, denn dieser zielt gerade darauf, seitens des Beklagten die Rechtmäßigkeit der Videoüberwachung zu überprüfen. Welche Konsequenzen sich für die Klägerin aus dieser Prüfung ergeben, ist als offen zu qualifizieren. Wenn die Klägerin dabei der Ansicht ist, die Videoüberwachung entspreche den gesetzlichen Vorgaben, so ist ihre beharrliche Weigerung zur Beantwortung des Fragebogens nicht ansatzweise nachvollziehbar.

Berichte, Informationen, Sonstiges

Datenschutzbeauftragte stärken Unternehmen

Die Bundesregierung hatte vor der Sommerpause die Änderung des BDSG in die Wege geleitet, wodurch die Benennungspflicht für Unternehmen „ge-lockert“ werden soll: Danach müssen private Firmen dann einen DSB benennen, wenn dort mehr als 20 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Bislang lag die Grenze bei 10 Mitarbeitern. Einer Umfrage des Fachmagazins „Datenschutz-Praxis“ zufolge, wollen von den betroffenen Unternehmen 19 Prozent künftig keinen DSB mehr benennen. 20 Prozent der Firmen, die nach der neuen Regel keinen DSB benennen müssen, wollen aber ihre Datenschutzorganisation nicht verändern. Nach der Lockerung der Benennungspflicht für Datenschutzbeauftragte (DSB) appellieren Aufsichtsbehörden an die betroffenen Unter-

nehmen, nicht auf das Datenschutz-Knowhow der DSBs zu verzichten. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, unterstrich nach dem ersten Jahr Datenschutz-Grundverordnung, dass die Aufsichtsbehörden ihre Kontrolltätigkeiten intensivierten. „Datenschutzbeauftragte sind für uns und die Unternehmen wichtige Ansprechpartner. Sie unterstützen Unternehmen dabei, sich gesetzeskonform aufzustellen und dadurch Zeit und Geld zu sparen – von etwaigen Bußgeldern bei Verstößen ganz abgesehen.“ Der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, Thomas Kranig, kritisierte, „mit der zahlenmäßigen Lockerung wird der Bundesgesetzgeber der Wirtschaft einen Bärendienst erweisen. Besser wäre gewesen, zu klären, was in einer Welt, in der jeder mit Tablet und Smartphone agiert, mit ständiger Be-

schäftigung wirklich gemeint ist.“ Und der Bayerische Landesbeauftragte für den Datenschutz, Professor Thomas Petri, betonte: „Zuverlässiger Datenschutz ist mittlerweile zu einem Markenzeichen geworden. Unternehmen, die jetzt auf einen DSB verzichten, geben einen wichtigen Teil ihres Kundenvertrauens preis.“

(Presseinformation vom 08.09.2019)

EuGH: Zum Kontaktangebot von Onlinehändlern

Online-Händler müssen für ihre Kunden nicht unbedingt telefonisch erreichbar sein. Das gebietet die unternehmerische Freiheit, so der EuGH. Es müsse lediglich eine schnelle und effiziente Kommunikation möglich sein. Sie müssen allerdings ein Kommunikationsmittel bereitstellen, über das sie schnell kontaktierbar sind und effizien-

ent kommunizieren können (Urt. v. 10.07.2019, Az. C-649/17).

Die deutsche Norm, mit welcher die Verbraucherrechtlinie (Verbraucherrechte-RL) unter anderem im nationalen Recht umgesetzt wird, ist Art. 246a §1 Abs. 1 S. 1 Nr. 2 Einführungsgesetz zum Bürgerlichen Gesetzbuch (EGBGB). Danach sind unter anderem FernAbs.-Händler verpflichtet, eine Telefonnummer und "gegebenenfalls" eine Faxnummer und eine E-Mail-Adresse zur Kontaktaufnahme zur Verfügung zu stellen.

Der Bundesgerichtshof (BGH) legte allerdings dem EuGH die Frage vor, ob die deutsche Regelung aus dem EGBGB mit der Verbraucherrechte-RL konform geht (Beschl. v. 05.10.2017, Az. I ZR 163/16).

Der EuGH verneinte dies nunmehr. Nach dem EuGH können Unternehmen nämlich nicht verpflichtet werden, einen Telefonanschluss oder ein E-Mail-Konto neu einzurichten, damit Verbraucher stets mit ihnen Kontakt aufnehmen können. Die Richtlinie diene nicht nur dem Verbraucherschutz. Es ginge indes auch darum, ein ausgewogenes Gleichgewicht zwischen einem hohen Verbraucherschutzniveau und der Wettbewerbsfähigkeit der Unternehmen sicherzustellen, wobei hier der unternehmerischen Freiheit der Händler der Vorzug zu geben sei.

Gleichzeitig betonte der Gerichtshof jedoch, dass Online-Händler den Verbrauchern zumindest ein anderes Kommunikationsmittel bereitstellen müssten, über das schnell Kontakt aufgenommen und effizient kommuniziert werden kann. Die Unternehmen könnten deswegen etwa elektronische Kontaktformulare, Internet-Chats oder ein Rückrufsystem nutzen, sofern die Informationen dazu den Kunden klar und verständlich zugänglich gemacht würden.

Der BGH muss nun noch abschließend entscheiden, ob die konkret zur Verfügung gestellten Kommunikationsmittel für die schnelle Kontaktaufnahme von Kunden ausreichen und ob die Informationen dazu leicht genug

zugänglich sind. Die Luxemburger Richter erklärten aber bereits, dass die Tatsache, dass eine Telefonnummer erst nach einigen Klicks auf einer Internetseite verfügbar sei, nicht unbedingt bedeutete, dass sie zu schwer zugänglich sei.

Datenschutz für Grundschulen – überarbeitetes und erweitertes Angebot der Berliner Beauftragten für Datenschutz und Informationsfreiheit

Die Berliner Datenschutzbeauftragte hat es sich zum Ziel gesetzt, bei Kindern so früh wie möglich das Bewusstsein für den Schutz ihrer Daten zu wecken. Um dies zu erreichen, startete die Behörde im Frühjahr 2018 ein bisher einzigartiges medienpädagogisches Angebot, das gezielt Kinder im Grundschulalter und deren Eltern und Lehrkräfte anspricht. Die dort angebotenen Materialien wurden in diesem Jahr gründlich auf den Prüfstand gestellt und mithilfe des Feedbacks von Schülerinnen und Schülern vollständig überarbeitet und erweitert.

In neuem farbenfrohem Design enthält das erweiterte Angebot nun auch interaktive Webmodule, Spiele und Mitmachhefte zum Ausdrucken. Neu entwickelte Figuren führen Kinder in die komplexe und abstrakte Welt des Datenschutzes ein. Ein kindgerechtes, anschauliches Lexikon erklärt die wichtigsten Begriffe rund um das Grundrecht auf informationelle Selbstbestimmung.

Als besonderes Angebot anlässlich des Relaunchs von www.data-kids.de können sich Berliner Grundschulen im ersten Schulhalbjahr 2019/2020 für Projektstunden bewerben, die die Berliner Datenschutzbeauftragte für Schulen anbietet, um gemeinsam mit den Kindern und Lehrkräften die neuen Materialien zu entdecken.

Interessierte Grundschulen richten ihre Bewerbung bitte ab sofort per E-Mail an medienkompetenz@datenschutz-berlin.de.

Bitkom: Fast jeder Zweite teilt Urlaubsfotos in sozialen Netzwerken

Der Tempel auf Bali, der Eiffelturm in Paris, der Sonnenuntergang über der Spree in Berlin: 45 Prozent der Bundesbürger laden ihre digitalen Urlaubsfotos bei Instagram oder einem anderen sozialen Netzwerk wie Facebook hoch. 61 Prozent teilen ihre Bilder über Messenger-Dienste wie WhatsApp oder Snapchat. Das hat eine repräsentative Umfrage im Auftrag des Digitalverbands Bitkom unter 1.003 Bundesbürgern ab 16 Jahren ergeben. Insgesamt geben mehr als 8 von 10 Deutschen (84 Prozent) an, im Urlaub digitale Bilder zu machen. Viele Menschen bearbeiten ihre Bilder zudem. 14 Prozent der Befragten geben an, hierfür eine Foto-App auf ihrem Smartphone oder Tablet zu nutzen. Doppelt so viele (28 Prozent) tun dies am Computer. Um ihre Urlaubsfotos zu sichern, nutzen 18 Prozent einen Cloud-Dienst wie iCloud oder Dropbox. 16 Prozent aller Befragten sichern ihre Bilder auf physischen Datenträgern wie USB-Sticks oder externen Festplatten.

Doch auch die analoge Aufbereitung digitaler Urlaubsfotos ist weiterhin beliebt: So geben 65 Prozent aller Befragten an, sich Bilder selbst auszudrucken. 34 Prozent bestellen Abzüge im Laden, 21 Prozent tun dies über das Internet. 19 Prozent gestalten mit ihren Bildern Fotobücher am Computer und lassen sie dann von einem Anbieter drucken. Nur 5 Prozent schauen sich ihre Urlaubsbilder ausschließlich auf dem Bildschirm an.

(Bitkom-Pressemitteilung vom 06.08.2019)

Die neue Datenschutz-Grundverordnung für Mitarbeiter

Informieren - Sensibilisieren - Dokumentieren



Mitarbeiterinformation Datenschutz

Merkblatt zum Datenschutz für Mitarbeiterinnen und Mitarbeiter nach DS-GVO und BDSG (neu)

GDD

DATAKONTEXT

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

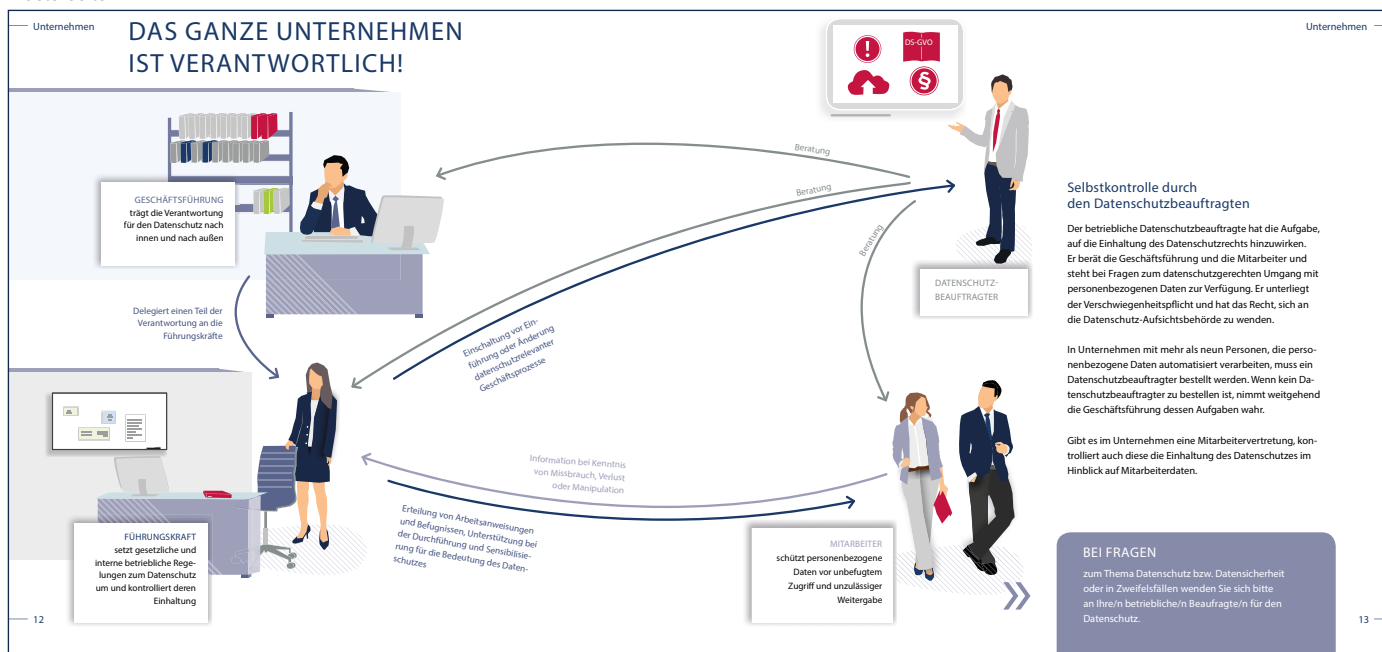
20 Seiten, Staffelpreise

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

Judith Todd
Kundenbetreuung



Musterseite



Muster unter www.datakontext.com

Literaturhinweise

Heidtmann, Jan, Internet abschalten – Das Digitale frisst uns auf, Süddeutsche Zeitung GmbH, München 2019, 72 S., 9,90 €

Der Autor geht dem von dem zweifelsohne unrealistischen Wunsch aus, dass man das Internet abschalten möge, bevor wir uns ihm vollständig ausliefern. Denn das Internet schaffe keine Freiheiten und auch keine Vielfalt. Monopolisten wie Facebook, Google oder Apple übernehmen die Macht über unser Leben. Fünfzig Jahre nach Erfindung des Ur-Internets sei es Zeit, einmal einen Strich zu ziehen: Was hat die Digitalisierung der Menschheit gebracht, Soll und Haben? Das Ergebnis werde in Tiefrot geschrieben.

(Redaktion)

Scheurer, Martin, Spielerisch selbstbestimmt, Rechtskonforme Einwilligungserklärungen in Zeiten ubiquitärer Digitalisierung, Internetrecht und Digitale Gesellschaft (IDG), Band 18, Duncker und Humblot, Berlin 2019, 390 S., 89,90 €

Auch nach den Vorgaben der DS-GVO ist die Einwilligungserklärung das zentrale Ausübungsinstrument datenschutzrechtlicher Selbstbestimmung. Allerdings wird das Versprechen einer freiwilligen, selbstbestimmten und allem voran informierten Einwilligung im Kontext der voranschreitenden Vernetzung und Verdichtung der Gesellschaft vermehrt kritisch beäugt. Gerade aber mit Blick auf die zunehmende Ökonomisierung personenbezogener Daten sollten die Vorgaben des Datenschutzrechts nicht als Antagonist der datengetriebenen Wirtschaft identifiziert werden, sondern vielmehr als Innovationsmotor bei der Ausgestaltung kreativer Einwilligungsprozesse. Vor diesem Hintergrund analysiert die vorliegende Arbeit die nunmehr geltenden grund- und datenschutzrechtlichen An-

forderungen an die Einwilligungserklärung und untersucht erste Lösungsansätze zur Gewährleistung einer effektiven, digitalisierten Selbstbestimmung.

(Redaktion)

Lutz Bergmann/Roland Möhrle/Armin Herb, Datenschutzrecht, Kommentar Bundesdatenschutzgesetz – Europäische Datenschutz-Grundverordnung – Datenschutzgesetzte der Länder – Bereichsspezifischer Datenschutz, Richard Boorberg Verlag, Stuttgart 2019, Loseblattwerk, etwa 3580 S., 96,- € einschl. 3 Ordnern und CD-Rom

Der in Wirtschaft und Verwaltung anerkannte Kommentar bietet zum komplizierten Datenschutzrecht des Bundes und der Länder eine umfassende und detaillierte Darstellung auf aktuellem Stand. Eine Vielzahl an Diagrammen, Mustern und Tabellen macht das Datenschutzrecht klar verständlich.

- Praxisgerechte Kommentierung des BDSG unter Berücksichtigung neuer Entwicklungen (z.B. Cloud Computing) mit Checklisten, Übersichten und Schaubildern
- EU-DS-GVO: Systematische Einführung und Synopse BDSG – EU-DS-GVO
- Text des Bundesmeldegesetzes
- Alle Landesdatenschutzgesetze sowie das LDSG BW mit Anmerkungen
- Multimedia und Datenschutz
- Datenschutzgesetze der Kirchen
- Datenschutzvorschriften aus allen Büchern des SGB mit Erläuterungen
- Arbeitshilfen und Sachregister auf CD-Rom

Die 57. Ergänzungslieferung, erschienen am 10. Mai 2019, ist auf dem Stand Februar 2019.

Diese Ergänzung enthält:

Kommentierung der §§ 8 bis 15 BDSG 2018 zu den Aufgaben und Befugnis-

sen des 1.1.2019 neu gewählten Bundesbeauftragten für den Datenschutz und die restlichen Gesetze.

Weitere Kommentierungen zur DS-GVO, nämlich:

- Art. 2: Neue Überblicke zu den neuen europäischen Datenschutz-Verordnungen und deutschen Datenschutzgesetzen
- Art. 11: Verarbeitung und Identifizierung betroffener Personen
- Art. 13: Informationspflicht bei der Erhebung direkt beim Betroffenen
- Art. 24: Verantwortung des für die Verarbeitung Verantwortlichen
- Art. 68: Europäischer Datenschutzausschuss.

(Schriftleitung)

Philipp Reimer, Verwaltungsdatenschutzrecht, Das neue Recht für die behördliche Praxis, Nomos-Verlag, Baden-Baden 2019, 210 S., 58,- €

Allzu oft fokussieren sich datenschutzrechtliche Abhandlungen auf den nichtöffentlichen Bereich. Reimer legt nun eine Systematisierung des Datenschutzrechts für den öffentlichen Sektor vor. Einen Ausblick auf das Thema lieferte der Verfasser zuvor in DÖV 2018, 881 ff.

Verwaltungsbehörden verarbeiten personenbezogene Daten „quer durch alle Gebiete des Besonderen Verwaltungsrechts hindurch“ (S. 16). Insoweit wird hier das Verwaltungsdatenschutzrecht als allgemein-verwaltungsrechtliche Querschnittsmaterie postuliert. Die behördliche Datenverarbeitung identifiziert Reimer als nichtregelndes Verwaltungshandeln und ordnet sie dementsprechend der Handlungsform des Realakts zu. Dies zeitige unmittelbare Folgen für etwaige Rechtsschutzmöglichkeiten der Bürger (S. 17).

Ausgangspunkt des Werks ist eine Darlegung der einschlägigen Rechtsgrundlagen für die Datenverarbeitung (S. 18-53). Unterschieden werden die

Sphäre der DS-GVO, die Sphäre der JI-RL sowie eine unionsrechtsfreie Sphäre. Letztere versammelt Verarbeitungen, welche gänzlich außerhalb des Anwendungsbereichs des Unionsrechts stattfinden, nicht personenbezogen sind oder nichtautomatisiert vorgenommen werden. Die Unterscheidung erfolgt dabei nicht um des bloßen Systematisierens willen: Je nachdem, in welcher Sphäre sich die Verwaltung bewegt, erkennt Reimer unterschiedliche Grade der Charta- und Verfassungsgrundrechtsbindung, des räumlichen Anwendungsbereichs und der Zulässigkeitsregelungen.

Ein knappes Kapitel skizziert mögliche Folgen von Datenschutzverstößen (S. 62-70), wobei zunächst Meldepflichten, aufsichtsbehördliche Befugnisse, Schadensersatzpflichten und disziplinarrechtliche Folgen ins Auge fallen. Ungeklärt sei bislang die spannende Frage, ob ein datenschutzrechtlicher Verfahrensverstoß zur Rechtswidrigkeit von ergangenen Verwaltungsakten führen könne.

Im breiter angelegten dritten Kapitel wird die Zulässigkeit der Datenverarbeitung dargestellt (S. 71-129). Ausgehend vom Verbot mit Erlaubnisvorbehalt füllt Reimer insbesondere Art. 6 Abs. 1 lit. c DS-GVO (Erfüllung einer rechtlichen Verpflichtung) und Art. 6 Abs. 1 lit. e DS-GVO (öffentliches Interesse/öffentliche Gewalt) mit Leben.

Im weiteren Fortgang behandelt Reimer die organisatorischen Anforderungen an den Datenschutz (S. 130-147, das Verhältnis zum Bürger (S. 148-175) und das Verhältnis zur Aufsichtsbehörde (S. 176-192). Die Ausführungen zum behördlichen Datenschutzbeauftragten klammern leider die Vertreterbestellung aus. Auch wären Anhaltspunkte zur nachvollziehbaren Dienstpostenbewertung wünschenswert gewesen. Ein Desiderat der behördlichen Praxis bleibt zudem eine klare Übersicht, welche Linienaufgaben und typischen Beauftragtenposten bzw. Sonderrollen innerhalb der Verwaltung einen Interessenkonflikt im Sinne von Art. 38 Abs. 6 DS-GVO be-

deuten und deshalb mit dem Amt des behördlichen Datenschutzbeauftragten inkompatibel sind.

Gar zu voreilig wird aus Sicht des Rezensenten die Möglichkeit des Verwaltungszwangs gegen Behörden vom Tisch gekehrt (S. 186 f.). Wegen des ernstlich zu befürchtenden Vollzugsdefizits wäre hier eine kritische Auseinandersetzung mit § 17 VwVG (bzw. dessen landesrechtlichen Äquivalenten) im Hinblick auf das europarechtliche Effizienzgebot (sog. „effet utile“) notwendig.

Insgesamt lässt sich festhalten: Der öffentliche Bereich hat Reimers „Verwaltungsdatenschutzrecht“ dringend nötig. Erfahrene Praktiker finden hierin eine wohlstrukturierte und knappe Übersicht vor, Neulinge werden den konzentrierten Einstieg zu schätzen wissen. Die Sicht der Darstellung ist zuvörderst eine bundesrechtliche, Parallelnormen im Landesrecht werden weitestgehend im Fußnotenapparat nachgereicht.

Die wenigen hier aufgeworfenen Kritikpunkte sind einer ersten Auflage eigen und werden hoffentlich in künftigen Auflagen aufgenommen. Eine Auswahlbibliographie und ein Stichwortverzeichnis schließen das Werk ab.

(Prof. Dr. Lorenz Franck)

*Weth, Stefan/Herberger, Maximilian/Wächter Michael/Sorge, Christoph (Hrsg.), **Datenschutz- und Persönlichkeitsschutz im Arbeitsverhältnis.** Praxishandbuch zum Arbeitnehmerdatenschutz, C.H. Beck-Verlag, München; 2. Aufl. 2019, 769 S., 109,- €*

Die Herausgeber haben zusammen mit 13 weiteren Autoren ein die Thematik des Buches umfassend darstellendes Werk vorgelegt, das sich die rechtsdogmatische Kooperation von Arbeitsrecht und Datenschutzrecht zum Ziel gesetzt hat. Laut Vorwort möchte das Werk dazu Orientierung schaffen und korrekte Hilfestellung geben. Das gilt in wesentlicher Weise für Unternehmen, die datenbasiert arbeiten, aber

auch für solche, die den Weg der Digitalisierung behutsam betreten. Insofern gelte es, Arbeitnehmerdatenschutz neu zu definieren.

Die 2. Auflage des Werks soll Praktikern und auch Wissenschaftlern in rechtsdogmatisch fundierter Weise Hilfestellung in neuen Entwicklungen geben. Demgemäß gliedert sich das Buch in 4 Teile (allgemeiner Teil, besonderer Teil, spezifische Bereiche, Praxisteil), mit insgesamt 39 die Themenbereich regelmäßig sehr detailliert darstellenden Einzelkapiteln. Dabei kann man die Einordnung der einzelnen Kapitel nachfragen. Arbeitnehmerdatenschutz bei Unternehmenstransaktionen ist Kapitel XIV des „besonderen Teils“. Internationaler Datentransfer findet man als Kapitel II im Teil „spezifische Bereiche“. Auffällig ist auch, dass gemessen am Umfang des Buches Themen auch recht kurz abgehandelt werden; so die Aufgabe des Betriebsrats beim Datenschutz auf 19 Seiten und die des Datenschutzbeauftragten auf gerade mal 9 Seiten. Andererseits werden die jeweiligen Rechte der Mitarbeitervertretung auch bei den in den Einzelkapiteln abgehandelten Themen detailliert aufgegriffen. Auch, wenn das Werk wohl die umfassende, derzeit auf dem Markt befindliche, Darstellung des Arbeitnehmerdatenschutz ist, trifft man auf Lücken. Nicht gefunden wurde in dem Kap. XII, das Datenabgleiche darstellt, und auch im Stichwortverzeichnis das Terrorlistenscreening.

Insgesamt gibt das Praxishandbuch einen wertvollen, systematischen Überblick über das sensible Thema des Schutzes von Arbeitnehmerdaten. Unter Berücksichtigung der aktuellen Rechtslage werden offene Fragen beantwortet und Lösungswege für Zweifelsfälle aufgezeigt. Gerade vor dem Hintergrund der neuen Datenschutzgrund-Verordnung und der Neufassung des BDSG gibt dieses Handbuch einen Überblick über die unregelmäßig gelösten Problemkreise und offenen Fragen.

(Schriftleitung)

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.

Dallmann, Michael/Busse, Phillip, Verarbeitung von öffentlich zugänglichen personenbezogenen Daten, ZD 2019, S. 394
Auf Grund der immer umfangreicheren Verarbeitung öffentlich zugänglicher Daten vermessen die Autoren diesbezüglich klare Regelungen in der DS-GVO. Maßgebend ist allein die Generalklausel in Art. 6 Abs. 1 lit. f DS-GVO mit der Folge, dass eine umfassende Interessenwägung in jedem Einzelfall erforderlich sei und je nach Betrachter zu unterschiedlichen Ergebnissen führen könne.

Dünke, Heiko, Kollektiver Rechtsschutz bei Datenschutzrechtsverstößen, DuD 2019, S. 483
Aufgezeigt werden die Möglichkeiten zur Durchsetzung der DS-GVO durch deutsche Verbraucherverbände.

Fuhlrott, Michael/Oltmanns, Sönke, Arbeitnehmerüberwachung und interne Ermittlungen im Lichte der Datenschutz-Grundverordnung, NZA 2019, S. 1105
Der Dokumentationsaufwand steigt, inhaltlich bleibt auch vieles im Lichte der DS-GVO und des § 26 BDSG beim Alten.

Gola, Peter, Spezifika bei der Benennung behördlicher Datenschutzbeauftragter, ZD 2019, S. 383
Der Beitrag zeigt die verschiedenen Gestaltungen der Benennung in Gestalt kumulativer, stellvertretender, gemeinsamer, Teilzeit- und befristeter Bestellung und die dabei bestehende Mitbestimmung im Rahmen von Bundes- und Landesnormen auf.

Gola, Peter/Klug, Christoph, Die Entwicklung des Datenschutzrechts im ersten Halbjahr 2019, NJW 2019, S. 2587
Der Beitrag setzt die seit der Verabschiedung des BDSG im Jahre 1979 stattfindende Berichterstattung mit u.a. den Schwerpunkten Beschäftigten- und Kundendatenschutz fort.

Golland, Alexander, Reichweite des „Joint Controllershship“: Neue Fragen der gemeinsamen Verantwortlichkeit, K&R 2019, S. 533
Aufgezeigt wird der derzeitige Stand der Diskussion um gemeinsame Verantwortlichkeiten i.S.d. Art. 26 DS-GVO.

Gündoğdu, Alev/Hurst, Sascha, Änderungen für den Schutz von Geschäftsgeheimnissen durch das GeschGehG: Eine Synopse, K&R 2019, S. 451
Der Beitrag gibt eine Übersicht zur Umsetzung der EU-RL 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen („Geschäftsgeheimnisse“) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung („Geheimnisschutzrichtlinie“) im Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG).

Kort, Michael, Schweigepflicht eines beim BEM-Gespräch hinzugezogenen Betriebsratsmitglieds, NZA 2019, S. 502
Der Beitrag geht der Frage nach, ob ein beim BEM-Erstgespräch vom Beschäftigten hinzugezogenes Betriebsratsmitglied einer Schweigepflicht gegenüber den anderen Betriebsratsmitgliedern unterliegt, und bejaht dies.

Riechert, Stefan, Der Rechtsanwalt als Datenschutzbeauftragter, AnwBl 2019, S. 418
Kanzleien benötigen einerseits selbst einen DSB, können aber auch selbst unternehmerisch tätig werden und einen Anwalt zum externen Datenschutzbeauftragten eines Unternehmens bestellen lassen.

Schulte, Willem/Welge, Jonas, Der datenschutzrechtliche Kopieanspruch im Arbeitsrecht, NZA 2019, S. 1110
Der datenschutzrechtliche Kopieanspruch aus Art. 15 III DS-GVO findet auch im Arbeitsverhältnis Anwendung. Seit einer Entscheidung des LAG Baden-Württemberg (NZA-RR 2019, 242) wird insoweit jedoch vor unüberwindbaren Schwierigkeiten gewarnt. Dieser Beitrag untersucht den Kopieanspruch im Kontext des Arbeitsverhältnisses samt seiner Einschränkungen, beleuchtet die Durchsetzbarkeit und zeigt dem Arbeitgeber Reaktions- und Verteidigungsmöglichkeiten auf.



Hosen lernen laufen

Dass Lahme gehen ist nach er der Bibel ein Wunder. Forscher an der US-Harvard-Universität wollen Querschnittsgelähmten und Schlaganfallpatienten nun auf irdische Weise helfen. Die Muskelkraft verstärkende Exoskelette werden etwa in der Medizin, in der Arbeitswelt und beim Militär dort eingesetzt, wo der menschliche Körper mehr Kraft braucht als er hat. Roboteranzüge, die man sich wie eine Rüstung überziehen kann, unterstützen die menschliche Bewegung etwa beim Heben schwerer Gegenstände. Sie haben aber den Alltag der Verbraucher noch nicht erobert, wie E-Bikes. In Harvard forscht

man nun an „Exosuits“. Das sind Roboterhosen, die man über Hüfte und Schenkel zieht damit sie den unteren Rücken um das Hüftgelenk herum beim Gehen und Laufen unterstützen. Es ist schwierig, der Hose „beizubringen“, ob der Mensch noch geht oder schon läuft. Das liegt am unterschiedlichen Charakter der Bewegungen. Gehen funktioniert nämlich physikalisch wie ein Pendel und Rennen wie eine Feder. Algorithmische Systeme sollen den Charakter der Bewegung erkennen und den von ihnen gesteuerten Kabeln in der Hose des Läufers den Impuls geben, langsam oder schnell am Ober-

schenkel zu ziehen, um die Muskeln auch richtig zu unterstützen. Das entlastet bei der Fortbewegung, und man bekommt einen Schub wie beim E-Bike-Fahren. Bestimmt können besonders sportliche Läufer ihre Hosen auch darauf trimmen, sie so anzutreiben wie ein Reiter sein Pferd. So bekommt die Reithose eine ganz neue Bedeutung.





Einführung in den Datenschutz

Mitarbeiter schulen via E-Learning.



- ✓ Moderation in TV-Studioqualität
- ✓ Rechtssicher gemäß DS-GVO
- ✓ von einem Experten entwickelt
- ✓ Dauer: 45 Minuten
- ✓ animierte Schaubilder und Grafiken
- ✓ interaktive Quizfolgen
- ✓ Abschlusszertifikat
- ✓ auch in englischer Sprache verfügbar

Sehen Sie sich jetzt unseren Trailer an:
www.datakontext.com/eLearning



DataAgenda.de

IHR PORTAL ZUM DATENSCHUTZ

- ✓ detaillierte Arbeitspapiere, Checklisten uvm.
- ✓ Videos in TV-Qualität zur aktuellen Gesetzeslage mit Handlungsempfehlungen
- ✓ aktuelle Nachrichten zum Datenschutz: Urteile, Fallbeispiele, Entwicklungen
- ✓ Datenschutz Newsbox - aktuelle Themen monatlich im Überblick

Expertenwissen
in GDD-Qualität



+++ DS-GVO Bußgelder +++ Löschpflichten und Löschkonzepte +++
Stellung des Betriebsrates nach DS-GVO +++ Fotos und die DS-GVO
+++ Datenschutz beim E-Mail-Versand +++ EuGH: Facebook Fanpages +++