

Zeitschrift für
Datenschutz-,
Informations- und
Kommunikationsrecht

RDV

3/2020

Recht der Datenverarbeitung

Herausgegeben von

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

Aufsätze

WERNER/WAGNER/PIEPER, Die datenschutzrechtliche Verantwortlichkeit
im Rahmen des automatisierten Fahrens

BERGER, Das neue Sozialdatenschutzrecht

DERFLER, „Haushaltsausnahme“ auch für juristische Personen
und Personengesellschaften?

Kurzbeiträge

GOLA, Aus den aktuellen Berichten und Informationen der
Aufsichtsbehörden (47): Einzelaspekte des Beschäftigten-
datenschutzes in den neuen Tätigkeitsberichten der
BremLfD und der BlnBfDI

CLAUS/REIF, Praxisfälle zum Datenschutzrecht V: Musterfalllösungen
zur automatisierten Kennzeichenerfassung im Parkhaus

WRONKA, Anwendung der EU-Standarddatenschutzklauseln (Art. 46
Abs. 2 lit c DS-GVO) auf Datenübermittlungen an unselbstständige
Niederlassungen in Drittländern

Rechtsprechung

Aus dem Inhalt

BGH, Zur Haftung für Kundenbewertungen bei Amazon

BGH, Zur Zulässigkeit der Bewertungsdarstellung von Unternehmen
auf einem Internet-Bewertungsportal (www.yelp.de)

BFH, Rechtsanwalt ist als externer Datenschutzbeauftragter
gewerblicher Unternehmer

OLG STUTTGART, Informationspflichten nach Art. 13 Abs. 1 lit. a, c und
Abs. 2 lit. b, d und e DS-GVO beinhalten Marktverhaltensregelungen (Ls)

LAG MECKLENBURG-VORPOMMERN, Abberufung eines Datenschutz-
beauftragten wegen fehlender Zuverlässigkeit

LSG DARMSTADT, Kein Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO
im Verwaltungsverfahren nach §§ 20, 67a Abs. 2 SGB X (Ls)

36. Jahrgang
Juni 2020
Seiten 109–166



Gesellschaft für Datenschutz
und Datensicherheit e.V.


DATAKONTEXT
www.rdv-online.de

Best Practice. Best Command.



Inklusive Datenbank

Redeker (Hrsg.),
Handbuch der IT-Verträge
Herausgegeben von RA, FA IT-Recht,
Dipl.-Informatiker Dr. Helmut Redeker.
Loseblatt, 3 Bände. Grundwerk mit
Fortsetzungsbezug für mindestens 2
Jahre, nur 159,- €, ca. 2-3 Ergänzungs-
lieferungen pro Jahr, je zzgl. 7,- € inkl.
MwSt. für Redeker online
ISBN 978-3-504-56008-9.

i **Das Werk online**
juris.de/pmitr
otto-schmidt.de/bmitr

Das praxisnahe Werk zur Vertragsgestaltung versorgt Rechtsberater und Entscheider in Unternehmen in verschiedensten IT- und telekommunikationsrechtlichen Bereichen mit **ausführlich kommentierten Vertragsmustern**. Klausel für Klausel nehmen erfahrene Praktiker zu allen praxisrelevanten Fragen u.a. des IT-Vertragsrechts, des Internetrechts und des Telekommunikationsrechts Stellung. Sonderfälle werden mit Alternativklauseln und -mustern berücksichtigt.

Update 40. Lieferung:

- › 1.4 Erstellung von Individualsoftware
- › 1.19 Hotlinevertrag
- › 5.2 Vertrag mit einem freien Mitarbeiter
- › 8.4 Mediation

Exklusiv für Abonnenten inklusive Datenbank mit folgenden Inhalten:

- › Redeker, Handbuch der IT-Verträge
- › Härting, Internetrecht
- › Schneider, Handbuch EDV-Recht
- › Rechtsprechung und Gesetze

Informationen, Bestellung und Leseprobe: www.otto-schmidt.de

Inhaltsverzeichnis

Editorial	109	
Veranstaltungen	110	
Aufsätze		
Christoph WERNER/Dr. Manuela WAGNER/Maria PIEPER Die datenschutzrechtliche Verantwortlichkeit im Rahmen des automatisierten Fahrens	111	Kein DS-GVO-Auskunftsanspruch bei unzumutbarem Aufwand (hier: Sichtung von ca. 10.000 E-Mails) (Ls) (LG Heidelberg, Urteil vom 06.02.2020) 154
Dr. iur. Hannes BERGER Das neue Sozialdatenschutzrecht	120	Zum Umfang des Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO (Ls) (LG Landau, Beschluss vom 17.09.2019) 154
Sophie DERFLER „Haushaltsausnahme“ auch für juristische Personen und Personengesellschaften?	128	Arbeitsunfähigkeitsbescheinigung per WhatsApp ist rechtswidrig (LG Hamburg, Urteil vom 03.09.2019) 154
Kurzbeiträge		
Prof. Peter GOLA Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (47): Einzelaspekte des Beschäftigten- datenschutzes in den neuen Tätigkeitsberichten der BremLFD und der BlnBfDI	133	Kündigung infolge unbefugter „Dokumentation“ einer Sicherheitslücke durch einen externen Sicherheitsberater (ArbG Siegburg, Urteil vom 15.01.2020) 155
Miriam CLAUS, LL.M./Rain Yvette REIF, LL.M. Praxisfälle zum Datenschutzrecht V: Musterfalllösungen zur automatisierten Kennzeichenerfassung im Parkhaus	135	Gesundheitsdaten eines Tieres als personenbezogene Daten des Tierhalters (VerwG Mainz, Urteil vom 20.02.2020) 157
Dr. Georg WRONKA Anwendung der EU-Standarddatenschutzklauseln (Art. 46 Abs. 2 lit c DS-GVO) auf Datenübermittlungen an unselbstständige Niederlassungen in Drittländern	139	Berichte, Informationen, Sonstiges
Rechtsprechung		
Zur Haftung für Kundenbewertungen bei Amazon (BGH, Urteil vom 20.02.2020)	143	LFD S-H: Plötzlich im Homeoffice – und der Datenschutz? 161
Zur Zulässigkeit der Bewertungsdarstellung von Unternehmen auf einem Internet-Bewertungsportal (www.yelp.de) (BGH, Urteil vom 14.01.2020)	143	BayLFD: Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie 161
Rechtsanwalt ist als externer Datenschutzbeauftragter gewerblicher Unternehmer (BFH, Urteil vom 14.01.2020)	144	Whitepaper zu rechtlichen Risiken bei der Nutzung internationaler Cloudanbieter 162
Informationspflichten nach Art. 13 Abs. 1 lit. a, c und Abs. 2 lit. b, d und e DS-GVO beinhalten Marktverhaltens- regelungen (Ls) (OLG Stuttgart, Urteil vom 27.02.2020)	147	Bitkom-Befragung: Der Chief Digital Officer bleibt die Ausnahme 162
Abberufung eines Datenschutzbeauftragten wegen fehlender Zuverlässigkeit (LAG Mecklenburg-Vorpommern, Urteil vom 25.02.2020)	148	Literaturhinweise
Kein Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO im Verwaltungsverfahren nach §§ 20, 67a Abs. 2 SGB X (Ls) (LSG Darmstadt, Beschluss vom 29.01.2020)	153	Buchbesprechungen
Auskunftgewährung nach dem Verbraucherinformationsgesetz: Übermittlung eines Kontrollberichts über eine gastronomische Betriebsprüfung (TopfSecret) (Ls) (OVG Lüneburg, Beschluss vom 16.01.2020)	153	<i>Louisa Specht-Riemenschneider/Nikola Werry/ Susanne Werry (Hrsg.)</i> Datenrecht in der Digitalisierung (REDAKTION) 163
		<i>Robert Kreyßing</i> Öffentliche Stellen in den Sozialen Medien – Die primären Rechtsfragen in der Praxis (REDAKTION) 163
		<i>Florian Sackmann</i> Datenschutz bei der Digitalisierung der Mobilität (REDAKTION) 163
		<i>Rolf Schwartmann/Heinz-Joachim Pabst (Hrsg.)</i> Landesdatenschutzgesetz Nordrhein-Westfalen (ZILKENS) 164
		Neuerscheinungen
		Aufsätze 165
		Nachgefasst 166

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 3/2020; DATAKONTEXT, Frechen; C.H. Beck, München

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:

Dieter Schulz

Tel.: 02234/98949-99

dieter.schulz@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
36. Jahrgang 2020 Heft 3
Seiten 109 – 166

RDV

Recht der Datenverarbeitung

36. Jahrgang · Juni 2020 · Seiten 109 – 166

Editorial

Steine statt Brot – Videokonferenz in der Coronakrise aus Sicht der Aufsichtsbehörden

Hals über Kopf mussten die Unternehmen und Behörden wegen der Coronakrise die Arbeitsorganisation auf Homeoffice umstellen. Schulen und Hochschulen mussten kurzfristig die Lehre online anbieten. Notwendiges Werkzeug ist der Einsatz von Tools, mit denen man die Arbeit digital organisieren und die Zusammenarbeit mit Videokonferenzen ermöglichen kann.

Insbesondere KMU mussten schnell und effektiv reagieren. Dabei musste auch die Kommunikation der Mitarbeiter organisiert und nach Möglichkeit die persönliche Zusammenarbeit virtualisiert werden. Dabei lag die Nutzung der am Markt gängigen Produkte auf der Hand. Für eine intensive Prüfung der Tools auf sämtliche Datenschutz- und Datensicherheitsaspekte war keine Zeit. Es musste schnell gehen und funktional sein.

Erst ab Mitte April begannen verschiedene Datenschutzaufsichtsbehörden mit der Veröffentlichung von Stellungnahmen und „Empfehlungen“ zum Einsatz von Video- oder Telefonkonferenzsystemen. Diesen Stellungnahmen ist gemein, dass zunächst ein umfangreicher Anforderungskatalog zur Datenschutzkonformität vorangestellt wird. Sodann wird ausgeführt, dass die insbesondere von KMU, Schulen und Hochschulen kurzfristig angepassten

und genutzten Tools wie Zoom, Skype oder Microsoft Teams diese Anforderungen sämtlich nicht erfüllen. Der BfDI weist darauf hin, dass „in der Praxis es derzeit leider so ist, dass diese Anforderungen von den verfügbaren Angeboten nur teilweise erfüllt werden“. Datenschutzfreundlicher sei es, so der LfDI Baden-Württemberg, Systeme zu nutzen, die selbst betrieben werden können („On Premises“), beispielsweise auf eigenen Servern oder mit Hilfe von Dienstleistern mit Auftragsverarbeitungsverträgen. Dass dies nicht einfach umzusetzen ist, belegt ein bei Twitter veröffentlichter Screenshot einer Videokonferenz der europäischen Aufsichtsbehörden unter Teilnahme des BfDI, die erkennbar mittels Zoom(!) durchgeführt wurde. Ein Tool, das der BfDI mangels geeigneter Verschlüsselung für den geschäftlichen Einsatz für datenschutzwidrig erachtet. Nur bedingt hilfreich sind auch so weitreichende Ratschläge, wonach „Videokonferenzen nur dann genutzt werden sollten, wenn es wirklich notwendig ist, zum Beispiel wenn Präsentationen mit einer Bildschirmfreigabe gehalten werden sollen“, so der LfDI Baden-Württemberg. Videokonferenzen sollen sicherlich unter Beachtung der Privatsphäre der Betroffenen statt-

finden, jedoch darf die soziale Komponente des Kontaktes der Kollegen, Mitschüler und Geschäftsfreunde in Zeiten von Abstandsregelungen nicht unberücksichtigt bleiben.

Die meisten Unternehmen und öffentlichen Stellen sind redlich bemüht, den Anforderungen des Datenschutzes gerecht zu werden und sie leisten viel. Was dürfen sie von der Datenschutzaufsicht erwarten? Vor allem praktische Hilfe bei der Umsetzung der Pflichten. Gerade jetzt kommt es nicht darauf an, in einer Vielzahl von Stellungnahmen zu erklären, was beim Einsatz von Videokonferenzsystemen und anderen digitalen Anwendungen grundsätzlich zu beachten ist und dafür hohe Hürden aufzustellen. Entscheidend ist es jetzt, konkret zu erklären und im Dialog mit der Wirtschaft konstruktiv zu erarbeiten, welcher Dienst wie verbessert werden muss, damit er guten Gewissens eingesetzt werden kann. Das soll nicht von der Verantwortung der Unternehmen ablenken, die die DS-GVO zu Recht diesen überträgt. Die Aufsichtsbehörden sind aber in der Pflicht, die Praxis durch einheitliche und umsetzbare Impulse positiv zu prägen, um Sicherheit zu erzeugen.

Prof. Dr. Rolf Schwartmann
RA Andreas Jaspers

Online-Schulungen von GDD und DATAKONTEXT

Covid-19 verändert unser Leben in rasender Geschwindigkeit.

Sehen wir die aktuelle Situation auch als Chance, neue Formen der Fortbildung zu nutzen. Im Datenschutz müssen Sie aktuell neue Herausforderungen meistern. Die GDD und ihr Partner Datakontext möchten Sie dabei trotz social distancing weiterhin wie gewohnt zuverlässig unterstützen.

Damit Sie sich in der aktuellen Situation professionell informieren und weiterbilden können, bieten wir unsere Präsenzseminare ab sofort als Online-Schulung an. Die neuen Online-Angebote von GDD und DATAKONTEXT sind live, interaktiv und dialogorientiert. Sie können unseren Experten via Chat oder per Mikrofon Fragen stellen. Für die Teilnahme benötigen Sie einen Lautsprecher, der an Ihrem Endgerät funktioniert und ggf. ein Headset sowie eine Kamera.

**BILDEN SIE
SICH WEITER!**

Alle digitalen Angebote finden Sie unter:
www.datakontext.com/online-angebote

39. RDV-Forum

18. November 2020
im Maternushaus Köln

**BITTE
VORMERKEN!**

44. DAFTA

Leitthema: „DS-GVO – vom Projekt
hin zur bußgeldresistenten Praxis“

vom 19. – 20. November 2020
im Maternushaus Köln

Aufsätze

Christoph Werner/Dr. Manuela Wagner/Maria Pieper

Die datenschutzrechtliche Verantwortlichkeit im Rahmen des automatisierten Fahrens

Eine exemplarische Untersuchung anhand des Fahrmodusspeichers

Um zu verhindern, dass Fahrer von automatisierten Fahrzeugen sich im Fall eines Unfalls oder Fehlverhaltens künftig pauschal auf ein Systemversagen berufen können, verpflichtet § 63a StVG zur Speicherung der Daten im Zusammenhang mit dem Wechsel der Fahrzeugsteuerung zwischen dem automatisierten System

und dem Fahrer. Unbeantwortet bleibt insoweit aber bislang, wer nach der DS-GVO für diese Speicherung verantwortlich ist. Dieser Aufsatz soll einen Beitrag bieten, um diese Frage unter Berücksichtigung des Straßenverkehrs-, Datenschutz- und Haftungsrechts kohärent aufzulösen.

I. Einleitung

Die Entwicklung des autonomen Fahrens schreitet weiter voran. Auch wenn einige Automobilhersteller nach Ansicht der Wettbewerbshüter die Autonomiefähigkeit ihrer Fahrzeuge noch etwas zu optimistisch darstellen,¹ sind die technologischen Fortschritte unverkennbar. Weniger fortschrittlich hingegen ist bislang noch die Anpassung des Rechts an diese neue Technologie.

So ist insbesondere die datenschutzrechtliche Einordnung der Datenverarbeitung bei sog. hoch- und vollautomatisierten Fahrzeugen noch nicht vollständig geklärt. Diese zeichnen sich im Gegensatz zu tatsächlich autonomen Fahrzeugen der Stufe 5 dadurch aus, dass weiterhin die „Erforderlichkeit der eigenhändigen Fahrzeugsteuerung durch den Fahrer“ bestehen kann.² Das Fahrzeug muss in diesen Fällen in der Lage sein, den Fahrer bei Bedarf zur Übernahme der Fahrzeugsteuerung aufzufordern. Diese Aufforderung, der Wechsel der Fahrzeugsteuerung zwischen Fahrer und System sowie technische Störungen des Systems werden durch das Fahrzeug gemäß § 63a Abs. 1 StVG im sog. „Fahrmodusspeicher“ (FMS)³ unter Einbeziehung der aktuellen Positions- und Zeitangaben protokolliert. Im Falle der Speicherung außerhalb des Fahrzeugs muss der Speicher außerdem logisch zwingend eine Kennung enthalten, die die Daten mit dem jeweiligen Fahrzeug verknüpft (z.B. amtliches Kennzeichen oder Fahrzeug-Identifizierungsnummer).

Wie ein solcher FMS auszugestalten ist, wird aktuell auch auf internationaler Ebene diskutiert. Geplant ist eine Regelung der UNECE⁴ zu einem „Data Storage System for Automated Driving (DSSAD)“.⁵ Nach derzeitigen Vorschlägen soll das DSSAD ein System bezeichnen, das darauf abzielt, durch die Speicherung eines Datensatzes ein klares Bild der wesentlichen Wechselwirkungen zwischen dem Fahrer und dem autonomen Fahrsystem zu vermitteln.⁶

Nachdem zunächst die Anwendbarkeit des Datenschutzrechts, d.h. das Vorliegen personenbezogener Daten, festgehalten (II.) und skizziert wird, welche Rollen als Verantwortlicher in Frage kommen (III.), konzentriert sich die Betrachtung einerseits auf die Definition des Verantwortlichen nach Art. 4 Nr. 7 DS-GVO (IV.) und andererseits auf die Regelungen der §§ 63a f. StVG (V.). Ergänzend wird die Möglichkeit der neuen Rolle des „Datentreuhänders“ besprochen (VI.) und schließlich ein Ausblick auf die weitere Entwicklung gegeben (VII.).

II. Verarbeitung personenbezogener Daten im Fahrmodusspeicher

Die im FMS aufgezeichneten Informationen sind personenbezogene Daten i.S.d. Art. 4 Nr. 1 DS-GVO, wenn sie sich auf eine betroffene Person beziehen, d.h. eine natürliche Person, die identifiziert oder zumindest identifizierbar ist. Identifizierbarkeit ist gegeben, sofern eine Zuordnung zu einer indi-

1 <https://www.golem.de/news/irrefuehrende-angaben-wettbewerbszentrale-verklagt-tesla-wegen-autopilot-werbung-1910-144694.html> [letzter Abruf aller Onlinequellen: 12.02.2020].

2 Vgl. § 1a Abs. 2 Nr. 4, 5 StVG; BR-Drs 69/17, S. 6; vgl. zur Definition der Stufen und zur Kritik an der zugehörigen Regelung: Wissenschaftlicher Dienst des Bundestages, WD 7-3000 111/18, abrufbar unter <https://www.bundestag.de/resource/blob/562790/c12af1873384bcd1f8604334f97ee4b9/wd-7-111-18-pdf-data.pdf>; Verbraucherzentrale Bundesverband, Rechtssicher fahren mit automatisierten Fahrzeugen (2017), S. 7 ff.

3 Der Begriff dient als abstrakte Umschreibung für den Datenspeicher, ohne damit festzulegen, ob dieser sich im Fahrzeug befindet oder ein externes Backend-System verwendet wird.

4 United Nations Economic Commission for Europe.

5 Siehe hierzu die Diskussionen der Unterarbeitsgruppe zu DSSAD/EDR der Working Party on Automated/Autonomous and Connected Vehicles (GRVA): <https://wiki.unece.org/pages/viewpage.action?pageId=87621709>.

6 Proposal for DSSAD Section in ALKS requirements, abrufbar unter <https://wiki.unece.org/pages/viewpage.action?pageId=92012869> (eingebracht von Japan).

viduellen Person möglich ist, selbst wenn hierfür weitere Informationen, die legal und mit verhältnismäßigem Aufwand erreichbar sind, zur Hilfe genommen werden.⁷ Soweit es sich bei dem Fahrzeughalter um eine natürliche Person handelt, ist dieser u.a. durch eine Halterabfrage nach § 39 StVG⁸ identifizierbar, so dass personenbezogene Daten vorliegen.

Ist der Fahrzeughalter hingegen eine juristische Person,⁹ kommt als natürliche Person nur der Fahrer in Betracht, auf den sich die Informationen beziehen könnten. Hierbei dürfte der Halter regelmäßig Kenntnis von der Identität des Fahrers haben. Für Dritte hängt die Identifizierbarkeit vom Mitwirken des Halters,¹⁰ oder eigenen Informationsbeschaffungsmöglichkeiten¹¹ ab. Für den Personenbezug ist es dabei nach Art 4 Nr. 1 DS-GVO nicht erforderlich, dass der Betroffene namentlich erkennbar ist, es reicht eine Identifizierbarkeit anhand von Referenzdaten.¹² Bereits die Speicherung von GPS-Position und Zeitangabe im Moment des Wechsels der Fahrzeugsteuerung kann zur Identifikation anhand des konkreten Aufenthaltsortes führen.¹³

III. Beteiligte Rollen

Im Weiteren soll untersucht werden, wer für die Verarbeitung dieser personenbezogenen Daten verantwortlich ist. Als potentielle Kandidaten nennt der Bundesrat: Fahrer, Fahrzeughalter, Fahrzeughersteller oder den für den Vertrieb in Deutschland zuständigen Fahrzeughändler.¹⁴

Von Bedeutung sind die Hersteller, da sie die technischen Spezifikationen umsetzen und maßgeblich das Fahrzeug gestalten. Daneben besitzt der Halter die allgemeine Verfügungsgewalt, bestreitet die Kosten und zieht den Nutzen aus der Verwendung.¹⁵ Der Fahrer selbst ist zentrale Figur des zivilrechtlichen Haftungs- sowie des Straf- und Ordnungswidrigkeitenrechts bei Verkehrsverstößen und Unfällen.

In ihrem Verhältnis untereinander sind für die Verantwortlichkeit generell folgende Varianten denkbar: Der Hersteller kann sowohl gegenüber Halter und Fahrer Verantwortlicher sein, der Halter nur gegenüber dem Fahrer und der Fahrer umgekehrt nur gegenüber dem Halter, wenn letzterer eine natürliche Person ist. Eine Verantwortlichkeit zwischen Halter und Fahrer ist indes immer dann ausgeschlossen, wenn sie personenidentisch sind oder die DS-GVO nach Art. 2 Abs. 2 lit c), EWG 18 DS-GVO nicht zur Anwendung kommt (Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten).

IV. Allgemeine Bestimmung der Verantwortlichkeit

Nach Art. 4 Nr. 7 DS-GVO ist Verantwortlicher „jede [...] Person, die die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; [...]“ Sind hingegen Mittel und Zwecke bereits rechtlich vorgegeben, kann auch die Verantwortlichkeit gesetzlich zugewiesen werden. §§ 63a, 63b StVG verpflichten zwar zur Datenverarbeitung, enthalten aber noch keine explizite Zuweisung des Speicheradressaten.

Art. 4 Nr. 7 DS-GVO entspricht ihrem Vorgänger in Art. 2 lit d) RL 95/46/EG (DS-RL).¹⁶ Bereits damals wurde nach dem

Vorschlag der Kommission die Entscheidungsbefugnis in den Mittelpunkt gestellt.¹⁷ Diese soll aus einer „Analyse der faktischen Elemente und Umstände“ des Falls abgeleitet werden.¹⁸

1. Entscheidungsbefugnis über den Zweck

Der Zweck ist demnach das „erwartete Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet“ und das Mittel beschreibt die „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird.“¹⁹ In aktuellen Entscheidungen hob der EuGH mehrfach hervor, dass durch eine weite Definition des Begriffs des Verantwortlichen ein wirksamer und umfassender Schutz der betroffenen Personen gewährleistet werden soll.²⁰ Grundlegend kommt es darauf an, ob Daten zu eigenen Zwecken oder im Auftrag verarbeitet werden bzw. ob aus einem Eigeninteresse heraus Einfluss auf die Verarbeitung genommen wird. Dabei kann es ausreichen, dass ein Beitrag im Sinne einer Mitwirkung zur Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten geleistet wird.²¹ Ein tatsächlicher Zugang jedes Verantwortlichen zu den Daten wird hingegen nicht gefordert, wenn eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DS-GVO vorliegt,²² was auch vorliegend nicht ausgeschlossen ist.

a) Hersteller

Ein Eigeninteresse bzw. ein eigener Zweck könnte darin bestehen, dass sich der Fahrzeughersteller durch die Datenspeicherung gegen Haftungsansprüche zur Wehr setzen

7 Siehe zur Identifizierbarkeit: EuGH, 19.10.2016 – C-582/14 – Breyer.

8 Zu den Anforderungen: VG Augsburg, Urteil vom 14.07.2015 – Au 3 K 15.348, BeckRS 2015, 49296.

9 Zu jur. Person als Halter: Geigel, Haftpflichtprozess, 2. Teil Haftpflichttatsachen, 25. Kapitel. Haftung des Kraftfahrzeughalters und -führers Rn. 47.

10 Der Halter muss Information zwar grundsätzlich nicht herausgeben. Die Verweigerung der Mitwirkung kann allerdings eine Fahrtenbuchauflage nach § 31a Abs. 1 StVZO nach sich ziehen (OVG Münster, Beschluss vom 21.04.2008 – 8 B 491/08, NZV 2008, 479), welches nach § 31a Abs. 3 StVZO jederzeit von der zuständigen Stelle herausverlangt werden kann. Daneben bestehen strafprozessuale Möglichkeiten der Informationsbeschaffung (§§ 94, 98, 103 StPO). Vgl. spezifisch zur digitalen Informationsbeschaffung von Servern: Basar/Hieramente, NSTZ 2018, 681.

11 Bspw. Bildaufzeichnung bei Geschwindigkeitsüberschreitung, Unfallzeugen etc.

12 Paal/Pauly/Ernst, 2. Aufl. 2018, DS-GVO Art. 4 Rn. 8.

13 Brockmeyer ZD 2018, 258 (260 f.).

14 BT-Drs. 18/11534, S. 8.

15 Vgl. zum Halterbegriff: BGH, 22.03.1983 – VI ZR 108/81.

16 Im dt. BDSG wurde verantwortliche Stelle nach § 3 Abs. 7 BDSG definiert als „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“; allerdings wurde insoweit eine richtlinienkonforme Auslegung vorgenommen, vgl. Plath/Schreiber, in: Plath, BDSG, 2013, § 3 BDSG, Rn. 69 m.w.N.

17 Vgl. Art.-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ WP 169, S. 10 f.

18 Art.-29-Datenschutzgruppe, WP 169, S. 11.

19 Art.-29-Datenschutzgruppe, WP 169, S. 16.

20 EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 66; EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 28; EuGH, Urteil vom 13.05.2014 – C-131/12 – Google Spain, Rn. 34; kritisch Hoeren, ZD 2018, 472 (473); Schulz, ZD 2018, 363 (364).

21 EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 68; EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 31.

22 EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 69; EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 38; Marosi/Matthé, ZD 2018, 361 (362).

kann, soweit ein Geschädigter ein Versagen der automatisierten Systeme behauptet. Dagegen spricht aber, dass den Geschädigten als Anspruchsinhaber regelmäßig zunächst die Beweislast treffen wird, nachzuweisen, dass das System aktiv und damit kausal für einen Unfall war.²³

Ein Eigeninteresse könnte an der Datennutzung zur Marktforschung oder zum Training von Algorithmen liegen. Diese Weiternutzung geht aber über den von § 63a StVG vorgezeichneten Zweck der Beweissicherung hinaus und müsste folglich auf eine andere Legitimationsgrundlage gestützt werden oder mit anonymisierten Daten erfolgen.

b) Halter

Da den Halter gemäß § 7 Abs. 1 StVG zunächst verschuldensunabhängig die Haftung trifft, kann er die FMS-Daten nicht zur Anspruchsabwehr nutzen.²⁴ Allerdings kann er über die Datenaufzeichnung erfahren, ob ein Unfall auf einem Systemfehler oder menschlichem Versagen beruht und er Fahrer oder Hersteller in Regress nehmen kann. In der Gesamtschau dient die Speicherpflicht im FMS allerdings vielmehr der Datenbereitstellung gegenüber Behörden und Dritten, die am Unfall beteiligt sind. Ein eigener Auskunftsanspruch des Halters ist hingegen gar nicht vorgesehen. Außerdem werden Zweifel daran geäußert, ob mit den nach § 63a StVG aufgezeichneten Daten der Beweis eines Systemfehlers gelingen kann.²⁵ Im Übrigen kann das Eigeninteresse des Halters freilich geringer ausfallen, wenn er zugleich Fahrer war und die Aufzeichnung die eigene Verantwortlichkeit belegt.

c) Fahrer

Die Datenspeicherung dient jedenfalls auch dem Zweck, dass es dem Fahrer im Falle eines Unfalls durch Systemversagen gelingen kann, einen gegen ihn gerichteten Schuldvorwurf positiv zu entkräften.²⁶ Der Fahrer ist gemäß § 18 Abs. 1 S. 2 StVG insoweit auch anders als nach § 823 Abs. 1 BGB beweispflichtig.²⁷ Das Eigeninteresse entfällt wie zuvor, wenn die Zurechnung eigenen Fehlverhaltens im Raum steht.

d) Zwischenergebnis

Weder beim Hersteller noch beim Halter oder Fahrer kann überzeugend ein eigenes Interesse bzw. eine Verfolgung eigener Zwecke durch die Datenspeicherung begründet werden. Trotz Ambivalenz kann am ehesten ein Eigeninteresse des Fahrers bestehen, um sich zu exkulpieren; beziehungsweise des Halters, um Regressansprüche erfolgreich durchzusetzen.

2. Entscheidungsbefugnis über die Mittel

Fraglich ist, ob einer der genannten Akteure über die „Art und Weise“, d.h. die Modalitäten der Verarbeitung entscheiden kann. Dies erscheint für den Fahrer selbst derzeit ausgeschlossen, da nach aktuellen Konzepten der FMS durch diesen nicht deaktiviert oder sonst beeinflusst werden kann.

a) Hersteller

Hier bestehen insoweit Zweifel, als nach § 63b Nr. 1 StVG insbesondere die „technische Ausgestaltung und der Ort des

Speichermediums²⁸ sowie die „Art und Weise der Speicherung“ bereits durch Rechtsverordnung vorgegeben werden soll. Sollte die RVO hier allerdings nur grobe Vorgaben bzw. Leitlinien enthalten, könnte freilich wieder ein gewisser Entscheidungsspielraum auf Seiten des Herstellers entstehen. Dies erscheint aber aufgrund des umfassenden Katalogs der Norm bislang eher unwahrscheinlich. In § 63a Abs. 4 StVG ist darüber hinaus auch die Löschfrist und damit die Dauer der Datenverarbeitung festgeschrieben. Ein verbleibender Entscheidungsspielraum ist insoweit kaum mehr ersichtlich – wenn auch nicht ausgeschlossen.

b) Halter

Die Entscheidungsmöglichkeiten des Halters begrenzen sich auf eine Auswahlentscheidung. Inwiefern hier ein signifikanter Einfluss auf Mittel der Datenverarbeitung genommen werden kann, ist auch aus den folgenden Gründen fraglich: Obwohl das Datenschutzrecht an Produkthersteller, die nicht Verantwortliche sind, keine unmittelbaren Designanforderungen stellt, werden die Vorgaben zum FMS Bestandteil des Zulassungsrechts sein. So dürften die §§ 63a f. StVG wenn auch nicht ausdrücklich, so doch zumindest implizit die Pflicht enthalten, entsprechende Fahrzeuge mit den zur Erfüllung der Speicherpflicht erforderlichen Instrumenten auszustatten,²⁹ die den Anforderungen der Verordnung nach § 63b Nr. 1, 3 StVG entsprechen. Außerdem beschränkt § 1a Abs. 3 i.V.m. Abs. 1 StVG die Zulassungsfähigkeit automatisierter Fahrzeuge auf solche, die die UNECE-Regelungen einhalten bzw. eine entsprechende Typgenehmigung nach Art. 20 der RL 2007/46/EG erhalten haben.³⁰ Im Ergebnis kann der (potenzielle) Halter dann nur solche Fahrzeuge erwerben, deren FMS auch zulassungsrechtskonform arbeitet. Ihm verbleibt daher faktisch keine große Entscheidungsbefugnis über das Datenschutzniveau – sofern die RVO erschöpfend ist. Im Übrigen entzieht sich den Erwerbenden von Fahrzeugen regelmäßig bereits die Kenntnis der Datenverarbeitungsvorgänge im Fahrzeug.³¹

23 Vgl. § 823 Abs. 1 BGB, § 1 Abs. 1, Abs. 4 S. 1 ProdHaftG. Dies gilt ebenso bei vertraglichen Ansprüchen.

24 Dies gilt unabhängig davon, ob Fahrer oder System für den Unfall verantwortlich sind, vgl. auch Schmid/Wessels, NZV 2017, 357 (360). Es bestehen lediglich Ausschlussstatbestände in § 7 Abs. 2, 3 StVG, höhere Gewalt und Entwendung des Fahrzeugs. Vgl. zur Halterhaftung bei (teil)automatisierten Fahrzeugen ausführlich: Buck-Heeb/Dieckmann, in: Oppermann/Stender-Vorwachs „Autonomes Fahren“, 2. Aufl. 2020, S. 143 ff.

25 Schmid/Wessels, NZV 2017, 357 (360).

26 Vgl. BT-Drs. 18/11300, S. 24.

27 Vgl. Greger, NZV 2018, 1 (1); BHHJ/Heß, 25. Aufl. 2018, StVG § 18 Rn. 8 f.

28 Diskutiert wird neben der Speicherung im Fahrzeug das Modell eines Datentreuhänders sowie eine Speicherung auf den Backend-Systemen der Hersteller; siehe hierzu: Brockmeyer, ZD 2018, 258 ff., der sich im Ergebnis für eine lokale Speicherung im Fahrzeug ausspricht.

29 Schmid/Wessels, NZV 2017, S. 357 (359); entscheidend wird es darauf ankommen, wie konkret die geplante RVO ausfallen wird. Sofern nur grundsätzliche Zielsetzungen definiert würden, deren technische Umsetzung auf unterschiedlichen Wegen vorstellbar sind, wird es der Hersteller sein, der über die entsprechenden Hard- und Softwarekonfigurationen entscheidet.

30 Zum möglichen Konflikt mit dem europäischen Zulassungsrecht siehe: Lutz DAR 2019, 125 (126 f.).

31 In diese Richtung zum Fahrzeugführer auch: BeckOK StVR/Will StVG § 63a Rn. 9a.

3. Zwischenfazit

Fahrer und Halter haben zwar am ehesten ein Eigeninteresse an der Funktionalität des FMS, allerdings fehlt ihnen tatsächlich jede Einflussmöglichkeit auf technischer Ebene. Diese ist eher beim Hersteller anzusiedeln, wobei ihm wiederum ein positives Eigeninteresse fehlt. Im Gesamtergebnis lässt sich damit allein nach den Kriterien der DS-GVO die Verantwortlichkeit nicht sicher bestimmen.

V. Gesetzliche Zuweisung der Verantwortlichkeit nach §§ 63a, 63b StVG

Allerdings könnte in den §§ 63a, 63b StVG eine Zuweisung der Verantwortlichkeit i.S.d. Art. 4 Nr. 7 Hs. 2 DS-GVO enthalten sein. Voraussetzung ist, dass Zweck und Mittel der Verarbeitung durch das nationale Recht vorgegeben sind sowie das Vorliegen einer Öffnungsklausel für die mitgliedstaatliche Regelung, bspw. über Art. 6 Abs. 1 S. 1 lit. c oder e i.V.m. Art. 6 Abs. 3 DS-GVO.³² In Frage käme die Annahme einer Verarbeitung im öffentlichen Interesse.³³ Die Regelung muss zusätzlich im angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen. Bedenken bestehen hinsichtlich der Speicherdauer. Denn nur im Falle eines Unfallereignisses besteht ein Grund die Daten des letzten Fahrzeugsteuerungswechsels vor dem Unfall dauerhaft zu speichern.³⁴ Dieser Aspekt soll an dieser Stelle aber nicht betrachtet werden.

Geht man davon aus, dass eine mitgliedstaatliche Regelung wie § 63a StVG DS-GVO-konform zulässig wäre, kann festgehalten werden, dass der Zweck (Beweissicherung) bestimmt wurde und Mittel (technische Ausgestaltung / Art und Weise der Speicherung) per RVO festgelegt werden sollen. Ebenso soll der Adressat der Speicherpflicht benannt werden. Ob die exekutive Bestimmung des datenschutzrechtlich Verantwortlichen in Verbindung mit einer wie hier zwingenden Datenerhebung im Sinne des Wesentlichkeitsgebots³⁵ verfassungsrechtlich zulässig ist, soll in diesem Aufsatz ebenfalls dahingestellt bleiben.

Fraglich ist aber jedenfalls, welcher Gestaltungsspielraum dem BMVI bei der Zuweisung der Verantwortlichkeit noch offensteht. Insoweit steht das BMVI vor der Herausforderung, eine Lösung finden zu müssen, die sowohl mit den Festlegungen in §§ 63a ff. StVG als auch mit den datenschutzrechtlichen Pflichten des Verantwortlichen nach DS-GVO ein kohärentes Ergebnis bildet. Schließlich gilt es weitere verfassungsrechtliche Aspekte zu beachten.

Die Frage der Verantwortlichkeit bleibt in der Gesetzesbegründung ausdrücklich offen, soweit es heißt: „Die Verpflichtung zur Übermittlung der Daten trifft den Datenverantwortlichen.“³⁶ Damit brachte die Bundesregierung in ihrem Entwurf aber zumindest zum Ausdruck, dass ihres Erachtens ein vom Fahrer zu unterscheidender Datenverantwortlicher regelmäßig gegeben ist. Dagegen erkannte der Bundesrat, dass es noch einer Klärung, wen die Speicherpflicht treffen sollte, bedarf, und nannte insoweit auch den Fahrzeugführer.³⁷ Unter Berücksichtigung dessen hat der Ausschuss für Verkehr und digitale Infrastruktur daraufhin in § 63b Nr. 2 StVG die final auch übernommene Verordnungsermächtigung an das BMVI vorgeschlagen. Zur Begründung wird

insoweit ausgeführt, dass die Anforderungen an den Datenspeicher in internationalen Vorgaben festgelegt werden³⁸ und diese so ins nationale Recht eingeführt werden können.³⁹

1. Historie des § 63a Abs. 2 Satz 1 StVG

Erste Anhaltspunkte hinsichtlich der Verantwortlichkeit könnten sich aus der historischen Entwicklung des § 63a Abs. 2 S. 1 StVG ergeben. Diese Vorschrift regelt die Übermittlung der nach Abs. 1 erhobenen Daten an die nach Landesrecht für die Ahndung von Verkehrsverstößen zuständige Behörde und adressiert damit zwangsläufig ebenfalls den datenschutzrechtlich Verantwortlichen, denn eine isolierte Verantwortlichkeit für Speicherung oder Übermittlung derselben Daten erscheint kaum denkbar.

a) Ursprüngliche Entwurfsfassung

Ursprünglich als Verpflichtungsnorm⁴⁰ ausgestaltet, konnte die Norm einerseits so verstanden werden, dass die Vorschrift eine gesetzliche Schranke der informationellen Selbstbestimmung⁴¹ setzt, die den Fahrer selbst zur Preisgabe der ihn betreffenden Daten zwingt. Andererseits denkbar war, dass sie eine Übermittlungspflicht nach Art. 6 Abs. 1 lit c) DS-GVO an den „Datenverantwortlichen“ richtet und damit für den Hersteller, einen vom Fahrer personenverschiedenen Halter oder einen Dritten (z.B. Treuhänder) die Verantwortlichkeit indiziert. Trotz anders intendierender Gesetzesbegründung war nach diesem Wortlaut auch eine Festlegung des Fahrers grundsätzlich möglich.

b) Empfehlung des Ausschusses für Verkehr und Digitale Infrastruktur

In der endgültigen Fassung wurde Satz 1 auf Empfehlung des benannten Ausschusses nun jedoch als Befugnisnorm ausgestaltet.⁴² Eine unmittelbare Anwendung auf den Fahrer erscheint hier denklösig ausgeschlossen, da es keiner Befugnis bedarf, über die ihn betreffenden Daten verfügen zu „dürfen“.

32 Gola, in: Gola, DS-GVO, 2. Aufl. 2018, DS-GVO Art. 4 Rn. 55.

33 Befürwortend: Lutz DAR 2019, 125 (126), Schmidt/Wessels, NZV 2017, 357 (364).

34 Verbraucherzentrale Bundesverband, Rechtssicher fahren mit automatisierten Fahrzeugen (2017), S. 6.

35 Maunz/Dürig/Scholz, 87. EL März 2019, GG Art. 12 Rn. 324; BVerfG 33, 125 (157); vgl. zu den zulässigen Rechtssetzungsformen im Rahmen der DS-GVO: BeckOK Datenschutz/Albers/Veit, 30. Ed. 01.11.2019, DS-GVO Art. 6 Rn. 58.

36 BT-Drs. 18/11300, S. 25; BR-Drs. 69/17, S. 18; als Antwort auf die Kritik des Bundesrats an dieser Unbestimmtheit antwortete die Bundesregierung, dass eine abschließende Festlegung des „Datenverantwortlichen“ als Adressat zum Zeitpunkt noch nicht möglich war, BT-Drs. 18/11534, S. 16.

37 BT-Drs. 18/11534, S. 8.

38 Vgl. Diskussion zur UNECE-Regelung zu Data Storage Systems for Automated Driving (DSSAD, Dokumente abrufbar unter: <https://wiki.unece.org/pages/viewpage.action?pageId=92012869>).

39 BT-Drs. 18/11776, S. 12.

40 „Die gemäß Abs. 1 aufgezeichneten Daten sind den nach Landesrecht für die Überwachung des Straßenverkehrs zuständigen Behörden auf deren Verlangen zu übermitteln.“

41 Auf EU-Ebene dem Datenschutzgrundrecht nach Art. 8 GRC.

42 BT Drs. 18/11776, S. 3, 11.

Mit der Schaffung einer Befugnisnorm folgte der Gesetzgeber dem durch das BVerfG vorgegebenen Doppeltürmodell,⁴³ wonach die Übermittlungsbefugnis und die Erhebungsbefugnis jeweils eigenständige normative Ermächtigungen voraussetzen.⁴⁴ Die entsprechende Erhebungsbefugnis besteht bei Verkehrsverstößen nach StPO bzw. OWiG.⁴⁵ Ob indes eine gesonderte Übermittlungsbefugnis in der StVG erforderlich war, ist zweifelhaft. Teilweise wird vertreten, dass bereits § 95 StPO die entsprechende Übermittlungsbefugnis enthalte und daher im Zusammenspiel mit § 94 StPO eine entsprechende „Doppeltür“ bilde.⁴⁶

Insgesamt lässt sich zwar bei diesem Hintergrund der Anpassung noch nicht zwingend schlussfolgern, dass der Gesetzgeber die Norm hinsichtlich des Adressaten bewusst reduziert hat. Im Übrigen ist denkbar, dass die Norm schlicht nur Fälle regeln soll, in denen ein vom Fahrer abweichender Verantwortlicher besteht, ohne dass dies durch die Norm als zwingend präjudiziert wird. Gleichwohl spricht der finale Wortlaut nun gegen den Fahrer.

2. Übermittlungspflicht nach § 63a Abs. 3 StVG

§ 63a Abs. 3 StVG enthält einen materiell-rechtlichen Auskunftsanspruch am Unfall beteiligter Personen (Dritte).⁴⁷ Auf Drängen des Ausschusses für Verkehr und digitale Infrastruktur wurde die ursprüngliche Fassung dahin geändert, dass der Fahrzeughalter explizit genannt wird.⁴⁸ Damit wird anders als in § 63a Abs. 2 der Normadressat ausdrücklich festgesetzt.

An der Bestimmung wurde kritisiert, dass die Regelung damit eine tatsächliche Zugriffsmöglichkeit durch den Halter vorsehe.⁴⁹ Dies ergibt sich aus dem Wortlaut indes nicht. Der Halter hat nach § 63a Abs. 3 StVG lediglich die Übermittlung an Dritte „zu veranlassen“. Diese indirekte Formulierung spricht eher dafür, dass der Halter selbst keinen tatsächlichen Zugang zu den Daten haben muss, sondern eine andere Person, z.B. den Hersteller, zur Übermittlung anweist oder zumindest auf die Mitwirkung einer weiteren Person wie etwa einer den Onboard-Speicher auslesenden Kfz-Werkstatt angewiesen ist.

Der Verpflichtete müsste das Vorliegen der Übermittlungsvoraussetzungen prüfen, wenn personenbezogene Daten an Dritte weitergeleitet werden. Auch hier wird kritisiert, der Halter sei für diese Prüfpflichten ungeeignet.⁵⁰ Dass der Hersteller geeigneter wäre, überzeugt allerdings nicht. Dieser wird regelmäßig keine Kenntnis von Unfällen haben und erst recht nicht von den Unfallbeteiligten. Der Halter hingegen ist entweder selbst Fahrer – dann droht keine datenschutzrechtliche Haftung – oder wird vom Fahrer über das Unfallgeschehen informiert.

Jedenfalls muss für die Bestimmung des Verantwortlichen beachtet werden, dass die Entscheidung für die Übermittlung nach § 63a Abs. 3 StVG explizit dem Halter zugewiesen ist und dieser somit eine wesentliche Rolle einnimmt.

3. Telos mit Blick auf den Speicherort

In engem Zusammenhang mit der Festlegung des Speicheradressaten steht die Bestimmung des Speicherorts, was ebenfalls durch RVO erfolgen soll (§ 63b Nr. 1 StVG). Um

das Regelungsziel zu erreichen, ist unter beiden Gesichtspunkten zu bedenken, welche der Rollen ein Interesse daran haben, die Datenaufzeichnung zu manipulieren, Daten vorzeitig zu löschen oder Informationen zweckentfremdend zu nutzen. Als mögliche Speicherorte werden insbesondere der Onboard-Speicher im Fahrzeug sowie das Backend-System des Herstellers oder bei einer vertrauenswürdigen Stelle (Treuhand – hierzu Kap. 6) diskutiert.⁵¹

a) Speicherung im Fahrzeug (Onboard)

Diese Lösung stärkt die „Datenhoheit“ des Fahrzeugbesitzers, d.h. desjenigen, der die Sachgewalt über das Fahrzeug ausübt, da ein Auslesen ohne dessen Kenntnis deutlich erschwert wird.⁵² Gleichzeitig erhöht sich die Gefahr der Manipulation durch den Fahrer, um in Haftungs- oder Strafprozessen eine Verursachung durch das Fahrsystem zu suggerieren.⁵³ Ein personenverschiedener Halter hätte hingegen kein Manipulationsinteresse, könnte allerdings die Daten zweckentfremdend nutzen, bspw. zur Erstellung von Bewegungsprofilen.

Problematisch sind somit weiterhin die Rückgabe des Fahrzeugs an den Halter,⁵⁴ sowie die Veräußerung⁵⁵ und der Diebstahl⁵⁶ des Fahrzeugs. Einer Manipulation kann zumindest entgegengewirkt werden, indem ausschließlich Lese- und keine Schreibrechte gewährt werden. Es verbleibt aber das Problem der Beseitigung des Fahrzeugs als Ganzes, etwa durch die genannte Veräußerung (ggf. auch ins Ausland) oder mutwillige Zerstörung.

b) Speicherung im Backend des Herstellers

Nicht zuletzt aufgrund dieser Schwierigkeiten bietet sich deshalb eine Speicherung in einem Backend-System an.⁵⁷ Beim Hersteller stellt sich hier allerdings die Problematik, dass im Haftungsfall kein Interesse desselben bestehen

43 BVerfG, Beschluss vom 24.01.2012 – 1 BvR 1299/05, NJW 2012, 1419 (1422 f.).

44 BT-Drs. 18/11776, S. 11, Lutz DAR 2019, 125 (127); Schmidt/Wessels, NZV 2017, 357 (360).

45 BT-Drs 18/11776, S. 11, demnach ergibt sich die Erhebungsbefugnis aus § 94 StPO, der über § 46 Abs. 2 OWiG auch für Ordnungswidrigkeiten anwendbar ist.

46 Hoeren/Sieber/Holznel, MMR-HdB, Teil 19.3 Strafprozessrecht, Rn. 106.

47 BT-Drs. 18/11300, S. 25; Hoeren, NZV 2018, 153 (153).

48 BT-Drs. 18/11776, S. 3, vgl. auch BT-Drs. 18/11534, S. 6.

49 Hoeren, NZV 2018, 153 (154).

50 Hoeren, NZV 2018, 153 (154).

51 BT-Drs. 18/115234, S. 8; Hoeren, NZV 2018, 153 (153); Wagner/Goebel, NZV 2017, 263 (267); Brockmeyer, ZD 2018, 258 (258); Empfehlungen des 56. Deutschen Verkehrsgerichtstags 2018, NZV 2018, 69; Verbraucherzentrale Bundesverband, Rechtssicher fahren mit automatisierten Fahrzeugen (2017), S. 6; Vd TÜV, DEKRA, FSD, Gemeinsame Position zur Ausgestaltung des Fahrmodusspeichers (DSSAD), abrufbar unter https://www.vdtuev.de/dok_view?oid=749911.

52 Wagner/Goebels, NZV 2017, 263 (267).

53 Bei Datenverlust kommt es dann entscheidend auf die jeweilige Beweislastverteilung an.

54 Es sei denn, dieser ist personenidentisch mit dem Fahrer.

55 ADAC, Standpunkt Fahrmodusspeicher für automatisierte Fahrfunktionen (11.07.2019), abrufbar unter <https://www.adac.de/-/media/pdf/vek/fachinformationen/automatisierung-und-digitalisierung/fahrmodusspeicher-adac-sp.pdf>; Vd TÜV, DEKRA, FSD, Fn. 51, S. 2.

56 Vd TÜV, DEKRA, FSD, Fn. 51, S. 2.

57 Ebd.

dürfte, am Nachweis eines Systemversagens mitzuwirken. Ganz im Gegenteil kommt auch hier in Betracht, dass der Hersteller die Daten vorzeitig manipuliert bzw. löscht, um einem gegen ihn gerichteten Haftungsprozess die Beweisgrundlage zu entziehen. Daneben fehlt der Norm im Hinblick auf die Auskunftspflicht des Halters gegenüber Dritten eine Mitwirkungspflicht desjenigen, der Zugriff auf die Daten hat – sofern dies nicht der Halter selbst ist. Weiterhin ist zu bedenken, dass ein Unfallbeteiligter seine Ansprüche nach § 7 Abs. 1 StVG ohne Informationen aus dem FMS geltend machen kann.⁵⁸ Sofern kein Dritter einen Auskunftsanspruch geltend macht, liegt es im alleinigen Interesse des Halters, über die Datenaufzeichnung nachvollziehen zu können, ob System oder Fahrer für den Unfall verantwortlich waren. Erforderlich wäre dann ein Auskunftsanspruch zwischen Halter und Hersteller.

Die Speicherung auf einem Server führt zu einer wenigstens teilweisen Redundanz der Daten und dürfte damit dem Grundsatz der Datensparsamkeit zuwiderlaufen.⁵⁹ Dafür dürfte sich durch die Redundanz aber die Verfügbarkeit und Integrität der Daten als Teilaspekte der Datensicherheit erhöhen.⁶⁰ In jedem Fall bestehen bei einer externen Speicherung aber erheblich höhere Risiken einer zweckwidrigen Weiterverarbeitung oder eines Zugriffs Dritter. Schließlich ist in Deutschland eine dauerhafte Datenübermittlung gerade im ländlichen Raum nicht gesichert.

c) Minimierung des Manipulationsrisikos

Nur ergänzend soll an dieser Stelle noch darauf hingewiesen werden, dass der Ordnungsgeber unabhängig davon welchen der Beteiligten er auswählt, Maßnahmen treffen muss, damit dieser die Daten nicht manipulieren oder löschen kann. Im Ausgangspunkt sollten die Hersteller deshalb verpflichtet werden, die Systeme so zu bauen, dass diese manipulationssicher sind.⁶¹ Systeme sind allerdings zumeist nur so lange sicher, bis die Überwindung der eingesetzten Schutzmechanismen gelingt. Eine derartige Vorgabe müsste sich am jeweiligen Stand der Technik orientieren. Sofern die Manipulationssicherheit versagt, sollten zumindest Mechanismen bestehen, die nachvollziehbar darstellen, in welcher Instanz die Daten verändert wurden, auch wenn dies ggf. dem Grundsatz der Datenminimierung zuwiderläuft. Schließlich kann die Etablierung von Straf- oder Ordnungswidrigkeitstatbeständen bei vorzeitiger Löschung oder Manipulation Abschreckungswirkung entfalten.⁶² Als weitere Option wird die Einrichtung einer neutralen, hoheitlichen Treuhandstelle vorgeschlagen.⁶³

4. Zwischenfazit

Der finale Wortlaut des Abs. 2: „dürfen“ und die Adressierung des Halters in Abs. 3 sprechen jeweils gegen den Fahrer als Speicheradressaten. Ein stimmiges Konzept ergibt sich unter Berücksichtigung beider Absätze eher dann, wenn der Hersteller oder ein sonstiger Dritter die Daten als (Mit-)Verantwortlicher speichert. Dieser „darf“ (Erlaubnis im Verhältnis zum Betroffenen nach dem Doppeltürmodell) die Daten an die zuständigen Verkehrsbehörden übermitteln, ohne dass es zu einer Prüfung durch den Halter oder Fahrer

kommt. Im Falle eines Auskunftsanspruchs Dritter nach Abs. 3 entscheidet hingegen der Halter als sachnähere Person, ob die Übermittlungsvoraussetzungen vorliegen, und weist ggf. den Fahrzeughersteller bzw. sonstigen Dritten entsprechend zur Übermittlung an.

Hinsichtlich des Speicherortes birgt sowohl eine Speicherung im Verantwortungsbereich des Herstellers (Backend) als auch des Halters/Fahrers (Fahrzeug) jeweils unterschiedliche Risiken. Die Speicherung im Fahrzeug hat den Nachteil, dass die Datenverfügbarkeit an die physische Unversehrtheit des FMS gebunden ist; bei einer Speicherung im Backend des Herstellers besteht das Risiko der Manipulation durch denselben sowie einer zweckfremden Weiterverarbeitung.

Insgesamt lässt sich aus dem StVG daher noch keine klare Determination für eine der beteiligten Rollen ermitteln. Einziger Fahrer erscheint aus o.g. Gründen eher unpassend.

5. Einschränkung durch das Datenschutzrecht

An dieser Stelle soll untersucht werden, ob sich aus der DSGVO auch Gründe ergeben, die eine gesetzliche Zuweisung der Verantwortlichkeit an eine der genannten Rollen ausschließen. Eine exekutive Festlegung des Verantwortlichen darf diesem keine Pflichten auferlegen, die von diesem nicht umsetzbar sind. Der Pflichtenkanon folgt aus der DSGVO, wozu u.a. die Gewährleistung der Betroffenenrechte (Art. 12 ff. DSGVO), der Grundsatz des Privacy-by-Designs (Art. 25 Abs. 1 DSGVO) mit der wirksamen Umsetzung der Datenschutzgrundsätze und die Gewährleistung der Sicherheit nach Art. 32 DSGVO zählen. All dies setzt aber voraus, dass zumindest ein Verantwortlicher auch tatsächlich Einsichts- und Steuerungsmöglichkeiten hinsichtlich der Verarbeitung innehat. Liegen diese Voraussetzungen faktisch nicht vor, sollte eine Person folglich auch nicht als (alleiniger) Verantwortlicher bestimmt werden.

Folglich erscheint eine alleinige Verantwortlichkeit von Fahrer oder Halter ausgeschlossen. Im Falle einer Sicherheitslücke müsste etwa der Fahrzeugeigentümer (ggf. identisch mit Halter) vom Hersteller nach Gewährleistungsrecht ein Update herbeiführen bzw. erzwingen. Schlägt dies fehl, so müsste er das Fahrzeug stilllegen, da er dieses nicht mehr auf einem nach Art. 32 Abs. 1 DSGVO erforderlichen angemessenen Schutzniveau betreiben kann. Diese „Verantwortung“ auf den Halter abzuwälzen, erscheint zumindest wenig sachgerecht.⁶⁴ Denkbar wäre allenfalls eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO.

58 Da die Gefährdungshaftung verschuldensunabhängig ausgestaltet ist, kommt es nicht darauf an, ob sich das Risiko des automatisierten Systems oder ein Fehlverhalten des Fahrers in einem Unfall manifestiert hat, vgl. Wagner/Goebele, ZD 2017, 263 (268). Ein Interesse des Dritten, den Fahrer über § 18 StVG ebenfalls zu verklagen, kann darin bestehen dessen Zeugenstellung auszuschalten. Um das Prozesskostenrisiko gering zu halten, wäre eine Anfrage auf Datenübermittlung somit grundsätzlich denkbar, aber nicht zwingend erforderlich.

59 Brockmeyer, ZD 2018, 258 (261).

60 ADAC, Fn. 55; Vd TÜV, DEKRA, FSD, Fn. 51, S. 2.

61 Wagner/Goebele, NZV 2017, 263 (267).

62 Vgl. BT-Drs. 18/11534, S. 10.

63 Siehe hierzu: Kapitel VI.

64 Gegen eine datenschutzrechtliche Verantwortlichkeit von Privatpersonen ebenso: Conrad, DuD 2019, 563 (567).

6. Weitere verfassungsrechtliche Aspekte

a) Minimierung von Risiken für das Recht auf informationelle Selbstbestimmung

Schließlich muss der Ordnungsgeber die Verantwortlichkeit so festlegen, dass der Eingriff für den Betroffenen in sein Recht auf informationelle Selbstbestimmung möglichst gering ausfällt. Da private Stellen zu dieser Datenverarbeitung durch die StVG verpflichtet werden, kommt es insoweit nicht auf grundrechtliche Schutzpflichten an, vielmehr handelt es sich um einen staatlichen Eingriff,⁶⁵ der daher verhältnismäßig auszugestalten ist.

Insoweit ist die Frage des Speicheradressaten eng mit der Frage nach der Möglichkeit der Identifizierung verknüpft. Im Falle einer Identifikation ist es dem Verantwortlichen möglich, Bewegungsprofile durch die Kombination von Zeitpunkt und Positionsangabe zu erstellen.⁶⁶ Je häufiger ein Wechsel der Fahrzeugsteuerung erfolgt, desto aussagekräftiger kann dieses Profil ausfallen und den Eingriff entsprechend vertiefen. Folglich sollte der Adressat der Speicherpflicht so gewählt werden, dass dieser möglichst wenig Möglichkeiten hat, den Betroffenen tatsächlich zu identifizieren. Umgekehrt ist zur Bestimmung der Datenschutzrisiken entscheidend, welche Rolle die „betroffene Person“ ist.

Sind Fahrer und Halter identisch, würden die Risiken der Datenverarbeitung höher ausfallen, wenn Hersteller oder sonstiger Dritter die Daten (ggf. auch fahrzeugextern) speichern. Über eine Halterabfrage ließe sich leicht die Identität ermitteln. Eine Speicherung Onboard im Hoheitsbereich des Halters wäre hier eindeutig vorzugswürdig.

In der eingangs beschriebenen Dreieckskonstellation aus Hersteller, Halter und Fahrer hingegen, wäre die Identität des Fahrers zunächst dem Halter bekannt – nicht unbedingt jedoch dem Hersteller oder einem Dritten (bspw. bei Miet- oder Dienstfahrzeugen). Könnte der Arbeitgeber als Halter die FMS-Daten frei auslesen, wäre ggf. eine heimliche Leistungskontrolle möglich.⁶⁷ In dieser Konstellation wäre die Speicherung fahrzeugextern außer Reichweite des Halters günstiger.

b) Nemo Tenetur

Grundsätzlich darf niemand gezwungen werden sich selbst zu belasten.⁶⁸ Pflichten zur Mitwirkung an der Aufzeichnung von potentiell selbstbelastenden Informationen sind allerdings verfassungsrechtlich nicht grundsätzlich unzulässig.⁶⁹ Bekannte Beispiele sind Fahrtenbuch oder Fahrtenschreiber.⁷⁰ Ausgehend von den hier untersuchten Varianten des Herstellers, Halters oder Fahrers als Adressat der Speicherpflicht gilt jedoch folgendes festzuhalten: sofern Halter und Fahrer personenidentisch sind, könnten sowohl Hersteller als auch Halter und Fahrer durch die Speicherung zur eigenen Belastung beitragen: für alle kann sich die Information positiv entlastend oder negativ belastend auswirken und mögliche Straf-/Haftungsprozesse nach sich ziehen. Dies spricht eher für die Wahl einer neutralen Instanz, die Zugriffsrechte unter Berücksichtigung datenschutzrechtlicher Vorgaben verwaltet.

7. Fazit

Bereits die Auslegung der StVG sprach gegen den Fahrer als Adressaten; auch zeigte sich, dass er den Pflichten eines Verantwortlichen nicht sinnvoll gerecht werden kann. Schließlich besteht bei dann gleichzeitig naheliegender onboard-Speicherung ein hohes Risiko der nachträglichen Datenvernichtung.

Indes begegnet es auch Bedenken, den Halter als allein Verantwortlichen zu bestimmen: Insbesondere soweit es um die Gewährleistung der Sicherheit und datenschutzkonformen Technik nach Art. 32, 25 DS-GVO geht, ist er kaum geeigneter als der Fahrer selbst. Allerdings ist er nach § 63a Abs. 3 StVG ausdrücklich für die Entscheidung der Übermittlung an Dritte bestimmt worden.

Es bietet sich daher eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO von Halter und Hersteller an. Die Rechte und Pflichten untereinander lassen sich dabei auch durch die RVO bestimmen.⁷¹ Allerdings kann der Halter nur dann sinnvoll mitadressiert werden, wenn Halter und Fahrer auseinanderfallen und die Überlassung nicht in nur in einem persönlichen oder familiären Kontext erfolgt.⁷² Dies ist insbesondere bei Miet- oder Firmenwagen denkbar, so dass hier die entsprechenden Unternehmen als Mitverantwortliche bestimmt werden können. Hinsichtlich der Betroffenenrechte hat dies den Vorteil, dass der Fahrer diese dann gegenüber seinem Arbeitgeber oder dem Mietwagenunternehmen ausüben kann und nicht auf den Hersteller angewiesen ist, zu dem er selbst keine Rechtsbeziehung unterhält.

Die Mitverantwortlichkeit des Herstellers ist gleichwohl nicht unproblematisch. Trotz einer möglichen Reduktion der Missbrauchsrisiken durch das Vier-Augen-Prinzip im Rahmen einer gemeinsamen Verantwortlichkeit kann kaum ausgeschlossen werden, dass der Hersteller den Fahrer durch die Aggregation mit Daten aus Zusatzdiensten identifiziert und diese Daten unbefugt weiterverarbeitet. Auch ist der Hersteller, wie gezeigt, nicht frei von dem Verdacht, Daten im Eigeninteresse zu löschen oder zu manipulieren.

Da damit aus den verschiedenen, dargestellten Gründen kein Akteur bedenkenlos geeignet ist, wird teilweise die Einführung eines neuen Akteurs, nämlich eines sog. Datentreuhänders gefordert.⁷³ Der Treuhänder würde – anstelle

65 Schantz/Wolff, Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen, Rn. 153, beck-online; BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08 u.a., NJW 2010, 833 (836), Rn. 193.

66 Wagner/Goebele, NZV 2017, 263 (267). Dagegen soll das DSSAD es nicht erlauben, ein Fahrprofil zu erstellen: BMVI, EDR & DSSAD – Current understanding, EDR-DSSAD-03-05, S. 16, abrufbar unter <https://wiki.unece.org/pages/viewpage.action?pageId=92012869>.

67 Ggf. bedürfte ein solches System dann der Zustimmung des Betriebsrats nach § 87 Abs. 6 BetrVG.

68 Wagner/Goebele, ZD 2017, 263.

69 Schmid/Wessels, NZV 2017, 357 (360); Lutz DAR 2019, 125 (126); vgl. auch Schlanstein NZV 2016, 201 (203) zur Forderung eines Unfalldatenspeichers.

70 BVerfG, Beschl. v. 07.12.1981 – 2 BvR 1172/81 – NJW 1982, 568.

71 Auch wenn unter den Voraussetzungen des Art. 4 Nr. 7 Hs. 2 DS-GVO im Singular nur „der Verantwortliche“ normativ bestimmt werden darf, spricht viel dafür, dass dies auch für mehrere gemeinsame Verantwortliche gilt.

72 Siehe oben, Abschnitt 3 a.E.

73 Vd TÜV, DEKRA, FSD, Fn. 51; kritisch Brockmeyer, ZD 2018, 258.

des Herstellers – das Backend-System betreiben, das die vom Fahrzeug übermittelten Daten speichert, verwaltet und ggf. auf Behördenanforderung (§ 63a Abs. 2) oder Anweisung des Halters (§ 63a Abs. 3 StVG) weiterleitet.

VI. Treuhand

Das Treuhandmodell fußt auf dem Gedanken, dass eine zugangsoffene, diskriminierungsfreie Plattform zur Verfügung stehen sollte, deren Betreiber weder ein Eigeninteresse an den Daten selbst noch an deren Manipulation hat und Auskunftsanfragen professionell entsprechen kann.⁷⁴ Präferiert man ein Treuhändermodell, gilt es zu bedenken, dass zur Wahrung der erforderlichen Neutralität diese Rolle frei von Sachzwängen und Eigeninteressen sein müsste, wofür eine Eigenfinanzierung ein wesentlicher Baustein wäre.⁷⁵

Im Hinblick auf die technische Umsetzbarkeit wird kritisiert, dass die Einbindung eines Treuhänders aufgrund der Menge der im automatisierten Fahrzeug anfallenden Daten nicht sach- und zeitgerecht erfolgen könne.⁷⁶ Zudem wird die durchgehende Gewährleistung der Daten- und IT-Sicherheit erschwert, da die Onboard-Einrichtung (Hersteller) und das Backend (Treuhand) nicht mehr von derselben Person betrieben werden. Insoweit ist aber möglicherweise auch eine Konstruktion der Auftragsdatenverarbeitung denkbar, welche nach Art. 28 Abs. 3 DS-GVO auch gesetzlich ausgestaltet werden könnte. Ebenso möglich wäre die Annahme einer gemeinsamen Verantwortlichkeit zwischen Halter bzw. Hersteller und Treuhand. Dass der Hersteller an der tatsächlichen Durchführung der Verarbeitung dann nicht mehr direkt beteiligt wäre, hindert die Einordnung als Verantwortlichen nach der weiten Definition nicht.⁷⁷

Da eine solche Instanz bislang aber nicht existiert, müsste sie neu geschaffen werden. In Betracht kommt insoweit die Einrichtung einer neuen hoheitlichen Stelle oder die Ausschreibung an eine private Institution. Es darf allerdings bezweifelt werden, dass die § 63a f. StVG hierfür eine taugliche Grundlage bieten. Es ist schon nicht erkennbar, dass der Gesetzgeber diese Datenverarbeitung überhaupt an sich ziehen wollte. Jedenfalls stellt § 63b Nr. 2 StVG keine hinreichende Ermächtigungsgrundlage dar, auf Basis derer das BMVI eine entsprechende Aufgabenzuweisung an eine Behörde vornehmen oder diese Treuhandaufgabe ausschreiben dürfte. Vielmehr erscheint es naheliegend, dass diese Vorschrift lediglich die Bestimmung eines Adressaten aus den bestehenden Akteuren zulassen sollte.

VII. Ausblick

Insgesamt ist an der Konzeption des FMS zu kritisieren, dass eine Datenspeicherungspflicht statuiert wird, ohne dass die Verantwortlichkeit klar mitgeregelt wird. Wie gezeigt wurde, sind hierfür nämlich verschiedenste rechtliche und tatsächliche Implikationen zu berücksichtigen. Darüber hinaus stellt sich das hier nicht thematisierte Problem der Speicherdauer. Insofern ist offen, ob § 63a StVG in seiner aktuellen Form überhaupt mit den Grundsätzen der DS-GVO und den Verbürgungen der Da-

tenschutzgrundrechte vereinbar ist. Die Entscheidung über die konkrete Ausrüstung von Fahrzeugen mit dem FMS wird ohnehin auf Ebene der UNECE-Regelungen getroffen werden, an denen sich eine Regelung im StVG oder per Rechtsverordnung orientieren muss.⁷⁸

Aus wissenschaftlicher Sicht stellt sich die Einführung des FMS indes als spannendes Phänomen dar, dass verschiedene Rechtsgebiete (Datenschutzrecht, Haftungsrecht, Straf- und Ordnungswidrigkeitenrecht) miteinander verschränkt. Dabei besteht eine gewisse Ähnlichkeit mit der Vorratsdatenspeicherung von TK-Daten, die gerade erneut Gegenstand eines Verfahrens am EuGH ist:⁷⁹ In beiden Fällen werden privaten Stellen Speicherpflichten zum Zwecke der Informationsbeschaffung im öffentlichen Interesse auferlegt; darüber hinaus beim FMS auch zur Verfolgung private Beweisinteressen (§ 63a Abs. 3 StVG). Spannend ist an dieser Gegenüberstellung insbesondere, ob ungeachtet des Datenumfangs eine anlasslose Speicherung aus den im StVG genannten Zielen heraus grundrechtlich Bestand haben kann, wenn bereits eine anlasslose Speicherung zur Terrorabwehr zweifelhaft ist.



Christoph Werner

Akademischer Mitarbeiter am Zentrum für Angewandte Rechtswissenschaft des Karlsruher Instituts für Technologie in der Forschungsgruppe ITR mit Schwerpunkt im Datenschutz- und IT-Sicherheitsrecht.



Dr. Manuela Wagner

Wissenschaftliche Mitarbeiterin am FZI Forschungszentrum Informatik und Projektleitung in dem vom Land Baden-Württemberg geförderten Projekt Smart Mobility – Rechtliche Begleitforschung.



Maria Pieper

Wissenschaftliche Mitarbeiterin am FZI Forschungszentrum Informatik.

74 Brockmeyer, ZD 2018, 258 (259).

75 Hoeren, NZV 2018, 153 (154).

76 Ebd.

77 Vgl. Klabunde, in: Ehmann/Selmayr, 2. Aufl. 2018, DS-GVO Art. 4 Rn. 36; Spindler/Dalby, in: Spindler/Schuster Elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 4 Rn. 18.

78 Vgl. Lutz DAR 2019, 125 (127).

79 Campos Sánchez-Bordona, Schlussanträge vom 15.01.2020 – C-623/17; C-511/18; C-512/18; C-520/18.



**Datenschutz-
Wissen aus
erster Hand**

GDD-Datenschutz-Akademie goes digital:

Online-Schulungen für Ihre professionelle Weiterbildung

■ live ■ interaktiv ■ dialogorientiert

Alle digitalen Angebote finden Sie unter:
www.datakontext.com/online-angebote

Dr. iur. Hannes Berger

Das neue Sozialdatenschutzrecht

Anpassungen des Sozialgesetzbuches an die DS-GVO und aktuelle Rechtsprechung

Mit dem Inkrafttreten der Datenschutz-Grundverordnung musste auch der Datenschutz im deutschen Sozialrecht überarbeitet werden. Mittlerweile liegen nach einem zwei-

stufigen Reformprozess auch erste Gerichtsentscheidungen vor, die sich mit dem neuen Sozialdatenschutzrecht auseinandersetzen.

I. Einleitung

Ohne Informationen ist ein Handeln der Sozialverwaltung nicht möglich. Um zu wissen, welche Kosten für Krankenbehandlungen eine gesetzliche Krankenversicherung übernehmen muss, benötigt sie auch gewisse Angaben über die Krankheit des Versicherten und deren Behandlung; die Rentenversicherung benötigt für den Rentenbescheid Informationen über das zurückliegende Arbeitsleben einer Versicherten, und das Jobcenter muss für die Bewilligung von Leistungen zur Sicherung des Lebensunterhalts die Hilfebedürftigkeit der Antragstellenden prüfen. Da diese Daten über natürliche Personen im Rahmen des Sozialverwaltungsverfahrens oftmals persönlicher Natur und sensibler Art sind, kommt auch im Sozialrecht der Datenschutz zu einer immer größeren Bedeutung.¹ Dieser Beitrag hat das Ziel, nach einer kurzen Einführung in die europarechtlichen und verfassungsrechtlichen Grundlagen des Sozialdatenschutzrechts (II. 1.), die beiden umfangreichen Reformen des Sozialdatenschutzrechts aus den Jahren 2017 (II. 2.) und 2019 (II. 3.) in ihren wesentlichen Inhalten darzustellen und zu systematisieren. Darüber hinaus werden erste Entscheidungen des Bundessozialgerichts und zweier Landessozialgerichte, die aufgrund der neuen Rechtslage ergangen sind, an den entsprechenden inhaltlichen Ausführungen besprochen.

II. Neue Rechtsgrundlagen für den Sozialdatenschutz

Seit dem Mai 2018 besteht durch die Datenschutz-Grundverordnung (DS-GVO) ein neuer datenschutzrechtlicher Rahmen auf der Ebene des europäischen Rechts. Dessen Vorgaben binden das nationale Datenschutzrecht in weiten Teilen, weshalb es in der Folge zu umfassenden Reformen im nationalen Recht kam. Auch das bereichsspezifische Recht des Sozialdatenschutzes richtet sich nunmehr nach den Bestimmungen der DS-GVO,² wodurch nunmehr ein datenschutzrechtliches Mehrebenensystem auch im Sozialrecht vorherrscht.³ Die Rechtsvorschriften über den Datenschutz im Regelungsbereich des Sozialgesetzbuches wurden deshalb in einem ersten Schritt durch Gesetz vom 17. Juli 2017 novelliert.⁴ Dabei musste sich das Gesetzgebungsverfahren durchaus Kritik gefallen lassen. Unbeachtet von der Fachöffentlichkeit wurden die Änderungen im Sozialdatenschutzrecht erst im Laufe des Gesetzgebungsverfahrens zur Neuregelung des Bundesversorgungsgesetzes aufgenommen; eingeforderte Stellungnahmen von Datenschutzbeauftragten konn-

ten in der Kürze der Zeit nicht erstellt werden, und die letzte Abstimmung erfolgte im Bundestag ohne Aussprache nach Mitternacht, auch der Bundesrat kritisierte seine fehlende Beteiligung.⁵ Der zweite Reformschritt erfolgte erst kürzlich zum Ende des Jahres 2019 und nahm Änderungen an vielen Detailregelungen zum Datenschutz in den einzelnen Sozialgesetzbüchern vor.

1. Europarechtliche und verfassungsrechtliche Grundlagen

Das europäische Datenschutzrecht erstreckt seine Geltung auf alle Datenverarbeitungen, die im Anwendungsbereich des Unionsrechts liegen.⁶ Welche Materien vom Anwendungsbereich des Unionsrechts erfasst werden, ergibt sich aus den vertraglichen Kompetenztiteln der Europäischen Union.⁷ Die Sozialpolitik fällt gemäß Art. 4 Abs. 2 lit. b AEUV, Art. 48 AEUV und Art. 151-161 AEUV maßgeblich in die geteilte Zuständigkeit zwischen EU und den Mitgliedstaaten. Die europäische Sozialpolitik erstreckt sich, unter ständiger Anerkennung der Verschiedenheit der nationalen Sicherungssysteme, hauptsächlich auf unterstützende und ergänzende Maßnahmen der nationalen Sozialpolitiken, auf eine verstärkte Abstimmung der nationalen Sicherungssysteme bei grenzüberschreitender Beschäftigung sowie auf die Festlegung gewisser Mindeststandards.⁸ Eine Rechtsharmonisierung des nationalen Sozialrechts ist dabei gemäß Art. 153 Abs. 2 AEUV ausgeschlossen. Dementsprechend verbleiben auf dem Gebiet des Sozialrechts viele Kompetenzen bei den Mitgliedstaaten, die demzufolge nicht eindeutig in den Anwendungsbereich des Unionsrechts und somit auch nicht eindeutig in den Anwendungsbereich der DS-GVO

1 Vgl. Binne/Kremer, in: Ruland/Becker/Axer, Sozialrechtshandbuch, 2018, Rn. 1.

2 Vgl. Muckel/Ogorek/Rixen, Sozialrecht, 2019, 534; Shagdar/Freund, SGB 2018, 195; Freund/Shagdar, SGB 2018, 267.

3 Vgl. Waltermann, Sozialrecht, 2018, Rn. 667; ebenso LSG Bayern, Urteil vom 6. Juni 2019, L 7 R 5188/17 = BeckRS 2019, 14934, Rn 79.

4 BGBl. I 2017, 2541; BT-Drs. 18/12611, 101, 115; Hoidn/Roßnagel, DuD 2018, 487, 488; Bieresborn, NZS 2017, 887.

5 Dazu Hoidn/Roßnagel (o. Fn. 4), 488.

6 Mit Art. 2 Abs. 2 lit. a DS-GVO hat der europäische Gesetzgeber den Kompetenzrahmen des Art. 16 Abs. 2 AEUV zur Gänze ausgeschöpft und das Datenschutzrecht auf jegliche Verarbeitungen im Anwendungsbereich des EU-Rechts ausgeweitet.

7 Vgl. Schröder, in: Streinz/Michl, EUV/AEUV. Kommentar, 2018, Art. 16, Rn. 8; Klement, JZ 2017, 161, 165; von Lewinski, DuD 2012, 564, 565.

8 Vgl. Schaumberg, Sozialrecht, 2018, 48ff; Oppermann/Classen/Nettesheim, Europarecht, 2018, 498ff; Brox/Rüthers/Henssler, Arbeitsrecht, 2016, 38 f.

fallen.⁹ Um Klarheit bei der Anwendung des Datenschutzrechts in der Sozialverwaltung zu schaffen, hat der deutsche Gesetzgeber mit § 35 Abs. 2 SGB I entschieden, dass die Datenschutzvorschriften der DS-GVO und des Sozialgesetzbuches für alle datenverarbeitenden Tätigkeiten entsprechend angewendet werden sollen, unbenommen, ob sie im Anwendungsbereich liegen oder nicht.¹⁰ Dem folgen auch das Bundessozialgericht und das LSG Berlin-Brandenburg in jüngerer Rechtsprechung.¹¹ Der Bundesgesetzgeber verfolgte damit das Ziel, im Sozialrecht „entsprechend der bisherigen Regelungssystematik ein datenschutzrechtliches Vollregime“ anzubieten.¹²

Das neue Datenschutzrecht der DS-GVO und des angepassten SGB I und SGB X folgt grundsätzlich dem gleichen Datenschutzkonzept, wie es einst das Bundesverfassungsgericht mit seiner Rechtsprechung zu Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entwickelt hat: Eingriffe in das Recht auf informationelle Selbstbestimmung durch staatliche Stellen können nur aus Gründen des Allgemeinwohls und nur auf der Grundlage eines Gesetzes erfolgen.¹³ Die Grundsatznormen der DS-GVO, Art. 5 und 6, bestimmen ebenfalls, dass Datenverarbeitungen nur zulässig und rechtmäßig sein können, wenn sie sich insbesondere auf eine Einwilligung¹⁴ oder eine verhältnismäßige Rechtsgrundlage des europäischen oder des nationalen Rechts stützen können.¹⁵ Solche finden sich nunmehr an verschiedenen Stellen des Sozialgesetzbuchs.¹⁶ Dabei folgt das Sozialdatenschutzrecht der Systematik des Sozialgesetzbuchs, welches in allgemeine (vor allem SGB I, SGB X und SGB IV) und spezielle Bücher unterteilt ist.¹⁷ Die allgemeinen Bestimmungen des Sozialdatenschutzrechts gelten für das gesamte Sozialrecht und sind im SGB I und im SGB X geregelt. Daneben gibt es jedoch für jeden besonderen Bereich des Sozialrechts (z.B. Krankenversicherung, Rentenversicherung etc.) einzeln festgelegte Datenschutzvorschriften, die nur für das spezifische Buch gelten.¹⁸ Beispielsweise enthalten die §§ 50ff. SGB II spezielle Datenübermittlungsvorschriften, die jedoch ausschließlich im Recht der Grundsicherung für Arbeitslose Anwendung finden.

2. Erster Reformschritt: Neuregelung des Datenschutzes im SGB I und SGB X im Jahr 2017

Die für den Sozialdatenschutz einschlägigen Normen im SGB I und SGB X sind solche nationalen gesetzlichen Grundlagen für Beschränkungen des Datenschutzes im Sinne des Art. 6 DS-GVO auf dem Gebiet des Sozialrechts. Diese für das gesamte Sozialrecht geltenden Datenschutzbestimmungen wurden im Jahr 2017 reformiert, hier sollen sie in ihren Grundzügen erläutert werden.

a) Das Sozialgeheimnis

Zunächst findet sich im SGB I – Allgemeiner Teil – eine für das gesamte Sozialrecht übergreifende Datenschutznorm, die mit „Sozialgeheimnis“ überschrieben wird.¹⁹ Durch § 35 Abs. 1 S. 1 SGB I wird das Sozialgeheimnis als das zugrundeliegende Prinzip des Sozialdatenschutzes festgelegt. Dieses besagt, dass jeder über einen Anspruch darauf verfügt, dass

Sozialdaten von Leistungsträgern des Sozialrechts nicht unbefugt erhoben, verarbeitet oder genutzt werden dürfen.²⁰ Dies impliziert einerseits, dass es einen spezifischen Begriff der Sozialdaten gibt, der definiert und ausgelegt werden muss, und andererseits, dass Datenverarbeitungen im Sozialrecht zulässig sein können, solange diese auf einer Befugnis des Leistungsträgers beruhen. Sozialdaten dürfen dementsprechend nur verarbeitet werden, wenn eine Verarbeitungsbefugnis aus der DS-GVO oder aus dem SGB hervorgeht.²¹

Unter Sozialdaten²² werden personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO verstanden, die von einer in § 35 SGB I genannten Stellen im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden.²³ Sozialdaten werden also nicht inhaltlich definiert, etwa im Sinne von Daten, die die Gesundheit, eine Behinderung oder ähnliches betreffen, sondern sie definieren sich über die Stelle, die sie zur Erfüllung einer Aufgabe aus dem Sozialrecht verarbeitet.²⁴ Diese Stellen können u.a. sein die Kranken-, Pflege-, Renten-, Unfall-, Arbeitslosenversicherung, aber auch die Künstlersozialkasse, Zollbehörden oder die Deutsche Post AG, sofern sie sozialrechtliche Aufgaben erfüllen.²⁵

§ 35 Abs. 1 S. 2 SGB I bestimmt weiterhin, dass innerhalb der Leistungsträger sichergestellt werden muss, dass nur befugte Personen Zugang zu den Sozialdaten haben. Diese Norm lässt sich auch als organisatorische Datenschutzvorschrift begreifen. Konkretisiert wird dies noch durch § 35 Abs. 1 S. 3 SGB I, dem zufolge Personen, die Personalentscheidungen treffen oder daran mitwirken, keinen Zugang zu den Sozialdaten der Betroffenen und ihrer Angehörigen erhalten dürfen und auch nicht von Zugangsberechtigten weitergeleitet bekommen dürfen.²⁶

9 Vgl. Bieresborn (o. Fn. 4), 891.

10 Vgl. BT-Drs. 18/12611, S. 96 f.; Bieresborn (o. Fn. 4), 891.

11 Vgl. BSG, Urteil vom 18.12.2018, B 1 KR 40/17 R = BeckRS 2018, 42368, Rn. 29; LSG Berlin-Brandenburg, Urteil vom 30. April 2019, L 26 AS 2621/17 = BeckRS 2019, 9038, Rn. 20.

12 BT-Dr. 18/12611, S. 97.

13 Grundlegend dazu BVerfGE 65, 1, 43f; dazu auch Scholz/Pitschas, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, 1984; Schlink, Der Staat 25 (1986), 233-250.

14 Vgl. Bieresborn, NZS 2017, 926.

15 Vgl. Bieresborn (o. Fn. 14), 926; Kühling/Martini et al., Die Datenschutz-Grundverordnung und das nationale Recht, 2016, 27f.; Buchner, DuD 2016, 155, 159.

16 Vgl. Waltermann (o. Fn. 3), Rn. 669.

17 So auch BSG (o. Fn. 11), Rn. 24.

18 Vgl. Binne/Kremer (o. Fn. 1), Rn. 17.

19 Vgl. Hoidn/Roßnagel (o. Fn. 4), 487.

20 Vgl. Muckel/Ogorek/Rixen (o. Fn. 2), 534.

21 Vgl. Waltermann (o. Fn. 3), Rn. 668; Bieresborn (o. Fn. 4), 890.

22 Grundsätzlich ist das nationale Datenschutzrecht streng an die Terminologie der DS-GVO gebunden und darf etwa auch keine unbestimmten Rechtsbegriffe autonom definieren. Jedoch können Begriffe, die die DS-GVO nicht enthält, über die Öffnungsklausel des Art. 6 Abs. 2 und 3 DS-GVO beibehalten werden, weshalb der Begriff der Sozialdaten nach § 67 Abs. 2 SGB X auch nach der Reform Bestand hat, vgl. Bieresborn (o. Fn. 4), 889.

23 Vgl. Binne/Kremer (o. Fn. 1), Rn. 51.

24 Vgl. Hoidn/Roßnagel (o. Fn. 4), 487; „im Rahmen der Sozialverwaltung“.

25 Näher dazu § 35 Abs. 1 SGB I.

26 Vgl. Muckel/Ogorek/Rixen (o. Fn. 2), 535.

b) Sozialverwaltungsverfahren und Sozialdatenschutz

Neben den Vorschriften über das Sozialgeheimnis im SGB I enthält das SGB X – Sozialverwaltungsverfahren und Sozialdatenschutz – im Zweiten Kapitel weitergehende Vorschriften zum Datenschutz im Sozialrecht. Die §§ 67-85a SGB X enthalten für verschiedene Verarbeitungssituationen sowie über die Rechte der Betroffenen im Sozialverwaltungsverfahren bereichsspezifische Vorschriften.²⁷

c) Erhebung von Sozialdaten

Nach Begriffsbestimmungen, die in § 67 SGB X ergänzend zu jenen des Art. 4 DS-GVO eingeführt werden, wozu die wichtigste Definition jener der Sozialdaten ist, erklärt § 67a SGB X jede Erhebung von Sozialdaten nur für zulässig, wenn die Kenntnis der Daten zur Erfüllung einer Aufgabe der erhebenden Stelle erforderlich ist.²⁸ Eine solche Erhebung kann beispielsweise erforderlich sein für die Leistungsgewährung und die Unterstützung bei der Aufnahme einer Erwerbstätigkeit im Recht der Grundsicherung (Aufgaben gemäß § 1 Abs. 2 SGB II), für die die Voraussetzungen der Antragstellung (§ 37 Abs. 1 SGB II) und der Mitwirkung (§ 60 SGB I i.V.m. §§ 56 und 59 SGB II), verbunden mit den entsprechenden Angaben personenbezogener Daten, vorgesehen sind. Die Erhebung der Sozialdaten zur Erfüllung der gesetzlichen Aufgabe soll nach § 67a Abs. 2 S. 1 SGB X grundsätzlich bei den Betroffenen selbst erfolgen, womit das SGB X dem Transparenzgrundsatz des Art. 5 Abs. 1 lit. a DS-GVO folgt.²⁹ Die DS-GVO wirkt sich auf das Sozialdatenschutzrecht auch dergestalt aus, dass der Grundsatz der Datenminimierung und der Speicherbegrenzung aus Art. 5 Abs. 1 lit. c und e DS-GVO verwirklicht werden müssen. Dies heißt, dass die Sozialverwaltung mit möglichst wenigen und nur den notwendigen Daten ihre gesetzlichen Aufgaben erfüllen soll, was sich auch aus dem Effizienzgedanken des Sozialrechts gemäß § 17 Abs. 1 Nr. 1 SGB I ableiten lässt.³⁰

d) Verarbeitung und Übermittlung von Sozialdaten

Die Verarbeitung von Sozialdaten³¹ ist gemäß § 67b SGB X nur zulässig, wenn eine gesetzliche Grundlage oder eine hinreichende Einwilligung der Betroffenen vorliegt.³² Insofern sind besonders die Art. 6 und 9 DS-GVO von großer Bedeutung auch für die Arbeit der Sozialverwaltung.³³ Ebenfalls als Konkretisierung zur DS-GVO existieren in den §§ 67ff. SGB X mehrere Vorschriften, die die Übermittlung von Sozialdaten unter spezifischen Voraussetzungen erlauben.³⁴ Für die Rechtmäßigkeit der Datenübermittlungen legt § 67d Abs. 1 SGB X eine geteilte Verantwortlichkeit fest. Die übermittelnde Stelle trifft stets die Verantwortlichkeit, bei Übermittlungen auf Ersuchen durch eine andere Stelle trägt letztere die Verantwortlichkeit für die Richtigkeit der Angaben im Ersuchen.³⁵ Insbesondere sind hierzu erwähnenswert die Übermittlungen von Sozialdaten zur Bekämpfung von Leistungsmissbrauch gemäß § 67e SGB X, zur Erfüllung von Aufgaben von Gefahrenabwehrbehörden, Staatsanwaltschaften und Gerichten gemäß § 68 SGB X sowie zur Durchführung von Forschungsvorhaben im Sozialleistungsbereich und in der wissenschaftlichen Arbeitsmarkt- und Berufsforschung gemäß § 75 SGB X.³⁶

Besonders zur Frage der Rechtmäßigkeit von Datenübermittlungen im Sozialrecht hat es zuletzt mehrere Gerichtsentscheidungen gegeben, die die neuen Rechtsgrundlagen für die Praxis handhabbar gemacht haben, weshalb hier drei Urteile angesprochen werden sollen.

Zunächst hat das Bundessozialgericht in einem jüngeren Urteil erstmals zu diesen Fragen der Erhebung und Übermittlung von (sensiblen) Daten im neuen Datenschutzrecht Ausführungen getroffen. In dem konkreten Fall ging es um das Recht einer Krankenkasse, Einsicht in Behandlungsunterlagen eines Krankenhauses zu erhalten, um die Korrektheit der Behandlungsabrechnung prüfen zu können. Die Behandlungsunterlagen enthielten auch besondere Kategorien personenbezogener Daten, nämlich Gesundheitsdaten im Sinne des Art. 9 DS-GVO. In übergreifender Anwendung des Art. 9 DS-GVO, § 67b Abs. 1 S. 2 SGB X, § 301 SGB V befand das BSG, dass das Sozialdatenschutzrecht einer Übermittlung und einer Einsicht in Gesundheitsdaten in Behandlungsunterlagen durch eine Krankenkasse nicht entgegensteht.³⁷ Gerade auch die DS-GVO, so das BSG, kenne in Art. 9 Abs. 2 eine Ausnahme vom Verbot der Verarbeitung von besonderen Kategorien personenbezogener Daten, die für die Versorgung und Behandlung im Gesundheits- und Sozialbereich besteht.³⁸ Die Übermittlung und Einsicht einer Krankenkasse in Behandlungsunterlagen zum Zwecke der Abrechnungsprüfung und Verbesserung der Qualität und Wirtschaftlichkeit der Abrechnungsverfahren in Krankenversicherungssystemen sah das BSG unter Hinweis auf Art. 9 Abs. 2 DS-GVO sowie auf Erwägungsgrund 52 der DS-GVO als mit dem Datenschutzrecht konform an.³⁹

In einem weiteren Fall zog das BSG ebenfalls das neue europäische Datenschutzrecht als Rechtsgrundlage für Datenübermittlungen im Recht der gesetzlichen Krankenversicherung heran. Gemäß § 295 Abs. 2 SGB V haben Kassenärztliche Vereinigungen die Pflicht, im Wege der elektronischen Datenübertragung für jedes Quartal und für jeden Behandlungsfall eine Reihe von Sozialdaten zum Zwecke der Abrechnung der Vergütung an die Krankenkassen zu übermitteln. Nach einer Klage einer Kassen(zahn)ärztlichen Vereinigung gegen diese Übermittlungspflicht urteilte das BSG, dass § 295 Abs. 2 SGB V nicht gegen die DS-GVO ver-

27 Vgl. Bieresborn (o. Fn. 14), 927.

28 Vgl. Muckel/Ogorek/Rixen (o. Fn. 2), 535; Hoidn/Roßnagel (o. Fn. 4), 487.

29 Vgl. Bieresborn (o. Fn. 14), 927.

30 Vgl. Öndül, in: Schlegel/Voelzke, jurisPK-SGB I, 2018, § 17 SGB I, Rn. 23ff.

31 § 67b SGB X spricht hier von „Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung von Sozialdaten durch die in § 35 des Ersten Buches genannten Stellen“.

32 Vgl. Bieresborn (o. Fn. 14), 927f.

33 Vgl. Muckel/Ogorek/Rixen (o. Fn. 2), 535.

34 Vgl. Muckel/Ogorek/Rixen (o. Fn. 2), 536.

35 Vgl. Bieresborn (o. Fn. 14), 928.

36 Zur Forschung mit Sozialdaten siehe neben § 75 SGB X auch § 65c SGB V zum Datenaustausch über Krebsregister; weiterhin Spindler, MedR 2016, 691-699.

37 Vgl. BSG (o. Fn. 11), Rn. 23f.

38 Vgl. BSG (o. Fn. 11), Rn. 30.

39 Vgl. BSG (o. Fn. 11), Rn. 30.

stoße.⁴⁰ Zunächst ist interessant, dass das BSG die Regeln der DS-GVO heranzieht, obwohl der Rechtsstreit über die Pflicht zur Datenübermittlung bereits deutlich vor dem Inkrafttreten der DS-GVO (Mai 2018) entstanden war. Dass die DS-GVO trotzdem zur Beurteilung der Rechtslage heranzuziehen sei, begründete das BSG damit, dass seit dem Inkrafttreten der DS-GVO jede Verarbeitung von personenbezogenen Daten im Anwendungsbereich des Unionsrechts auch an der DS-GVO gemessen werden muss.⁴¹ Da die Verpflichtung zur Datenübermittlung nach § 295 Abs. 2 SGB V eine dauerhafte Rechtspflicht sei und da das BSG ein vollstreckbares Urteil über die Rechtmäßigkeit dieser Datenverarbeitung fälle, auf dessen Grundlage nach dem 24. Mai 2018 dann tatsächlich eine solche Datenverarbeitung stattfinden könnte, müsse das Urteil auch im Einklang mit den europäischen Vorgaben stehen.⁴² Im Weiteren sah das BSG die Anforderungen des Art. 9 Abs. 2 lit. h, Abs. 3 und Abs. 4 DS-GVO für die Verarbeitung von sensiblen Gesundheitsdaten im konkreten Fall als erfüllt an.⁴³ Das innerstaatliche Recht des § 67b Abs. 1 S. 3 und 4 SGB X sowie des § 295 Abs. 2 SGB V nutze die Öffnungsklausel zum Zwecke der Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich in zulässiger Weise, und eine Übermittlung von Abrechnungsdaten an die Krankenkassen sei demzufolge vom europäischen Datenschutzrecht gedeckt.⁴⁴

Das LSG Bayern hatte darüber hinaus im Juni 2019 zu klären, ob die Prüfverfahren gemäß § 212a SGB VI, die die Rentenversicherung bei den zur Beitragszahlung verpflichteten Stellen durchführt, datenschutzkonform sind.⁴⁵ Bei diesen Betriebsprüfungen untersucht die Rentenversicherung, ob die Stellen, die die Pflichtbeiträge für die in der Rentenversicherung versicherten Personen zahlen müssen, ihren Meldepflichten und Zahlungspflichten nachgekommen sind (§ 212a Abs. 1 SGB VI). Dazu haben die zahlungspflichtigen Stellen gemäß § 212a Abs. 3 SGB VI angemessene Prüfhilfen zu leisten, bei denen Sozialdaten zum Zwecke der Prüfung übermittelt werden. In dem der Entscheidung zugrundeliegenden Fall klagte der Freistaat Bayern (Bayerisches Landesamt für Finanzen) gegen die Rentenversicherung, da streitig war, inwiefern der Freistaat Bayern als zu prüfende Stelle verpflichtet war, Prüfhilfen an die Rentenversicherung zu gewähren.⁴⁶ Konkret ging es um die Einsichtnahme in Leistungsunterlagen von beihilfeberechtigten Pflegebedürftigen.⁴⁷ Das LSG befand, dass die Datenverarbeitungen im Rahmen der Prüfung gemäß § 212a SGB VI datenschutzkonform seien.⁴⁸ Die Erhebung der Daten stünde im Einklang mit den Vorgaben der Art. 6 und 9 DS-GVO i.V.m. § 67a SGB X, da sie auf das für die rentenversicherungsrechtliche Betriebsprüfung Erforderliche beschränkt sei.⁴⁹ Die Prüfungen zielten auf die Funktionsfähigkeit und finanzielle Stabilität der Sozialversicherung ab, wodurch ein überragend wichtiger Gemeinwohlbelang verfolgt würde, weshalb die entsprechenden Datenverarbeitungen von Art. 6 und Art. 9 Abs. 2 lit. b und j DS-GVO gedeckt seien.⁵⁰

e) Zweckbindung und Zweckänderung

Durch § 67c Abs. 1 SGB X wird der Zweckbindungsgrundsatz aus Art. 5 Abs. 1 lit. b DS-GVO, wonach Datenverarbeitun-

gen nur zu den vorher eindeutig festgelegten Zwecken vorgenommen werden dürfen, auch für das Sozialrecht übernommen.⁵¹ Der Zweckbindungsgrundsatz wird für deutsche Sozialverwaltungsbehörden zudem noch um den Grundsatz der Gesetzmäßigkeit der Verwaltung ergänzt, der eine Bindung der Sozialleistungsträger an die gesetzlich festgelegten Aufgaben bei den Datenverarbeitungen verlangt.⁵² Wie es auch die DS-GVO in Art. 6 Abs. 4 erlaubt, so hat der Bundesgesetzgeber auch für das Sozialdatenschutzrecht die Möglichkeit geschaffen, eine zweckändernde Verarbeitung, das heißt eine Datenverarbeitung zu anderen Zwecken als zu den ursprünglichen Erhebungszwecken, zuzulassen. Eine zweckändernde Verarbeitung von Sozialdaten ist gemäß § 67c Abs. 2 Nr. 1 SGB X nur zulässig, wenn die Daten für andere Aufgaben desselben Leistungsträgers, die sich ebenfalls aus dem Sozialgesetzbuch ergeben, erforderlich sind.⁵³ Dadurch soll vor allem die doppelte Datenerhebung durch die Sozialverwaltung vermieden werden, da die Erhebung von Sozialdaten zur sozialrechtlichen Aufgabenerfüllung ohnehin gemäß § 67a SGB X zulässig ist.⁵⁴ Eine zweckändernde Datenverarbeitung im Sozialrecht ist gemäß § 67c Abs. 2 Nr. 2 SGB X außerdem zulässig, wenn die Daten für ein Forschungsprojekt im Sinne des § 75 SGB X verwendet werden.⁵⁵ Die Daten sollen hierbei möglichst anonymisiert werden (§ 67c Abs. 5 S. 2 SGB X).

f) Betroffenenrechte

Schließlich schaffen die DS-GVO und das SGB X ein Rechtsschutzsystem für die Betroffenen von Verarbeitungen ihrer Sozialdaten. So enthält etwa § 81 Abs. 1 SGB X den Anspruch jedermanns, sich bei vermuteten Datenschutzverstößen an den Datenschutzbeauftragten zu wenden. Gemäß § 81 Abs. 2 SGB X sind die Aufsichtsbehörden für den Sozialdatenschutz der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nach Kapitel 4 des BDSG oder bei öffentlichen Stellen der Länder die Datenschutzbeauftragten nach Landesrecht. Außerdem sind bei den Sozialbehörden im Sinne des § 35 SGB I interne Datenschutzbeauftragte gemäß §§ 5-7 BDSG einzurichten.⁵⁶

40 Vgl. BSG, Urteil vom 27.06.2018, B 6 KA 27/17 R = MedR 2019, 405.

41 Vgl. dazu auch Maus, MedR 2019, 410.

42 Vgl. BSG (o. Fn. 40), 410.

43 Vgl. Deister, NZS 2019, 37.

44 Vgl. BSG (o. Fn. 40), 410.

45 Vgl. LSG Bayern (o. Fn. 3), Rn. 79ff.

46 Vgl. Hebel, NZS 2019, 633.

47 Vgl. LSG Bayern (o. Fn. 3), Rn. 1.

48 Vgl. LSG Bayern (o. Fn. 3), Rn. 79.

49 Vgl. LSG Bayern (o. Fn. 3), Rn. 80.

50 Vgl. LSG Bayern (o. Fn. 3), Rn. 79f.

51 Vgl. Fromm, in: Schlegel/Voelzke, jurisPK-SGB X, 2018, § 67c SGB X, Rn. 14.

52 Vgl. BT-Drs. 18/12611, S. 112; Hoidn/Roßnagel (o. Fn. 4), 489.

53 Vgl. Fromm (o. Fn. 51), Rn. 23f.

54 Vgl. Fromm (o. Fn. 51), Rn. 24.

55 Vgl. Bieresborn (o. Fn. 14), 929 und 931; Fromm (o. Fn. 51), Rn. 28.

56 Vgl. Bieresborn, NZS 2018, 10, 14f.

§ 81b SGB X enthält die prozessrechtliche Vorschrift, nach der für Klagen von Betroffenen wegen der Verletzung von Datenschutzrechten gegen die Sozialverwaltung der Klageweg zur Sozialgerichtsbarkeit eröffnet ist.⁵⁷ Für spezifische Betroffenenrechte im Sozialdatenschutzrecht müssen so dann die DS-GVO und das SGB X zusammen gelesen werden. So schaffen etwa Art. 13 DS-GVO und § 82 SGB X aktive Informationspflichten der datenverarbeitenden Stelle. Die Informationspflichten müssen erfüllt werden, wenn Daten beim Betroffenen direkt oder indirekt bei Dritten erhoben werden; die Information muss in präziser, transparenter, verständlicher Weise erfolgen und durch ein aktives Handeln des sozialrechtlichen Datenverarbeiters geschehen. § 82 Abs. 1 SGB X schränkt die Informationspflichten jedoch deutlich ein, etwa in Situationen, in denen der Betroffene nach den Umständen des Einzelfalls mit der Verarbeitung rechnen musste.⁵⁸ Das neue Sozialdatenschutzrecht schränkt auch die Informationspflichten bei einer zweckändernden Datenverarbeitung gemäß Art. 13 Abs. 3 DS-GVO durch § 82 Abs. 2 Nr. 1 und 2 SGB X empfindlich ein, etwa dann, wenn die Ausübung der Informationserteilung die ordnungsgemäß sozialrechtliche Aufgabenerfüllung gefährden würde oder durch die Informationserteilung die öffentliche Sicherheit und Ordnung gefährdet wäre bzw. in sonstiger Weise dem Wohl des Bundes oder der Länder Nachteile entstünden.⁵⁹ Vor dem Hintergrund des eigentlichen Regelungskonzeptes der DS-GVO, das eine größtmögliche Transparenz der Datenverarbeitungen verfolgt, sollten diese Ausnahmevorschriften nur behutsam eingesetzt werden. § 83 SGB X regelt darüber hinaus die Anpassung der Auskunftsrechte der Betroffenen im Sozialrecht.⁶⁰ Die Nutzung der Öffnungsklauseln der DS-GVO bei der Regelung des neuen Sozialdatenschutzrechts wurde, dies wird bei der Lektüre der neuen Vorschriften deutlich, verschiedentlich genutzt, um Betroffenenrechte im Sozialrecht im Vergleich zur Reichweite nach der DS-GVO einzuschränken, was berechtigterweise auf Kritik gestoßen ist.⁶¹

Im Hinblick auf die Betroffenenrechte im Sozialrecht hat das LSG Berlin-Brandenburg am 30. April 2019 eine Entscheidung getroffen, die sich im Wesentlichen auf die DS-GVO stützt.⁶² Vorliegend klagte eine frühere Leistungsbezieherin gegen das Jobcenter. Sie begehrte die Löschung von allen sie betreffenden Personalausweis- und Krankenversicherungsausweiskopien in den Papierakten und den elektronischen Akten des Jobcenters.⁶³ Das Jobcenter teilte daraufhin zunächst mit, dass alle Lichtbilder und Ausweiskopien aus der Papierakte entnommen und vernichtet worden seien und die restliche Papierakte in das Archiv übergeben wurde. Jedoch wies das Jobcenter darauf hin, dass sämtliche Daten noch in der elektronischen Akte vorhanden seien.⁶⁴ Infolge des erhobenen Widerspruches der Klägerin half das Jobcenter dem Widerspruch insoweit ab, dass auch aus der elektronischen Akte das Lichtbild der Personalausweiskopie gelöscht wurde. Im Übrigen wies das Jobcenter den Widerspruch jedoch zurück und befand, dass die weiter anhaltende Speicherung der Kopien des Personalausweises und der Krankenversicherungskarte für die Aufgabenerfüllung nach dem SGB II erforderlich sei. Im Fortgang entschied das LSG Berlin-Bran-

denburg im April 2019, dass die Rechtsgrundlage für die Löschung der (nach der bereits erfolgten Löschung des Ausweises) nur noch unvollständig vorhandenen Kopie des Personalausweises in der elektronischen Akte des Jobcenters Art. 17 Abs. 1 DS-GVO darstelle.⁶⁵ Demnach hätten Betroffene das Recht, von der verarbeitenden Stelle zu verlangen, sie betreffende Daten zu löschen, sofern sie für die ursprünglichen Erhebungszwecke nicht mehr erforderlich sind, was im Grunde auch der früheren Regelung des § 84 Abs. 2 SGB X entspreche.⁶⁶ Das LSG sah die Voraussetzungen für den Lösungsanspruch nach Art. 17 Abs. 1 DS-GVO im Hinblick auf die Ausweiskopien in der elektronischen Akte als erfüllt an.⁶⁷ Die ursprüngliche Erhebung und Speicherung der Ausweisdaten der Klägerin durch das Jobcenter war durch die entsprechenden Rechtsgrundlagen aus Art. 6 DS-GVO, §§ 67a Abs. 1 SGB X i.V.m. § 35 SGB I i.V.m. §§ 50ff. SGB II gedeckt. In § 51b Abs. 1 SGB II erkannte das LSG die einschlägige Rechtsgrundlage für Datenerhebungen zur Erfüllung der Grundsicherung für Arbeitsuchende. Die Erhebung der Daten wird neben dem Zweck der Leistungsgewährung auch für die Überprüfung der korrekten und wirtschaftlichen Leistungserbringung und zum Zwecke der Bekämpfung von Leistungsmissbrauch durchgeführt, was sich aus § 51b Abs. 3 SGB II ergibt.⁶⁸ Das Jobcenter argumentierte, dass die in der elektronischen Akte verbleibenden Angaben der Personalausweiskopie für die Erfüllung dieser Zwecke weiterhin gespeichert werden müssten. Dies bezweifelte das LSG. So seien die notwendigen Angaben aus dem Personalausweis der Klägerin zugleich auch im von der Klägerin unterschriebenen Antragsformular enthalten. Und die Daten, die sich ausschließlich aus der Ausweiskopie und nicht aus der übrigen Akte ergeben, nämlich die Augenfarbe und Körpergröße der Klägerin sowie die Personalausweisnummer seien für die Zwecke der Überprüfung der Leistungserbringung und der Bekämpfung von Leistungsmissbrauch nicht erforderlich.⁶⁹ Da für die weitere Speicherung der Ausweiskopie der Klägerin in der elektronischen Akte des Jobcenters keine Erforderlichkeit erkennbar war, sah das LSG den Anspruch auf Löschung gemäß Art. 17 Abs. 1 DS-GVO als gegeben an.⁷⁰ Damit wurde erstmals ein Lösungsanspruch gegenüber der Sozialverwaltung auf Art. 17 DS-GVO gestützt und gerichtlich bestätigt. Auch

57 Vgl. Bieresborn (o. Fn. 56), 15.

58 Vgl. Bieresborn (o. Fn. 56), 11.

59 Vgl. Bieresborn (o. Fn. 56), 11.

60 Vgl. Muckel/Ogorek/Rixen (o. Fn. 2), 536f.

61 Vgl. Hoidn/Roßnagel (o. Fn. 4) 499f., die zunehmende Verarbeitungsbefugnisse und eingeschränkte Betroffenenrechte als insgesamt „unausgewogen“ beklagen.

62 Vgl. LSG Berlin-Brandenburg (o. Fn. 11).

63 Vgl. LSG Berlin-Brandenburg (o. Fn. 11), Rn. 1ff.

64 Vgl. LSG Berlin-Brandenburg (o. Fn. 11), Rn. 3.

65 Vgl. LSG Berlin-Brandenburg (o. Fn. 11), Rn. 16.

66 Vgl. LSG Berlin-Brandenburg (o. Fn. 11), Rn. 17.

67 Vgl. LSG Berlin-Brandenburg (o. Fn. 11), Rn. 22ff.

68 Vgl. LSG Berlin-Brandenburg (o. Fn. 11), Rn. 26.

69 Vgl. LSG Berlin-Brandenburg (o. Fn. 11), Rn. 29.

70 Vgl. LSG Berlin-Brandenburg (o. Fn. 11), Rn. 28f.

dieses Urteil verdeutlichte, dass der Datenschutz im Sozialrecht nur adäquat umgesetzt werden kann, wenn das datenschutzrechtliche Mehrebenensystem aus der europäischen DS-GVO, dem allgemeinen Sozialdatenschutz aus dem SGB I und SGB X sowie dem bereichsspezifischen Datenschutz der übrigen Sozialgesetzbücher in einer Gesamtschau herangezogen und angewendet wird.

3. Zweiter Reformschritt: Neuregelung des bereichsspezifischen Datenschutzes in den Sozialgesetzbüchern im Jahr 2019

Zum Ende des Jahres 2019 hat der Bundesgesetzgeber einen weiteren Schritt zur Umsetzung des europäischen Datenschutzrechts vorgenommen. In einer äußerst detaillierten Gesetzgebung wurden Datenschutzbestimmungen in unterschiedlichsten Bundesgesetzen neu geregelt. Teil des „Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 – Zweites Datenschutz-Anpassungs- und Umsetzungsgesetzes EU“ vom 20. November 2019⁷¹ – ist auch die Anpassung des bereichsspezifischen Datenschutzes im Sozialgesetzbuch. Diese Änderungen finden sich in den Art. 119 bis 123, 125 und 128 bis 133 des „2. DSAnpUG-EU“.⁷²

a) Ziel des Gesetzgebers

In der Gesetzesbegründung führt die Bundesregierung aus, dass zwischen der DS-GVO und dem sehr ausdifferenzierten Datenschutzrecht auf nationaler Ebene ein reibungsloses Zusammenspiel sichergestellt werden soll.⁷³ Zwar habe man bereits im Jahr 2017 die allgemeinen Regeln des Sozialdatenschutzes im SGB I und SGB X reformiert. Doch im Hinblick auf das verbleibende bereichsspezifische Datenschutzrecht im Sozialrecht bestünde weiterer Anpassungsbedarf.⁷⁴ Dabei weist die Gesetzesbegründung selbst darauf hin, dass ein Großteil der spezifischen Anpassungen der Angleichung von Begriffsbestimmungen und der Aktualisierung von Gesetzesverweisen dient⁷⁵, also kaum inhaltliche Neuerungen enthält. Gleichwohl enthält 2. DSAnpUG-EU auch die Schaffung neuer Rechtsgrundlagen für die Verarbeitung und Übermittlung von Daten.⁷⁶

b) Sprachliche Anpassungen an die DS-GVO

Die ganz überwiegende Anzahl der Anpassungen im Sozialdatenschutzrecht durch das 2. DSAnpUG-EU ist sprachlicher und redaktioneller Natur. Die frühere Rechtslage wird daher im spezifischen Sozialdatenschutz in materieller Hinsicht in den meisten Fällen beibehalten und lediglich an Begriffe und neue Verweisnormen angeglichen.⁷⁷ Beispiele für redaktionelle Anpassungen an die Begriffe der DS-GVO finden sich etwa in Art. 125 Nr. 4 2. DSAnpUG-EU zu § 127a SGB VI, der die Wörter „erheben, verarbeiten und nutzen“ durch „verarbeiten“ ersetzt, da die DS-GVO allein von diesem Begriff ausgeht; weiterhin Art. 125 Nr. 5 2. DSAnpUG-EU, durch den in § 145 SGB VI die Wörter „eine Datei mit Sozialdaten“ durch „ein Dateisystem mit Sozialdaten“ ausgetauscht wird.⁷⁸ Solche Veränderungen wurden in allen zwölf Sozialgesetzbüchern vorgenommen und stellen seitenweise den Inhalt der zweiten Reform des Sozialdatenschutzrechts dar.

c) Streichung früherer bereichsspezifischer Rechtsgrundlagen

Durch den Geltungsvorrang der DS-GVO und aufgrund der Neuregelung des allgemeinen Sozialdatenschutzes im SGB I und SGB X durch die Reform des Jahres 2017 kam es verschiedentlich zu der Situation, dass bereichsspezifische Rechtsgrundlagen für Datenverarbeitungen in den Sozialgesetzbüchern verdrängt oder obsolet wurden. Beispielsweise wurden die Bußgeld- und Strafvorschriften in §§ 63a und 63b SGB II bei Verstößen gegen das Datenschutzrecht aufgehoben, weil Art. 83 DS-GVO diese nunmehr abschließend regelt. Die entsprechenden Verfahrensvorschriften finden sich nunmehr in § 85 SGB X, der auch für das SGB II gilt. Insofern bedurfte es der spezifischen Regelungen im SGB II nicht mehr.⁷⁹ Ein anderes Beispiel für eine Streichung einer früheren Rechtsgrundlage für Datenverarbeitungen findet sich im Recht der Unfallversicherung. Durch Art. 128 Nr. 10 2. DSAnpUG-EU wurde § 292 S. 2 SGB VII gestrichen. Das darin bisher geregelte Informationsrecht von Betroffenen, den Inhalt von Anzeigen über eine Berufskrankheit durch Ärzte und Zahnärzte an die Unfallversicherung mitgeteilt zu bekommen, wird gestrichen, da dieses Betroffenenrecht nunmehr direkt aus Art. 12ff. DS-GVO entnommen wird.⁸⁰

d) Neu geregelte spezifische Rechtsgrundlagen im Sozialdatenschutzrecht

Die Anpassung des bereichsspezifischen Sozialdatenschutzrechts enthält jedoch nicht nur sprachliche Anpassungen und Streichungen obsolet gewordener Vorschriften. Vereinzelt wurden durch die Reform von November 2019 auch neue Rechtsgrundlagen für Datenverarbeitungen geschaffen. Hier sollen nun einige dieser Neuregelungen angesprochen werden.

Beispiel SGB III, Recht der Arbeitsförderung: § 41 SGB III regelt die Einschränkung des Fragerechts der Agentur für Arbeit.⁸¹ Diese Einschränkung gleicht dem Fragerecht eines Arbeitgebers, der bestimmte Informationen etwa bei Bewerbern in einem Vorstellungsgespräch nicht erheben darf (z.B. Familienplanung oder sexuelle Orientierung). Informationen über eine Gewerkschaftszugehörigkeit oder eine Parteimitgliedschaft darf die Agentur für Arbeit ebenfalls nur unter strengen Voraussetzungen erheben. Die bisherige Regelung des § 41 Abs. 1 S. 3 SGB III enthielt keine Rechtsgrundlage, solche erfragten Daten auch zu speichern, sondern

71 BGBl. 2019 I, S. 1626.

72 So die amtliche Abkürzung laut BGBl. 2019 I, S. 1626.

73 Vgl. BT-Drs. 19/4674, S. 2.

74 Vgl. BT-Drs. 19/4674, S. 2.

75 Vgl. BT-Drs. 19/4674, S. 181.

76 Vgl. BT-Drs. 19/4674, S. 181.

77 Vgl. die reihenweise genutzte Formulierung der Gesetzesbegründung „Das geltende Recht wird beibehalten und lediglich redaktionell an die Begriffsbestimmungen aus Art. 4 der Verordnung (EU) 2016/679 angepasst“, BT-Drs. 19/4674, S. 343ff.

78 Dazu BT-Drs. 19/4674, S. 386f.

79 Vgl. BT-Drs. 19/4674, S. 343.

80 Vgl. BT-Drs. 19/4674, S. 394.

81 Vgl. Brand, in: Brand, Sozialgesetzbuch III. Kommentar, 2018, § 41, Rn. 2.

lediglich, sie zu erheben und zu nutzen. Art. 121 Nr. 3 2. DSAnpUG-EU ändert § 41 SGB III nunmehr dahingehend, dass die Agentur für Arbeit eine Rechtsgrundlage auch zur Speicherung dieser Daten erhält.⁸²

Beispiel SGB IV: Die Träger der Sozialversicherung sind rechtsfähige Körperschaften des öffentlichen Rechts mit der Befugnis zur Selbstverwaltung gemäß § 29 Abs. 1 SGB IV. Als solche unterliegen sie der staatlichen Aufsicht gemäß § 87 SGB IV. Die bundes- oder landesrechtlichen Aufsichtsbehörden (§ 90 SGB IV) haben deshalb gegenüber den Trägern der Sozialversicherung ein Prüfungsrecht, das gemäß § 88 SGB IV die Geschäfts- und Rechnungsprüfung sowie Auskunftsrechte umfasst. Mit der zweiten Datenschutzreform hat der Gesetzgeber den Aufsichtsbehörden neue Befugnisse eingeräumt. So ergänzt Art. 122 Nr. 10 2. DSAnpUG-EU den § 88 Abs. 2 SGB IV dahingehend, dass die Aufsichtsbehörden ein Zugangsrecht zu allen für die Prüfung erforderlichen elektronisch gespeicherten Daten der Sozialversicherungsträger haben und dieser Anspruch auch einen automatisierten Datenabruf umfasst.⁸³ Hiermit erfolgte ganz offenbar eine Angleichung auch an die Vorschrift des § 95 Bundeshaushaltsordnung, die ein gleiches Recht zum automatisierten Datenabruf dem Bundesrechnungshof gewährt.⁸⁴

Beispiel SGB V, Gesetzliche Krankenversicherung: Die gesetzliche Krankenversicherung kann gemäß § 20 Abs. 4 Nr. 1 und Abs. 5 SGB V Versicherten Leistungen zur verhaltensbezogenen Prävention anbieten. Diese richten sich an Einzelpersonen, die durch die Maßnahmen langfristig befähigt werden sollen, einen gesundheitsförderlichen Lebensstil zu führen und Krankheiten vorzubeugen.⁸⁵ Für die Gewährung dieser Leistungen wird gemäß § 20 Abs. 5 S. 2 SGB V eine vorherige Empfehlung eines Arztes aufgrund einer gesundheitlichen Untersuchung, beispielsweise nach § 25 Abs. 1 SGB V, herangezogen. Die gesetzlichen Krankenversicherungen dürfen die in dem Empfehlungsschreiben enthaltenen personenbezogenen Daten nur dann verarbeiten, wenn die betroffene Person hierin eingewilligt hat und wenn diese Person darüber vorher informiert wurde. Art. 123 Nr. 1 a) 2. DSAnpUG-EU ergänzt die Regelung des § 20 Abs. 5 SGB V nunmehr dahingehend, dass die Einwilligung des Patienten in die Verarbeitung von biometrischen, genetischen oder Gesundheitsdaten und die Informierung durch die Krankenversicherung entweder schriftlich oder elektronisch erteilt werden können.⁸⁶ Dabei stützte sich der Gesetzgeber auf die Öffnungsklausel des Art. 9 Abs. 4 DS-GVO.⁸⁷

Beispiel SGB VIII, Kinder- und Jugendhilferecht: Beamte oder Angestellte, denen die Ausübung einer Beistandschaft, Amtspflegschaft oder Amtsvormundschaft für ein Kind oder einen Jugendlichen übertragen ist, dürfen gemäß § 68 Abs. 1 SGB VIII Sozialdaten verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Dadurch unterliegen sie grds. auch den Informationspflichten der DS-GVO. Die Informationspflichten aus Art. 13 und 14 DS-GVO werden durch Art. 129 Nr. 5 a) bb) 2. DSAnpUG-EG für diese Personen eingeschränkt. Zweck dieser neuen Vorschrift in § 68 SGB VIII ist es, dass der Beistand, Amtspfleger oder Amtsvormund abwägen soll, inwieweit die Kinder und Jugendlichen vor einer Datenübermittlung an Dritte geschützt werden können.⁸⁸ Sobald eine Informati-

onserteilung nicht mit der Wahrung der Interessen des Kindes oder des Jugendlichen vereinbar ist, entfällt die Pflicht.⁸⁹

Insgesamt zeichnet sich die zweite Reform des Sozialdatenschutzrechts in Anpassung an die DS-GVO weitgehend durch einen hohen Detailgrad bei niedrigem materiellen Regelungsgehalt aus. Der maßgebliche Anteil der Gesetzesänderungen sind bloße Begriffsanpassungen und Verweisungen auf andere Vorschriften. Die Schaffung neuer datenschutzrechtlicher Rechtsgrundlagen ist rar und beläuft sich ebenfalls nur auf Detailfragen.

III. Zusammenfassung

Der Datenschutz im Sozialrecht musste durch die Änderungen auf der europäischen Ebene neu aufgestellt werden. Der Bundesgesetzgeber setzte dies in zwei Reformschritten in den Jahren 2017 und 2019 um. Die erste Reform, die sich auf die übergreifenden Datenschutzbestimmungen im Sozialrecht bezogen, war weitgehend von Kontinuität geprägt. Die allgemeinen Prinzipien des Sozialdatenschutzes sind ganz wesentlich die gleichen geblieben, wie sie auch im alten Recht bestanden. Gleichwohl hat der Gesetzgeber die Reform genutzt, um der Sozialverwaltung mehr Verarbeitungsbefugnisse einzuräumen und gleichzeitig Betroffenenrechte einzuschränken, was durchaus kritikwürdig ist. Die zweite Reform war zwar von hohem Detailgrad, aber auch von geringer materieller Regelungstiefe geprägt. Nur in wenigen Punkten wurden neue Befugnisse in das bereichsspezifische Sozialdatenschutzrecht eingeführt. Bei der Analyse der jüngeren Rechtsprechung zum neuen Sozialdatenschutz fiel hauptsächlich auf, dass die Gerichte dazu übergegangen sind, die Datenschutzvorschriften der verschiedenen Ebenen in einer Gesamtschau zur Beurteilung heranzuziehen, wodurch abschließend ein deutlicher Einfluss des Europarechts auf das Sozial(datenschutz)recht anzuerkennen ist.



Dr. iur. Hannes Berger

Der Autor hat im Bereich des Datenschutzrechts promoviert und ist im Geschäftsbereich IV – Bildung und Soziales bei der Stadtverwaltung Halle (Saale) beschäftigt. Zudem ist er Lehrbeauftragter an der Universität Erfurt und Mitherausgeber der Zeitschrift für Landesverfassungsrecht und Landesverwaltungsrecht.

82 Vgl. BT-Drs. 19/4674, S. 344: bislang ließ sich die Speicherbefugnis allenfalls durch Auslegung begründen.

83 Vgl. BT-Drs. 19/4674, S. 354.

84 Vgl. BT-Drs. 19/4674, S. 354.

85 Vgl. Joussem, in: Knickrehm/Kreikebohm/Waltermann, Kommentar zum Sozialrecht, 2019, SGB V, § 20 Rn. 2.

86 Vgl. BT-Drs. 19/4674, S. 356.

87 Vgl. BT-Drs. 19/4674, S. 356.

88 Vgl. BT-Drs. 19/4674, S. 398f.

89 Vgl. BT-Drs. 19/4674, S. 399.



Ihre DS-GVO
Umsetzung
smart auditiert
und visualisiert.

DS-GVO Compliance Check

Wie DS-GVO-konform arbeitet Ihr Unternehmen?

Machen Sie den Test mit dem neuen
Excel-Tool »DS-GVO Compliance Check«!

weitere Informationen unter:
www.datakontext.com/compliancecheck

Sophie Derfler

„Haushaltsausnahme“ auch für juristische Personen und Personengesellschaften?

Anwendbarkeit der DS-GVO auf die Datenverarbeitung im persönlichen und familiären Bereich durch Vereine und Gesellschaften bürgerlichen Rechts

Die sog. „Haushaltsausnahme“ nach Art. 2 Abs. 2 lit. c DS-GVO (und § 1 Abs. 1 S. 2 a.E. BDSG) nimmt die Datenverarbeitung im persönlichen und familiären Bereich durch natürliche Personen von der Anwendung des Datenschutzrechts aus. Die Beschränkung der Ausnahme auf natürliche Personen als Verarbeitende schließt juristische Personen

und Personengesellschaften von der Möglichkeit der Ausnahme aus. Aber auch juristische Personen und Personengesellschaften können in Einzelfällen Daten im persönlichen und familiären Bereich verarbeiten. Fraglich ist also, ob in einem solchen Fall der Art. 2 Abs. 2 lit. c DS-GVO auch auf juristische Personen anwendbar sein müsste.

I. Anwendbarkeit des europäischen Datenschutzrechtes

1. Sachliche und räumliche Bestimmungen

Die Anwendbarkeit der DS-GVO ergibt sich zum einen aus einem sachlichen (Art. 2 DS-GVO) und zum anderen aus einem räumlichen Bezugspunkt (Art. 3 DS-GVO).

Nach Art. 2 DS-GVO muss eine Verarbeitung personenbezogener Daten vorliegen. Diese Verarbeitung kann ganz oder teilweise automatisiert sein; die Daten können zudem rein manuell verarbeitet werden, dann aber in einem Dateisystem, also einer strukturierten Sammlung. Der sachliche Anwendungsbereich ist also weit, erfasst ist die Verarbeitung in fast jeder Verarbeitungssituation, unabhängig davon, welche Person die Daten verarbeitet.¹ Die Prozesse, die unter den Verarbeitungsbegriff fallen, sind ähnlich allumfassend, denn es sind alle Tätigkeiten von der Datenerhebung bis zur Löschung oder Vernichtung erfasst, vgl. Art. 4 Nr. 2 DS-GVO. Die Daten müssen bekanntermaßen personenbezogen sein, aber auch dies ist ein weitreichendes Kriterium, denn es reichen Informationen aus, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, Art. 4 Nr. 1 DS-GVO.

Die DS-GVO ist räumlich überall dort anwendbar, wo der Datenverarbeitende (Verantwortlicher oder Auftragsverarbeiter) eine Niederlassung in der EU hat, unabhängig davon, ob die Datenverarbeitung innerhalb des Unionsgebiets stattfindet oder nicht, Art. 3 Abs. 1 DS-GVO. Nach dem Marktortprinzip ist die DS-GVO ferner anwendbar, wenn die Daten einer Person in der EU verarbeitet werden, soweit diese Verarbeitung mit dem Anbieten von Waren oder Dienstleistungen in der EU zu tun hat, Art. 3 Abs. 2 lit. a DS-GVO, oder wenn das Verhalten von Personen innerhalb des Unionsgebiets beobachtet wird, Art. 3 Abs. 2 lit. b DS-GVO.

Die Anwendung der DS-GVO bestimmt sich also grundsätzlich nach formalen Kriterien, welche dazu führen, dass sich der Anwendungsbereich und somit der Schuttschirm der DS-GVO möglichst weit sowohl über das Unionsgebiet als auch über alle sich in der Union befindlichen natürlichen Personen erstreckt. Die DS-GVO macht grundsätzlich keinen Unterschied zwischen der Person des Verarbeitenden, sondern knüpft an

die Verarbeitung an sich an. So ist die Verarbeitung von Daten durch eine natürliche Person genauso erfasst wie die durch eine juristische Person oder Personengesellschaft.

2. Die Ausnahme des Art. 2 Abs. 2 lit. c DS-GVO

Auch wenn die digitale Datenverarbeitung durch Smartphones, Messenger-Apps und unter den heutigen Umständen mehr und mehr auch durch Video-Konferenzen und Anrufen flächendeckend Einzug gehalten hat, so kennt die DS-GVO trotzdem – oder gerade deswegen – eine Ausnahme für die Datenverarbeitung im privaten und familiären Bereich, Art. 2 Abs. 2 lit. c DS-GVO. Denn die Datenverarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten fällt nicht in den Anwendungsbereich der DS-GVO, Art. 2 Abs. 2 lit. c DS-GVO. Diese Ausnahme ist Ausdruck der grundrechtlich geschützten Privatsphäre und des Familienlebens (vgl. Art. 7 GRCh, Art. 8 EMRK), welche im Vergleich zur beruflichen und geschäftlichen Sphäre schützenswerter ist.² In Erwägungsgrund 18 DS-GVO sind Beispiele von normalerweise persönlichen oder familiären Tätigkeiten aufgelistet: der private Schriftverkehr, Bildaufnahmen oder auch die Nutzung sozialer Netzwerke. Die DS-GVO versteht dem Wortlaut nach unter der Datenverarbeitung im familiären und persönlichen Kontext allein die Verarbeitung von Daten natürlicher Personen durch natürliche Personen (Individuum-Individuum).³

Es ist nicht endgültig festgelegt, wie die Begriffe „persönlich“ und „familiär“ definiert werden, denn die DS-GVO orientiert sich weder am Familienrecht noch definiert sie den Begriff eigenständig.⁴ Allerdings gibt Erwägungsgrund 18 DS-GVO einen Hinweis in Form einer negativen Abgrenzung: Familiär und persönlich ist demnach alles, was keinen

1 Kühling/Raab, in: Kühling/Buchner, DS-GVO, 2. Aufl. 2018, Art. 2 Rn. 12.

2 Gusy/Eichenhofer, in: BeckOK DatenschutzR BDSG, 31. Ed. Stand: 01.11.2019, § 1 BDSG Rn. 75a.

3 Vgl. von Lewinski, in: Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, § 1 BDSG Rn. 12.

4 Kühling/Raab, in: Kühling/Buchner, DS-GVO, 2. Aufl. 2018, Art. 2 Rn. 23. Von Lewinski schreibt, dass eine „verobjektivierte subjektive Sichtweise“ gewählt werden muss, um Missbrauch vorzubeugen. Es wird aber nicht klar, was dies genau bedeutet: von Lewinski, in: Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, § 1 BDSG Rn. 13.

Bezug zur beruflichen oder wirtschaftlichen Tätigkeit der natürlichen Personen hat. Weiterhin bezieht sich der Begriff „familiär“ nicht nur auf die „traditionelle Familie“, sondern bezeichnet die gesamte Privat- oder Familiensphäre, welche auch im Rahmen von Art. 7 GRCh erfasst ist. Ausschlaggebend ist also der besonders geschützte persönliche Kontext der Informationen, welcher zwar durch persönliche Beziehungen der natürlichen Personen untereinander indiziert werden kann, allerdings ist auch die persönliche Beziehung nicht allein geeignet, den persönlichen und familiären Kontext der Datenverarbeitung zu begründen.⁵

So nimmt Art. 2 Abs. 2 lit. c DS-GVO jedenfalls und zunächst nur die Datenverarbeitung im persönlichen und familiären Kontext durch natürliche Personen vom Anwendungsbereich der DS-GVO aus. Dies gilt freilich nur so weit, wie die Datenverarbeitung durch natürliche Personen geschieht; sobald juristische Personen oder Personengesellschaften die Daten verarbeiten, scheidet die „Haushaltsausnahme“ ausweislich des klaren Wortlauts aus – selbst wenn die Datenverarbeitung im familiären und persönlichen Bereich geschieht.

Die oben erwähnte natürliche Person, die Daten im persönlichen und familiären Bereich verarbeitet, fällt also gerade nicht unter den Anwendungsbereich der DS-GVO, während beispielsweise eine GmbH, welche Daten im großem oder kleinen Maß verarbeitet, darunterfällt. Aber genauso fallen auch Vereine und Gesellschaften bürgerlichen Rechts in den Anwendungsbereich der DS-GVO – selbst wenn sie Daten für den familiären und persönlichen Bereich verarbeiten. Dies liegt einzig darin begründet, dass es sich bei Vereinen und GbR auch um juristische Personen bzw. Personengesellschaften handelt, und Art. 2 Abs. 2 lit. c DS-GVO ausdrücklich nur natürliche Personen privilegiert.

II. Datenverarbeitung im persönlichen, familiären Bereich durch Vereine⁶ und Gesellschaften bürgerlichen Rechts (GbR)

Es könnte jedoch sein, dass sich die unterschiedliche Behandlung von juristischen und natürlichen Personen durch Art. 2 Abs. 2 lit. c DS-GVO daraus ergibt, dass juristische Personen ihrem Charakter nach schon keine Daten im familiären und persönlichen Bereich verarbeiten können.⁷ Dass eine Verarbeitung im familiären und persönlichen Bereich bei den meisten datenverarbeitenden juristischen Personen, welche beim Thema Datenschutz in den Sinn kommen, außer Frage steht, liegt auf der Hand: Weder Facebook noch Google verarbeiten Daten im familiären und persönlichen Bereich. Allerdings gibt es auch noch viele andere Konstellationen an juristischen Personen, deren Zweck ein anderer ist, sodass das generelle Verneinen der Möglichkeit der Datenverarbeitung im familiären und persönlichen Bereich für juristische Personen (und Personengesellschaften) vorschnell erscheint.

Als Beispiel wird hier einerseits der nicht-wirtschaftliche Verein verwendet, dessen Zweck es ist, den Zusammenschluss eines Familienverbandes zu fördern⁸ (III.1.a), und andererseits eine konkludent gegründete Gesellschaft bürgerlichen Rechts, welche die Förderung einer Wohngemeinschaft zum Zweck hat (III.1.b).⁹

1. Existenz einer Datenverarbeitung im persönlichen und familiären Bereich durch juristische Personen

a) Der eingetragene Familienverbandverein, § 21 BGB

Es gibt keine gesetzliche Definition des Vereins, jedoch wird sich generell an der Definition des Reichsgerichts für Zivilsachen orientiert: Ein Verein ist „eine auf Dauer berechnete Verbindung einer größeren Anzahl von Personen zur Erreichung eines gemeinsamen Zweckes, die nach ihrer Satzung körperschaftlich organisiert ist, einen Gesamtnamen führt und auf einen wechselnden Mitgliederbestand angelegt ist“.¹⁰

Der gemeinsame Zweck ist das konstituierende Merkmal jeder Personenvereinigung. Der Verein ist dazu verpflichtet, diesen Zweck zu fördern, denn der Verein existiert alleinig, um den gemeinsamen Zweck durch die körperschaftliche Organisation zu erreichen.¹¹ Der Vereinszweck kann frei bestimmt werden, dies ergibt sich aus der Vereinigungsfreiheit, Art. 9 Abs. 1 GG, er darf nur nicht wirtschaftlich sein (arg. e. cont. § 22 BGB), vor allem kommt aber gerade auch ein familiärer oder persönlicher Zweck in Frage. Ein Verein kann, wie im vorliegenden Beispiel, eben gerade gegründet werden, um einen großen, verästelten Familienverband zu organisieren und verbinden. Dabei kommt es nicht unbedingt auf die Familienbeziehung (im Sinne des BGB) zwischen den einzelnen Mitgliedern an, diese kann allerdings ein Indiz für den familiären und persönlichen Zweck sein. Aber auch außerhalb von Verwandtschaftsverhältnissen sind mindestens persönliche Vereinszwecke denkbar, wie zum Beispiel die Gründung eines Vereins zur Organisation von Nachbarschaftsfeiern oder der Instandhaltung von Wohneigentum.

Die Einigung zwischen den Gründern auf den Vereinszweck ist der eigentliche Gründungsakt des Vereins,¹² durch die Eintragung in das Vereinsregister erreicht der Verein den Status einer juristischen Person.¹³ Die Eintragung hat also nur konstitutive Wirkung für das Entstehen der juristischen Person.¹⁴

Soweit der Vereinszweck ein familiärer oder persönlicher Zweck ist, wie zum Beispiel die Pflege der Zusammengehörigkeit eines Familienverbandes, kann die Datenverarbei-

5 Gusy/Eichenhofer, in: BeckOK DatenschutzR BDSG, 31. Ed. Stand: 01.11.2019, § 1 Rn. 75a.

6 Von Lewinski, in: Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, § 1 BDSG Rn. 18: Von Lewinski thematisiert die Frage, ob persönliche und familiäre Vereine auch unter die „Haushaltsausnahme“ fallen sollten, nur im Rahmen von § 1 BDSG. Dies ist jedoch systematisch verfehlt, denn die Frage, ob die „Haushaltsausnahme“ nur für die Datenverarbeitung persönliche und familiären Zweckes durch natürliche Personen gilt oder ob diese auch auf juristische Personen erweitert werden kann, ist keine Frage des mitgliedstaatlichen Rechts, sondern eine Frage des Anwendungsbereichs der DS-GVO. Systematisch stellt sich diese Frage also schon bei Art. 2 DS-GVO und nicht erst bei § 1 BDSG. Im Ergebnis hat von Lewinski Recht.

7 So Kühling/Raab, in: Kühling/Buchner, DS-GVO, 2. Aufl. 2018, Art. 2 Rn. 23 m.w.N.

8 So zum Beispiel die Lutheriden-Vereinigung e.V., dessen Zweck nach § 2 der Satzung unter anderem die Organisation von Familientreffen und die genealogische Nachforschung ist.

9 Auf die spezifischen Rechtsfragen zur Wohngemeinschaft als GbR und vor allem auf die Abgrenzung zur Mietmehrheit, wird hier nicht weiter eingegangen. Zum Weiterlesen: Bühler, in: NJOZ 2019, 529 ff.

10 Zitat nach: RGZ 143, 212, 213; so auch bspw. in der Literatur: Hadding, in: Soergel, Band 1, Stand: Frühjahr 2000, Vor § 21 Rn. 44.

11 Schöpflin, in: BeckOK BGB, 53. Ed. Stand: 01.02.2020, § 21 Rn. 87.

12 Schöpflin, in: BeckOK BGB, 53. Ed. Stand: 01.02.2020, § 21 Rn. 121.

13 Leuschner, in: MüKo BGB, 7. Aufl. 2017, § 21 § 22 Rn. 83.

14 Schöpflin, in: BeckOK BGB, 53. Ed. Stand: 01.02.2020, § 21 Rn. 124.

tung um dieses Zweckes willen dann folglich auch im familiären oder persönlichen Bereich stattfinden. Legt der Vorsitzende des beispielhaft gewählten Vereins zur Förderung des Familienzusammenschlusses die Korrespondenz zwischen den Mitgliedern und die Mitgliedsregister mit den persönlichen Daten aller Mitglieder strukturiert ab, so ist die DS-GVO grundsätzlich anwendbar, denn die Datenverarbeitung wurde von einer juristischen Person, dem Verein, vorgenommen. Hätte dieser Familienverband allerdings keinen Verein gegründet – und diesen vor allem nicht eingetragen, sondern nur eine Person als zuständig bestimmt, so würde die Ablage der Korrespondenz und Führung des Registers mit persönlichen Daten der Familienmitglieder nicht in den Anwendungsbereich der DS-GVO fallen, da die Datenverarbeitung durch eine natürliche Person im familiären Bereich stattfände. Die „Haushaltsausnahme“ aus Art. 2 Abs. 2 lit. c DS-GVO ist also nur deswegen nicht anwendbar, weil ein Zusammenschluss der Personengruppe in einem eingetragenen Verein existiert, durch welchen dieser den Status einer juristischen Person erlangt hat.

b) Die Wohngemeinschaft, § 705 BGB

Im zweiten Beispiel hat eine Wohngemeinschaft konkludent durch ihr Zusammenleben eine Gesellschaft bürgerlichen Rechts nach § 705 BGB gegründet.

Eine Gesellschaft bürgerlichen Rechts setzt voraus, dass die Gesellschafter vertraglich miteinander verbunden, gesamthänderisch an der Gesellschaft beteiligt und außerdem nicht beliebig auswechselbar sind. Ähnlich wie beim Verein setzt auch die GbR einen gemeinsamen Zweck und darauf gerichtete Förderpflichten voraus. Der gemeinsame Zweck ist nach § 705 BGB konstitutives Merkmal. Es muss also (möglicherweise konkludent¹⁵) ein Gesellschaftsvertrag abgeschlossen werden, welcher den gemeinsamen Zweck und die Förderungspflicht festhält.¹⁶ Grundsätzlich ist auch bei der GbR jeder Zweck möglich, allerdings sind gesetzes- oder sittenwidrige Zwecke sowie das Führen eines Handelsgewerbes ausgenommen.¹⁷

Nur die sog. Außen-GbR ist (teil-)rechtsfähig, sodass eine weitere Voraussetzung für die hier gewählte Wohngemeinschaft ist, dass diese durch ihre Vertreter – als Gesellschaft – am Rechtsverkehr teilnimmt.¹⁸

Die Voraussetzungen zur Gründung einer GbR sind, ähnlich wie beim Verein, niedrighschwellig, im Mittelpunkt steht die Förderung eines gemeinsamen Zwecks durch mehr als eine Person. So werden Gesellschaften bürgerlichen Rechts nicht nur für Wohngemeinschaften, sondern auch aus steuerlichen oder haftungsrechtlichen Gründen zwischen sich nahestehenden Personen gegründet, wie zum Beispiel die Familien-/ Ehepartner-GbR oder Fahrgemeinschafts-GbR, aber auch in Nachbarschaften sind Gesellschaften bürgerlichen Rechts denkbar, zum Beispiel zur Organisation von Festen oder Flohmärkten. Vorliegend besteht der Zweck der GbR darin, die Wohngemeinschaft zu fördern und das Zusammenleben in einer Wohngemeinschaft zu organisieren. Werden im Rahmen dieses Zwecks Daten verarbeitet, so geschieht die Verarbeitung im privaten Bereich, würde diese von einer natürlichen Person vorgenommen werden, und nicht von der GbR, so

würde Art. 2 Abs. 2 lit. c DS-GVO greifen. Auch hier lässt sich die Frage stellen, warum die Datenverarbeitung im familiären und persönlichen Bereich nur aufgrund des Zusammenschlusses in einer Personengesellschaft unter die Anwendung der DS-GVO fallen sollte, wenn dieselbe Datenverarbeitung durch eine natürliche Person vorgenommen unter die Ausnahme des Art. 2 Abs. 2 lit. c DS-GVO fallen würde.

c) Ergebnis

Betrachtet man hier also den Verein als juristische Person und die GbR als Personengesellschaft, so kann festgestellt werden, dass es für beide Konstellationen die Möglichkeit gibt, Daten in einem persönlichen und familiären Bereich zu verarbeiten. Auch wenn dies sicherlich in der geringeren Anzahl der Fälle vorkommen wird, so kann nicht grundsätzlich in Abrede gestellt werden, dass juristische Personen oder Personengesellschaften Daten im familiären und persönlichen Bereich verarbeiten können. Solange dies aber nicht grundsätzlich abgelehnt werden kann, sollte hinterfragt werden, warum juristische Personen und Personengesellschaften grundsätzlich von der „Haushaltsausnahme“ ausgeschlossen werden.

2. Begründung der Restriktion des Art. 2 Abs. 2 lit. c DS-GVO auf natürliche Personen

Im familiären und persönlichen Datenverarbeitungskontext werden schon dann erhöhte Anforderungen an den Datenschutz (nämlich die Befolgung der Regelungen der DS-GVO (siehe IV.)) gestellt, wenn ein Verein oder eine GbR besteht. Würde dieselbe Datenverarbeitung durch eine natürliche Person geschehen, wäre diese Datenverarbeitung durch Art. 2 Abs. 2 lit. c DS-GVO privilegiert. Und dies, obwohl es keinen Unterschied machen kann, ob eine eng oder lose verbundene und möglicherweise (bluts-)verwandte Gruppe von Personen (Familie nach Art. 7 GRCh) Daten im persönlichen und familiären Bereich verarbeitet, oder ob sich diese Gruppe von Personen zu einer juristischen Person oder Personengesellschaft zusammenschließt und dieselben Daten verarbeitet. Eine Ausdehnung des Art. 2 Abs. 2 lit. c DS-GVO auf juristische Personen wäre somit angebracht. Es könnte jedoch sein, dass dem Schutzziele, höherrangiges Recht oder die Systematik der DS-GVO entgegenstehen.

a) Schutzziel der DS-GVO

Die Schutzziele der DS-GVO sind in Art. 1 DS-GVO festgehalten, dort wird zum einen der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen genannt, Art. 1 Abs. 2 DS-GVO, und zum anderen der Schutz des freien Datenverkehrs im Binnenmarkt, Art. 1 Abs. 3 DS-GVO. Die Vorschrift des Art. 1 DS-GVO wird vor allem dann als Anleitung für den normativen Umgang herangezogen, wenn es Unsicherheiten

15 Schäfer, in: MüKo BGB, 7. Aufl. 2017, § 705 Rn. 25-28.

16 Schäfer, in: MüKo BGB, 7. Aufl. 2017, § 705 Rn. 128, 142.

17 Schäfer, in: MüKo BGB, 7. Aufl. 2017, § 705 Rn. 146.

18 BGH, Urt. v. 29.01.2001 – II ZR 331/00, NJW 2001, 1056 ff.; ausführlich zur Rechtsentwicklung: Schäfer, in: MüKoBGB, 7. Aufl. 2017, Vorb. vor § 705 Rn. 9-11.

bei der Auslegung gibt.¹⁹ Die richtungsweisenden Hinweise des Art. 1 DS-GVO sind also auch hier zu beachten, wenn es um die Auslegung der „Haushaltsausnahme“ geht. Im Rahmen der familiären und persönlichen Tätigkeit steht der Schutz des Binnenmarkts nicht in Frage, es liegt also kein Spannungsverhältnis zwischen den beiden Schutzziele vor. Vielmehr geht es nur darum, ob durch die Erweiterung von Art. 2 Abs. 2 lit. c DS-GVO die Grundrechte und Grundfreiheiten der natürlichen Personen gefährdet werden.

Art. 2 Abs. 2 lit. c DS-GVO soll gewährleisten, dass die Verarbeitung von Daten im familiären und privatem Bereich keinen unnötigen Aufwand für die Verarbeitenden darstellt.²⁰ Und dies, obwohl die typische Gefahrensituation einer Persönlichkeitsverletzung, vor welcher die DS-GVO schützen will, gerade auch im familiären und persönlichen Bereich besteht (Geheimnisverrat, Revenge Porn etc.).²¹ Diese Gefahr besteht unabhängig davon, ob die Verarbeitung durch natürliche Personen oder juristische Personen oder Personengesellschaften geschieht. Durch die Existenz von Art. 2 Abs. 2 lit. c DS-GVO adressiert die DS-GVO diese Gefährdungslage schon grundsätzlich nicht adäquat. Die Beschränkung von Art. 2 Abs. 2 lit. c DS-GVO auf natürliche Personen trägt jedenfalls nicht zum Schutz der Persönlichkeitssphäre bei. Folglich steht eine Erweiterung des Art. 2 Abs. 2 lit. c DS-GVO auf juristische Personen und Personengesellschaften schon mangels effektivem Rechtsschutz durch die DS-GVO, deren Schutzziel nicht entgegen.

Da die DS-GVO schon gar nicht adäquat vor den Risiken einer Persönlichkeitsverletzung in der Privatsphäre schützt, stellt die Verarbeitung der Daten durch eine juristische Person oder eine Personengesellschaft keinen größeren Eingriff in die Grundrechte dar als die Verarbeitung der Daten durch eine natürliche Person.

b) Europarechtliche Vorgaben

Eine erweiterte Auslegung der DS-GVO, wie sie hier vorgeschlagen wird, muss auch mit dem höherrangigen Recht vereinbar sein, welches im Falle von Unionsrechtsakten eben nicht das Grundgesetz, sondern das europäische Recht ist, namentlich die GRCh (und auch die EMRK).²²

Die „Haushaltsausnahme“ beruht auf dem Grundrecht der Achtung des Privat- und Familienlebens (Art. 7 GRCh). Demnach hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. Die „Haushaltsausnahme“ schützt durch die Ausnahme von der DS-GVO das Familien- und Privatleben. Als Grundrecht adressiert Art. 7 GRCh zuvorderst natürliche Personen. So könnte also die grundrechtliche Verankerung des Art. 2 Abs. 2 lit. c DS-GVO einer Erweiterung dieser auf juristische Personen und Personengesellschaften entgegenstehen, denn die GRCh kennt keine dem Art. 19 Abs. 1 GG entsprechende Vorschrift. Allerdings ist anerkannt, dass Art. 7 GRCh in Bezug auf das Privatleben, die Wohnung und die Korrespondenz auch auf juristische Personen und Personengesellschaften anwendbar ist,²³ nicht aber in Bezug auf das Familienleben, da dieses dem Wesen nach nicht auf juristische Personen oder Personengesellschaften übertragbar ist.²⁴ So steht auch die grund-

rechtliche Verankerung des Art. 2 Abs. 2 lit. c DS-GVO dessen Erstreckung auf juristische Personen nicht entgegen.

c) Systematische Erwägungen

Weiterhin könnte jedoch die Systematik der DS-GVO einer weitergehenden Auslegung von Art. 2 Abs. 2 lit. c DS-GVO entgegenstehen. Die DS-GVO macht grundsätzlich keinen Unterschied, wer die Daten verarbeitet: Verantwortlicher im Rahmen der DS-GVO ist „jede natürliche oder juristische Person (...)“, Art. 4 Nr. 7 DS-GVO. So nimmt die DS-GVO also nicht grundsätzlich die Verarbeitung durch natürliche Personen von ihrem Anwendungsbereich aus. Art. 2 Abs. 2 lit. c DS-GVO trifft hier also nicht nur eine Ausnahmeregelung zum Anwendungsbereich, sondern bricht auch mit dem System der DS-GVO, keinen Unterschied zwischen der Verarbeitung durch juristische oder natürliche Personen zu machen. Dies könnte nur dann gerechtfertigt sein, wenn es keine Situationen gibt, in denen juristische Personen oder Personengesellschaften Daten im persönlichen oder familiären Bereich verarbeiten.²⁵ Wie oben dargelegt, gibt es aber Situationen, in denen Vereine oder Gesellschaften bürgerlichen Rechts Daten bei der Ausübung persönlicher oder familiärer Tätigkeiten verarbeiten.

Die DS-GVO unterscheidet zwar grundsätzlich nicht nach dem Risiko oder der Größe der Datenverarbeitung, sondern regelt die Datenverarbeitung umfassend. So kennt die DS-GVO grundsätzlich keine kategorialen „Sektorausnahmen“ für besonders risikoreiche Verarbeitungen oder strengere Regelungen für besonders risikoreiche Verarbeitungen.²⁶ Allerdings stellt die „Haushaltsausnahme“ letztendlich eine der wenigen Ausnahmen solcher Art dar, denn im familiären und persönlichen Verarbeitungsbereich ist das Risiko der Datenverarbeitung spezifisch. Aufgrund des familiären und persönlichen Kontexts kommt es gerade nicht zu der typischen Gefahrenlage, vor welcher die DS-GVO die Betroffenen (zu Recht) schützt. Dies ist unabhängig davon, ob der Verarbeitende natürliche oder juristische Person oder Personengesellschaft ist.

d) Ergebnis

Der Erweiterung von Art. 2 Abs. 2 lit. c DS-GVO auf juristische Personen und Personengesellschaften stehen also weder die Schutzziele oder die Systematik der DS-GVO, noch das höherrangige Recht entgegen.

19 Hornung/Spiecker gen. Döhmman, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Aufl. 2019, Art. 1 Rn. 2, mit Hinweis auf: Spiecker gen. Döhmman, Staatliche Entscheidungen unter Unsicherheiten, i.E. 2019.

20 Zerdick, in: Ehmman/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, DS-GVO Art. 2 Rn. 10.

21 Von Lewinski, in: Auernhammer, DS-GVO/BDSG, 7. Aufl. 2020, § 1 BDSG Rn. 10.

22 Hier wird nur auf die näherliegende GRCh eingegangen. Zum Verhältnis: Gusy/Eichenhofer, in: BeckOK Datenschutzrecht, 31. Ed. Stand: 01.11.2019, BDSG § 1 Rn. 42.

23 EuGH, Urt. v. 14.02.2008 – C-450/06, NVwZ 2008, 651 ff. – Varec.

24 Jarass, in: Jarass, Charta der Grundrechte der EU, 3. Aufl. 2016, EU-GRCh Art. 7 Rn. 21 m.w.N.

25 Dieser Auffassung folgt: Kühling/Raab, in: Kühling/Buchner, DS-GVO, 2. Aufl. 2018, Art. 2 Rn. 23 m.w.N.

26 Hornung/Spiecker gen. Döhmman, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Aufl. 2019, Art. 1 Rn. 6.

III. Auswirkungen der Anwendung der DS-GVO auf die Datenverarbeitung von Vereinen und Gesellschaften bürgerlichen Rechts im familiären und persönlichen Bereich

Zuletzt lässt sich noch fragen, welche Auswirkungen die Pflicht zur Anwendung der DS-GVO auf den hier als Beispiel gewählten Familienverein und die Wohngemeinschafts-GbR hat. Werden Fotos aufgenommen und den Vereinsmitgliedern oder Mitgliedern der Wohngemeinschaft zur Verfügung gestellt, so ist unter Umständen sogar die dokumentierte Einwilligung aller auf den Bildern abgebildeten Personen einzuholen, vgl. Art. 6 lit. a, 7 DS-GVO; es ist aber mindestens die Rechtmäßigkeit der Verarbeitung nach Art. 6 lit. a-f DS-GVO nachzuweisen. Wird ein Kontaktverzeichnis mit den Kontakten aller Mitglieder geführt, so ist bei der erstmaligen Erhebung der Daten die Informationspflicht nach Art. 13 DS-GVO einzuhalten. Werden die Treffen des Familienvereins heutzutage online per Video-Konferenz abgehalten oder verwendet die Wohngemeinschaft als GbR eine Messenger-Applikation und einen gemeinsamen Google-Kalender zu Organisation des täglichen Lebens, so ist die Verantwortlichkeit zu klären, und es sind möglicherweise Verträge über die Auftragsverarbeitung mit den jeweiligen Anbietern zu schließen, Art. 24 ff. DS-GVO. Es ist generell zu beachten, dass die Datenverarbeitung nach den Grundsätzen der DS-GVO eingehalten wird, Art. 5 ff. DS-GVO, was gerade den Aufwand mit sich bringt, welcher im Rahmen des Familienlebens verhindert werden sollte und weswegen die „Haushaltsausnahme“ eingeführt wurde.

IV. Ergebnis

Eine generelle Unterwerfung der privaten Lebensgestaltung unter das Datenschutzregime scheint angesichts der Berührungspunkte zur Privat- und Intimsphäre wenig sachgerecht,²⁷ dies gilt auch dann, wenn die Verarbeitung de facto durch eine juristische Person oder Personengesellschaft vorgenommen wird. Im Ergebnis spricht also alles dafür die Art. 2 Abs. 2 lit. c DS-GVO auf juristische Personen und Personengesellschaften zu erweitern, soweit diese die Daten im Rahmen einer persönlichen und familiären Tätigkeit verarbeiten.

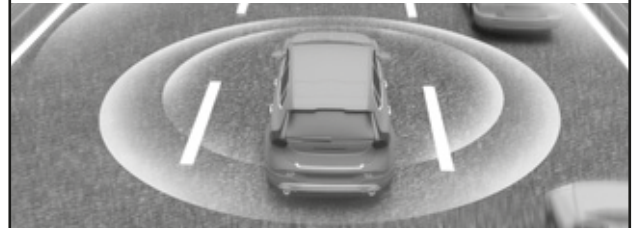


Sophie Derfler

Die Autorin ist wissenschaftliche Mitarbeiterin und Doktorandin am Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht an der Universität Passau. In dieser Kapazität forscht und lehrt Frau Derfler im Medien- und Datenschutzrecht.

27 Kühling/Raab, in: Kühling/Buchner, DS-GVO, 2. Aufl. 2018, Art. 2 Rn. 28, m.w.N.

DATENDEBATTEN



Unbeobachtete Fahrt für freie Bürger?



Datenschutz im vernetzten Fahrzeug

Herausgegeben von der **Stiftung Datenschutz**
Mit einem Geleitwort von **Gerhart R. Baum**,
Bundesminister a. D.

2020, ca. 208 Seiten, fester Einband,
€ (D) 44,-, ISBN 978-3-503-18754-6
eBook: € (D) 40,40, ISBN 978-3-503-18755-3
DatenDebatten, Band 4

Wie sich **Sicherheitsgewinne und Komfort** des vernetzten Fahrens mit dem **Grundrechtsschutz der Fahrenden** vereinigen lassen, beleuchtet der neueste Band der DatenDebatten, der Expertenbeiträge über das gesamte Spektrum beteiligter Perspektiven enthält.

Online informieren und bestellen:

 www.ESV.info/18754

ESV ERICH
SCHMIDT
VERLAG

Auf Wissen vertrauen

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

Kurzbeiträge

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (47): Einzelaspekte des Beschäftigtendatenschutzes in den neuen Tätigkeitsberichten der BremLfD und der BlnBfDI

Zusammengestellt und erläutert von Prof. Peter Gola*

In ihrem am 20.03.2020 vorgelegten 2. TB (2019) zur DS-GVO greift die Landesdatenschutzbeauftragte von Bremen u.a. folgende den Beschäftigtendatenschutz betreffende Fälle auf (Kap. 11):

I. Aufzeichnung von Call-Center-Telefonaten (2. TB, Ziff. 11.2)

Weiterhin vertritt die LfD eine sehr einschränkende Auffassung zur Zulässigkeit von Aufzeichnungen von Anrufen durch ein Callcenter. Danach sollen die Aufzeichnungen von eingehenden Anrufen in einem Callcenter zum Zweck der späteren Auswertung zur Schulung der Beschäftigten in der Regel mangels deren Erforderlichkeit gegen Datenschutzrecht verstoßen (§ 26 Abs. 1 S. 1 BDSG). Eine Einwilligung komme mangels Freiwilligkeit als Rechtsgrundlage ebenfalls im Regelfall nicht in Betracht (siehe zu den besonderen Anforderungen an die Erteilung einer Einwilligung durch Beschäftigte auch Ziffer 11.8 dieses Berichts).

II. Unzulässigkeit der Kenntlichmachung des Herkunftslands für Hilfskräfte im Supermarkt

Als unzulässig bewertete es die LfD auch, dass ein Arbeitgeber von in einem Supermarkt beschäftigten Flüchtlingen verlangte, bei der Arbeit ein Schild mit ihrem Namen und einer Flagge des Herkunftslands zu tragen. Auch von Beschäftigten mit Außenkontakt dürfe ein Arbeitgeber nicht verlangen, ihr Herkunftsland während der Arbeitszeit offenzulegen, insbesondere nicht durch das Tragen entsprechender Schilder oder Kennzeichnungen auf der Kleidung. Dies gelte auch für Hilfskräfte. Angesichts des Beschäftigungskontexts sei auch eine wirksame Einwilligung nicht denkbar.

III. Aufforderung zur Einrichtung eines Zugriffs auf dienstliche E-Mail-Postfächer

Ebenfalls als unzulässig bewertete die LfD eine Aufforderung an Bedienstete, für eventuelle Vertretungsfälle die

Möglichkeit eines Vertretungszugriffs auf die personalisierten dienstlichen E-Mail-Postfächer einzurichten. Dies gelte nicht nur, wenn das Konto auch privat genutzt werden darf. Die geltenden Vorschriften in der Freien Hansestadt Bremen enthielten hierfür keine Rechtsgrundlage; vgl. die Verwaltungsvorschrift zu Kommunikation und Dokumentenverwaltung in der Freien Hansestadt Bremen (VV KommDok). Eine Einwilligung als Rechtsgrundlage sei angesichts des Beschäftigtenkontexts nur in Ausnahmefällen denkbar und könnte allenfalls die Bedenken im Hinblick auf den Beschäftigtendatenschutz ausräumen.

IV. Zurücksetzung des Passworts von Mitarbeitern bei Abwesenheit

Nach der LfD kann jedoch der Zugriff auf passwortgeschützte Beschäftigtenkonten bei insbesondere längerer oder unvorhergesehener Abwesenheit auch ohne vorherige Zustimmung der Betroffenen zulässig sein. Der dienstlich unvermeidbare Zugriff ist auf das Mindestmaß zu beschränken und genau zu dokumentieren. Im Anschluss ist für einen erneuerten Passwortschutz zu sorgen und der Betroffene unverzüglich zu informieren.

V. Zum Einsatz von Ortungssystemen in Firmenfahrzeugen

Auch in Fahrzeugen von Fahrdiensten für Senioren oder Menschen mit Behinderungen beurteilt die LfD eine kontinuierliche Echtzeitbeobachtung des Standorts der Fahrzeuge schon wegen des dadurch erzeugten lückenlosen Überwachungsdrucks idR für unzulässig; um so mehr gelte das für eine längerfristige Speicherung der erfassten Ortungsdaten zwecks der Erstellung von Bewegungsprofilen. Da der Einsatz von Ortungssystemen wie dem Global Positioning System (GPS) oder ähnlicher Technologie in den den Beschäftigten zur Nutzung überlassenen Firmenfahrzeugen nicht

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

zur Verhaltenskontrolle genutzt werden dürfe, müsse der Arbeitgeber ein anderes legitimes Interesse haben und die Verarbeitung auf das für diesen Zweck erforderliche Maß begrenzen sowie gegen anderweitige Nutzung technisch und organisatorisch absichern.

VI. Ineffektivität der Aufzeichnung elektronischer Zugangsdaten

Unzulässig sind elektronische Zugangssysteme, die mithilfe personalisierter elektronischer Schlüssel die genauen Zutrittszeiten der Beschäftigten aufzeichnen, wenn gleichzeitig die gesicherten Türen mit einem anderen Schlüsselinhaber ohne Nutzung des eigenen Schlüssels passiert werden können. Insbesondere für eine Prävention oder Verfolgung von Straftaten sei eine derart gestaltete Datenerhebung nicht geeignet.

VII. Keine Anwendung des § 4 BDSG auf Videoüberwachungen zu privaten Zwecken

Die LfD weist insoweit auf das Urteil des Bundesverwaltungsgericht vom 27. März 2019 (Aktenzeichen 6 C 2.18) hin, nach dem § 4 BDSG mangels diesbezüglicher mitgliedstaatlicher Gesetzgebungskompetenz auf private Stellen nicht anwendbar sei. Rechtsgrundlage für Videoüberwachungen durch nicht öffentliche Stellen selbst und in deren Auftrag tätige Verarbeitende könnten nur die Regelungen der Datenschutzgrundverordnung (DS-GVO) sein. Die LfD stellt jedoch die Frage, ob in dem vorliegenden Fall der Videoüberwachung in einer ärztlichen Praxis nicht auf Art. 6 Abs. 1 DS-GVO, sondern allenfalls auf Art. 9 DS-GVO als Rechtsgrundlage hätte zurückgegriffen werden müssen, da von der Videoüberwachung insbesondere Patientinnen und Patienten und damit Gesundheitsdaten als besondere Kategorien personenbezogener Daten betroffen seien, wobei sie offen lässt, ob dies zu einem anderen Ergebnis führen würde.

--> *Die Berliner Beauftragte für Datenschutz und Informationsfreiheit berichtet im 8. Kapitel ihres im März 2020 erschienenen Tätigkeitsbericht u.a. über nachfolgende Fälle des Beschäftigtendatenschutzes.*

I. Herausgabe der E-Mail-Kommunikation eines Beschäftigten

Die LfDI hält zunächst fest, dass ein Arbeitgeber einem Beschäftigten spätestens innerhalb eines Monats nach Eingang eines Auskunftsersuchens die gesetzlich gebotenen Informationen zur Verfügung zu stellen habe. Das Auskunftsrecht gewähre jedoch keinen umfassenden Anspruch auf Herausgabe der kompletten Kommunikation, die über das E-Mail-System eines Unternehmens geführt wurde. Dies begründet die LfDI wie folgt: Eine vollständige Herausgabe aller E-Mails aus dem System des Unternehmens, in denen der Name der Beschwerdeführerin auftaucht, ist schon allein deshalb nicht möglich, weil das Recht auf Herausgabe einer Datenkopie durch die Rechte und Freiheiten anderer

Personen beschränkt wird. In einer E-Mail-Kommunikation tauchen ggf. zahlreiche andere Personen (insbesondere andere Mitarbeitende des Unternehmens und Externe) auf, so dass hier umfangreiche Rückschlüsse auf personenbezogene Daten Dritter möglich waren. Des Weiteren wäre mit einer umfassenden Herausgabe auch die Kenntniserlangung über interne Abläufe, Betriebsgeheimnisse und Know-how des Unternehmens oder der mit ihm verbundenen Unternehmen verbunden gewesen. Dem standen berechnete Unternehmensinteressen entgegen.

Damit kommt die LfDI zu folgendem Ergebnis: An der Aushändigung von rein dienstlich veranlasster Korrespondenz besteht nach der Beendigung des Arbeitsverhältnisses kein berechtigtes Interesse. Andererseits seien Daten von Unterhaltungen, die die Beschäftigte im erlaubten Umfang zu privaten Zwecken geführt hatte, an sie herauszugeben. Ehemalige Beschäftigte haben somit grundsätzlich einen Anspruch darauf, ihre privaten E-Mails zu erhalten.

II. Löschung von Daten nach Ende des Beschäftigungsverhältnisses

Eine Beschäftigte hatte mit ihrem Arbeitgeber einen Aufhebungsvertrag zur Beendigung des Beschäftigungsverhältnisses geschlossen. Dieser enthielt die Verpflichtung des Arbeitgebers, spätestens sechs Wochen nach Beendigung des Arbeitsverhältnisses das Profil der Beschäftigten auf der Webseite des Unternehmens zu löschen. Eine Bestätigung dieser Löschung erhielt die Beschwerdeführerin wenig später. In der Folgezeit stellte sie jedoch fest, dass durch Verlinkung auf der Webseite des Unternehmens noch ein Lebenslauf von ihr zu finden war. Nachdem sie hiergegen Widerspruch eingelegt hatte, hat das Unternehmen diese Verlinkungen unverzüglich gelöscht.

Die LfDI stellt dazu fest, dass ungeachtet einer möglicherweise erteilten Einwilligung der Beschwerdeführerin zur Bekanntgabe des Lebenslaufs diese jedenfalls nach Beendigung des Arbeitsverhältnisses keine Wirkung mehr hatte. Zwar könne die DS-GVO keine Geltungsdauer einer Einwilligung, allerdings unterliege auch die Verarbeitung personenbezogener Daten aufgrund einer Einwilligung im Rahmen eines Arbeitsverhältnisses dem Gebot der Zweckbindung. Unter Berücksichtigung dieses Gebots müsse deshalb davon ausgegangen werden, dass eine Einwilligung zur Veröffentlichung eines Lebenslaufs – auch ohne deren jederzeit zulässigen Widerruf – auf den Zeitraum des Beschäftigungsverhältnisses beschränkt ist.

III. Notizen im Verfahren des betrieblichen Eingliederungsmanagements

Dass auch bei einem dienstlichen Gespräch geführte Notizen dem Auskunftsrecht unterliegen legte die LfDI im Zusammenhang mit einem Verfahren zum betrieblichen Eingliederungsmanagement (BEM) klar. Das bei einem diesbezüglichen Gespräch mit einer Beschäftigten geführte Protokoll fehlte jedoch bei der von ihr genommenen Akten-

einsicht. Auf Nachfrage wurde ihr mitgeteilt, dass ein entsprechendes Protokoll nicht existiere bzw. noch nicht freigegeben sei und im Übrigen auch nicht Bestandteil der BEM-Akte wäre, da es sich um handschriftliche Notizen eines BEM-Beteiligten handle und daher eine Einsichtnahme nicht gewährt werden könne. Dagegen wandte sich die Betroffene mit ihrer Beschwerde.

Die LfDI stellt hierzu fest: Nach der DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden bzw. wurden. Der Verantwortliche hat insbesondere eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind bzw. waren, der oder dem Betroffenen zur Verfügung zu stellen oder, wie im vorliegenden Fall erwünscht, eine Einsichtnahme in die Daten zu gewähren. Das gilt auch für handschriftliche Notizen eines Teilnehmers bei einem sog.

Erörterungsgespräch. Diese waren für den Dienstbetrieb erforderlich, da ohne schriftliche Fixierung bzw. ohne Protokolle Maßnahmen oder Hilfestellungen nicht konkret und korrekt umgesetzt und die Betroffene nicht umfassend über das Ergebnis der Fallbesprechung informiert werden konnte.

Damit konnte sich der Arbeitgeber vorliegend nicht auf eine Entscheidung des Bundesverwaltungsgerichts (Urteil vom 19. Oktober 2005 – 1 D 14/04) berufen, nach der Notizhefte, Tagebuchkladden etc. keine Personalvorgänge sind, soweit sie durch individuelle Bestimmung des Besitzers für den ausschließlich persönlichen Gebrauch geführt werden, selbst wenn ihr Inhalt dienstliche Bezüge aufweist. Als einzige Voraussetzung bzw. Bedingung für die Führung solcher Kladden oder Hefte mit persönlichen Notizen ist nach dieser Entscheidung eine sichere Aufbewahrung vor dem Zugriff von Dritten bzw. anderen Personen (z.B. Kolleginnen und Kollegen, Reinigungskräfte etc.).

Praxisfälle zum Datenschutzrecht V: Musterfalllösungen zur automatisierten Kennzeichenerfassung im Parkhaus

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

I. Sachverhalt

Der Baumarkt B möchte für seine Kunden ein von diesen kostenlos zu nutzendes Parkhaus betreiben. Dabei soll die Parkzeit auf maximal zwei Stunden beschränkt sein, wodurch regelmäßig genügend Kundenparkplätze bereitstehen sollen. Zum Zwecke eines verbesserten Parkraummanagements ist beabsichtigt, die Kennzeichen der ein- und ausfahrenden Fahrzeuge per Videoaufzeichnung zu erfassen. Die Systemsoftware liest aus den Videosequenzen automatisch das Kennzeichen ab und speichert es in digitalisierter Form zusammen mit der Einfahrtszeit. Bei der Ausfahrt, die durch eine Schranke abgesichert ist, soll dann ein Abgleich mit dem hinterlegten Kennzeichen erfolgen. Hat der Kunde die Kurzparkzeit eingehalten, wird die Ausfahrtsschranke automatisch geöffnet. Hat jemand die kostenlose Kurzparkzeit überschritten, muss er gegen Zahlung einer bewusst hoch angesetzten Parkgebühr ein Ticket ziehen, und die Schranke öffnet sich erst nach Eingabe des bezahlten Tickets. Nach Verlassen des Parkhauses werden die Kennzeichen der Kfz und Kunden gelöscht.

B wendet sich an die Aufsichtsbehörde und bittet um Beurteilung der Zulässigkeit des geplanten Kennzeichenerfassungssystems.

II. Musterfalllösung

1. Die Aufsichtsbehörde als „Berater“

Fraglich ist zunächst, inwieweit die zuständige Aufsichtsbehörde verpflichtet ist, den Baumarkt B im Hinblick auf die Zulässigkeit des geplanten Kennzeichenerfassungssystems zu beraten.

Die DS-GVO enthält keine umfassende Beratungspflicht der Aufsichtsbehörde gegenüber den Verantwortlichen bzw. Auftragsverarbeitern. Zwar haben die Aufsichtsbehörden gemäß Art. 57 Abs. 1 lit. d DS-GVO die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten zu sensibilisieren. Gemeint ist hiermit aber v.a. eine allgemeine Ansprache, z.B. durch Informationsmaterial oder die Durchführung von Informationsveranstaltungen.¹ Eine „echte“ Beratungspflicht ist lediglich für solche Fälle vorgesehen, in denen die

* Miriam Claus, LL.M. ist Referentin bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.; RAin Yvette Reif, LL.M. ist stellvertretende Geschäftsführerin der GDD und Mitautorin des Werks Gola/Reif, Praxisfälle Datenschutzrecht, 2. Aufl. 2016.

¹ Wolff/Brink/Eichler BeckOK Datenschutzrecht, 31. Edition (Stand: 01.05.2019), Art. 57 Rn. 13; Aussagen zum „Kameraeinsatz bei der Bewirtschaftung von Parkflächen“ bzw. zu „Kennzeichenerfassungssystemen im Bereich von Parkflächen“ finden sich beim Unabhängigen Datenschutzzentrum Saarland, 25. Tätigkeitsbericht (2013/2014), Ziff. 19.10 sowie bei der LDI NRW, 22. Datenschutzbericht (2015), Ziff. 6.4.

Aufsichtsbehörde im Rahmen der vorherigen Konsultation (Art. 36 DS-GVO) zu dem Ergebnis gekommen ist, dass die geplante Verarbeitung nicht im Einklang mit der Verordnung stünde (Art. 57 Abs. 1 lit. l DS-GVO). Ein solcher Fall liegt hier nicht vor.

Der DS-GVO wird man allerdings eine allgemeine Beratungspflicht gegenüber dem/der Datenschutzbeauftragten des Verantwortlichen bzw. Auftragsverarbeiters entnehmen müssen. Nach Art. 39 Abs. 1 lit. e DS-GVO ist der/die Datenschutzbeauftragte „Anlaufstelle“ der Aufsichtsbehörde in mit der personenbezogenen Datenverarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 DS-GVO, und berät mit dieser ggf. zu allen sonstigen Fragen. Hieraus resultieren nicht nur Pflichten auf Seiten des/der Datenschutzbeauftragten, sondern auch das Recht, Beratung durch die Aufsichtsbehörde in Anspruch zu nehmen. Nach Art. 57 Abs. 3 DS-GVO sind die Leistungen der Aufsichtsbehörde für den DSB unentgeltlich. Die Beratungspflicht im Verhältnis zum Datenschutzbeauftragten hilft vorliegend allerdings nicht weiter, weil es sich um ein Beratungersuchen des Verantwortlichen selbst handelt, nämlich des Baumarkts B.

Auch die Beratungspflicht der Aufsichtsbehörden aus § 40 Abs. 6 S. 1 BDSG bezieht sich nur noch auf den/die Datenschutzbeauftragte/n und anders als die Vorgängernorm in § 38 Abs. 1 S. 2 BDSG 2009 nicht mehr auf die verantwortliche Stelle.

Ergebnis: Ein entsprechender Beratungsanspruch des Baumarktes B besteht nicht. Soweit ein/e Datenschutzbeauftragte/r benannt ist, könnte von der Beratung der Aufsichtsbehörde ggf. über diesen „Umweg“ profitiert werden. Angesichts der begrenzten Ressourcen der Aufsichtsbehörden wird sich dessen Rechtsanspruch allerdings auch nicht auf eine umfassende Beratung in allen technischen und rechtlichen Detailfragen beziehen können.²

2. Datenschutzrechtliche Zulässigkeit der Verarbeitung von Kfz-Kennzeichen

a) § 4 BDSG

Bei dem Parkhaus handelt es sich um einen öffentlich zugänglichen Raum, dessen Nutzung durch eine automatisierte Verarbeitung der mittels der Videoaufnahmen erhobenen Kennzeichen überwacht werden soll. Die DS-GVO enthält keine besondere Regelung zur Videoüberwachung, allerdings hat der nationale Gesetzgeber mit § 4 BDSG eine Bestimmung geschaffen, welche die Videoüberwachung öffentlich zugänglicher Räume speziell regelt. Damit könnte vorliegend § 4 Abs. 1 BDSG als Zulässigkeitsnorm für die Beobachtung und § 4 Abs. 3 BDSG für die nachfolgende Speicherung und Auswertung der erhobenen Daten heranzuziehen sein. Keine Rolle dürfte es für die Anwendung der Norm spielen, dass die Videokamera die betroffenen Personen nicht als Bild erfasst. Als ausreichend wird man ansehen müssen, wenn die Beobachtung und Erfassung durch das optisch-elektronische Verfahren gleichwohl Rückschlüsse auf eine konkrete natürliche Person zulässt.

Der Schutz der DS-GVO dient der Vermeidung von Verletzungen der Grundrechte und -freiheiten natürlicher Personen im Hinblick auf ihre personenbezogenen Daten. Personenbezogene Daten gem. Art. 4 Nr. 1 DS-GVO umfassen alle Informationen, die Rückschlüsse auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) zulassen. „Identifizierbar“ ist eine betroffene Person, wenn diese direkt oder auch indirekt mittels Zuordnung bspw. zu einer Kennung identifiziert werden kann.³ Beispiele für solche Kennungen sind Konto- oder Personalausweisnummern oder das Kfz-Kennzeichen (vgl. hierzu die diesbezügliche Aussage in § 45 S. 2 StVG).⁴ Mittels des Kfz-Kennzeichens kann der Halter des Fahrzeugs ermittelt werden. Dieser kann sowohl eine juristische als auch eine natürliche Person sein. Die bei den Kfz-Zulassungsstellen gespeicherten Halterdaten sind zwar nicht öffentlich zugänglich, jedoch kann auch Privatpersonen Auskunft aus dem Fahrzeugregister nach § 39 StVG erteilt werden, wenn diese ein verkehrsbezogenes Interesse an der Auskunft haben und die entsprechenden Gründe in ihrem Antrag darlegen. Damit ist die Identifizierbarkeit des Halters für die einschlägigen Behörden wie auch für Privatpersonen gegeben.⁵ Mithin sind Kfz-Kennzeichen personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO.

Jedoch hat das BVerwG in seiner Entscheidung vom 27.03.2019⁶ festgestellt, dass die DS-GVO die Videoüberwachung durch nichtöffentliche Stellen zu privaten Zwecken abschließend regelt und daher insoweit Art. 6 Abs. 1 S. 1 lit. f DS-GVO als Maßstab für die Rechtmäßigkeit heranzuziehen sei. Eine Öffnung für den nationalen Gesetzgeber sei gem. Art. 6 Abs. 2 DS-GVO nur für die Fälle nach Art. 6 Abs. 1 S. 1 lit. c und e DS-GVO vorgesehen. Die gleiche Ansicht wie das BVerwG vertritt auch die Datenschutzkonferenz in ihrem Kurzpapier Nr. 15.⁷ Demnach ist für die Beurteilung der datenschutzrechtlichen Zulässigkeit der Kennzeichendatenverarbeitung hier Art. 6 Abs. 1 S. 1 lit. f DS-GVO heranzuziehen.

b) Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f DS-GVO)

Die geplante Kennzeichendatenverarbeitung müsste zunächst für die Wahrung eines berechtigten Interesses des Bauhauses erforderlich sein. Auch wenn Art. 6 Abs. 1 S. 1 lit. f DS-GVO anders als § 4 BDSG nicht zwischen den Phasen der „Beobachtung“ und der „Speicherung oder Verwendung“ unterscheidet, sondern nur allgemein an die „Verarbeitung“ i.S.v. Art. 4 Nr. 2 DS-GVO anknüpft, ist im Hinblick auf die

2 Kühling/Buchner/Dix, DS-GVO BDSG, 2. Aufl. 2018, § 40 BDSG Rn. 16; Simitis/Hornung/Spiecker gen. Döhmman/Polenz, Datenschutzrecht, 1. Aufl. 2019, Art. 57 Rn. 22.

3 Siehe hierzu Weichert, Der Personenbezug von Kfz-Daten, NZV 2017, 507 ff., 509.

4 Siehe hierzu ausführlich Bergt, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts, ZD 2015, 365.

5 Vgl. auch bei Buschbaum/Rosak, Kfz-Kennzeichenerfassung in Parkhäusern, ZD 2015, 354 ff., 355.

6 BVerwG, Urteil vom 27.03.2019 – BVerwG 6 C 2.18 (<https://www.bverwg.de/270319U6C2.18.0>).

7 DSK Kurzpapier Nr. 15 – Videoüberwachung nach der Datenschutz-Grundverordnung, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf.

Rechtmäßigkeit im Grundsatz gleichwohl jede Verarbeitungsphase isoliert zu betrachten. So kann es etwa sein, dass die ursprüngliche Videobeobachtung und Speicherung der Daten zulässig waren, eine spätere (zweckändernde) Verwendung aber nicht zulässig ist. Auch gibt es Fälle, in denen zwar die Videobeobachtung also solche erlaubt ist, nicht aber die Speicherung der Daten.

Ein berechtigtes Interesse i.S.v. Art. 6 Abs. 1 S. 1 lit. f DS-GVO können nicht nur rechtliche, sondern auch rein tatsächliche, wirtschaftliche oder ideelle Interessen begründen. In jedem Fall dürfen nur solche Interessen im Rahmen der Abwägung berücksichtigt werden, die mit der Rechtsordnung vereinbar sind. Das Interesse des das Parkhaus betreibenden Baumarktes an einem geordneten Parkhausmanagement, insbesondere an einer Vermeidung einer Überschreitung der eingeräumten Zeit zum kostenfreien Parken, stellt ein berechtigtes Interesse im vorgenannten Sinne dar.

Fraglich ist allerdings, ob die geplante Kennzeichendatenverarbeitung zum Erreichen des berechtigten Interesses „geordnetes Parkhausmanagement“ auch i.S.v. Art. 6 Abs. 1 S. 1 lit. f DS-GVO erforderlich ist.

Erforderlichkeit setzt zum einen voraus, dass die Maßnahme geeignet ist, das Überwachungsziel zu erreichen. Zum anderen ist unter dem Gesichtspunkt der Verhältnismäßigkeit eine Überwachungsmaßnahme nicht erforderlich, wenn das Ziel auch durch ein gleichermaßen wirksames, aber die betroffene Person in ihren Rechten weniger beeinträchtigendes „milderes Mittel“ erreicht werden kann. Das mildere Mittel muss für den Verantwortlichen aber auch zumutbar sein. Investitionen in unzumutbarer Höhe müssen nicht vorgenommen werden.⁸ Ein milderes Mittel im vorliegenden Fall läge insbesondere dann vor, wenn der Zweck der Verarbeitung auch ohne Verarbeitung personenbezogener Daten erreicht werden könnte. Das gewünschte Ziel des Parkraummanagements, nämlich die Einhaltung der maximal vorgesehenen Parkdauer, um konstant ausreichend Parkmöglichkeiten für die Kunden vorzuhalten, könnte durch ein anonymes Ticketsystem, bei dem die ersten zwei Stunden kostenfrei sind, ebenfalls erreicht werden. Die Kunden würden also von Anfang an ein Ticket ziehen und nicht nur dann, wenn sich die Schranke nicht öffnet. Wird das Zeitlimit zum kostenfreien Parken eingehalten, kommt der Kunde ohne Zahlung mit dem Ticket wieder durch die Schranke heraus. Sofern das Limit nicht eingehalten wird, muss er zuvor am Parkautomat bezahlen. Voraussetzung ist insofern allerdings, dass der Einsatz des Ticketsystems wirtschaftlich

zumutbar ist. Dies ist hier wohl anzunehmen, da die Ausfahrtkontrolle ohnehin mittels entsprechender Technik erfolgen soll, wenn die maximale kostenfreie Parkdauer überschritten wurde.

Die geplante automatisierte Kennzeichenerfassung ist also nicht über Art. 6 Abs. 1 S. 1 lit. f DS-GVO erlaubt.

c) Einwilligung

Die geplante Kennzeichenerfassung kann auch nicht per Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO) legitimiert werden. Ein vor der Einfahrt angebrachtes Schild mit der Aufschrift „Videoüberwachung“ oder „Kennzeichenerfassung“ würde den Informationspflichten vor Einholung einer – hier konkludenten⁹ – Einwilligung nicht genügen. Durch diese Maßnahmen erhalten die Betroffenen nicht alle Informationen, die notwendig sind, um Anlass, Ziel und Folgen der Datenverarbeitung abschätzen zu können.¹⁰ Zudem muss die Einwilligung von der betroffenen Person erteilt werden, wobei die fahrzeugführende Person aber nicht selten mit dem Halter nicht identisch sein wird.

d) Gesamtergebnis

Das geplante Kennzeichenerfassungssystem ist datenschutzrechtlich unzulässig, und anstelle dessen sollte ein anonymes Ticketsystem in Betracht gezogen werden.

Ergänzender Hinweis: Für den vorliegenden Fall ist von wesentlicher Bedeutung, dass die Nutzung des Parkhauses unentgeltlich ist. In anderen Fällen kann eine automatisierte Kennzeichenerfassung ggf. unter Berücksichtigung der spezifischen Gegebenheiten des Einzelfalls als datenschutzrechtlich zulässig erachtet werden, wenn ihr Einsatz zu einer besseren Sicherung der Parkeinahmen erforderlich ist.¹¹ Aufgetretene Probleme bei unlesbaren, verlorenen oder ausgetauschten Tickets können dann unstrittig klargestellt werden. Die gesetzlichen Informationspflichten aus Art. 13 f. DS-GVO sind zu beachten.

⁸ Vgl. Taeger/Gabel/Taeger, DS-GVO BDSG, 3. Aufl. 2019, Art. 6 Rn. 112.

⁹ Eine „Einwilligung“ ist gemäß Art. 4 Nr. 11 DS-GVO „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.

¹⁰ LDI NRW, a.a.O.; zu den Informationspflichten bei der Einwilligung vgl. auch Gola/Schulz, DS-GVO, Art. 7 Rn. 36

¹¹ Zu den Voraussetzungen im Einzelnen vgl. LDI NRW, a.a.O.

powered by

GDD



**Erfüllen
Sie Ihre Rechen-
schaftspflicht!**

DA DATA AGENDA **Datenschutz Manager**

Gemeinsam Datenschutz gestalten!

- ✓ webbasiertes Management System
- ✓ für alle Datenschutzverantwortlichen im Unternehmen
- ✓ einfaches Erfassen und Dokumentieren aller Datenschutzmaßnahmen
- ✓ erleichtert die Zusammenarbeit aller verantwortlichen Stellen
- ✓ expertengeprüft und revisionsicher

Jetzt informieren: www.DataAgenda.de/datenschutzmanager

Anwendung der EU-Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DS-GVO) auf Datenübermittlungen an unselbständige Niederlassungen in Drittländern*

Dr. Georg Wronka**

I. Ausgangslage

Ebenso wie zahlreiche in der EU ansässige Wirtschaftsunternehmen von ihnen als Repräsentanzen, Zweigniederlassungen oder Verbindungsstellen bezeichnete Einrichtungen in Drittländern unterhalten, so verfügen auch international operierende Umweltschutzorganisationen, caritative Einrichtungen, politische Institutionen und viele weitere NGO's über Auslandsbüros zur Erreichung der von ihnen verfolgten Ziele. Dazu zählen etwa die Kunden- und Interessentenakquisition, der Aufbau von Kontakten zu Politik und Verwaltung des betreffenden Landes, die Anbahnung von Kooperationen, die Durchführung von Schulungen oder PR-, Bildungs- und sonstigen Veranstaltungen. Viele Dutzend politische Stiftungen – um ein Beispiel zu nennen – organisieren ihren Geschäftsbetrieb „vor Ort“ durchweg völlig selbständig, verfügen über eigene Budgets, entscheiden über die Auswahl benötigter lokaler Mitarbeiter und werden regelmäßig auch die datenschutzrechtlichen Qualifikationsmerkmale einer „Niederlassung“¹ aufweisen.² Sie sind, um es anders auszudrücken, keine bloßen von ihrer EU-„Zentrale“ ausgelagerten Fachabteilungen, sondern relativ komplexe Organisationen mit einem weiten Kompetenzbereich. Allerdings sind diese Funktionseinheiten großenteils nicht rechtsfähig – und das ist ein Kriterium, das hinsichtlich der datenschutzrechtlichen Einordnung ihrer Beteiligung an einzelnen grenzüberschreitenden Datenverarbeitungsprozessen nicht unbeachtet bleiben sollte.

Dass bei der Wahrnehmung sozialer, kultureller, gesellschaftlicher oder wirtschaftlicher Interessen in der jeweiligen Region auf zweckdienliche Informationen mit Bezügen zu konkreten Personen zugegriffen werden muss, bedarf keiner näheren Begründung. Sie werden üblicherweise unmittelbar von den Auslandseinrichtungen generiert, gespeichert, genutzt und in den weiteren in Art. 4 Nr. 2 DS-GVO aufgelisteten Formen verarbeitet, ohne dass die „hinter ihnen stehende“ Zentralinstitution oftmals überhaupt von ihnen Kenntnis erhält oder gar steuernd darauf Einfluss nehmen würde. Zur Unterstützung ihrer Arbeit erhalten sie aber auch ergänzende Informationen aus den Datenbeständen ihrer „Zentralen“ – Daten von Kunden, Interessenten, Wettbewerbern, Beratern, Politikern, Wissenschaftlern, Journalisten usw., über deren Verarbeitungszwecke und –mittel sie dann zumindest faktisch mitbestimmen. Derartige Datenleitungen aus der EU in ein Drittland sind an Zulässigkeitsregeln gebunden.

II. Rechtsrahmen

Bei der Übermittlung personenbezogener Daten aus der EU in ein Drittland sind nach Maßgabe der üblichen sog. Zweistufenprüfung neben dem Vorliegen der allgemeinen Zulässig-

keitsvoraussetzungen des Kapitels II der DS-GVO (1. Stufe) zusätzliche im Kapitel V der DS-GVO normierte Legitimationstatbestände (2. Stufe) zu berücksichtigen. Zu den letzteren zählen nach Art. 46 Abs. 2 lit. c DS-GVO „Standarddatenschutzklauseln“, die die EG-Kommission bereits in den Jahren 2001 und 2004³ erlassen hatte und die gem. Art. 46 Abs. 5 Satz 2 DS-GVO fortgelten. Sie werden in der verbindlichen Textvorgabe in Anlehnung an Art. 26 Abs. 4 der DS-Richtlinie⁴ mit „Standardvertragsklauseln“ überschrieben und beziehen sich auf die „Übermittlung zwischen für die Verarbeitung Verantwortlichen“ („controller to controller transfers“).

Daraus leiten sich vor dem Hintergrund der zu behandelnden Themenstellung einige grundsätzliche Fragen ab: Erfüllt der Datentransfer von der EU-„Zentrale“ an ihre unselbstständige Auslandsniederlassung das Merkmal der Übermittlung, sind zu den „Verantwortlichen“ auch nicht-rechtsfähige Einrichtungen wie unselbstständige Niederlassungen zu zählen, und können sie überhaupt als Parteien rechtswirksam ein solches „data transfer agreement“ vereinbaren? Immerhin: Auch wenn sich unter mehreren Gesichtspunkten Zweifel an der Einsatzfähigkeit der Vertragsklauseln geradezu aufdrängen, die Datenschutz-Aufsichtsbehörden wollen ihre Verwendbarkeit jedenfalls auch in Bezug auf derartige Rechtsbeziehungen nicht ausschließen.⁵

III. „Datenübermittlung“

Das bis zum 24.5.2018 in Deutschland geltende BDSG verlangte für die Annahme einer „Übermittlung“ durch eine verantwortliche Stelle für den Empfänger der Daten die Eigenschaft eines „Dritten“ (§ 3 Abs. 4 Satz 2 Nr. 3 BDSG alt), der wiederum selbst als (neue) verantwortliche Stelle anzu-

* Vortrag anlässlich des 80. Geburtstags von Peter Gola. Prof. Gola, Königswinter, Autor von über 200 Beiträgen zum Datenschutz und u.a. Verfasser eines Grundlagenwerks zum Beschäftigtendatenschutz sowie Herausgeber und Bearbeiter von Standardkommentaren zur DS-GVO und zum BDSG (Red.).

** Dr. Georg Wronka ist Rechtsanwalt in Bonn mit den Arbeitsschwerpunkten Datenschutz- und Wettbewerbsrecht.

1 Im Sinn von Art. 3 DS-GVO.

2 Vgl. ErwG 22 DS-GVO; EuGH Rs. C-131/12 – Google Spain; EuGH Rs. C-230/14 – Weltimmo.

3 Entscheidungen 2001/497 EG, ABL. EG 2001 L 181, S. 19 und 2004/915 EG, ABL. EU 2004 L 385, S. 74.

4 EG-Datenschutz-Richtlinie vom 24.10.1995 (95/46/EG), ABL. EG 1995 L 281, S. 31.

5 Beschluss des Düsseldorfer Kreises vom 19./20. April 2007 zu den „Abgestimmten Positionen der Aufsichtsbehörden in der AG, Internationaler Datenverkehr am 12./13. Februar 2007 unter Ziffer I.4.; 19. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucksache 16/5892, S. 26 f; Hillenbrand-Beck, RDV 2007, S. 231 (232 f); Gola, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 4 c Rn. 12.

sehen war (§ 3 Abs. 8 i.V. mit Abs. 7 BDSG alt). Diese Prämisse ist in Art. 4 Nr. 2 DS-GVO entfallen.⁶ So stellt nunmehr beispielsweise entgegen der früheren Rechtslage die Datenübertragung an einen Auftragsdatenverarbeiter eine Übermittlung dar,⁷ und nicht anders dürfte die Weitergabe von Personaldaten durch den Arbeitgeber an den Betriebsrat, dessen Qualifikation als Dritter immer noch überwiegend abgelehnt wird, zu beurteilen sein. Darauf hinzuweisen ist, dass der in den Vertragsklauseln verwandte Begriff der Übermittlung zurückgeht auf den in Art. 2 lit. b DS-Richtlinie benannten, der ebenfalls keinen Dritten voraussetzte. Darauf nehmen auch die Datenschutz-Aufsichtsbehörden Bezug und weiten den nationalrechtlichen Begriff der Übermittlung im Licht der übergeordneten europarechtlichen Vorgabe durch den Verzicht auf das Merkmal des Dritten inhaltlich aus.⁸ Kommt es mithin nicht auf dieses Charakteristikum des Datenempfängers an, so scheidet eine Datenübermittlung an eine unselbständige Auslandsniederlassung jedenfalls nicht bereits an diesem Kriterium.

IV. Datenexporteur und -importeur als „Verantwortliche“

Agiert auf Seiten des Datenexporteurs eine natürliche oder – so der Regelfall – juristische Person (AG, GmbH, Verein, Stiftung usw.), dürfte die Einordnung als Verantwortliche i.S. von Art. 4 Nr. 7 DS-GVO kaum in Frage gestellt werden. Nicht so eindeutig scheint hingegen die Zuweisung dieses Merkmals – in der Variante als „andere Stelle“ – an nicht rechtsfähige Empfänger zu sein, wie dies z.B. bei unselbständigen Zweigstellen (unselbständigen Niederlassungen, Betriebsstätten⁹) der Fall ist. Nach verbreiteter Auffassung sollen unselbständige Niederlassungen eines Unternehmens grundsätzlich nicht selbst als Verantwortliche in Betracht kommen können, sondern müssten diesem in dessen jeweiliger Rechtsform zugerechnet werden.¹⁰ Das gleiche sollte logischerweise auch für nicht-gewerblich/kaufmännisch operierende Einrichtungen von NGO's gelten.

Die Gegenansicht hält die Rechtsfähigkeit nicht für konstitutiv und vertritt gegenüber einer rein juristischen Betrachtungsweise¹¹ einen funktionalen Ansatz¹² für das Verständnis der „anderen Stelle“ als alternative Erscheinungsform des Verantwortlichen. Zur Begründung dieser Auffassung ließen sich durchaus mehrere Aspekte anführen. Zwar bleiben die Niederlassungen zivilrechtlich Teil der EU-„Zentrale“, also des Datenexporteurs, gleichwohl üben sie auf Grund des weiten Handlungs- und faktischen Entscheidungsspielraums, der den meisten Niederlassungen eingeräumt wird, bestimmen den Einfluss auf Art, Umfang und Verarbeitungsweise der ihren Zwecken dienenden Daten aus. An eine unselbständige Niederlassung knüpfen sich diverse Verpflichtungen – in Deutschland beispielsweise (bei wirtschaftlicher Betätigung) die Gewerbeanmeldung, in Polen die Registrierung der Datenverarbeitungsmaßnahmen bei der Datenschutzaufsichtsbehörde oder nach türkischem Recht die Benennung einer für die Datenverarbeitung der Stelle zuständigen Ansprechperson. Für die datenschutzrechtliche Unabhängigkeit der Niederlassung vom Vorliegen ihrer Rechtsfähigkeit könnte im

Übrigen auch die im ErWG 22 Satz 3 explizit zum Ausdruck gebrachte Vorstellung des europäischen Ordnungsgebers sprechen, derzufolge der Rechtsform einer Niederlassung keine maßgebliche Bedeutung zuzumessen sei.

Gleichwohl ist eine entscheidende Schwäche dieser Überlegungen nicht zu verkennen. Als Verantwortliche hätte eine nicht-rechtsfähige Niederlassung, auch wenn ihr die faktische Datenherrschaft übertragen wurde,¹³ in eigener Zuständigkeit die Voraussetzungen für die Rechtmäßigkeit ihrer Datenverarbeitung zu erfüllen (Art. 5 Abs. 2 DS-GVO) und wäre auch Adressat der datenschutzrechtlichen Pflichten sowie der Ansprüche der Betroffenen (Auskunft, Berichtigung, Löschung usw.). Diese hätten aber kaum – und dies ist ein entscheidendes Kriterium – die Möglichkeit, ihre Rechte gerichtlich durchzusetzen, da die dafür erforderlichen Voraussetzungen (Passivlegitimation) nicht vorliegen dürften. Eine Stelle, der gegenüber kein Rechtsschutz besteht, lässt sich schwerlich als Verantwortliche apostrophieren.

Kurzum: Von einer „controller to controller“-Übermittlung zu sprechen, wäre im vorliegenden Fall nicht korrekt, so dass sich eigentlich an diesem Punkt die Unanwendbarkeit der Vertragsklauseln in der vorgesehenen Form erweist. Hinzu tritt das zivilrechtliche Manko: Wenn der nicht rechtsfähige Datenimporteur Teil der rechtsfähigen datenexportierenden Zentrale bleibt, müsste eine Vereinbarung der Datenschutzklauseln zwischen der (von ihrem Leiter vertretenen) importierenden Stelle mit der Zentrale als unzulässiges In-sich-Geschäft bewertet werden¹⁴ – es sei denn, sie ließe sich rechtstechnisch anders verorten und würde z.B. durch Umdeutung Rechtswirkungen erzeugen.

V. Vorstellungen des Düsseldorfer Kreises

Die Aufsichtsbehörden hatten sich 2007 im Fall eines Drittlandbezogenen Datentransfers zwischen einem in Deutsch-

6 Herbst, in: Kühling/Buchner, DS-GVO – BDSG, 2. Aufl. 2018, Art. 4 Nr. 2 Rn. 29 f.; zur Diskussion, ob unselbständige Zweigstellen in Drittländern als Dritte angesehen werden können vgl. Hartung, in: Kühling/Buchner, Art. 4 Nr. 10 Rn. 6 m.N. in Fn. 8.

7 Roßnagel, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 4 Nr. 2 Rn. 26.

8 15. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucksache 15/4659, S. 14.

9 Zur Terminologie vgl. § 15 HGB, § 14 GewO und die dazu erlassenen Verwaltungsvorschriften der Länder, z.B. für Brandenburg die „Allgemeine Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c der Gewerbeordnung“ vom 25.01.1996, ABL. S. 186, Ziff. 3.2.

10 So etwa Weichert, in: Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG n.F., 2018, Art. 4 Rn. 88. I. E. ebenso Hartung, in: Kühling/Buchner, Art. 4 Nr. 7 Rn. 9. Die Aussagen von Schwartmann, in: Schwartmann/Jaspers/Thüsing/Kugelman, Datenschutz-Grundverordnung mit Bundesdatenschutzgesetz (Heidelberger Kommentar), 2018 wiederum sind nicht widerspruchsfrei. Einerseits spricht er unselbständigen Zweigstellen aufgrund der ihnen mangelnden Rechtsfähigkeit die Eigenschaft als Verantwortliche ab (Art. 4 Rn. 111), andererseits billigt er sie nicht rechtsfähigen Vereinen zu (Art. 4 Rn. 114).

11 Weichert, in: Däubler/Wedde/Weichert/Sommer, Art. 4 Rn. 88.

12 So Petri, in: Simitis/Hornung/Spiecker, Art. 4 Nr. 7 Rn. 16.

13 Vgl. Art.-29-Datenschutzgruppe, WP 169 vom 16.02.2010, S. 10 ff.; die Gruppe geht im Übrigen durchgängig davon aus, dass Verantwortliche stets entweder natürliche oder juristische Personen sind.

14 Beschluss des Düsseldorfer Kreises a.a.O. (Fn. 4); Hartung, in: Kühling/Buchner, Art. 4 Nr. 10 Rn. 6; Däubler, in: Däubler/Wedde/Weichert/Sommer, Art. 46 Rn. 16.

land ansässigen Unternehmen und seiner unselbständigen Niederlassung auf die grundsätzliche Einsetzbarkeit der Standardvertragsklauseln verständigt. Erforderlich sei dazu aber „eine (Zugangs-, aber nicht Empfangsbedürftige) Garantieerklärung (durch die ein Garantievertrag mit den betroffenen Personen zustande kommt)“.¹⁵

Die hessische Datenschutzaufsicht erläutert dieses Konzept näher: „Zur Herstellung der externen Verbindlichkeit bietet sich vor allem eine einseitige zugangsbedürftige, aber nicht annahmebedürftige, Garantieerklärung durch den Datenimporteur bzw. das Unternehmen (da ja eine rechtliche Einheit besteht) an, durch welche ein Garantievertrag mit den betroffenen Datensubjekten zustande käme. Dies könnte erfolgen, indem die Standardvertragsklauseln nebst entsprechender Erklärung, sich an diese zu halten, in das Internet oder Intranet gestellt werden (je nach betroffenem Personenkreis) oder in sonstiger Weise gegenüber den betroffenen Personen zugänglich gemacht werden“.¹⁶

Bei dieser Konstruktion bestünden weder eine Genehmigungs- noch eine Vorlagepflicht bei der (deutschen) Aufsichtsbehörde. Die aufsichtsbehördliche Auffassung deckt beide Konstellationen ab, also sowohl die Datenweitergabe durch das Unternehmen mit Hauptsitz in Deutschland an seine Niederlassung als auch (den hier nicht näher interessierenden) Fall einer Übermittlung von der Niederlassung zum Unternehmen in Deutschland. Entscheidend ist, dass eine Garantiezusage nur rechtsverbindlich sein kann, wenn sie durch eine rechtsfähigen Stelle erteilt wird – und das wäre die deutsche „Zentrale“.

Erstaunlicherweise hat sich das Schrifttum mit diesen dogmatisch nicht uninteressanten Überlegungen kaum auseinandergesetzt, sondern sich allenfalls ohne erkennbare Einwände auf die Wiedergabe der Ausführungen der Aufsichtsbehörden beschränkt.¹⁷ Nur vereinzelt wurde kritisch zu ihnen Stellung genommen: Die Standardvertragsklauseln setzten einen Vertragspartner voraus, der ihre Einhaltung zu überwachen habe – eine Bedingung, die durch das Konstrukt einer einseitigen Verpflichtung jetzt weggefallen sei; da das von den Aufsichtsbehörden entwickelte Modell nicht mehr mit Art. 46 Abs. 2 lit. c DS-GVO vereinbar sei, müsse es entgegen ihrer Auffassung als sonstige Garantieform im Rahmen von Art. 46 Abs. 3 DS-GVO eingeordnet und ihrer Genehmigung unterworfen werden.¹⁸

VI. Düsseldorfer Kreis – Einzelfragen

1. Zustandekommen eines Garantievertrages

Die Aufsichtsbehörden gehen davon aus, dass mit einer Veröffentlichung der Vertragsklauseln – nebst einer Erklärung des Unternehmens,¹⁹ sich an diese zu halten – im Internet oder Intranet bzw. ihrer sonstigen Zugänglichmachung ein Garantievertrag zustande kommen würde.²⁰ M. a. W., diese Vorgehensweise soll offenbar sowohl das Garantieangebot des Unternehmens als auch seine Annahme durch die von der Übermittlung Betroffenen einschließen.

Ohne Weiteres gefolgt werden kann der Auffassung der Behörden, dass das einseitig verpflichtende Angebot rechtswirksam werden kann, wenn es den Betroffenen lediglich zugeht; empfangsbedürftig ist diese Willenserklärung des

Unternehmens nicht. Für den Zugang wäre auch die vorgeschlagene Form völlig ausreichend.

Nicht so überzeugend wirkt aber die Vorstellung – von der die Aufsichtsbehörden anscheinend ausgehen –, dass mit der den von der Übermittlung Betroffenen eingeräumten bloßen Möglichkeit der Kenntnisnahme der Garantieerklärung (= des Garantieangebots) zugleich auch die Bedingungen für das Vorliegen einer Annahmeerklärung erfüllt seien; eine äußerlich irgendwie erkennbare Reaktion der Betroffenen wird also nicht vorausgesetzt. Zwar mag auch hier gem. § 151 BGB der Zugang der auf die Annahme gerichteten Willenserklärung entbehrlich sein,²¹ ein entsprechender Wille muss aber gleichwohl gebildet worden sein.²² Dabei ist anerkannt, dass das Vorhandensein eines Annahmewillens auch aufgrund äußerer Indizien festgestellt werden kann.²³ Zu ihnen zählt maßgeblich – und rückt hier ins Blickfeld –, ob der Vertrag für den Annehmenden lediglich rechtlich vorteilhaft ist.²⁴ Ein solcher Vorteil erschließt sich im vorliegenden Fall nicht zwangsläufig.

Der Garantievertrag soll dazu dienen, eine Bedingung für die Zulässigkeit der Datenübermittlung in ein Drittland zu erfüllen (2. Prüfstufe, s.o.). In aller Regel versorgt ein Unternehmen seine Niederlassung im eigenen (kommerziellen o.ä.) Interesse, also zu seinem und weniger zum Vorteil des Betroffenen – oder als Frage formuliert: Welchen rechtlichen Vorteil sollte der Betroffene von der Mitwirkung an einem Vertrag haben, der dem Unternehmen zur Legitimation der ansonsten unzulässigen Datenverarbeitung verhilft?

Es ist unklar, ob die Aufsichtsbehörden sich auf andere „Konkludenzindizien“²⁵ stützen wollen, die für eine Vertragsannahme als tragfähig erachtet werden. Die Praxis jedenfalls dürfte ihre Rechtsauffassung begrüßen. Schließlich verdankt sie der durch den Beschluss herbeigeführten Selbstbindung bei der Beurteilung derartiger grenzüberschreitender Datenübermittlungen ein gewisses Maß an Handlungssicherheit. Verhalten sich die Unternehmen entsprechend dem vorgegebenen Muster, dürften ihnen die Beanstandung einer Datenübermittlung als unzulässig oder gar Sanktionen nicht drohen, wenn die Behörden sich nicht dem Vorwurf des *venire contra factum proprium* aussetzen wollen.

15 Beschluss des Düsseldorfer Kreises a.a.O. (Fn. 4).

16 19. Bericht der hessischen Landesregierung a.a.O. (Fn. 5); wortgleich wiedergegeben bei Hillenbrand-Beck, RDV 2007, S. 231 (232).

17 Vgl. Däubler, in: Däubler/Wedde/Weichert/Sommer, Art. 46 Rn. 16; Pauly, in: Paal/Pauly, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Aufl. 2018, Art. 46 Rn. 11; Gola, in: Gola/Schomerus, § 4c BDSG a.F. Rn. 12; von dem Bussche, in: Plath, BDSG – DS-GVO, 2. Aufl. 2016, § 4c BDSG a.F. Rn. 37.

18 Schantz, in: Simitis/Hornung/Spiecker, Art. 46 Rn. 35.

19 Das als alleiniger Verantwortlicher, aber in seiner Doppelfunktion zugleich als Ex- und Importeur agiert, Hillenbrand-Beck, RDV 2007, S. 231 (232).

20 19. Bericht der hessischen Landesregierung a.a.O. (Fn. 5).

21 Vgl. zur Annahme eines selbständigen Garantievertrages, BGH, NJW 1988, 1726.

22 Brinkmann, in: Prütting/Wegen/Weinreich, BGB-Kommentar, 14. Aufl. 2019, § 151 Rn. 7.

23 Vgl. BGH, NJW 1990, S. 1655; Armbrüster, in: Erman, Bürgerliches Gesetzbuch, 11. Aufl. 2004, § 147 Rn. 3; Kramer, in: Münchener Kommentar zum BGB, Allgemeiner Teil, 5. Aufl., § 151 Rn. 5: „Konkludenzindizien“.

24 Vgl. BGH, NJW 2000, 276.

25 Kramer a.a.O. (Fn. 23).

2. Inhalt des Garantievertrages

Die Einbindung der Standardvertragsklauseln in einen Garantievertrag begegnet an sich keinen Bedenken, zumal der Verordnungsgeber eine solche Möglichkeit nicht ausschließt.²⁶ Fraglich ist allerdings, ob es genügt, auf das Vertragsmuster, also den Blanko-Text der Klauseln, zu verweisen und auf individuelle Angaben im Anhang B bzw. überhaupt auf einen konkreten Vertragsabschluss zu verzichten.

Eine wirksam getroffene Vereinbarung der Vertragsklauseln würde interne (inter partes) und externe Wirkungen erzeugen. Der Garantievertrag hingegen soll nur eine externe Verbindlichkeit gegenüber den Betroffenen als Drittbegünstigten herstellen,²⁷ auf interne, bilaterale Pflichten stellt er nicht ab. Wenn man vom Fehlen einer zum Abschluss des EU-Übermittlungsvertrages (rechts-)fähigen Partei ausgeht, erscheint das folgerichtig. Insoweit würden sozusagen im Mantel des Garantievertrages die EU-Standardvertragsklauseln zu einem bloßen Katalog von Pflichten und Maßnahmen mutieren, deren Erfüllung und Durchführung allein das Unternehmen als solches zusichert – einschließlich solcher, die nach Ziffer II der Klauseln ausschließlich dem Importeur auferlegt sind.

Die Ausklammerung einer in den EU-Regeln vorgesehenen weiteren verpflichteten Stelle – des Importeurs – aus dem Gegenstand des Garantievertrages stößt an Verständnis- und wahrscheinlich, wichtiger noch, auch Akzeptanzgrenzen seitens der EU-Kommission. Einen Sinn könnte die Integration der Standardvertragsklauseln in den Garantievertrag indes dann ergeben, wenn sie in geeigneter Weise in der von der Kommission vorgesehenen Vertragsform zum Tragen kämen.

Eine Auslandsniederlassung wird üblicherweise von einer Person geleitet, die das „Zentralunternehmen“ mit der Führung der Geschäfte vor Ort betraut hat und die dieses tatsächlich oder auch rechtlich vertritt. Nichts hindert das Unternehmen, diesen Funktionsträger auf der Basis und in Ergänzung des mit ihm bestehenden Arbeits-/Dienstvertrages zu verpflichten, dafür Sorge zu tragen, dass die einen Datenimporteur treffenden Pflichten in analoger Anwendung der Ziffern II ff. in geeigneter Weise erfüllt werden. Zugleich müsste der Arbeitgeber/Dienstherr ihm die erforderlichen Ermächtigungen erteilen, Mittel bereitstellen und Vorkehrungen treffen, damit der Beauftragte in seiner Eigenschaft als „Quasi-Importeur“ dazu auch in der Lage ist; eine adäquate vertragliche Haftungsentlastung würde die Risiken des Beauftragten reduzieren.

Die Existenz spezifischer, auf die jeweiligen Auslandsniederlassungen abstellender Verträge wäre im Übrigen auch im Hinblick auf das Auskunftsrecht gem. Art. 15 Abs. 2 und die Informationspflichten nach Art. 13 Abs. 1 lit. f, Art. 14 Abs. 1 lit. f DS-GVO geboten; mit einem Verweis auf abstrakte, bezugslose Vertragsformeln kann es nicht sein Bewenden haben.

3. Veröffentlichung – Umsetzung

Unterhält ein Unternehmen oder eine sonstige verantwortliche Stelle mehrere unselbständige Niederlassungen im EU-Ausland und würden die Angaben im Anhang B der Klauseln

in allen Individualverträgen gleichlautend ausfallen, begegnete eine Veröffentlichung aller nahezu identischen Vertragstexte einige Skepsis. Die notwendige Transparenz (Art. 5 Abs. 1 lit. a DS-GVO) wäre damit kaum gewährleistet. Insofern ist folgendes Modell für die Umsetzung des aufsichtsbehördlichen Konzepts in Erwägung zu ziehen:

In der üblichen Datenschutzerklärung auf der Homepage des Verantwortlichen könnte auf den Mustertext der EU-Vertragsklauseln verwiesen werden, der als Anhang der Datenschutzerklärung wiedergegeben wird. Für die Platzierung des Hinweises bietet sich der Passus mit der Beschreibung der Verarbeitungszwecke und der sie legitimierenden Rechtsgrundlagen an. Dort könnte auch die Garantieerklärung angesprochen werden, die im Wortlaut ebenso wie eine Auflistung der in Betracht kommenden Niederlassungen gleichfalls im Anhang der Datenschutzerklärung zu verorten wäre.

4. Formulierungsbeispiel

„Die von (Verantwortlicher) verarbeiteten Daten können auch an Niederlassungen des (Verantwortlichen) im EU-Ausland* zur Erfüllung der Geschäftszwecke des (Verantwortlichen) unter Beachtung der Voraussetzungen von Art. 46 Abs. 2 DS-GVO übermittelt werden. Soweit eine Weitergabe nach Maßgabe von Art. 46 Abs. 2 lit. c DS-GVO erfolgt, garantiert (Verantwortlicher) die strikte Einhaltung der Verträge.“**

(weiterer Text der Datenschutzerklärung)

Anlage

* Niederlassungen unterhält (Verantwortlicher) in ...

** Die mit den Niederlassungen bestehenden Verträge beruhen auf dem von der EU-Kommission vorgegebenen Standardtext und haben folgenden Wortlaut:

„.....“

(Verantwortlicher) garantiert den Betroffenen die Beachtung sämtlicher Bestimmungen dieser Verträge durch alle beteiligten Stellen.“

VII. Résumé

Eine Datenübermittlung von einer in Deutschland ansässigen verantwortlichen Stelle an seine in Drittstaaten operierenden unselbständigen Niederlassungen lässt sich auch mit Hilfe der EU-Standardvertragsklauseln legitimieren. Obwohl sich diese Klauseln mangels eigener Rechtsfähigkeit der Niederlassungen nicht zwischen ihnen und der verantwortlichen Stelle vertraglich vereinbaren lassen, können sie nach Auffassung des Düsseldorfer Kreises gleichwohl in Verbindung mit einer Garantieerklärung der verantwortlichen Stelle die von Art. 46 Abs. 2 lit. c DS-GVO beabsichtigten Zwecke erreichen und eine weitere aufsichtsbehördliche Beteiligung entfallen lassen. Die von den Aufsichtsbehörden nicht im Einzelnen erläuterte rechtliche Konstruktion dieses Modells wirft Fragen auf, denen nachzugehen ist.

²⁶ Vgl. ErwG 109.

²⁷ 19. Bericht der hessischen Landesregierung a.a.O. (Fn. 5).

Rechtsprechung

Zur Haftung für Kundenbewertungen bei Amazon

(Bundesgerichtshof, Urteil vom 20. Februar 2020 – I ZR 193/18 –)

Den Anbieter eines auf der Online-Handelsplattform Amazon angebotenen Produkts trifft für Bewertungen des Produkts durch Kunden grundsätzlich keine wettbewerbsrechtliche Haftung.

Sachverhalt:

Der Kläger ist ein eingetragener Wettbewerbsverein. Die Beklagte vertreibt Kinesiologie-Tapes. Sie hat diese Produkte in der Vergangenheit damit beworben, dass sie zur Schmerzbehandlung geeignet seien, was jedoch medizinisch nicht gesichert nachweisbar ist. Die Beklagte hat deshalb am 4. November 2013 gegenüber dem Kläger eine strafbewehrte Unterlassungserklärung abgegeben.

Die Beklagte bietet ihre Produkte auch bei der Online-Handelsplattform Amazon an. Dort wird für jedes Produkt über die EAN (European Article Number) eine diesem Produkt zugewiesene ASIN (Amazon-Standard-Identifikationsnummer) generiert, die sicherstellen soll, dass beim Aufruf eines bestimmten Produkts die Angebote sämtlicher Anbieter dieses Produkts angezeigt werden. Käuferinnen und Käufer können bei Amazon die Produkte bewerten. Amazon weist eine solche Bewertung ohne nähere Prüfung dem unter der entsprechenden ASIN geführten Produkt zu. Das hat zur Folge, dass zu einem Artikel alle Kundenbewertungen angezeigt werden, die zu diesem – unter Umständen von mehreren Verkäufern angebotenen – Produkt abgegeben wurden.

Am 17. Januar 2017 bot die Beklagte bei Amazon Kinesiologie-Tapes an. Unter diesem Angebot waren Kundenrezensionen abrufbar, die unter anderem die Hinweise „schmerzlinderndes Tape!“, „This product is perfect for pain...“, „Schnell lässt der Schmerz nach“, „Linderung der Schmerzen ist spürbar“, „Die Schmerzen gehen durch das Bekleben weg“ und „Schmerzen lindern“ enthielten. Der Kläger forderte von der Beklagten die Zahlung einer Vertragsstrafe. Die Löschung der Kundenrezensionen lehnte Amazon auf Anfrage der Beklagten ab.

Der Kläger begehrt Unterlassung und Zahlung der Vertragsstrafe sowie der Abmahnkosten. Die Beklagte habe sich die Kundenrezensionen zu Eigen gemacht und hätte auf ihre Löschung hinwirken müssen. Falls dies nicht möglich sei, dürfe sie die Produkte bei Amazon nicht anbieten.

Das Landgericht hat die Klage abgewiesen. Es bestehe kein Anspruch aus § 8 Abs. 1, § 3a* UWG in Verbindung mit § 11 Abs. 1 Satz 1 Nr. 11 HWG. Die Berufung des Klägers hatte keinen Erfolg. Zwar seien die in den Kundenrezensionen enthaltenen gesundheitsbezogenen Angaben irreführend. Sie stellten aber keine Werbung dar. Zumindest wäre eine solche Werbung der Beklagten nicht zuzurechnen.

Aus den Gründen:

Das Berufungsgericht hat mit Recht angenommen, dass die Beklagte für Kundenbewertungen der von ihr bei Amazon angebotenen Produkte keine wettbewerbsrechtliche Haftung trifft.

Ein Unterlassungsanspruch des Klägers ergibt sich nicht aus der Vorschrift des § 11 Abs. 1 Satz 1 Nr. 11 und Satz 2 HWG, die Werbung für Medizinprodukte mit irreführenden Äußerungen Dritter verbietet. Die Kundenbewertungen sind zwar irreführende Äußerungen Dritter, weil die behauptete Schmerzlinderung durch Kinesiologie-Tapes medizinisch nicht gesichert nachweisbar ist. Die Beklagte hat mit den Kundenbewertungen aber nicht geworben. Nach den rechtsfehlerfrei getroffenen Feststellungen des Berufungsgerichts hat sie weder selbst aktiv mit den Bewertungen geworben oder diese veranlasst, noch hat sie sich die Kundenbewertungen zu eigen gemacht, indem sie die inhaltliche Verantwortung dafür übernommen hat. Die Kundenbewertungen sind vielmehr als solche gekennzeichnet, finden sich bei Amazon getrennt vom Angebot der Beklagten und werden von den Nutzerinnen und Nutzern nicht der Sphäre der Beklagten als Verkäuferin zugerechnet.

Die Beklagte traf auch keine Rechtspflicht, eine Irreführung durch die Kundenbewertungen gemäß § 5 Abs. 1 Satz 1 und 2 Fall 2 Nr. 1 UWG zu verhindern. Durch ihr Angebot auf Amazon wird keine Garantienstellung begründet. Von ausschlaggebender Bedeutung ist dabei, dass Kundenbewertungssysteme auf Online-Marktplätzen gesellschaftlich erwünscht sind und verfassungsrechtlichen Schutz genießen. Das Interesse von Verbraucherinnen und Verbrauchern, sich zu Produkten zu äußern und sich vor dem Kauf über Eigenschaften, Vorzüge und Nachteile eines Produkts aus verschiedenen Quellen, zu denen auch Bewertungen anderer Kunden gehören, zu informieren oder auszutauschen, wird durch das Grundrecht der Meinungs- und Informationsfreiheit des Art. 5 Abs. 1 Satz 1 GG geschützt. Einer Abwägung mit dem Rechtsgut der öffentlichen Gesundheit, die als Gemeinschaftsgut von hohem Rang einen Eingriff in dieses Grundrecht rechtfertigen könnte, bedarf es hier nicht.

(Auszugsweise Wiedergabe der Entscheidung gem. PM 021|2020 des Gerichts vom 20.02.2020)

Zur Zulässigkeit der Bewertungsdarstellung von Unternehmen auf einem Internet-Bewertungsportal (www.yelp.de)

(Bundesgerichtshof, Urteil vom 14. Januar 2020 – VI ZR 496/18 –)

Die in einem Internet-Bewertungsportal erfolgt Anzeige des Bewertungsdurchschnitts und der Einstufung von Nutzerbewertungen als „empfohlen“ oder „nicht empfohlen“ ist durch die Berufs- sowie Meinungsfreiheit geschützt; ein Gewerbetreibender muss Kritik an seinen Leistungen und die öffentliche Erörterung geäußelter Kritik grundsätzlich hinnehmen.

Sachverhalt:

Die Klägerin nimmt wegen ihrer Bewertungsdarstellung auf einem Internetportal dessen Betreiber auf Unterlassung, Feststellung und Schadensersatz in Anspruch.

Die Beklagte betreibt im Internet unter www.yelp.de ein Bewertungsportal, in dem angemeldete Nutzer Unternehmen durch die Vergabe von einem bis zu fünf Sternen und einen Text bewerten können. Das Internetportal zeigt alle Nutzerbeiträge an und stuft sie ohne manuelle Kontrolle durch eine Software automatisiert und tagesaktuell entweder als „empfohlen“ oder als „(momentan) nicht empfohlen“ ein. Bei Aufruf eines Unternehmens werden mit dessen Bezeichnung und Darstellung bis zu fünf Sterne angezeigt, die dem Durchschnitt der Vergabe in den „empfohlenen“ Nutzerbeiträgen entsprechen (Bewertungsdurchschnitt). Unmittelbar daneben steht „[Anzahl] Beiträge“. Unter der Darstellung des Unternehmens ist eine entsprechende Anzahl von Bewertungen – überschrieben mit „Empfohlene Beiträge für [Unternehmen]“ – jeweils mit den vergebenen Sternen und dem Text wiedergegeben. Am Ende dieser Wiedergabe steht „[Anzahl] andere Beiträge, die momentan nicht empfohlen werden“. Nach Anklicken der daneben befindlichen Schaltfläche wird folgender Text angezeigt:

"Was sind empfohlene Beiträge?"

Unsere User veröffentlichen auf Yelp Millionen von Beiträgen. Aus diesem Grund benutzen wir eine automatisierte Software, um die hilfreichsten Beiträge hervorzuheben. Diese Software zieht mehrere Faktoren in Betracht, wie z.B. die Qualität, die Vertrauenswürdigkeit und die bisherige Aktivität des Users auf Yelp. Dieser Vorgang ist gleich für alle Geschäftsauflistungen und hat nichts damit zu tun, ob ein Unternehmen ein Anzeigenkunde bei uns ist oder nicht. Die Beiträge, die nicht direkt auf der Geschäftsseite hervorgehoben und auch nicht in die Gesamtbewertung einberechnet werden, sind aber unten aufgeführt. Hier mehr darüber erfahren."

Darunter befindet sich die Überschrift "[Anzahl] Beiträge für [Unternehmen] werden momentan nicht empfohlen" mit dem nachfolgenden "Hinweis: Die Beiträge unten werden nicht in der gesamten Sternchen-Bewertung für das Geschäft berücksichtigt." Danach folgt die Wiedergabe der nicht empfohlenen Beiträge.

Die Klägerin betreibt ein Fitness-Studio, zu dem das Bewertungsportal am 10. Februar 2014 aufgrund eines empfohlenen Beitrags vom 7. Februar 2014 drei Sterne und 24 ältere Beiträge mit überwiegend positiven Bewertungen als momentan nicht empfohlen anzeigte.

Nach Auffassung der Klägerin hat die Beklagte den unzutreffenden Eindruck erweckt, dass der Bewertungsdurchschnitt aller Beiträge angezeigt worden sei. Die Unterscheidung zwischen empfohlenen und momentan nicht empfohlenen Beiträgen sei willkürlich und nicht anhand nachvollziehbarer Kriterien erfolgt, wodurch ein verzerrtes und unrichtiges Gesamtbild entstehe.

Das Landgericht hat die Klage abgewiesen. Das Oberlandesgericht hat die Beklagte verurteilt, es zu unterlassen, auf ihrer Internetseite für das Fitness-Studio eine Gesamtbewertung oder eine Gesamtzahl der Bewertungen auszuweisen, in die Beiträge (Bewertungen), die von Nutzern der vorgenannten Internetseite abgegeben worden waren und welche die Beklagte als "momentan nicht empfohlen" wertet, nicht einbezogen werden. Außerdem hat das Oberlandesgericht die Verpflichtung der Beklagten zum Ersatz entstandenen sowie noch entstehenden Schadens festgestellt und die Beklagte zur Zahlung von Rechtsanwaltskosten verurteilt.

Aus den Gründen:

Der unter anderem für Rechtsstreitigkeiten über Ansprüche aus unerlaubten Handlungen zuständige VI. Zivilsenat hat auf die Revision der Beklagten das klageabweisende Urteil des Landgerichts wiederhergestellt. Die von der Klägerin geltend gemachten Ansprüche ergeben sich nicht aus § 824 Abs. 1 BGB. Die Beklagte hat nicht – wie in dieser Bestimmung vorausgesetzt – unwahre

Tatsachen behauptet oder verbreitet. Entgegen der Auffassung des Berufungsgerichts äußerte die Beklagte mit der angegriffenen Bewertungsdarstellung nicht, dass es sich bei dem angezeigten Bewertungsdurchschnitt um das Ergebnis der Auswertung aller für das Fitness-Studio abgegebenen Beiträge handele und dass der danebenstehende Text deren Anzahl wiedergebe. Denn der unvoreingenommene und verständige Nutzer des Bewertungsportals entnimmt der Bewertungsdarstellung zunächst, wie viele Beiträge die Grundlage für die Durchschnittsberechnung bildeten, und schließt daraus weiter, dass Grundlage für die Durchschnittsberechnung ausschließlich der "empfohlene" Beitrag ist sowie dass sich die Angabe der Anzahl nur darauf bezieht. Die Bewertungsdarstellung der Beklagten greift auch nicht rechtswidrig in das Unternehmenspersönlichkeitsrecht und in das Recht am eingerichteten und ausgeübten Gewerbebetrieb der Klägerin ein (§ 823 Abs. 1 BGB). Die rechtlich geschützten Interessen der Klägerin überwiegen nicht die schutzwürdigen Belange der Beklagten.

(Auszugsweise Wiedergabe der Entscheidung gem. PM 014|2020 des Gerichts vom 19.03.2020)

Rechtsanwalt ist als externer Datenschutzbeauftragter gewerblicher Unternehmer

(Bundesfinanzhof, Urteil vom 14. Januar 2020 – VIII R 27/17 –)

- 1. Ein externer Datenschutzbeauftragter ist gewerblicher Unternehmer, auch wenn er zugleich als Rechtsanwalt tätig ist.**
- 2. Ein Datenschutzbeauftragter übt keine dem Beruf des Rechtsanwaltes vorbehaltene Tätigkeit aus. Vielmehr wird er in einem eigenständigen, von einer parallel ausgeübten Anwaltstätigkeit abzugrenzenden, interdisziplinären und insoweit auch datenschutzrechtliche Fachkenntnisse erforderndem Beruf tätig.**
- 3. Da die Berufsausübung ohne eine spezifische akademische Ausbildung möglich sei, ist ein Datenschutzbeauftragter auch nicht in einem dem Rechtsanwalt ähnlichen Beruf tätig. Gleichfalls liegt keine sonstige selbständige Arbeit i.S.d. § 18 Abs. 1 Nr. 3 EStG vor.**
- 4. Da keine freiberufliche Tätigkeit i.S.d. § 18 Abs. 1 EStG vorliegt, ist der externe Datenschutzbeauftragte gewerbsteuer- und – bei Überschreiten bestimmter Gewinn Grenzen – auch buchführungspflichtig.**

Sachverhalt:

Der Kläger und Revisionskläger (Kläger) ist als selbständiger Rechtsanwalt im Bereich des IT-Rechts tätig. Neben seiner anwaltlichen Tätigkeit arbeitet er als externer Datenschutzbeauftragter u.a. für verschiedene größere Unternehmen aus unterschiedlichen Wirtschaftszweigen. Nach den Feststellungen des Finanzgerichts (FG) ist er vertraglich verpflichtet, zum Aufbau bzw. zur Vervollständigung der Datenschutzorganisation des jeweiligen Auftraggebers unter Berücksichtigung der §§ 4f und 4g des Bundesdatenschutzgesetzes – BDSG – (in Fassungen nach Novellierung des BDSG

1990 im Jahr 2003) beizutragen. Zu seinen Aufgaben gehören die datenschutzrechtliche Prüfung der formalrechtlichen Anforderungen an die bestehende Datenschutzorganisation, die (datenschutzrechtliche) Prüfung von Datenverarbeitungsprogrammen, mit deren Hilfe personenbezogene Daten verarbeitet werden, die (datenschutzrechtliche) Vorabkontrolle von geplanten Vorhaben zur Verarbeitung von personenbezogenen Daten, die (datenschutzrechtliche) Beratung zur datenschutzrechtskonformen Gestaltung von Prozessabläufen und Anwendungsverfahren sowie die datenschutzrechtliche Stellungnahme zu Einzelfragen. Weiter ist in den jeweiligen Verträgen geregelt, dass in technischer Hinsicht der Auftraggeber zuständig bleibt und der Kläger sich bezüglich der technischen Sicherheit an den Auftraggeber wenden kann. Zusätzlich ist der Kläger verpflichtet, den Auftraggeber über Entwicklungen im Datenschutzrecht zu informieren. Er ist teilweise auch berechtigt, zu Beginn seiner Tätigkeit eine datenschutzrechtliche Status-quo-Analyse durchzuführen, soweit eine solche nicht vorhanden ist. Der Kläger ist jeweils gemäß § 4f BDSG als Datenschutzbeauftragter für die Unternehmen bestellt.

Der Beklagte und Revisionsbeklagte (das Finanzamt – FA –) ordnete die Tätigkeit des Klägers als externer Datenschutzbeauftragter als gewerblich ein und setzte für die Jahre 2010 bis 2014 jeweils Gewerbesteuermessbeträge fest. Da der nach § 4 Abs. 3 des Einkommensteuergesetzes (EStG) ermittelte Gewinn aus der Tätigkeit als Datenschutzbeauftragter im Jahr 2010 mehr als 150.000 EUR betragen hatte, teilte das FA dem Kläger mit Bescheid vom 08.08.2012 mit, dass er nach § 141 der Abgabenordnung in der im Jahr der Mitteilung geltenden Fassung (AO) verpflichtet sei, ab dem 01.01.2013 für den Gewerbebetrieb Datenschutzbeauftragter Bücher zu führen und auf Grund jährlicher Bestandsaufnahmen Abschlüsse zu machen. Der hiergegen eingelegte Einspruch des Klägers blieb ohne Erfolg, ebenso die nachfolgende Klage. Das FG war in seinem in Entscheidungen der Finanzgerichte (EFG) 2018, 345 veröffentlichten Urteil der Auffassung, das FA habe den Kläger in Bezug auf seine Tätigkeit als externer Datenschutzbeauftragter zutreffend als gewerblichen Unternehmer i.S. des § 141 Abs. 1 Satz 1 AO eingeordnet. Der Kläger übe als externer Datenschutzbeauftragter weder den Beruf eines Rechtsanwalts aus, noch sei seine Tätigkeit diesem Beruf ähnlich. Die Tätigkeit des Datenschutzbeauftragten stelle nach der Rechtsprechung des Bundesfinanzhofs – BFH – (Urteile vom 05.06.2003 – IV R 34/01, BFHE 202, 336, BStBl II 2003, 761, und vom 26.06.2003 – IV R 41/01, BFH/NV 2003, 1557, noch zum BDSG 1990) einen völlig eigenständigen und neuen Beruf dar.

Seine hiergegen gerichtete Revision begründet der Kläger mit der Verletzung von Bundesrecht.

Aus den Gründen:

Die Revision des Klägers ist unbegründet. Sie war daher zurückzuweisen (§ 126 Abs. 2 der Finanzgerichtsordnung – FGO –).

Das FG hat zu Recht entschieden, dass die Mitteilung des FA vom 08.08.2012 in Gestalt der Einspruchsentscheidung vom 25.04.2016 über den Beginn der Buchführungspflicht nach § 141 Abs. 2 Satz 1 AO rechtmäßig ist. Der Kläger ist in Bezug auf seine Tätigkeit als externer Datenschutzbeauftragter gewerblicher Unternehmer i.S. des § 141 Abs. 1 AO, denn er übt keine freiberufliche Tätigkeit i.S. des § 18 Abs. 1 Nr. 1 EStG aus. Der Kläger übt als Datenschutzbeauftragter weder eine dem Beruf des Rechtsanwalts vorbehaltene noch eine diesem Beruf ähnliche Tätigkeit aus. Seine Tätigkeit als Datenschutzbeauftragter ist auch nicht § 18 Abs. 1 Nr. 3 EStG zuzuordnen.

1. Nach § 141 Abs. 1 Satz 1 AO sind gewerbliche Unternehmer, für die sich die Buchführungspflicht nicht aus § 140 AO ergibt, u.a. dann verpflichtet, für diesen Betrieb Bücher zu führen und auf Grund jährlicher Bestandsaufnahmen Abschlüsse zu machen, wenn sie nach den Feststellungen der Finanzbehörde für den einzelnen Betrieb einen Gewinn aus Gewerbebetrieb von

mehr als 50.000 EUR (ab 2016: 60.000 EUR) im Wirtschaftsjahr gehabt haben. Die Verpflichtung nach § 141 Abs. 1 AO ist gemäß § 141 Abs. 2 Satz 1 AO vom Beginn des Wirtschaftsjahres an zu erfüllen, das auf die Bekanntgabe der Mitteilung folgt, durch die die Finanzbehörde auf den Beginn dieser Verpflichtung hingewiesen hat.

Die Voraussetzungen des § 141 AO liegen vor. Der Kläger ist – was zwischen den Beteiligten allein streitig ist – gewerblicher Unternehmer im Sinne dieser Vorschrift.

a) Gewerbliche Unternehmer in diesem Sinne sind u.a. solche Unternehmer, die einen Gewerbebetrieb i.S. des § 15 Abs. 2, Abs. 3 EStG unterhalten (vgl. z.B. BFH-Urteil vom 21.01.1998 – I R 3/96, BFHE 185, 262, BStBl II 1998, 468; Drüen, in: Tipke/Kruse, Abgabenordnung, Finanzgerichtsordnung, § 141 AO Rz 3). Nicht gewerblich sind Unternehmen, deren Betätigung als Ausübung eines freien Berufs oder als eine selbständige Tätigkeit (§ 18 Abs. 1 Nrn. 1 und 3 EStG) anzusehen ist.

b) Der Kläger ist in Bezug auf seine Tätigkeit als externer Datenschutzbeauftragter gewerblicher Unternehmer i.S. des § 141 Abs. 1 AO. Seine Tätigkeit ist nicht als Ausübung eines Katalogberufs – insbesondere den des Rechtsanwalts – bzw. einer diesem ähnliche Tätigkeit anzusehen (vgl. bereits BFH-Urteile in BFHE 202, 336, BStBl II 2003, 761, und in BFH/NV 2003, 1557, zum BDSG 1990; vgl. auch Levedag, Deutsches Steuerrecht 2018, 2094 f.; Schmidt/Wacker, EStG, 38. Aufl., § 18 Rz 155; Brandt, in: Hermann/Heuer/Raupach – HHR –, § 18 EStG Rz 219, 600; Jahn, Der Betrieb 2005, 692, 694; Moritz in Bordewin/Brandt, § 18 EStG Rz 416; Lutter, EFG 2018, 347).

aa) Gemäß § 18 Abs. 1 Nr. 1 EStG gehört zu den freiberuflichen Tätigkeiten u.a. die selbständige Berufstätigkeit des Rechtsanwalts, vorausgesetzt die tatsächlich ausgeübte Tätigkeit ist für diesen Beruf berufstypisch, d.h. sie ist in besonderer Weise charakterisierend und diesem Katalogberuf vorbehalten (vgl. z.B. BFH-Urteile vom 12.12.2001 – XI R 56/00, BFHE 197, 442, BStBl II 2002, 202, m.w.N.; vom 15.06.2010 – VIII R 10/09, BFHE 230, 47, BStBl II 2010, 906). Dies ist beim externen Datenschutzbeauftragten nicht der Fall.

aaa) Der Datenschutzbeauftragte, der sowohl als interner wie externer Beauftragter bestellt werden kann, hat gemäß § 4g BDSG auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hinzuwirken. Er hat insbesondere die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen und die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften des BDSG sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen (vgl. § 4g Abs. 1 Sätze 1 und 3 BDSG).

bbb) In diesem Sinne war auch der von den Unternehmen jeweils gemäß § 4f BDSG zum externen Datenschutzbeauftragten bestellte Kläger tätig. Er hatte sich vertraglich verpflichtet, zum Aufbau bzw. zur Vervollständigung der Datenschutzorganisation des jeweiligen Auftraggebers unter Berücksichtigung der §§ 4f und 4g BDSG beizutragen. Zu seinen Aufgaben gehörten die (datenschutzrechtliche) Prüfung der formalrechtlichen Anforderungen an die bestehende Datenschutzorganisation, die (datenschutzrechtliche) Prüfung von Datenverarbeitungsprogrammen, mit deren Hilfe personenbezogene Daten verarbeitet werden, die (datenschutzrechtliche) Vorabkontrolle von geplanten Vorhaben zur Verarbeitung von personenbezogenen Daten, die (datenschutzrechtliche) Beratung zur datenschutzrechtskonformen Gestaltung von Prozessabläufen und Anwendungs-

verfahren sowie die (datenschutzrechtliche) Stellungnahme zu Einzelfragen. Zudem war der Kläger verpflichtet, den Auftraggeber über Entwicklungen im Datenschutzrecht zu informieren. Auch war er teilweise berechtigt, zu Beginn seiner Tätigkeit eine datenschutzrechtliche Status-quo-Analyse durchzuführen, soweit eine solche nicht vorhanden war.

ccc) Diese Tätigkeit des Klägers ist – auch wenn sie in der von ihm ausgeübten Art und Weise im Schwerpunkt rechtsberatend ist – nicht für den Beruf des Rechtsanwalts berufstypisch, insbesondere ist sie dem Beruf des Rechtsanwalts nicht vorbehalten (vgl. schon BFH-Urteile in BFHE 202, 336, BStBl II 2003, 761, und in BFH/NV 2003, 1557, zum BDSG 1990, betreffend die Abgrenzung der Tätigkeit des Datenschutzbeauftragten zur Tätigkeit des Ingenieurs und des beratenden Betriebswirts). Vielmehr übt der Kläger insoweit einen eigenständigen – von seiner Tätigkeit als Rechtsanwalt abzugrenzenden – Beruf aus. Dies folgt daraus, dass die Tätigkeit des Datenschutzbeauftragten (weiterhin) durch eine Beratung in interdisziplinären Wissensgebieten gekennzeichnet ist, ohne dass hierfür eine spezifische akademische Ausbildung, wie diese z.B. für die Ausübung des Berufs des Rechtsanwalts notwendig ist, nachgewiesen werden muss (vgl. schon BFH-Urteile in BFHE 202, 336, BStBl II 2003, 761, und in BFH/NV 2003, 1557, zum BDSG 1990).

Gemäß § 4f Abs. 2 BDSG darf zum Datenschutzbeauftragten nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Dabei bestimmt sich das Maß der erforderlichen Fachkunde insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. Um die in § 4g BDSG geregelten Aufgaben erfüllen zu können, muss der Datenschutzbeauftragte Kenntnisse in verschiedenen Wissensbereichen besitzen. Allerdings ist das jeweils erforderliche Wissen auf Teilbereiche verschiedener Studiengänge beschränkt, ohne dass es eines entsprechenden Hochschulabschlusses bedarf (vgl. schon BFH-Urteile in BFHE 202, 336, BStBl II 2003, 761, und in BFH/NV 2003, 1557, zum BDSG 1990).

So muss der Datenschutzbeauftragte, wie bereits nach Maßgabe des BDSG 1990, zwar über umfangreiche juristische Kenntnisse im Datenschutzrecht, umfangreiche technische Kenntnisse auf dem Gebiet der sog. Computer-Hardware und der unterschiedlichen System- und Anwendersoftware, über betriebswirtschaftliche Grundkenntnisse und pädagogische Fähigkeiten und Kenntnisse verfügen (vgl. schon BFH-Urteile in BFHE 202, 336, BStBl II 2003, 761, und in BFH/NV 2003, 1557, zum BDSG 1990). Dies bestätigen auch die im Beschluss des Düsseldorfener Kreises vom 24./25.11.2010 (vgl. hierzu z.B. Moos in Wolff/Brink, Datenschutzrecht in Bund und Ländern, § 4f BDSG Rz 43) formulierten Anforderungen an die Berufsausübung und die vom Bundesverband der Datenschutzbeauftragten Deutschlands formulierten Voraussetzungen (vgl. Das berufliche Leitbild der Datenschutzbeauftragten – Stand 4/2018, www.bvdnet.de), die verlangen, dass der Datenschutzbeauftragte neben datenschutzrechtlichem Fachwissen insbesondere auch Fachwissen in der Informations- und Kommunikationstechnik sowie betriebswirtschaftliches und organisatorisches Fachwissen besitzen muss.

Jedoch kann der Datenschutzbeauftragte ungeachtet der danach in den verschiedenen Bereichen erforderlichen Fachkunde, über die er insbesondere auch im Bereich des Datenschutzrechts verfügen muss, ohne eine der Ausbildung des Rechtsanwalts vergleichbare akademische Ausbildung tätig sein (vgl. schon BFH-Urteile in BFHE 202, 336, BStBl II 2003, 761, und in BFH/NV 2003, 1557, zum BDSG 1990).

bb) Erfordert die Tätigkeit des Datenschutzbeauftragten – wie dargelegt – keine der Ausbildung des Rechtsanwalts vergleichbare akademische Ausbildung, übt der externe Datenschutzbeauftragte auch keinen dem Beruf des Rechtsanwalts ähnlichen Beruf gemäß § 18 Abs. 1 Nr. 1 Satz 2 EStG aus (vgl. zu den Anforderungen an einen dem Katalogberuf ähnlichen Beruf z.B. BFH-Urteile vom 07.05.2019 – VIII R 2/16, BFHE 264, 325, BStBl II 2019, 528, und VIII R 26/16, BFHE 264, 334, BStBl II 2019, 532, zum Rentenberater; vgl. auch BFH-Urteile in BFHE 202, 336, BStBl II 2003, 761, und in BFH/NV 2003, 1557, zum BDSG 1990).

c) Entgegen der Auffassung des Klägers hat sich an dieser Beurteilung durch die Novellierung des BDSG 1990, insbesondere die Neufassung der Aufgabenbeschreibung in § 4g BDSG (vorher: § 37 BDSG 1990), nichts geändert, auch wenn der Datenschutzbeauftragte nicht mehr die Ausführung des BDSG sowie anderer Vorschriften über den Datenschutz sicherzustellen (so § 37 Abs. 1 Satz 1 BDSG 1990), sondern auf deren Einhaltung hinzuwirken hat. Für die Auffassung des Klägers gibt auch die Gesetzesbegründung (BRDrucks 461/00, S. 89 f.) nichts her. Vielmehr übt der Datenschutzbeauftragte seine Tätigkeit, die letztlich der Selbstkontrolle der Daten verarbeitenden Stelle dient, weiterhin weisungsfrei und unabhängig aus (vgl. § 4f Abs. 3 Satz 2 BDSG).

d) Dieser Einordnung der Tätigkeit des Datenschutzbeauftragten steht die aktuelle Rechtsprechung des Bundesgerichtshofs (BGH) zur Zulassung von Datenschutzbeauftragten als Syndikusrechtsanwalt nicht entgegen. Nach dieser kann eine Tätigkeit als interner Datenschutzbeauftragter grundsätzlich die für eine Zulassung als Syndikusrechtsanwalt erforderlichen Tätigkeitsmerkmale des § 46 Abs. 3 Nrn. 1 bis 4 der Bundesrechtsanwaltsordnung erfüllen und das Arbeitsverhältnis von diesen Merkmalen auch geprägt sein (vgl. insbesondere BGH-Urteile vom 15.10.2018 – AnwZ (Brfg) 20/18, Neue Juristische Wochenschrift – NJW – 2018, 3701; vom 02.07.2018 – AnwZ (Brfg) 49/17, NJW 2018, 3100). Dabei betont der BGH, der Kern und Schwerpunkt der Tätigkeit eines Datenschutzbeauftragten liege auf der rechtlichen Ebene, auch wenn Sachkunde in weiteren Bereichen erforderlich sei (vgl. BGH-Urteil in NJW 2018, 3701, Rz 71 bis 73). Dass die Tätigkeit des (internen) Datenschutzbeauftragten mit den für Rechtsanwälte geltenden berufsrechtlichen Vorschriften in Einklang steht, ist für die steuerliche Qualifizierung der Tätigkeit als solche i.S. des § 18 EStG allerdings ebenso wenig maßgebend (vgl. z.B. BFH-Urteil in BFHE 197, 442, BStBl II 2002, 202) wie der Umstand, dass eine Zulassung als Syndikusrechtsanwalt im Einzelfall möglich ist.

e) Auch widerspricht das Gebot verfassungsrechtlicher Gleichbehandlung in Art. 3 Abs. 1 des Grundgesetzes einer abweichenden steuerrechtlichen Behandlung. Denn für eine unterschiedliche steuerrechtliche Beurteilung der Ausübung eines verselbständigten Berufs wie den des Datenschutzbeauftragten je nach Vorliegen oder Nichtvorliegen einer freiberuflichen Qualifikation i.S. des § 18 Abs. 1 Nr. 1 EStG findet sich keine Rechtfertigung, wenn der verselbständigte Beruf seinem Berufsbild nach keine Ausbildung oder Zulassung für einen der Katalogberufe i.S. des § 18 Abs. 1 Nr. 1 EStG voraussetzt (vgl. BFH-Urteil in BFHE 230, 47, BStBl II 2010, 906, zum Rechtsanwalt als Berufsbetreuer).

f) Die Tätigkeit des Klägers als Datenschutzbeauftragter ist auch nicht § 18 Abs. 1 Nr. 3 EStG zuzuordnen.

aa) Danach gehören zu den Einkünften aus selbständiger Arbeit auch "Einkünfte aus sonstiger selbständiger Arbeit, z.B. Vergütungen für die Vollstreckung von Testamenten, für Vermögensverwaltung und für die Tätigkeit als Aufsichtsratsmitglied".

§ 18 Abs. 1 Nr. 3 EStG enthält keinen abschließenden Katalog in Betracht kommender "Einkünfte aus sonstiger selbständiger Arbeit", sondern lediglich die Auflistung von Regelbeispielen. Weitere Tätigkeiten fallen ebenfalls in den Anwendungsbereich der Norm, wenn sie ihrer Art nach den Regelbeispielen des § 18 Abs. 1 Nr. 3 EStG ähnlich sind (Grundsatz der sog. Gruppenähnlichkeit). Das ist z.B. der Fall, wenn die Tätigkeit die Betreuung fremder Vermögensinteressen umfasst, aber darüber hinaus auch dann, wenn es sich um eine selbständig ausgeübte fremdnützige Tätigkeit in einem fremden Geschäftskreis handelt (BFH-Urteile in BFHE 264, 325, BStBl II 2019, 528, und in BFHE 264, 334, BStBl II 2019, 532, zum Rentenberater; in BFHE 230, 47, BStBl II 2010, 906, und vom 15.06.2010 – VIII R 14/09, BFHE 230, 54, BStBl II 2010, 909, zu Berufsbetreuern und Verfahrenspflegern; vom 31.01.2017 – IX R 10/16, BFHE 256, 250, BStBl II 2018, 571; vgl. auch BFH-Beschluss vom 13.06.2013 – III B 156/12, BFH/NV 2013, 1420). Eine rein beratende Tätigkeit, die sich z.B. auf die Erteilung von Anlageempfehlungen beschränkt, ohne dass die zur Vermögensanlage erforderlichen Verfügungen selbst vorgenommen werden können oder ein Depot betreut wird, ist nicht von § 18 Abs. 1 Nr. 3 EStG erfasst (vgl. z.B. BFH-Urteile in BFHE 264, 325, BStBl II 2019, 528, und in BFHE 264, 334, BStBl II 2019, 532; vom 02.09.1988 – III R 58/85, BFHE 154, 332, BStBl II 1989, 24; vgl. auch BFH-Beschluss vom 08.02.2013 – VIII B 54/12, BFH/NV 2013, 1098, zum Anlageberater/Finanzanalysten).

§ 18 Abs. 1 Nr. 3 EStG kommt nicht die Funktion eines Aufwandsbestands zu. Ihm sind daher insbesondere nicht jene (rechts-)beratenden Tätigkeiten zuzuordnen, die – mangels vergleichbarer Ausbildung oder Tätigkeit – keinem der in § 18 Abs. 1 Nr. 1 EStG genannten Katalogberufe ähnlich sind. Auch solche fallen nur dann in den Anwendungsbereich der Norm, wenn sie ihrer Art nach den Regelbeispielen des § 18 Abs. 1 Nr. 3 EStG ähnlich sind (BFH-Urteile in BFHE 264, 325, BStBl II 2019, 528, und in BFHE 264, 334, BStBl II 2019, 532, zum Rentenberater).

bb) Nach diesen Grundsätzen übt der Kläger als Datenschutzbeauftragter keine sonstige selbständige Arbeit i.S. des § 18 Abs. 1 Nr. 3 EStG aus. Seine Tätigkeit ist nicht – wie die gesetzlichen Regelbeispiele – berufsbildtypisch durch eine selbständige fremdnützige Tätigkeit in einem fremden Geschäftskreis sowie durch Aufgaben der Vermögensverwaltung geprägt, sondern im Schwerpunkt beratender Natur. Daran ändert der Umstand, dass der Kläger den jeweiligen Auftraggeber bei der Einhaltung der datenschutzrechtlichen Vorgaben unterstützt und ihn so vor negativen Rechtsfolgen bewahrt, nichts.

cc) Seine Tätigkeit als Datenschutzbeauftragter ist – anders als der Kläger meint – auch nicht mit der eines Aufsichtsrats i.S. des § 18 Abs. 1 Nr. 3 EStG vergleichbar.

Hierunter fallen Mitglieder von Organen einer Körperschaft wie Aufsichtsrat oder Verwaltungsrat oder andere Personen, die mit der Überwachung der Geschäftsführung beauftragt sind. Wesentliches Merkmal der Überwachung ist das Recht und die Pflicht zur Kontrolle der Geschäftsführung (vgl. BFH-Urteil vom 28.08.2003 – IV R 1/03, BFHE 203, 438, BStBl II 2004, 112; Schmidt/Wacker, a.a.O., § 18 Rz 150; Korn in Korn, § 18 EStG Rz 101; HHR/Brandt, § 18 EStG Rz 266, m.w.N.). Für die Einordnung kommt es nicht auf die tatsächliche Bezeichnung dieser Personen, sondern die von ihnen ausgeübte Tätigkeit an (BFH-Urteile in BFHE 203, 438, BStBl II 2004, 112; vom 11.03.1981 – I R 8/77, BFHE 133, 193, BStBl II 1981, 623). Der Begriff der überwachenden Tätigkeit ist weit auszulegen (BFH-Urteile in BFHE 203, 438, BStBl II 2004, 112, und vom 31.01.1978 – VIII R 159/73, BFHE 124, 345, BStBl II 1978, 352, m.w.N.). Eine

überwachende Funktion liegt nicht vor, wenn jemand gegenüber der Geschäftsführung einer Kapitalgesellschaft lediglich beratend tätig wird, denn der Berater hat nicht das Recht und die Pflicht zur Kontrolle (vgl. BFH-Urteil in BFHE 203, 438, BStBl II 2004, 112).

Hiernach fehlt eine Vergleichbarkeit mit der Tätigkeit eines Aufsichtsrats. Die Tätigkeit des Datenschutzbeauftragten ist im Schwerpunkt beratend, nicht kontrollierend. Sie dient zudem, soweit sie kontrollierend ist, der Einhaltung datenschutzrechtlicher Bestimmungen und damit dem Schutz der Persönlichkeitsrechte derjenigen, deren personenbezogene Daten das Unternehmen verarbeitet. Sie umfasst mithin insbesondere die Prüfung der Datenschutzorganisation des Auftraggebers, der Datenverarbeitungsprogramme und die Vorabkontrolle geplanter Vorhaben zur Verarbeitung personenbezogener Daten, sie dient jedoch nicht der unternehmerischen Kontrolle der Tätigkeit der Geschäftsführung als solcher. Dementsprechend sind auch die dem Datenschutzbeauftragten zustehenden Befugnisse nicht mit denen eines Aufsichtsrats (z.B. § 111 Abs. 3, Abs. 4 des Aktiengesetzes) vergleichbar.

Informationspflichten nach Art. 13 Abs. 1 lit. a, c und Abs. 2 lit. b, d und e DS-GVO beinhalten Marktverhaltensregelungen (Ls)

(Oberlandesgericht Stuttgart, Urteil vom 27. Februar 2020 – 2 U 257/19 –)

1. § 13 Abs. 1 Satz 1 TMG wird durch die Bestimmungen der Datenschutz-Grundverordnung verdrängt.
2. Art. 80 DS-GVO enthält keine abschließende Regelung über die Rechtsdurchsetzung von Verstößen gegen die DS-GVO. Wettbewerbsverbände sind gemäß § 8 Abs. 3 Nr. 2 UWG i.V.m. § 8 Abs. 1 und § 3a UWG befugt, solche Verstöße gegen Bestimmungen der DS-GVO geltend zu machen, bei denen es sich um Marktverhaltensregelungen handelt.
3. Eine Vorschrift, die dem Schutz von Rechten, Rechtsgütern oder sonstigen Interessen von Marktteilnehmern dient, ist eine Marktverhaltensregelung, wenn das geschützte Interesse gerade durch die Marktteilnahme, also durch den Abschluss von Austauschverträgen und den nachfolgenden Verbrauch oder Gebrauch der erworbenen Ware oder in Anspruch genommenen Dienstleistung berührt wird (BGH, Urteil vom 27.04.2017 – I ZR 215/15 – Aufzeichnungspflicht). Nicht erforderlich ist dabei eine spezifisch wettbewerbsbezogene Schutzfunktion. Die Vorschrift muss aber zumindest auch den Schutz der wettbewerblichen Interessen der Marktteilnehmer bezwecken (BGH, Urteil vom 28.11.2019 – I ZR 23/19, MIR 2020, Dok. 012 – Pflichten des Batterieherstellers). Dem Interesse der Verbraucher und sonstigen Marktteilnehmer im Sinne von § 3a UWG dient eine Norm, wenn sie deren Informationsinteresse und Entscheidungs- und Verhaltensfreiheit in Bezug auf die Marktteilnahme schützt.

4. Insofern beinhalten Informationspflichten nach Art. 13 Abs. 1 lit. a, c und Abs. 2 lit. b, d und e DS-GVO auch Marktverhaltensregelungen.

(Nicht amtliche Leitsätze)

Abberufung eines Datenschutzbeauftragten wegen fehlender Zuverlässigkeit

(Landesarbeitsgericht Mecklenburg-Vorpommern, Urteil vom 25. Februar 2020 – 5 Sa 108/19 –)

1. Das Gesetz knüpft die Tätigkeit als Datenschutzbeauftragter nicht an eine bestimmte Ausbildung oder näher bezeichnete Fachkenntnisse. Welche Sachkunde hierfür erforderlich ist, richtet sich insbesondere nach der Größe der zu betreuenden Organisationseinheit, dem Umfang der anfallenden Datenverarbeitungsvorgänge, den eingesetzten IT-Verfahren, dem Typus der anfallenden Daten usw. Regelmäßig sind Kenntnisse des Datenschutzrechts, zur Technik der Datenverarbeitung und zu den betrieblichen Abläufen erforderlich.
2. Die nach § 20 DSGVO M-V a. F. erforderliche Zuverlässigkeit eines internen Datenschutzbeauftragten kann nicht nur in Frage stehen, wenn er die mit dieser Aufgabe verbundenen Pflichten verletzt, sondern auch bei einer schwerwiegenden Verletzung von allgemeinen arbeitsvertraglichen Pflichten. Bei einem internen Datenschutzbeauftragten lässt sich dessen Stellung als Datenschutzbeauftragter nicht vollständig von dem zugrundeliegenden Arbeitsverhältnis trennen. Eine schwerwiegende Verletzung arbeitsvertraglicher Pflichten kann dazu führen, dass eine zuverlässige Ausübung der datenschutzrechtlichen Selbstkontrolle nicht mehr möglich ist.

Sachverhalt:

Die Parteien streiten über die Wirksamkeit der Abberufung des Datenschutzbeauftragten.

Die Beklagte betreibt als Körperschaft des öffentlichen Rechts ein Universitätsklinikum mit mehr als 4100 Beschäftigten. Zur Unternehmensgruppe gehören weitere 11 Gesellschaften mit insgesamt rund 900 Beschäftigten. Der im November 1966 geborene Kläger ist Assessor der Rechte (ass. jur.), also Volljurist. Er schloss am 07.05.2007 mit der Beklagten einen Sonderdienstvertrag über eine Beschäftigung als Personaldezernent ab dem 01.08.2007.

Wenige Monate nach seiner Einstellung verfasste der Kläger mit Datum vom 19.12.2007 einen Verfügungsvermerk, in dem er zu dem Ergebnis kam, dass dem ihm vorgesetzten Kaufmännischen Vorstand, Herrn G., eine betriebliche Altersversorgung zusteht. Zur Begründung verwies er auf die Bezugnahme Klausel im Dienstvertrag mit Herrn G. vom 24./30.10.2006, nach der die jeweils geltenden Tarifverträge Anwendung finden, soweit im Dienstvertrag nichts Abweichendes geregelt ist. Der Kläger bezog sich auf die schriftliche Geltendmachung durch Herrn G. vom 18.12.2007 und hielt eine im Rahmen der Ausschlussfrist rückwirkende Einrichtung einer betrieblichen Altersversorgung nach dem Leistungsplan des DUK Versorgungswerks für geboten. Die Beklagte richtete daraufhin für Herrn G. eine solche betriebliche Altersversorgung ein.

Im Jahr 2008 wurde der Kläger zum Geschäftsführer der Personalservice Gesundheitswesen GmbH, einer Tochtergesellschaft der Beklagten, bestellt. Zum 01.11.2009 begründete der Kläger mit einer anderen Tochtergesellschaft der Beklagten, der HKS Rettungsdienst A-Stadt GmbH, ein Arbeitsverhältnis über eine geringfügige Beschäftigung.

Am 23.10.2014 schlossen die Parteien mit Wirkung zum 01.01.2015 einen Änderungsvertrag, in dem u.a. die Bezugnahme Klausel, die Vergütungsregelung und die Arbeitsaufgabe neu gefasst sind. Einbezogen ist zudem die Bestellung des Klägers zum Datenschutzbeauftragten (soweit Angelegenheiten des Personaldezernats nicht berührt werden) und seine Bestellung zum 2. Abfallbeauftragten. Herr G. schied zum 31.12.2014 bei der Beklagten aus und wurde mit Wirkung zum 01.01.2015 von Frau L. abgelöst.

Mit Schreiben vom 10.07.2015 teilte der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern dem Kläger auf dessen Nachfrage hin mit, den Arbeitsumfang des Datenschutzbeauftragten an der Universitätsmedizin als Vollzeitbeschäftigung einzustufen. Die Parteien schlossen am 18.09.2015 einen weiteren Änderungsvertrag. Danach wird der Kläger ab 17.09.2015 im Umfang von 25 % seiner Arbeitszeit als Justiziar sowie als 2. Abfallbeauftragter weiterbeschäftigt. Als Justiziar wird er dem Bereich des Kaufmännischen Vorstandes zugeordnet, ohne mit Aufgaben aus dem Personalwesen und/oder der Datenverarbeitung inhaltlich betraut zu werden. Im Übrigen sieht der Vertrag eine Freistellung zu 75 % seiner Arbeitszeit für Aufgaben des behördlichen Datenschutzbeauftragten sowie des Konzernbeauftragten für den Datenschutz vor. Des Weiteren regelt der Änderungsvertrag, dass die betriebliche Altersversorgung zum 30.09.2015 geschlossen wird und kein Anspruch auf zukünftige Arbeitgeberleistungen zur Altersversorgung bestehen. Als Ausgleich hierfür erhält der Kläger eine Zulage.

Der Kläger veranstaltete interne Datenschutzkonferenzen, zu denen er die lokalen Datenschutzverantwortlichen einlud. Im Rahmen von innerbetrieblichen Fortbildungen bot er Schulungen zu verschiedenen Themen des Datenschutzes an. Er wirkte in verschiedenen Gremien und Arbeitskreisen mit. Bei der Beklagten und ihren Tochterunternehmen fallen täglich mehr als 10.000 Datenverarbeitungsvorgänge an. Mit der E-Mail vom 17.02.2017 bat der Kläger den Kaufmännischen Vorstand darum, wieder in die Abteilungsleiterrunde aufgenommen zu werden, um seiner Kontroll- und Beratungspflicht als Datenschutzbeauftragter nachkommen zu können. Die Bitte blieb erfolglos.

Seit 2017 ist der Kläger Mitglied des Gesamtpersonalrats der Beklagten.

Der frühere Kaufmännische Vorstand, Herr G., erhielt im Jahr 2017 eine Einmalzahlung aus der betrieblichen Altersversorgung in Höhe von € 260.395,91.

Am 30.01.2018 führte die Beklagte mit dem Kläger ein Gespräch zum Stand der Umsetzung der im Mai des Jahres in Kraft tretenden EU-Datenschutzgrundverordnung (DS-GVO) im eigenen Haus und bei den Tochtergesellschaften. Mit Schreiben vom 31.01.2018 nahm der Kläger hierzu Stellung und berichtete über die noch laufenden Gesetzgebungsverfahren im Land Mecklenburg-Vorpommern zur Anpassung des allgemeinen und des bereichsspezifischen Datenschutzrechts, insbesondere des Datenschutz- und des Landeskrankenhausgesetzes (DSG M-V, LKHG M-V). Des Weiteren verwies er auf einen von ihm verfassten Aufsatz zur DS-GVO in der Zeitschrift "f&w führen und wirtschaften im Krankenhaus", Ausgabe 02/17. Im vorletzten Satz des Schreibens vom 31.01.2018 heißt es: "Die konkrete Umsetzung der Datenschutzgesetze des Landes kann durch die Datenschutzverantwortlichen denklogisch erst nach Inkrafttreten der Gesetze erfolgen."

Mit den im Wesentlichen gleichlautenden Schreiben vom 19.02.2018 widersprachen die Tochtergesellschaften der Beklagten mit sofortiger Wirkung die Bestellung des Klägers zum Konzern- bzw. zum Datenschutzbeauftragten:

Mit Schreiben vom 20.02.2018 widerrief die Beklagte mit sofortiger Wirkung die Bestellung des Klägers zum Konzerndatenschutzbeauftragten. Sämtliche Schreiben gingen dem Kläger am 24.02.2018 zu.

Am 27.02.2018 führte die Beklagte mit dem Kläger erneut ein Gespräch, in dem sie ihm jegliche Tätigkeit als Datenschutzbeauftragter für die Beklagte und die genannten Tochtergesellschaften untersagte. Nachdem der Kläger in dem Gespräch auf den bislang unterbliebenen Widerruf seiner Bestellung zum Datenschutzbeauftragten bei der Beklagten selbst hingewiesen hatte, holte die Beklagte dies mit Schreiben vom 27.02.2018, dem Kläger am 01.03.2018 zugegangen, nach.

Mit Schreiben vom 28.02.2018 beantragte die Beklagte beim Gesamtpersonalrat die Zustimmung zu einer beabsichtigten außerordentlichen Änderungskündigung des Klägers, versehen mit dem Änderungsangebot, anschließend als Jurist beim Kaufmännischen Vorstand und als 2. Abfallbeauftragter mit einer regelmäßigen wöchentlichen Arbeitszeit von 39 Stunden und der dem Tarifvertrag entsprechenden Vergütung weiterzuarbeiten. Der Gesamtpersonalrat stimmte der außerordentlichen Änderungskündigung unter dem 08.03.2018 nicht zu. Ebenso lehnte der Personalrat für die nichtwissenschaftlich Beschäftigten mit Schreiben vom 13.03.2018 eine solche Änderungskündigung ab. Die Beklagte wandte sich daraufhin an das Verwaltungsgericht, um die Zustimmung gerichtlich ersetzen zu lassen. Eine Entscheidung liegt noch nicht vor.

Mit Schreiben vom 13.08.2018, der Beklagten zugegangen am 15.08.2018, rügte der Landesbeauftragte für Datenschutz und Informationsfreiheit M-V, nachdem der Personalrat für die nichtwissenschaftlichen Beschäftigten dort eine Beschwerde wegen der im elektronischen Dienstplansystem TDA einsehbaren Personaldaten eingereicht hatte, einen Verstoß gegen Datenschutzbestimmungen. Das Dienstplansystem TDA war bereits seit mehreren Jahren in Betrieb. Dort waren u.a. Personalnummern, geleistete Arbeitszeiten, Beschäftigungsverbote und Krankmeldungen hinterlegt, die alle Mitarbeiter der Station einsehen konnten. Der Landesbeauftragte hielt insbesondere die Offenlegung von Gesundheitsdaten ("krank") gegenüber allen Stationsmitarbeitern für nicht erforderlich und damit für unzulässig. Er forderte die Beklagte auf, das Verarbeitungsverzeichnis zum TDA vorzulegen, insbesondere forderte er ein Rechte- und Rollenkonzept und Löschfristenbestimmungen. Andernfalls stellte er ein Bußgeld in Aussicht. Der neu bestellte externe Datenschutzbeauftragte war in seiner Stellungnahme gegenüber dem Personalrat am 20.07.2018 ebenfalls von einer Unzulässigkeit ausgegangen, wovon die Beklagte am 24.07.2018 erfahren hatte.

Die Beklagte widerrief mit Schreiben vom 27.08.2018 vorsorglich erneut die Bestellung des Klägers zum Konzern- und zum Datenschutzbeauftragten. Ebenso erklärten die 10 genannten Tochtergesellschaften nochmals den Widerruf der Bestellung, ebenfalls unter dem 27.08.2018.

Am 10.09.2018 führte die Beklagte mit dem Kläger ein Personalgespräch zu den Vorwürfen, für den damaligen Kaufmännischen Vorstand, Herrn G., in kollusivem Zusammenwirken rechtswidrig eine Versorgungszusage eingerichtet zu haben und bei der eigenen Versorgungszusage ebenfalls ohne wirksame Rechtsgrundlage vorgegangen zu sein. Anschließend stellte die Beklagte ihn unwiderruflich von der Arbeit frei und erteilte ihm Hausverbot. Des Weiteren beantragte die Beklagte mit Schreiben vom 13.09.2018 sowohl beim Personalrat für die nichtwissenschaftlichen Beschäftigten als auch beim Gesamtpersonalrat die Zustimmung zur beabsichtigten außerordentlichen Kündigung des Klägers, hilfsweise mit Auslauffrist. Da die Personalräte ihre Zustimmung verweigerten, wandte sich die Beklagte mit Schriftsatz vom 23.09.2018 an das VG Greifswald (Aktenzeichen 7 A 1419/18). Gegenstand eines weiteren Rechtsstreits ist der Fortbestand des Arbeitsverhältnisses mit der HKS Rettungsdienst A-Stadt GmbH nach Ausspruch einer außerordentlichen, hilfsweise ordentlichen Kündigung am 21.09.2018 (ArbG Stralsund, Urteil vom

03.04.2019, Aktenzeichen 3 Ca 239/18; LAG Mecklenburg-Vorpommern, Urteil vom 16.10.2019, Aktenzeichen 4 Sa 104/19).

Nachdem die Beklagte die Tätigkeit des Klägers als Mitglied des Gesamtpersonalrates zunächst vom Hausverbot ausgenommen hatte, berief sie sich mit Schreiben vom 09.11.2018 nunmehr auf ein Ruhen seiner Mitgliedschaft im Gesamtpersonalrat nach § 22 Abs. 3 PersVG M-V. Nach dieser Vorschrift ruht die Mitgliedschaft im Personalrat, solange einem Beschäftigten die Führung der Dienstgeschäfte verboten oder ein Beamter wegen eines schwebenden Disziplinar- oder Untersuchungsverfahrens vorläufig des Dienstes entzogen ist. Des Weiteren erstattete die Beklagte Strafanzeige gegen den Kläger (StA Stralsund, Aktenzeichen 534 Js 23379/18).

Der Kläger hat erstinstanzlich die Ansicht vertreten, dass die Widerrufe der Bestellung zum Konzern- bzw. Datenschutzbeauftragten unwirksam seien. Ein wichtiger Grund im Sinne des § 626 Abs. 1 BGB, § 20 DSGVO (a. f.) liege nicht vor. Zudem sei die Ausschlussfrist des § 626 Abs. 2 BGB nicht gewahrt. Der Kläger habe seine Pflichten als Datenschutzbeauftragter nicht verletzt. Die Beklagte vermische die Aufgaben des Datenschutzverantwortlichen mit denen des Datenschutzbeauftragten. Aufgabe des Datenschutzbeauftragten sei nicht die operative Umsetzung der gesetzlichen Vorgaben, sondern die Kontrolle der Umsetzung. Als Datenschutzbeauftragter sei der Kläger Berater des Arbeitgebers und der Mitarbeiter. Keinesfalls sei er untätig gewesen. Er habe sich intensiv mit den neuen Datenschutzregelungen befasst, wie der Aufsatz in der f&w zeige. Er habe die Datenschutzbelange in der IT-Kommission eingebracht. Des Weiteren habe er maßgeblich an der Gründung des Arbeitskreises Datenschutz an Universitätsklinikum mitgewirkt. Er sei Mitglied des Arbeitskreises Datenschutzrecht der Krankenhausgesellschaft Mecklenburg-Vorpommern. Er habe Handlungsempfehlungen an die zuständigen Stellen weitergeleitet.

Der Kläger habe die Altersversorgungsangelegenheit G. nicht fehlerhaft behandelt. Die rechtliche Grundlage der Versorgungszusage ergebe sich aus dem vom Aufsichtsrat abgeschlossenen Anstellungsvertrag. Dieser enthalte keine Regelung zur betrieblichen Altersversorgung, sodass die Bezugnahme Klausel Anwendung finde. In dem Anstellungsvertrag seien zwar bestimmte Regelungsbereiche des Tarifvertrages ausdrücklich ausgenommen worden, wie beispielsweise die Arbeitszeit, Eingruppierung oder Vergütung. Die tarifvertraglichen Bestimmungen zur Altersversorgung seien davon aber gerade nicht erfasst. Demnach sei § 25 TV-L anzuwenden, wonach Herr G. eine betriebliche Altersversorgung unter Eigenbeteiligung haben beanspruchen können. Auch anderen Vorstandsmitgliedern sei eine betriebliche Altersversorgung gewährt worden, u.a. Herrn B. und Herrn H. Herr G. sei auf den Kläger zugetreten und habe mitgeteilt, dass ursprünglich für ihn eine Umlage an die VBL (Versorgungsanstalt des Bundes und der Länder) gezahlt worden sei, was jedoch nach dem Wechsel zum DUK Versorgungswerk nicht mehr geschehe. Herr G. sei von einem Verwaltungsversehen ausgegangen und habe den Kläger um rechtliche Prüfung gebeten. Da dem Kläger die Hintergründe nicht bekannt gewesen seien und er sich in der Probezeit nicht habe blamieren wollen, habe er sich hierzu mit Herrn B. aus der Rechtsabteilung abgestimmt. In gleicher Weise seien auch die Anstellungsverträge der Vorstandsmitglieder B. und H. geprüft worden, ebenfalls mit positivem Ergebnis. Der Ordner mit den Unterlagen zur betrieblichen Altersversorgung für Herrn G. sei nicht, wie die Beklagte behauptete, versteckt aufbewahrt worden, sondern für alle Mitarbeiter der Personalabteilung einsehbar gewesen.

Die für den Kläger eingerichtete Altersversorgung habe den vertraglichen Regelungen entsprochen. Die Beitragsanpassung habe sich nach den jeweils von der Beklagten übermittelten Jahresgehältern gerichtet. Soweit das DUK Versorgungswerk im Jahr 2008 für den Kläger zunächst eine weitere betriebliche Altersversorgung eingerichtet habe, sei dies ein Versehen des Versorgungswerks gewesen, wie das Versorgungswerk mit Schreiben vom 17.09.2018 bestätigt habe. Ausweislich des Schreibens habe das Versorgungswerk aus nicht mehr

nachvollziehbaren Gründen irrtümlich eine zweite Versorgung für den Kläger eingerichtet. Die Beiträge seien der Beklagten deshalb im Januar 2019 wieder gutgeschrieben worden. Der Beitragssatz sei nicht für alle Mitarbeiter einheitlich, sondern werde individuell bestimmt nach Alter, Rentenanspruch, Nachversicherungszeiten etc. Satzungs-gemäß habe sein Beitragssatz 9,65 % betragen; der gemittelte Beitragssatz aller Beschäftigten habe seinerzeit bei 3,9 % gelegen.

Die Beklagte hat die Auffassung vertreten, dass die Widerrufe berechtigt seien. Der Kläger habe es vollständig unterlassen, auf eine Umsetzung der Vorgaben aus der DS-GVO hinzuwirken. Die Umsetzung der DS-GVO und der ergänzenden Bestimmungen sei mit einem erheblichen zeitlichen und inhaltlichen Aufwand verbunden. Zunächst sei eine Bestandsaufnahme der eigenen Datenverarbeitung vorzunehmen. Sodann seien der Anpassungsbedarf festzustellen und konkrete Maßnahmen daraus abzuleiten sowie umzusetzen. Komme die Beklagte dem nicht nach, müsse sie mit erheblichen Sanktionen, nämlich Geldbußen bis zu 10 oder sogar 20 Millionen Euro, rechnen. Der Datenschutzbeauftragte habe die Umsetzung der DS-GVO proaktiv zu begleiten und eigene Vorschläge einzubringen. Mit dem Schreiben vom 31.01.2018 habe der Kläger zu erkennen gegeben, dass er nicht gewillt sei, seinen Verpflichtungen nachzukommen. Auf die datenschutzrechtlichen Probleme des Dienstplansystems TDA habe er zu keinem Zeitpunkt hingewiesen, sondern diesen mitgetragen. Erst der neu bestellte externe Datenschutzbeauftragte habe gegenüber dem Personalrat Bedenken geäußert.

Darüber hinaus fehle dem Kläger die erforderliche Zuverlässigkeit für die Tätigkeit des Datenschutzbeauftragten. Der Kläger sei kurz nach Aufnahme des Beschäftigungsverhältnisses auf den damaligen Kaufmännischen Vorstand, Herrn G., zugegangen und habe ihm angeboten, ihn in das betriebliche Altersversorgungssystem einzubeziehen. Zwar verweise der Vorstands-Anstellungsvertrag von Herrn G. auf Tarifverträge. Das gelte aber nur, soweit sich aus dem Vertrag nichts anderes ergebe. Die systematische Auslegung des Vertrages führe dazu, dass ein Anspruch auf eine betriebliche Altersversorgung nicht bestehe. Das zeige die Überschrift des § 4 „Arbeitsunfähigkeit/Altersversorgung“. Unter § 4 gebe es eben nur Regelungen zur Arbeitsunfähigkeit, weshalb die Altersversorgung also ausgeschlossen sei. Die Rechtsauffassung des Klägers sei nicht vertretbar. Für die Zusage einer Altersversorgung sei nur der Aufsichtsrat zuständig. Über die von Frau K., Leiterin Personalabrechnung, und Frau T., Lohnbuchhalterin, geäußerten Einwände, dass Herr G. als Vorstandsmitglied eine betriebliche Altersversorgung nicht beanspruchen könne, habe sich der Kläger hinweggesetzt, indem er sich gegenüber den beiden ihm unterstellten Mitarbeiterinnen auf seine Stellung als Vorgesetzter berufen habe. Auch habe er den Aufsichtsrat der Beklagten nicht eingebunden. Die Unterlagen zur Altersversorgung G. habe er in einem separaten Ordner abgelegt. Den wesentlichen Teil der Korrespondenz mit der Unterstützungskasse habe er persönlich geführt. Von diesen Vorgängen habe die seit 01.01.2016 eingesetzte, jetzige Kaufmännische Vorständin erstmalig am 27.08.2018 erfahren.

Zudem habe der Kläger bei seiner eigenen Altersversorgung mit Billigung von Herrn G. eine Erhöhung der Beiträge von 3,9 % des anrechenbaren Nettoaufkommens auf 9,65 % veranlasst. Der monatliche Beitrag habe sich dadurch von € 275,68 auf € 671,54 erhöht. Damit habe sich der Kläger einer strafbewehrten Untreue schuldig gemacht.

Das Arbeitsgericht hat der Klage gegen den Widerruf der Bestellung als Datenschutzbeauftragter im Umfang der hier noch maßgeblichen Anträge stattgegeben. Die Widerrufe der Bestellung des Klägers zum Datenschutzbeauftragten sowie Konzerndatenschutzbeauftragten seien unwirksam. Es gebe hierfür keine Gründe im Sinne des § 20 Abs. 2 Satz 2 DSGVO M-V a. F. in Verbindung mit § 626 BGB. Angesichts der unabhängigen Stellung des Datenschutzbeauftragten sei eine Abberufung nur aus schwerwiegenden Gründen zulässig. Zwar könne sich aus der dauerhaften Verletzung der Kontrollpflichten ein Grund für die Abberufung ergeben. Die Beklagte

habe jedoch keine Umstände dargelegt, aus denen sich eine solche Pflichtverletzung herleiten lasse. Der Kläger habe sich rechtzeitig mit der DSGVO auseinandergesetzt. Deren tatsächliche Umsetzung habe erst nach Inkrafttreten erfolgen können. Gleiches gelte für die seinerzeit noch nicht verabschiedete Neufassung des DSGVO M-V und des LKHG M-V. Der Kläger habe zudem in verschiedenen Gremien und Arbeitskreisen mitgewirkt. Das elektronische Dienstplansystem TDA habe der Kläger nicht mitgetragen, da dieses während seiner Zeit als Datenschutzbeauftragter nicht eingeführt worden sei. Soweit sich die Beklagte auf evtl. Unregelmäßigkeiten bei der Einrichtung von Versorgungszusagen berufe, fehle es an einem Bezug zu den Tätigkeiten als Datenschutzbeauftragter.

Hiergegen wendet sich die Beklagte mit ihrer fristgerecht eingelegten und begründeten Berufung. Das Arbeitsgericht sei zu Unrecht davon ausgegangen, dass die Widerrufe der Bestellung des Klägers zum Datenschutzbeauftragten nicht wirksam seien. Trotz des unmittelbar bevorstehenden Inkrafttretens der DSGVO sei der Kläger vollständig untätig geblieben. Die Beklagte habe eine aktive Mitwirkung des Klägers an den Vorbereitungen zur Umsetzung der DSGVO erwarten dürfen. Der Kläger sei verpflichtet gewesen, sich einen Überblick über die datenschutzrechtlich relevanten Systeme zu verschaffen. Stattdessen habe sich der Kläger rein passiv und dilatorisch verhalten, um seine mangelnde Sachkunde und seine Unzuverlässigkeit zu verschleiern. Der Kläger habe den Umfang seiner Aufgaben überhaupt nicht erfasst. Die Beklagte sei im Sinne eines effektiven Datenschutzes gezwungen gewesen, einen fachlich geeigneten Nachfolger für den Kläger zu bestellen. Zudem habe das Arbeitsgericht verkannt, dass der Kläger arbeitsvertragliche Nebenpflichten in schwerwiegender Weise und strafrechtlich relevant verletzt habe. Dem Kläger fehle damit die persönliche Integrität. Die von ihm gewünschte Teilnahme an den erweiterten Abteilungsleiterrunden weise im Übrigen keinen Zusammenhang mit seinen Aufgaben als Datenschutzbeauftragter auf. Der Vorstand habe ihn stets ausreichend informiert.

Aus den Gründen:

Die Berufung der Beklagten ist zwar zulässig, aber nicht begründet. Das Arbeitsgericht hat der Klage im hier noch anhängigen Umfang zu Recht stattgegeben.

Die Beklagte hat die Bestellung des Klägers zum behördlichen Datenschutzbeauftragten und zum Konzerndatenschutzbeauftragten weder mit den Schreiben vom 19./20./27.02.2018 noch mit dem Schreiben vom 27.08.2018 wirksam widerrufen bzw. ihn wirksam abberufen.

Die Wirksamkeit der Widerrufe richtet sich nach der jeweils gültigen Gesetzeslage. Maßgebliche Beurteilungsgrundlage für die Rechtmäßigkeit eines Widerrufs sind ebenso wie bei einer Kündigung die objektiven Verhältnisse im Zeitpunkt des Zugangs der Widerrufserklärung (vgl. zur Kündigung: BAG, Urteil vom 05. Dezember 2019 – 2 AZR 223/19 – Rn. 39, juris = NZA 2020, 227). Für die Darlegungs- und Beweislast gelten die allgemeinen Grundsätze. Danach trägt der Anspruchsteller die Darlegungs- und Beweislast für die rechtsbegründenden, der Anspruchsgegner trägt sie für die rechtsvernichtenden, rechtshindernden und rechtshemmenden Tatbestandsmerkmale (BAG, Urteil vom 28. Februar 2019 – 8 AZR 201/18 – Rn. 32, juris = NZA 2019, 1279).

1. Widerrufe vom 19./20./27.02.2018

Nach § 20 Abs. 2 Satz 2 DSGVO M-V in der bis zum 24.05.2018 geltenden Fassung (a. F.) kann die Bestellung zum behördlichen Datenschutzbeauftragten schriftlich widerrufen werden, wenn ein Interessenkonflikt mit seinen anderen dienstlichen Aufgaben eintritt oder sonst ein wichtiger Grund in entsprechender Anwendung von § 626 BGB vorliegt. Vor der Ent-

scheidung über den Widerruf ist der behördliche Datenschutzbeauftragte zu hören (§ 20 Abs. 2 Satz 3 DSGVO a. f.).

Ein Interessenkonflikt besteht, wenn der Datenschutzbeauftragte in erster Linie seine eigene Tätigkeit kontrollieren muss (BAG, Urteil vom 05. Dezember 2019 – 2 AZR 223/19 – Rn. 25, juris = NZA 2020, 227; BAG, Urteil vom 23. März 2011 – 10 AZR 562/09 – Rn. 24, juris = ZTR 2011, 561). Die Mitgliedschaft im Betriebsrat ist grundsätzlich mit der Tätigkeit eines Datenschutzbeauftragten vereinbar (BAG, Urteil vom 23. März 2011 – 10 AZR 562/09 – Rn. 25, juris = ZTR 2011, 561).

Ein wichtiger Grund in entsprechender Anwendung von § 626 BGB ist gegeben, wenn Tatsachen vorliegen, auf Grund derer dem Arbeitgeber unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der Interessen beider Vertragsteile ein weiterer Einsatz des Mitarbeiters in der Funktion des Datenschutzbeauftragten nicht mehr zugemutet werden kann. Als wichtige Gründe kommen insbesondere solche in Betracht, die mit der Funktion und der Tätigkeit des Datenschutzbeauftragten zusammenhängen und eine weitere Ausübung dieser Tätigkeit unmöglich machen oder sie zumindest erheblich gefährden, beispielsweise ein Geheimnisverrat oder eine dauerhafte Verletzung der datenschutzrechtlichen Kontrollpflichten (BAG, Urteil vom 23. März 2011 – 10 AZR 562/09 – Rn. 15, juris = ZTR 2011, 561; Greiner/Senk, NZA 2020, S. 206 f.). Allerdings genügt es nicht, dass der Arbeitgeber eine andere Person, sei es ein anderer Arbeitnehmer oder ein externer Dienstleister, nunmehr für besser geeignet hält. Dem steht die Unabhängigkeit und Weisungsfreiheit des Datenschutzbeauftragten entgegen. Der Datenschutzbeauftragte soll seiner Kontrolltätigkeit im Interesse des Datenschutzes ohne Furcht vor einer Abberufung nachgehen können (BAG, Urteil vom 23. März 2011 – 10 AZR 562/09 – Rn. 14, juris = ZTR 2011, 561).

Zum Datenschutzbeauftragten darf nach § 20 Abs. 1 Satz 3 DSGVO a. f. nur bestellt werden, wer die zur Erfüllung seiner Aufgabe erforderliche Sachkunde und Zuverlässigkeit besitzt. Sind diese Voraussetzungen weggefallen, ist es dem Arbeitgeber grundsätzlich nicht zumutbar, den Betroffenen weiterhin in der Funktion des Datenschutzbeauftragten zu belassen, zumal er sich dadurch selbst gesetzeswidrig verhalten würde.

Der behördliche Datenschutzbeauftragte hat nach § 20 Abs. 3 DSGVO a. f. die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu überwachen und Hinweise zur Umsetzung zu geben. Er kann Auskünfte verlangen und Einsicht in Akten und Dateien nehmen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Berufs- und Amtsgeheimnisse können ihm nicht entgegengehalten werden. Zu seiner Unterstützung kann er sich jederzeit an den Landesbeauftragten für den Datenschutz wenden. Zu den Aufgaben des behördlichen Datenschutzbeauftragten gehört es insbesondere,

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Datenverarbeitungsmaßnahmen hinzuwirken,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
3. die Daten verarbeitende Stelle bei der Umsetzung der nach den §§ 18, 21 und 22 erforderlichen Maßnahmen zu unterstützen,
4. das Verzeichnis nach § 18 zu führen und
5. die Vorabkontrolle nach § 19 durchzuführen.

Nach § 18 Abs. 1 DSGVO a. f. ist die Daten verarbeitende Stelle verpflichtet, in einer Beschreibung für jedes von ihr eingesetzte

Verfahren festzulegen und dem behördlichen Datenschutzbeauftragten zur Führung des Verzeichnisses zu übermitteln:

1. die Bezeichnung des Verfahrens und der verarbeitenden Stelle,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Art der gespeicherten Daten,
4. den Kreis der Betroffenen,
5. den Kreis der Empfänger, denen die Daten mitgeteilt werden,
6. geplante Datenübermittlungen in Drittländer,
7. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Die Einrichtung oder die wesentliche Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten bedarf der Freigabe durch den Leiter der Daten verarbeitenden Stelle oder einen dafür beauftragten Vertreter (§ 19 Abs. 1 Satz 1 DSGVO a. f.). Dem behördlichen Datenschutzbeauftragten ist nach § 19 Abs. 2 Satz 1 DSGVO a. f. zuvor Gelegenheit zur Prüfung zu geben, ob die Datenverarbeitung zulässig ist und die vorgesehenen Maßnahmen nach den §§ 21, 22 DSGVO a. f. ausreichend sind (Vorabkontrolle).

In § 21 DSGVO a. f. sind allgemeine Maßnahmen zur Datensicherheit aufgeführt. Zu gewährleisten ist danach insbesondere, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unverändert, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können (Authentizität der Daten),
5. unter Beteiligung der Personal- oder Arbeitnehmervertretung von der Daten verarbeitenden Stelle ein Protokollierungsverfahren festgelegt wird, das die Feststellung erlaubt, wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit) und
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig und in zumutbarer Zeit nachvollzogen werden können (Transparenz).

§ 22 DSGVO a. f. beschreibt die besonderen Maßnahmen zur Datensicherheit beim Einsatz automatisierter Verfahren. Danach sind automatisierte Verfahren so zu gestalten, dass eine Verarbeitung personenbezogener Daten erst möglich ist, nachdem die Berechtigung des Benutzers festgestellt worden ist (Abs. 1). Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren (Abs. 2). Werden personenbezogene Daten mit Hilfe informationstechnischer Geräte von der verarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln (Abs. 3). Sollen personenbezogene Daten ausschließlich automatisiert gespeichert werden, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden, was ebenso für die Veränderung und Übermittlung der Daten gilt (Abs. 4 Sätze 1 und 2).

Der Kläger besitzt sowohl die erforderliche Sachkunde als auch die erforderliche Zuverlässigkeit zur Erfüllung der dem behördlichen Datenschutzbeauftragten obliegenden Aufgaben.

Das Gesetz knüpft die Tätigkeit des Datenschutzbeauftragten nicht an eine bestimmte Ausbildung oder näher bezeichnete Fachkenntnisse. Welche Sachkunde hierfür erforderlich ist, richtet sich insbesondere nach der Größe der zu betreuenden Organisati-

onseinheit, dem Umfang der anfallenden Datenverarbeitungsvorgänge, den eingesetzten IT-Verfahren, dem Typus der anfallenden Daten usw. Regelmäßig sind Kenntnisse des Datenschutzrechts, zur Technik der Datenverarbeitung und zu den betrieblichen Abläufen erforderlich (Däubler, EU-DS-GVO und BDSG, 2. Aufl. 2020, DS-GVO Art. 37, Rn. 18; Gola DS-GVO/Klug, 2. Aufl. 2018, DS-GVO Art. 37, Rn. 18). Verfügt der Datenschutzbeauftragte nur in einem Teilbereich über eine eigene Qualifikation, genügt es, wenn er im Übrigen auf fachkundige Mitarbeiter zurückgreifen kann (Kühling/Buchner/Bergt, 2. Aufl. 2018, DS-GVO Art. 37, Rn. 34). Des Weiteren sind Fortbildungen zu den neuen technischen Entwicklungen und Gesetzesänderungen bzw. Entwicklungen in der Rechtsprechung unerlässlich (BeckOK DatenschutzR/Moos, 31. Ed., Stand 01.11.2019, DS-GVO Art. 37, Rn. 60).

Als Volljurist ist der Kläger ohne weiteres in der Lage, sich mit dem einschlägigen Datenschutzrecht vertraut zu machen und dieses praktisch anzuwenden. Aufgrund der vorangegangenen langjährigen Tätigkeit als Personaldezernent waren ihm die wesentlichen Grundzüge des Datenschutzes ohnehin bereits geläufig. Die Einzelheiten des neuen Datenschutzrechts sind dem Kläger vertraut, wie seine Veröffentlichung in der Zeitschrift f&w zeigt. Dort hat er die Grundsätze des Datenschutzes und die wesentlichen Neuerungen durch die DS-GVO näher dargestellt. Des Weiteren hatte er sich zum Stand der landesrechtlichen Gesetzgebung informiert. Zu den technischen Fragen der Datenverarbeitung konnte sich der Kläger bei dem stellvertretenden Datenschutzbeauftragten, einem Informatiker, informieren.

Darüber hinaus verfügt der Kläger über die notwendige Zuverlässigkeit für die Tätigkeit des Datenschutzbeauftragten. Der Datenschutzbeauftragte muss nicht nur die nötigen Fachkenntnisse besitzen, sondern auch die Gewähr bieten, dass er seinen Aufgaben gewissenhaft nachkommt und nicht gegen seine Pflichten als Datenschutzbeauftragter, z.B. gegen seine Verschwiegenheitspflicht, verstößt. Eine schwerwiegende Verletzung allgemeiner arbeitsvertraglicher Pflichten kann ebenfalls die Zuverlässigkeit in Frage stellen, beispielsweise Diebstahl, Unterschlagung, vorsätzliche Rufschädigung, Tätlichkeiten gegen andere Beschäftigte etc. Die Zuverlässigkeit ist unter Berücksichtigung von Sinn und Zweck der Bestellung eines Datenschutzbeauftragten zu bewerten. Der Datenschutzbeauftragte hat die Aufgabe, eine wirkungsvolle Eigenkontrolle der datenschutzrechtlichen Vorschriften sicherzustellen, um dadurch zugleich öffentliche Kontrollstellen zu entlasten (BeckOK DatenschutzR/Moos, 31. Ed., Stand: 01.11.2019, DS-GVO Art. 37, Rn. 1; Däubler, EU-DS-GVO und BDSG, 2. Aufl. 2020, DS-GVO Art. 37, Rn. 1; Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, DS-GVO Art. 37, Rn. 3). Die zum Datenschutzbeauftragten bestellte Person muss – über die Sachkunde hinaus – eine wirksame Selbstkontrolle gewährleisten können. Bei einem internen Datenschutzbeauftragten lässt sich dessen Stellung als Datenschutzbeauftragter nicht vollständig von dem zugrundeliegenden Arbeitsverhältnis trennen. Eine schwerwiegende Verletzung arbeitsvertraglicher Pflichten kann dazu führen, dass eine zuverlässige Ausübung der datenschutzrechtlichen Selbstkontrolle nicht mehr möglich ist. Besitzt der Datenschutzbeauftragte aufgrund eines solchen Fehlverhaltens nicht mehr das nötige Vertrauen, ist es u.a. ausgeschlossen, ihm die für seine Tätigkeit erforderlichen Informationen unter Einschluss von Berufs- und Amtsgeheimnissen (§ 20 Abs. 3 Satz 3 DSGVO a. f.) anzuvertrauen.

Der Kläger hat weder seine Pflichten als Datenschutzbeauftragter noch seine Pflichten aus dem Arbeitsverhältnis schwerwiegend verletzt. Eine wirksame Selbstkontrolle der Datenschutzbelange ist weiterhin gesichert.

Der Kläger hat seine Aufgaben als Datenschutzbeauftragter, für die er mit einer regelmäßigen wöchentlichen Arbeitszeit von 34,5 Stunden zur Verfügung stand, nicht vernachlässigt. Angesichts der Größe des zu betreuenden Bereichs ist es zwingend erforderlich, Schwerpunkte zu setzen. Die Beklagte und ihre Tochtergesellschaften verarbeiten täglich Tausende von besonders schutzwürdigen medizinischen Daten. Hinzu kommen Personaldaten von insgesamt rund 5000 Beschäftigten. Es sind verschiedene Datenverarbeitungsprogramme im Einsatz. Der Kläger hat entsprechend § 20 Abs. 3 Satz 5 DSGVO a. f. auf die Einhaltung von Datenschutzvorschriften hingewirkt. Er hat die Beschäftigten mit den Vorschriften des Datenschutzes vertraut gemacht. Er hat zahlreiche Anfragen aus dem eigenen Haus und von Tochtergesellschaften beantwortet. Er hat in verschiedenen Gremien und Arbeitskreisen mitgewirkt.

Der Kläger hat mit seinem Schreiben vom 31.01.2018 nicht erklärt, seinen Verpflichtungen nicht nachkommen zu wollen. Die Einhaltung des aktuellen Datenschutzrechts unter Berücksichtigung der einschlägigen Rechtsprechung ist zunächst Aufgabe der Beklagten als Betreiberin der Kliniken. Der Kläger als Datenschutzbeauftragter ist Kontrollorgan. Er hat zwar die Beklagte bei der Umsetzung der erforderlichen Maßnahmen zu unterstützen (§ 20 Abs. 3 Satz 5 Nr. 3 DSGVO a. f.). Die Umsetzung selbst bleibt jedoch Aufgabe der Beklagten und ihrer Tochtergesellschaften. Die Beklagte kannte die DS-GVO ebenso wie der Kläger und war mit der Prüfung des Anpassungsbedarfs befasst. Der vorletzte Satz im Schreiben vom 31.01.2018 bezieht sich zum einen nur auf die „konkrete“ Umsetzung der Datenschutzgesetze des Landes Mecklenburg-Vorpommern, die zu diesem Zeitpunkt nur als Entwurf vorlagen. Zum anderen sind dort die Datenschutzverantwortlichen angesprochen. Im Übrigen enthält das Schreiben ausschließlich Informationen zum Stand der Gesetzgebung. Auf die zu erwartenden rechtlichen Änderungen hatte sich der Kläger bereits vorbereitet, indem er sich mit der DS-GVO auseinandergesetzt und das Gesetzgebungsverfahren zum Landesrecht verfolgt hatte.

Der Kläger hat gegenüber der Beklagten bis zu seiner Entbindung von den Aufgaben des Datenschutzbeauftragten keine datenschutzrechtlichen Einwände gegen das elektronische Dienstplansystem TDA erhoben. Daraus folgt aber nicht, dass er seine Pflichten als Datenschutzbeauftragter vernachlässigt hat. Die Vielzahl der Aufgaben eines Datenschutzbeauftragten lässt es häufig nicht zu, von sich aus sämtliche Datenverarbeitungsprozesse kurzfristig zu überprüfen. Die Tätigkeit erforderte es, Schwerpunkte zu setzen, insbesondere wenn diese nur einen Teil der Arbeitszeit ausmacht und zugleich weitere Unternehmen zu betreiben sind. Es sind Anfragen und Beschwerden zu bearbeiten, Fortbildungen durchzuführen, Informationsmaterialien auszuwerten etc. Die Kontrollpflichten werden nur dann vernachlässigt, wenn der Datenschutzbeauftragte die ihm hierfür zur Verfügung stehende Arbeitszeit nicht ausschöpft, obwohl die Aufgaben noch nicht erledigt sind. Das war bei dem Kläger nicht der Fall. Hinweise auf datenschutzrechtliche Probleme des TDA lagen erst vor, als der Kläger bereits von den Aufgaben des Datenschutzbeauftragten entbunden war. Der Kläger hat das Dienstplansystem nicht als datenschutzrechtskonform eingestuft. Vielmehr hat er ebenso wenig wie die Beklagte einen vordringlichen Anlass für eine tiefere datenschutzrechtliche Prüfung gesehen.

Der Kläger hat keine allgemeinen Pflichten aus dem Arbeitsverhältnis verletzt, die einem weiteren Einsatz in der Funktion des Datenschutzbeauftragten entgegenstehen. Der Kläger hat die Beklagte nicht zielgerichtet zum Vorteil des damaligen

Kaufmännischen Vorstands G. oder zum eigenen Vorteil geschädigt bzw. dieses versucht. Er hat sich nicht bewusst über vertragliche, tarifvertragliche oder gesetzliche Vorschriften hinweggesetzt, um Herrn G. oder sich selbst rechtswidrig zu begünstigen. Das Vertrauen in ein rechtskonformes Handeln des Klägers ist nicht zerstört.

Ob Herr G. eine betriebliche Altersversorgung Zustand, bedarf hier keiner abschließenden Bewertung. Die Rechtsauffassung des Klägers in dem Verfügungsvermerk vom 19.12.2007 erscheint jedenfalls vertretbar. Der Dienstvertrag mit Herrn G. vom 24./30.10.2006 enthält zwar den Begriff „Altersversorgung“ in der Überschrift zu § 4. Eine Regelung zur Altersversorgung findet sich dort jedoch nicht, weder positiv noch negativ. Weshalb die Vertragsparteien dort das Begriffspaar „Arbeitsunfähigkeit/Altersversorgung“ verwandt haben, ist nicht ersichtlich, zumal beide Regelungsgegenstände keinen inneren Zusammenhang aufweisen, sondern unterschiedliche Lebenssachverhalte und Leistungen bezeichnen. Zudem enthält § 4 des Dienstvertrages trotz der Überschrift keinerlei Aussagen zur Altersversorgung. Dort sind ausschließlich Rechtsfolgen für den Fall einer Arbeitsunfähigkeit festgelegt. Da der Vertrag auch an anderer Stelle eine betriebliche Altersversorgung nicht regelt bzw. ausschließt, liegt es nicht fern, auf die Bezugnahme Klausel zurückzugreifen. Der Kläger hat sich jedenfalls nicht klar und eindeutig über den Vertrag oder sonstige Regelungen hinweggesetzt, um Herrn G. einen ihm offensichtlich nicht zustehenden Vorteil zu verschaffen. Der Kläger war nicht gehalten, unter Umgehung seines Vorgesetzten an den Aufsichtsrat heranzutreten. Der Anspruch von Herrn G. ergab sich nach Ansicht des Klägers aus dem Dienstvertrag, den der Aufsichtsrat selbst geschlossen hatte.

Der Kläger hat sich nicht vertragswidrig eine zu hohe betriebliche Altersversorgung verschafft. Soweit zu seinen Gunsten ein Beitragssatz von 9,65 % abgeführt wurde, ist ein Verstoß gegen vertragliche, tarifvertragliche oder satzungrechtliche Vorschriften nicht feststellbar. Abgesehen davon haben die Parteien die betriebliche Altersversorgung mit dem Änderungsvertrag vom 18.09.2015 neu geregelt und mit Wirkung zum 30.09.2015 geschlossen. Eine Korrektur für die Vergangenheit wurde seinerzeit nicht vorgenommen.

2. **Widerrufe vom 27.08.2018**

Seit dem 25.05.2018 sind die DS-GVO sowie die hierauf abgestimmten bundes- und landesrechtlichen Datenschutzgesetze anzuwenden. Nach § 6 Abs. 4 Satz 1 BDSG ist die Abberufung des Datenschutzbeauftragten – wie schon nach der vorherigen Rechtslage – nur in entsprechender Anwendung des § 626 BGB zulässig. Die Ausführungen zu § 20 DSG M-V a. f. unter Ziffer 1 gelten deshalb entsprechend.

Der Datenschutzbeauftragte wird gemäß Art. 37 Abs. 5 DS-GVO auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DS-GVO genannten Aufgaben. Die zu § 20 DSG M-V a. f. genannten Maßstäbe sind entsprechend heranzuziehen. Die persönliche Zuverlässigkeit ist zwar nicht mehr als Voraussetzung erwähnt. Der Datenschutzbeauftragte muss jedoch über die Fähigkeit verfügen, seine in Art. 39 DS-GVO genannten Aufgaben zu erfüllen. Daraus ergeben sich ähnliche Anforderungen, sodass auf die obigen Ausführungen verwiesen werden kann. Eine abweichende Bewertung der Abberufung des Klägers ist auf der Grundlage des neuen Datenschutzrechts nicht veranlasst. Im Übrigen durfte der Kläger bereits seit Ende Februar 2018 seine

Tätigkeit als Datenschutzbeauftragter nicht mehr ausüben, sodass er seine Kontrollpflichten und sonstigen datenschutzrechtlichen Aufgaben seitdem nicht mehr verletzen konnte.

Die Kostenentscheidung folgt aus § 97 Abs. 1 ZPO. Gründe für die Zulassung der Revision liegen nicht vor. Der Rechtsstreit wirft keine entscheidungserheblichen Rechtsfragen von grundsätzlicher Bedeutung auf.

Kein Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO im Verwaltungsverfahren nach §§ 20, 67a Abs. 2 SGB X (Ls)

(Landessozialgericht Darmstadt, Beschluss vom 29. Januar 2020 – L 4 SO 154/19 B –)

1. Die Erhebung von Sozialdaten bei der betroffenen Person im Rahmen der Amtsermittlung im Verwaltungsverfahren zur Bewilligung von Sozialleistungen (§ 20 SGB X, § 67a Abs. 2 SGB X) mittels eines Überprüfungsboogens ist keinem Widerspruch nach Art. 21 Abs. 1 DS-GVO zugänglich, da diese Verarbeitung im konkreten Fall nach Art. 6 Abs. 1 lit. c DS-GVO zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.
2. Zur einschränkenden Auslegung von § 56a SGG wegen Art. 19 Abs. 4 GG und Art. 47 GrCh.

Auskunftsgewährung nach dem Verbraucherinformationsgesetz: Übermittlung eines Kontrollberichts über eine gastronomische Betriebsprüfung (TopfSecret) (Ls)

(Oberverwaltungsgericht Lüneburg, Beschluss vom 16. Januar 2020 – 2 ME 707/19 –)

1. Daten über festgestellte nicht zulässige Abweichungen von bestimmten Rechtsvorschriften im Sinne von § 2 Abs. 1 Satz 1 Nr. 1 VIG liegen vor, wenn die zuständige Behörde die entsprechenden Informationen tatsächlich und rechtlich gewürdigt und die Abweichung aktenkundig gemacht hat (Anschluss an BVerwG, Urt. v. 29.8.2019 – 7 C 29.17 –, juris Rn. 32). Ausreichend ist es, dass die Behörde erkennen lässt, gegen welche rechtlichen Bestimmungen verstoßen wurde; eine genaue Aufschlüsselung und Zuordnung einzelner Verstöße zu einzelnen Absätzen, Sätzen und Spiegelstrichen ist nicht erforderlich.
2. Der Erteilung von Informationen gemäß § 2 Abs. 1 Satz 1 Nr. 1 VIG steht nicht entgegen, dass der Antragsteller seinen Antrag im Rahmen einer Kampagne Dritter gestellt hat und die Informationen im Internet veröffentlicht werden sollen. Für diesbezügliche Verhältnismäßigkeitserwägungen jenseits der gesetzli-

chen Bestimmungen lässt das Verbraucherinformationsgesetz keinen Raum.

Kein DS-GVO-Auskunftsanspruch bei unzumutbarem Aufwand (hier: Sichtung von ca. 10.000 E-Mails) (Ls)

(Landgericht Heidelberg, Urteil vom 6. Februar 2020 – 4 O 6/19 –)

1. Für Verantwortliche, die eine große Menge von Informationen über die betroffene Person verarbeiten, sieht Erwägungsgrund 63 zunächst eine Erleichterung bei einem (pauschalen) Auskunftersuchen vor. So darf der Verantwortliche vor Auskunftserteilung von der betroffenen Person eine Präzisierung des Auskunftsbegehrens verlangen.
2. Stellt die betroffene Person nicht klar, an welchen Informationen bzw. welchen Verarbeitungsvorgängen sie interessiert ist, kann dem uneingeschränkt geltend gemachte Auskunftsanspruch ggf. entgegenstehen, dass der damit verbundene Aufwand unverhältnismäßig ist (hier: Sichtung und Schwärzung von ca. 10.000 E-Mails)

(Nicht amtliche Leitsätze)

Zum Umfang des Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO (Ls)

(Landgericht Landau, Beschluss vom 17. September 2019 – 3 O 389/17 –)

1. Art. 15 DS-GVO statuiert einen umfassenden Auskunftsanspruch.
2. Unter die Vorschrift fallen sämtliche Informationen, die die Identifizierbarkeit einer Person ermöglichen können.
3. Nach diesen Grundsätzen stellen auch ärztliche Unterlagen, Gutachten oder sonstige vergleichbare Mitteilungen anderer Quellen personenbezogene Daten in diesem Sinne dar.

(Nicht amtliche Leitsätze)

Arbeitsunfähigkeitsbescheinigung per WhatsApp ist rechtswidrig

(Landgericht Hamburg, Urteil vom 3. September 2019 – 406 HK O 56/19 –)

1. Ein der ärztlichen Sorgfalt gem. § 25 Hamburger Berufsordnung für Ärzte entsprechendes Attest setzt die zu-

verlässige Feststellung zur Person und zum Krankheitsbild voraus. Die Verifizierung dieser Daten ist ohne direkten Kontakt mit dem Patienten nicht möglich.

2. Eine Ferndiagnose per Whatsapp entspricht nicht der ärztliche Sorgfalt, da der Arzt sich aufgrund der Angaben des Patienten kein verlässliches Bild der Person und des Krankheitsbildes machen kann.
3. Auch die Ferndiagnose per Telefon oder Video-Chat entspricht nicht den geforderten Anforderungen an die ärztliche Sorgfaltspflicht.

Sachverhalt:

Der Kläger ist ein nach § 8 Abs. 3 Nr. 2 UWG klagebefugter Verein, dem u.a. die Ärztekammern Hamburg und Schleswig-Holstein angehören.

Die Beklagte bietet in der aus Anlage K 5 ersichtlichen und vorliegenden streitgegenständlichen Art und Weise die Erteilung von Arbeitsunfähigkeitsbescheinigungen durch einen mit der Beklagten zusammen arbeitenden Arzt für Patienten an, die an einer Erkältung leiden, und wirbt dabei mit den vorstehend zu I. 1. – 6. genannten Angaben.

Der Kläger macht geltend, die in Anlage K 5 beworbene Ausstellung von Arbeitsunfähigkeitsbescheinigungen allein aufgrund einer Ferndiagnose sei aus den in der Klageschrift genannten Gründen unlauter. Insbesondere verstoße diese Vorgehensweise gegen § 9 HWG und bewirke und fördere Verstöße der mit der Beklagten zusammenarbeitenden Ärzte gegen § 7 Abs. 4 und § 25 der Berufsordnung für Ärzte.

Der Kläger beantragt wie erkannt.

Die Beklagte beantragt Klageabweisung.

Die Beklagte macht geltend, die von ihr beworbene Erteilung von Arbeitsunfähigkeitsbescheinigungen sei aus den im Schriftsatz vom 18.06.2019 genannten Gründen nicht zu beanstanden. § 7 Abs. 4 der Berufsordnung sei bereits im April diesen Jahres so abgeändert worden, dass das hier beworbene Verfahren damit vereinbar sei. § 9 HWG werde kurzfristig ebenfalls entsprechend geändert. Außerdem könne der für die Beklagte tätige Arzt im Einzelfall per Telefon oder Video-Chat Rücksprache mit dem Patienten halten und so etwaige Zweifelsfragen klären.

Zur Ergänzung des Vorbringens der Parteien wird auf ihre Schriftsätze nebst Anlagen verwiesen.

Aus den Gründen:

Die zulässige Klage ist begründet.

Die streitige Werbung ist nach §§ 3, 3a UWG unlauter und verpflichtet den Beklagten daher gemäß §§ 8, 12 Abs. 1 Satz 2 UWG zur Unterlassung und Erstattung von Abmahnkosten.

Die hier beworbene Ausstellung von Arbeitsunfähigkeitsbescheinigungen im Wege der Ferndiagnose in der in Anlage K 5 beschriebenen Art und Weise verstößt gegen die ärztliche Sorgfalt. Diesbezüglich bestimmt § 25 der Musterberufsordnung für Ärzte ebenso wie § 25 der Hamburger Berufsordnung für Ärzte, dass Ärzte bei der Ausstellung ärztlicher Gutachten und Zeugnisse mit der notwendigen Sorgfalt zu verfahren und nach bestem Wissen ihre ärztliche Überzeugung auszusprechen haben. Damit ist es jedenfalls nicht zu vereinbaren, über den Einzelfall hinausgehend Arbeitsunfähigkeitsbescheinigungen auch nur bei leichteren Erkrankungen wie Erkältungen regelhaft ohne persönlichen Kontakt zu erteilen. Die nach § 25 der Berufsordnung notwendige Sorgfalt bei der Ausstellung ärztlicher Atteste erfordert grundsätzlich einen unmittelbaren Kontakt zwischen Arzt und Patienten, sei es, dass der Patient die Sprechstunde des

Arztes aufsucht oder dass der Arzt einen Hausbesuch beim Patienten macht. Nur so kann der Arzt sich einen unmittelbaren Eindruck von dem Gesundheitszustand des Patienten verschaffen und diesen erforderlichenfalls näher untersuchen. Ohne diesen persönlichen Kontakt kann der Arzt nicht mit der gebotenen Sorgfalt feststellen, ob der Patient tatsächlich an der von ihm vermuteten oder behaupteten Erkrankung leidet. Dabei kann jedenfalls für den Normalfall auch bei leichteren Erkrankungen für die Ausstellung einer Krankschreibung nicht auf den unmittelbaren persönlichen Kontakt mit den Patienten verzichtet werden, weil die Krankschreibung auch Grundlage für den Anspruch auf Entgeltfortzahlung im Krankheitsfall ist. Ein der ärztlichen Sorgfalt entsprechendes Attest setzt daher zuverlässige Feststellungen sowohl zu der Person des Patienten als auch zu seiner Erkrankung voraus. Beides ist ohne persönlichen Kontakt zum Patienten bei dem hier beworbenen Verfahren in keiner Weise sichergestellt. Im Normalfall wird hier die Arbeitsunfähigkeitsbescheinigung allein nach den Angaben des Patienten zu seiner Person und zu seiner angeblichen Erkrankung ausgestellt. Eine Verifizierung dieser Angaben ist selbst dann nicht möglich, wenn der Arzt Rücksprache mit dem Patienten per Telefon oder Video-Chat hält. Dies ermöglicht weder zuverlässige Feststellungen zur Person des Gesprächspartners noch zu seinem Gesundheitszustand. Insbesondere ist in Zweifelsfällen eine körperliche Untersuchung des Patienten – wie von Beklagtenseite ausdrücklich beworben – nicht möglich. Auch die für die Bescheinigung der Arbeitsunfähigkeit wichtige Schwere der Erkrankung kann ohne unmittelbaren persönlichen Eindruck nicht zuverlässig eingeschätzt werden. Daran ändert es auch nichts, dass auch herkömmliche, mit persönlichem Kontakt zum Patienten ausgestellte Krankschreibungen in einer mehr oder minder großen Zahl von Fällen nicht der ärztlichen Sorgfalt entsprechen. Auch derartige Fälle würden gegen § 25 der Berufsordnung verstoßen und können kein Verfahren rechtfertigen, dass bereits seiner Anlage nach ärztlicher Sorgfalt widerspricht.

Die Beklagte organisiert und bewirkt mit dem hier streitigen Verfahren daher eine fortgesetzte Verletzung der ärztlichen Sorgfalt, was sowohl nach § 3a UWG i.V.m. § 25 der Berufsordnung für Ärzte als auch nach § 3 Abs. 2 UWG unlauter ist. Nach § 3 Abs. 2 UWG sind geschäftliche Handlungen, die sich an Verbraucher richten, unlauter, wenn sie nicht der unternehmerischen Sorgfalt entsprechen und dazu geeignet sind, das wirtschaftliche Verhalten des Verbrauchers wesentlich zu beeinflussen. Die Beklagte verstößt auch ihrerseits gegen die unternehmerische Sorgfalt, in dem sie die Erteilung von Krankschreibungen in einer der ärztlichen Sorgfalt widersprechenden Art und Weise organisiert und bewirkt. Dies ist zu einer wesentlichen Beeinflussung des wirtschaftlichen Verhaltens des Verbrauchers dergestalt geeignet, dass er eine einfachere zu erlangende Krankschreibung bei der Beklagten erwirbt, anstatt einen niedergelassenen Arzt aufzusuchen.

Kündigung infolge unbefugter „Dokumentation“ einer Sicherheitslücke durch einen externen Sicherheitsberater

(Arbeitsgericht Siegburg, Urteil vom 15. Januar 2020 – 3 Ca 1793/19 –)

Die Offenbarung einer Sicherheitslücke der Datenverarbeitungen eines Kunden seines Arbeitgebers, bei dem der Beschäftigte als Berater eingesetzt ist, kann von die-

sem nicht durch den unbefugten Zugriff auf Bankdaten der Geschäftsführer des Kunden „dokumentiert“ werden.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Parteien streiten über die Wirksamkeit einer außerordentlichen sowie einer hilfsweise erklärten ordentlichen Kündigung der Beklagten. Der schwerbehinderte Kläger ist seit dem 01.07.2011 bei der Beklagten bzw. deren Rechtsvorgängerin als SAP-Berater tätig.

Nachdem der Kläger bereits am 28.07.2019 seinem Vorgesetzten von seiner Verhaftung wegen des Verdachts der Erpressung eines Kunden der Beklagten berichtet hatte, wobei dieser Sachverhalt nicht der streitgegenständlichen Kündigung zu Grunde liegt, räumte er am 29.07.2019 gegenüber seinem Vorgesetzten in einem weiteren Telefonat ein, dass er vom Rechner eines Spielcasinos aus Kopfschmerztabletten für zwei Vorstandsmitglieder der Kundin der Beklagten, für die er für die Beklagte tätig war, bestellt hatte, wobei er zwecks Zahlung per Lastschrift auf zuvor von einem verschlüsselten Rechner der Kundin auf einen privaten Memory-Stick heruntergeladene Namen, Anschriften und Bankverbindungsdaten von Kunden der Kundin zurückgriff. Tatsächlich hatte sich dies zuvor so ereignet. Im Rahmen der Bestellung ließ der Kläger nach eigenen Angaben den Vorständen der Kundin der Beklagten die Anmerkung zukommen, dass sie aufgrund der Bestellung sehen könnten, wie einfach Datenmissbrauch sei, was bei ihnen zu Kopfschmerzen führen müsste, wobei die bestellten Kopfschmerztabletten durchaus helfen könnten. Die Beklagte hatte er zuvor nicht über Sicherheitslücken bei der Kundin informiert.

Noch am gleichen Tag wurde der kündigungsberechtigte Geschäftsführer der Beklagten hierüber informiert. Die Beklagte beantragte daraufhin mit Schreiben vom 09.08.2019 die Zustimmung zur außerordentlichen, hilfsweise ordentlichen Kündigung des Klägers beim Integrationsamt, wobei der Kläger den Sachverhalt im Rahmen dieses Verfahrens einräumte. Das Integrationsamt ließ die bis zum 23.08.2019 laufende Entscheidungsfrist zur außerordentlichen Kündigung verstreichen, teilte dies der Beklagten mit Schreiben vom 26.08.2019 mit und stimmte der ordentlichen Kündigung unter dem 27.08.2019, der Beklagten am 29.08.2019 zugegangen, zu. Die Beklagte kündigte das Arbeitsverhältnis mit dem Kläger zunächst mit Schreiben vom 26.08.2019, dem Kläger am gleichen Tag zugegangen, fristlos und sodann mit Schreiben vom 30.08.2019 hilfsweise ordentlich zum 30.11.2019. Hiergegen wendet sich der Kläger mit seiner am 09.09.2019 erhobenen Klage.

Er behauptet, er habe bei der Kundin datenschutzrelevante Sicherheitslücken entdeckt, die sein Handeln erst möglich gemacht hätten und auf die er die Kunden der Beklagten zuvor mehrfach vergeblich aufmerksam gemacht habe, ohne dass diese reagiert habe. Eine Verknüpfung von Datensätzen sei für sein Vorgehen nicht erforderlich gewesen, da sich Name, Adresse und Bankdaten der Kunden der Kundin in dem gleichen Datensatz befunden hätten. Er habe im Sinne der Allgemeinheit und der Kundin datenschutzrechtliche Verstöße verhindern wollen. Er meint, sein Vorgehen sei gerechtfertigt und die effektivste Handlungsoption gewesen, jedenfalls aber weniger einschneidend als der Gang an die Öffentlichkeit. Vor einer Kündigung sei zunächst eine Abmahnung auszusprechen und zudem in der Kündigungsfrist keine Wiederholung zu befürchten gewesen, zumal er seine Handlung selbst offen gelegt habe. Zudem sei der Vortrag der Beklagten unsubstantiiert, da sie nicht erforscht habe, wann er genau was wem gegenüber getan habe.

Aus den Gründen:

Die Klage ist hinsichtlich des Antrags festzustellen, dass das Arbeitsverhältnis fortbesteht, unzulässig, im Übrigen ist sie unbegründet.

II. Das Arbeitsverhältnis zwischen den Parteien ist durch die fristlose Kündigung der Beklagten vom 26.08.2019 mit Ablauf des gleichen Tages aufgelöst worden.

1. Es liegt ein wichtiger Grund im Sinne des § 626 Abs. 1 BGB vor, der es der Beklagten unzumutbar macht, den Kläger bis zum Ablauf der ordentlichen Kündigungsfrist weiter zu beschäftigen. Gemäß § 626 Abs. 1 BGB kann das Arbeitsverhältnis aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, aufgrund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und bei Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses selbst bis zum Ablauf der Kündigungsfrist nicht zugemutet werden kann.

b) Ein wichtiger Grund zur Kündigung kann nicht nur in einer erheblichen Verletzung der vertraglichen Hauptleistungspflichten liegen. Auch die schuldhaftige Verletzung von Nebenpflichten kann ein wichtiger Grund zur außerordentlichen Kündigung sein. Da die ordentliche Kündigung die übliche und grundsätzlich ausreichende Reaktion auf die Verletzung einer Nebenpflicht ist, kommt eine außerordentliche Kündigung nur in Betracht, wenn das Gewicht dieser Pflichtverletzung durch erschwerende Umstände verstärkt wird (BAG, Urteil v. 12.05.2010 – 2 AZR 845/08 – juris, Rn 19).

2. Unter Zugrundelegung dieser Grundsätze liegt ein Pflichtenverstoß des Klägers vor, der an sich geeignet ist, Grund für eine außerordentliche Kündigung zu sein.

b) Durch sein Vorgehen hat der Kläger auch gegen seine Pflicht zur Rücksichtnahme auf die Interessen der Beklagten eklatant verstoßen. Die Beklagte ist im IT-Bereich tätig und setzt den Kläger bei ihren Kundinnen und Kunden dazu ein, IT-Lösungen zu finden bzw. umzusetzen. In der EDV werden oftmals hochsensible persönliche Daten, wie vorliegend Name, Anschrift und Bankverbindung von Kunden, gespeichert, die des Schutzes bedürfen, was die Beklagte im Rahmen ihrer Tätigkeit zu beachten hat. Sie muss das Interesse ihrer Kunden am Datenschutz und deren dabei bestehende Pflichten bei ihrer eigenen Tätigkeit beachten. Ist es aber auch Aufgabe der Beklagten, den Schutz von Daten beim Kunden zu gewährleisten, steht dem das Vorgehen des Klägers diametral entgegen, da dieser die ihm im Rahmen seiner Tätigkeit zugänglich gewordenen hochsensiblen Daten missbraucht hat, indem er für zwei Vorstandsmitglieder einer Kundin der Beklagten unter Nutzung von Name, Anschrift und Bankverbindung Dritter, namentlich Kunden der Kunden der Beklagten, im Lastschriftverfahren Medikamente bestellt hat, und damit offenbar ohne Offenlegung seiner Identität und damit seiner Nichtberechtigung, Zugriff auf Konten Dritter genommen hat. Die kündigungsrechtliche Beurteilung dieses Verhaltens hängt nicht von der strafrechtlichen Bewertung des mitgeteilten Kündigungssachverhalts ab. Entscheidend ist der mit dem Verhalten oder dem Verdacht einhergehende Vertrauensverlust (vgl. BAG, Urteil vom 20.06.2013 – 2 AZR 546/12 –, BAGE 145, 278-295, Rn. 15). Nach eigener Darstellung hat der Kläger für sein Vorgehen eine Sicherheitslücke bei der Kundin der Beklagten ausgenutzt. Die Kundin der Beklagten sah sich damit einem Verhalten des Klägers gegenüber ausgesetzt, vor dem sie naturgemäß geschützt sein wollte. Von Seiten der Beklagten und deren Mitarbeiter durfte sie allenfalls Schutz vor, keinesfalls aber Missbrauch von etwaigen Sicherheitslücken erwarten. Der Kläger hat somit massiv das Vertrauen der Kundin der Beklagten und deren Mitarbeiter gestört und damit die Kundenbeziehung gefährdet, aber nicht nur diese sondern auch die Geschäftsbeziehung zwischen den Kunden der Kundin und der Kundin selbst. Dies musste ihm auch klar sein. Der Kläger hat

also derart massiv seine Rücksichtnahmepflicht gegenüber der Beklagten verletzt, dass an sich ein wichtiger Grund für eine außerordentliche Kündigung anzunehmen ist.

3. Auch unter Berücksichtigung der Umstände des Einzelfalls macht dieses Verhalten des Klägers der Beklagten die Weiterbeschäftigung bis zum Ablauf der Kündigungsfrist nicht zumutbar.

a) Der Kläger hat durch seine Handlungsweise gezeigt, dass er grundlegende und offenkundige Grenzen zulässigen Handelns zu überschreiten bereit ist, was sein Verhalten in der Zukunft unkalkulierbar macht. Zu Gunsten des Klägers kann unterstellt werden, dass die von ihm in seinem Vorbringen nicht näher dargestellte Sicherheitslücke bei der Kundin der Beklagten tatsächlich bestand und es ihm bei seinem Vorgehen ausschließlich um deren Beseitigung ging. Das hierbei von ihm gewählte Mittel steht jedoch offensichtlich außer Verhältnis zu dem von ihm verfolgten Ziel, weil er nicht nur mit Worten auf die Sicherheitslücke aufmerksam gemacht, sondern sie nach eigener Darstellung gerade ausgenutzt hat. Während ein Hinweis auf eine Sicherheitslücke das Vertrauen der Kunden der Beklagten in diese zu verstärken vermag, muss das Vorgehen des Klägers genau das Gegenteil bewirken, wenn die Kundin gewahrt wird, dass ein Mitarbeiter der Beklagten unter Nutzung von hochsensiblen Daten unbefugt in dem Rechtskreis ihrer Kunden herumspioniert. Prekär ist das Vorgehen insbesondere durch den unbefugten Zugriff auf fremde Bankkonten, was für jeden – offenbar außer dem Kläger – erkennbar weder durch den Auftrag der Beklagten bei der Kundin noch die Aufgabenstellung des Klägers abgedeckt sein kann, zumal der Kläger unbeteiligte Dritte durch die unberechtigte Belastung von deren Konten mit einbezieht. Diese Nichtbeachtung jedem einleuchtender Grenzen zulässigen Handelns macht es der Beklagten unzumutbar, den Kläger noch bis zum Ablauf der angesichts der achtjährigen Beschäftigungszeit bis Ende November 2019 laufenden Kündigungsfrist weiter zu beschäftigen.

b) Dabei steht der Kündigung auch nicht entgegen, dass die Beklagte den Kläger nicht abgemahnt hat.

aa) Grundsätzlich gilt bei der Beurteilung der Frage, ob eine Kündigung wirksam ist, das Prognoseprinzip. Zweck einer verhaltensbedingten Kündigung ist nicht eine Sanktion für die begangene Pflichtverletzung, sondern die Vermeidung künftiger Pflichtenverstöße – ggf. selbst bis zum Ablauf der Kündigungsfrist. Die fragliche Pflichtverletzung muss sich deshalb noch für die Zukunft belastend auswirken. Eine entsprechende Prognose ist berechtigt, wenn aus der konkreten Vertragspflichtverletzung und der daraus resultierenden Vertragsstörung geschlossen werden kann, der Arbeitnehmer werde den Arbeitsvertrag auch künftig erneut in gleicher oder ähnlicher Weise verletzen. Das ist häufig ungewiss. Eine Kündigung wegen einer Vertragspflichtverletzung setzt deshalb regelmäßig eine einschlägige Abmahnung voraus. Diese dient der Objektivierung der negativen Prognose. Liegt eine solche Abmahnung vor und verletzt der Arbeitnehmer gleichwohl erneut seine vertraglichen Pflichten, kann regelmäßig davon ausgegangen werden, es werde auch künftig zu weiteren Vertragsstörungen kommen. Außerdem ist in Anwendung des Verhältnismäßigkeitsgrundsatzes die Abmahnung als milderes Mittel einer Kündigung vorzuziehen, wenn schon durch ihren Ausspruch das Ziel, die künftige Einhaltung der Vertragspflichten zu bewirken, erreicht werden kann (BAG, Urteil vom 26.11.2009 – 2 AZR 751/08 – juris, Rn. 10). Allerdings kann eine Abmahnung bei schweren Pflichtverletzungen entbehrlich sein. Bei einer schweren Pflichtverletzung ist nämlich regelmäßig dem Arbeitnehmer die Rechtswidrigkeit seines Handelns ohne weiteres genauso erkennbar, wie der Umstand, dass eine Hinnahe des

Verhaltens durch den Arbeitgeber offensichtlich ausgeschlossen ist (BAG, Urteil vom 23.06.2009 – 2 AZR 283/08 – juris, Rn. 18).

bb) Vorliegend ist eine schwere Pflichtverletzung des Klägers gegeben, die eine Abmahnung entbehrlich macht, da die Beklagte angesichts des „Exzesses“ des Klägers nicht ausschließen konnte, dass dieser weitere, nicht voraussehbare Grenzverletzungen begehen würde. Dies wird auch durch das Verhalten des Klägers im vorliegenden Prozess belegt. Anstatt das Gewicht seiner Pflichtverletzung einzusehen, sieht er sein Vorgehen geradezu als gerechtfertigt, jedenfalls aber als einzig effektiven und verhältnismäßigen Weg zur Erreichung seines Ziels an. Selbst der Ausspruch der Kündigung hat den Kläger mithin nicht zur Einsicht bewegen können. Soweit der Kläger zur Rechtfertigung seiner Handlung die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Whistleblowern heranziehen will, geht dies fehl. Nach dessen Urteil vom 21.07.2011 (28274/08 –, juris) fallen Strafanzeigen von Arbeitnehmern gegen ihren Arbeitgeber mit dem Ziel, Missstände in ihren Unternehmen oder Institutionen offenzulegen (whistleblowing), in den Geltungsbereich des die Meinungsfreiheit schützenden Art. 10 MRK. Vorliegend geht es jedoch nicht darum, dass der Kläger, und sei es auch aus einem an sich nicht zu beanstandenden Motiv, Missstände bei seinem Arbeitgeber oder Dritten öffentlich gemacht oder zur Anzeige gebracht hat, sondern dass er vermeintliche Missstände oder jedenfalls ihm bei seiner Tätigkeit zugänglich gewordene Daten für sein Vorgehen missbraucht hat. Der Kläger hat also überhaupt nicht von der durch Art. 10 MRK geschützten Meinungsfreiheit Gebrauch gemacht, so dass er sich auf die auf diese Vorschrift gestützte Entscheidung des Europäischen Gerichtshofs für Menschenrechte nicht berufen kann.

cc) Daran, dass mithin auch unter Berücksichtigung der Umstände des Einzelfalles ein Grund für eine fristlose Kündigung gegeben ist, ändert schließlich auch nicht der Umstand etwas, dass der Kläger sein Verhalten selbst offenbart hat. Diese Offenbarung ist nämlich offenbar nicht wegen besserer Einsicht erfolgt, sondern im Hinblick auf seine vorherige Verhaftung wegen eines anderen Sachverhaltes, sodass er seine Arbeitgeberin letztendlich lediglich Sachverhalte offenbart hat, von der diese früher oder später ohnehin Kenntnis erlangt hätte.

dd) Schließlich ist der Beklagten auch nicht zumutbar, den Kläger bis zum Ablauf der Kündigungsfrist anderweitig einzusetzen. Einen entsprechenden Arbeitsplatz im Unternehmen der Beklagten, mit dem der eingetretene Vertrauensverlust keine Rolle spielen würde, hat der Kläger nicht benennen können. Die von ihm in der mündlichen Verhandlung benannte Entwicklungsabteilung ist unstreitig bei der Beklagten nicht angesiedelt.

Gesundheitsdaten eines Tieres als personenbezogene Daten des Tierhalters

(Verwaltungsgericht Mainz, Urteil vom 20. Februar 2020 – 1 K 467/19.MZ –)

1. Die für die Forderungsdurchsetzung erforderlichen Daten dürfen von einem Tierarzt an ein Inkassounternehmen auf Grundlage von Art. 6 Abs. 1 Satz 1 lit. b DS-GVO bzw. von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO übermittelt werden. Dabei dürfen jedoch nur diejenigen Daten dem Inkassodienstleister übermittelt werden, die zur Forderungsbeitreibung benötigt werden.

2. Allein aufgrund der abstrakten Möglichkeit, dass aus Informationen über Tierbehandlungsverträge – wie Abrechnungsunterlagen – in besonderen Fällen Rückschlüsse auf die Gesundheit des Tierhalters gezogen werden können, werden diese nicht generell zu Gesundheitsdaten.

Sachverhalt:

Der Kläger wendet sich gegen eine datenschutzrechtliche Verwarnung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz – LfDI –.

Der Kläger ist Tierarzt und schloss mit der Verrechnungsstelle für Tierärzte – VTX – einen Abrechnungsvertrag und eine Vereinbarung zur Auftragsverarbeitung. Danach kann der Kläger seine Abrechnungstätigkeit an den Verein delegieren, ohne dass dafür die ausdrückliche Einwilligung der Tierbesitzer, die ihr Tier bei ihm behandeln gelassen haben, erforderlich ist. Forderungen des Tierarztes gegen seine Patienten bzw. die Tierhalter sollen nach den Bestimmungen des Vertrags auf die VTX übertragen werden, wenn Verzug eingetreten ist und die VTX die Abtretung angenommen hat. Mit der Annahme der Abtretung wird die VTX Forderungsinhaberin. Nach der Präambel des Abrechnungsvertrags soll die VTX vor der Forderungsabtretung eine Auftragsverarbeitung i.S.d. Art. 28 DS-GVO durchführen, die in der Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO näher ausgestaltet ist. Die Daten der Tierhalter werden für Abrechnungszwecke und die etwaige Durchsetzung von Forderungen der VTX übermittelt, bevor diese die Annahme einer Forderungsabtretung erklärt.

Nachdem ein Tierhalter eine Behandlungsrechnung des Klägers vom 5. Juni 2018 über 1.001,03 € nicht fristgemäß bezahlt hatte, stornierte der Kläger seine selbst erstellte Rechnung und übermittelte sie am 3. Juli 2018 an die VTX zur Durchführung des Inkassos. Der Tierhalter hatte für diese Datenübermittlung keine Einwilligung erteilt und reichte eine Beschwerde bei dem LfDI ein, nachdem er von der VTX zur Zahlung aufgefordert worden war.

Nach der Anhörung des Klägers erging mit Bescheid vom 16. April 2019 eine Verwarnung auf Grundlage von Art. 58 Abs. 2 lit. b DS-GVO. Die Verwarnung (Ziffer 1 des Bescheids) wurde damit begründet, dass der Kläger personenbezogene Daten eines Tierhalters an die VTX übermittelt habe, obwohl die datenschutzrechtlichen Voraussetzungen dafür nicht vorgelegen hätten.

Aus den Gründen:

I. Die Klage ist zulässig.

Statthaft ist gemäß § 42 Abs. 1 Var. 1 VwGO die Anfechtungsklage, da es sich bei der angefochtenen Verwarnung um einen – zumindest feststellenden – Verwaltungsakt im Sinne des § 35 Satz 1 Verwaltungsverfahrensgesetz – VwVfG – i.V.m. § 1 Landesverwaltungsverfahrensgesetz – LVwVfG – handelt. Schließlich wird mit der Verwarnung festgestellt, dass der Adressat gegen die Datenschutzgrundverordnung verstoßen hat. Zwar wird durch die Verwarnung keine konkrete, unmittelbare Rechtspflicht ausgelöst. Gleichwohl wird mit der Verwarnung implizit ausgedrückt, dass sich der Adressat künftig datenschutzkonform verhalten soll. Darüber hinaus handelt es sich bei der Verwarnung um eine Abhilfemaßnahme der Datenschutzbehörde, mit der ein – wenn auch regelmäßig eher geringfügiger – Datenschutzverstoß geahndet wird (vgl. Körffer, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, Art. 58, Rn. 18; Selmayr, in: Ehmann/Selmayr, 2. Aufl. 2018, Datenschutz-Grundverordnung, Art. 58, Rn. 20).

Der Kläger ist Adressat eines belastenden Verwaltungsakts (Verwarnung; Ziffer 1 des Bescheids) und damit klagebefugt im Sinne des § 42 Abs. 2 VwGO. Ein Vorverfahren war gemäß § 68

Abs. 1 Satz 2 Nr. 1 VwGO, § 20 Abs. 6 BDSG entbehrlich. Die Monatsfrist des § 74 Abs. 1 Satz 1 VwGO wurde gewahrt. Das Verwaltungsgericht Mainz ist gemäß § 20 Abs. 1 und Abs. 3 Bundesdatenschutzgesetz – BDSG – i.V.m. Art. 78 Abs. 1 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 – örtlich zuständig.

II. Die Klage ist auch begründet. Die in Ziffer 1 des Bescheids vom 16. April 2019 ausgesprochene Verwarnung ist aufzuheben, weil sie rechtswidrig ist und den Kläger in seinen Rechten verletzt (vgl. § 113 Abs. 1 Satz 1 VwGO).

Gemäß Art. 58 Abs. 2 lit. b) DS-GVO kann die Aufsichtsbehörde eine Verwarnung aussprechen, wenn eine datenverarbeitende Stelle gegen die Verordnung verstoßen hat. Die Rechtmäßigkeit einer Datenverarbeitung richtet sich nach Art. 5 ff. DS-GVO.

Der Kläger ist eine datenverarbeitende Stelle, weil er Daten eines Tierhalters an die VTX übermittelt hat. Bei der Datenübermittlung handelt es sich um die Verarbeitung von Daten i.S.v. § 4 Nr. 2 DS-GVO.

Diese Datenverarbeitung erfolgte hier rechtmäßig, sodass kein Verstoß gegen Art. 5 Abs. 1 lit. a) DS-GVO gerügt werden kann. Zwar kann die hier streitgegenständliche Datenverarbeitung nicht als Auftragsdatenverarbeitung im Sinne des Art. 28 DS-GVO angesehen werden (1.). Die Datenverarbeitung erfolgte aber in zulässiger Weise auf Grundlage des Art. 6 DS-GVO (2.). Die gesteigerten Anforderungen, die gemäß Art. 9 DS-GVO an die Verarbeitung besonderer Kategorien personenbezogener Daten gestellt werden, mussten im vorliegenden Fall nicht eingehalten werden (3.).

1. Die Übertragung von Daten des betroffenen Tierhalters von dem Kläger auf die VTX erfolgte vorliegend nicht im Rahmen einer Auftragsdatenverarbeitung gemäß Art. 28 DS-GVO. Die Vorgehensweise, wonach die Übermittlung der Daten vom Tierarzt zur Verrechnungs- und Inkassostelle vor der Forderungsabtretung grundsätzlich als Auftragsverarbeitung zu bewerten wäre, würde nicht nur einen Vertrag zu Lasten Dritter darstellen und eine Umgehung der eigentlich einschlägigen, strengeren Anforderungen der Art. 6 ff. DS-GVO für eine Datenübermittlung an einen nicht weisungsgebundenen Dritten bedeuten, sondern ist vor allem tatbestandlich nicht als Auftragsverarbeitung zu bewerten.

Gegen eine Auftragsverarbeitung und eine Weisungsgebundenheit der VTX spricht zunächst, dass die Abtretung – die nach der Vorstellung des Klägers den Wechsel von der Auftragsverarbeitung zur Datenverarbeitung der VTX als Verantwortliche bewirkt – letztlich auf einer freien Entscheidung der VTX beruht (so auch die Präambel des Abrechnungsvertrags): Die Forderungsabtretung bedarf nach dem Vertrag zwingend der Annahmeerklärung der VTX. Die von dem Kläger beabsichtigten weitreichenden datenschutzrechtlichen Veränderungen, die durch die Abtretung eingeleitet werden sollen, stehen damit nicht unter der Kontrolle des Verantwortlichen.

Zwar hat der Kläger die ihm vorliegenden Daten an die VTX möglicherweise zu einem Zeitpunkt übermittelt, als die Abtretung noch nicht wirksam war. Die VTX hatte jedoch auch nach erfolgter Abtretung noch Zugriff auf die Daten. Sie hat sie erst nach der Abtretung als Forderungsinhaber weiterverarbeitet und ist gegenüber dem betroffenen Tierhalter mit einer eigenen Rechnung über die Behandlungskosten in Erscheinung getreten. Diese Datenverarbeitung erfolgte nicht im Auftrag des Klägers,

weil der Kläger gemäß dem Vertrag seine Forderungen gegenüber dem Tierhalter an die VTX abgetreten hat. Die VTX kann als Zessionarin die Forderung gegenüber dem Tierhalter eigenständig durchsetzen und die ihr vorliegenden Daten selbstständig und weisungsfrei verarbeiten. Weisungsbefugnisse des Klägers bestehen gegenüber der VTX nach erfolgter Abtretung auf Grundlage des Vertrages nicht (so auch Schulz, in: Gola, DS-GVO, 2. Aufl. (2018), Art. 6, Rn. 136; Ziegenhorn/Fokken, ZD 2019, 194).

Sofern die tatbestandlichen Voraussetzungen des Art. 28 DS-GVO nicht erfüllt sind, ist es unerheblich, ob die VTX nach dem mit dem Kläger abgeschlossenen Abrechnungsvertrag im Zeitpunkt der Datenübermittlung als Auftragsverarbeiterin betrachtet werden soll.

2. Die Übermittlung von Daten des Tierhalters durch den Kläger an die VTX war gemäß Art. 6 Abs. 1 Satz 1 lit. b DS-GVO (a) bzw. gemäß Art. 6 Abs. 1 Satz 1 lit. f DS-GVO (b)) rechtmäßig.

a) Die Datenübertragung, die hier im Rahmen einer Abtretung an die TVG als Inkassounternehmen erfolgte, ist gemäß Art. 6 Abs. 1 Satz 1 lit. b DS-GVO zulässig.

Auf dieser Rechtsgrundlage kann eine Datenübertragung unabhängig vom Verhalten des Betroffenen – insbesondere ohne eine Einwilligung i.S.d. Art. 6 Abs. 1 Satz 1 lit. a, Art. 7 DS-GVO – zulässig sein. Schließlich sind die in Art. 6 Abs. 1 DS-GVO enthaltenen Zulässigkeitstatbestände ihrer rechtlichen Funktion nach gleichwertig und gelten nebeneinander, ohne dass von einem Stufenverhältnis ausgegangen werden müsste. Aus der Aufzählung der verschiedenen Zulässigkeitstatbestände kann nicht geschlossen werden, dass es sich bei der Einwilligung nach Art. 6 Abs. 1 Satz 1 lit. a DS-GVO um einen vorrangigen Erlaubnistatbestand handelt und etwa die allgemeine Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO als ultima ratio zu verstehen ist. Die gesetzlichen Erlaubnistatbestände berücksichtigen insofern nicht nur das Datenschutzinteresse der betroffenen Personen, sondern auch die anerkanntswerten Interessen des Verantwortlichen an einer ausnahmsweise zulässigen Datenverarbeitung (vgl. Schulz, in: Gola, DS-GVO, 2. Aufl. (2018), Art. 6, Rn. 10). Art. 6 Abs. 1 Satz 1 lit. b DS-GVO gestattet dem Verantwortlichen eine Datenverarbeitung in den Grenzen des jeweils abgeschlossenen Vertrags; ein weitergehender Schutz über eine Interessenabwägung ist nicht erforderlich, da sich die betroffene Person als Vertragspartei zum Abschluss des Vertrags und den damit verbundenen Rechten und Pflichten entschieden hat (vgl. Schulz, in: Gola, DS-GVO, 2. Aufl. (2018), Art. 6, Rn. 29; Albers/Veit, in: Wolff/Brink, BeckOK Datenschutzrecht, 30. Ed. Stand 1. November 2019, Art. 6, Rn. 29).

Gemäß Art. 6 Abs. 1 Satz 1 lit. b DS-GVO ist eine – grundsätzlich unzulässige – Datenverarbeitung unter anderem dann rechtmäßig (Verbot mit Erlaubnisvorbehalt), wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist. Grundsätzlich können sämtliche Verträge, die eine Datenverarbeitung betreffen, von diesem Erlaubnistatbestand umfasst sein (vgl. Schulz, in: Gola, DS-GVO, 2. Aufl. (2018), Art. 6, Rn. 28).

Der Vertrag, um dessen Erfüllung es geht, muss mit der Person, deren Daten verarbeitet werden, geschlossen worden sein. Nicht erforderlich ist es, dass der Vertragspartner des Betroffenen und der die Daten verarbeitende Verantwortliche personenidentisch sind. Daher sind auf Grundlage von Art. 6 Abs. 1 Satz 1 lit. b DS-GVO auch Datenverarbeitungen durch unbeteiligte Dritte legitimiert, die für die Erfüllung eines Vertrags, deren Partei der Betroffene ist, erforderlich sind (vgl. Albers/Veit, in: Wolff/Brink, BeckOK Datenschutzrecht, 30. Ed. Stand 1. Novem-

ber 2019, Art. 6, Rn. 30). Vorliegend haben der Kläger und der von der Datenverarbeitung betroffene Tierhalter einen Behandlungsvertrag für die Pferde des Tierhalters abgeschlossen.

Eine Datenverarbeitung gemäß Art. 6 Abs. 1 Satz 1 lit. b DS-GVO ist jedoch nur dann zulässig, wenn sie zu Vertragszwecken erforderlich ist. Dies ist in der Regel der Fall, wenn die *essentia negotii* des jeweiligen Vertrags betroffen sind. Dabei werden an die Erforderlichkeit der Datenverarbeitung jedoch keine zu strengen Anforderungen gestellt: Eine Datenverarbeitung ist nicht erst dann zur Erfüllung des Vertrags erforderlich, wenn der Vertrag ohne die Datenverarbeitung gar nicht durchgeführt werden könnte; vielmehr reicht es aus, wenn die Datenverarbeitung objektiv sinnvoll im Hinblick auf den Vertragszweck ist (vgl. Schulz, in: Gola, DS-GVO, 2. Aufl. (2018), Art. 6, Rn. 38; Albers/Veit, in: Wolff/Brink, BeckOK Datenschutzrecht, 30. Ed. Stand 1. November 2019, Art. 6, Rn. 32).

Zu den Hauptleistungspflichten des hier abgeschlossenen Behandlungsvertrags zählten die Pflicht des Klägers zur tierärztlichen Behandlung sowie die Pflicht des Tierhalters das Honorar des Tierarztes zu bezahlen. Dieser Pflicht ist der Tierhalter nicht nachgekommen, er hat den Rechnungsbetrag in Höhe von 1.001,03 € nicht innerhalb der Zahlungsfrist entrichtet. Die Durchsetzung dieser Forderung dient dem Zweck des Behandlungsvertrags. Dabei begegnet es keinen rechtlichen Bedenken, wenn der Forderungsinhaber – hier: der Kläger als Tierarzt – die Forderungen zum Zwecke der Effektivierung des Forderungsmanagements an einen Dritten – hier: die VTX – als Inkassounternehmen abtritt. Die Abtretung als solche bedarf nach den Regelungen des Bürgerlichen Gesetzbuchs – BGB – für ihre Wirksamkeit grundsätzlich keiner Einwilligung des Schuldners, sofern dadurch nicht gegen ein gesetzliches Verbot gemäß § 134 BGB verstoßen wird. Auf die Wirksamkeit der Abtretung kommt es für die Frage, ob eine unzulässige Datenübermittlung stattgefunden hat, jedoch nicht an.

Die für die Forderungsdurchsetzung durch das Inkassounternehmen erforderlichen Daten durften hier übermittelt werden. Schließlich ist die Datenübermittlung notwendiges Mittel zum Zweck: Es geht darum, die fällige Forderung beim Schuldner eintreiben zu können. Ohne die notwendigen Informationen wäre die übertragene Forderung für den Zessionar nutzlos (vgl. Lehmann/Wancke, WM 2019, 613 [615; 618]; Schulz, in: Gola, DS-GVO, 2. Aufl. (2018), Art. 6, Rn. 136; Abel/Djagani, ZD 2017, 114 [117]). Dabei dürfen jedoch nur diejenigen Daten dem Inkassodienstleister übermittelt werden, die zur Forderungsbeitreibung benötigt werden. Dass der Kläger mehr Daten übertragen hat, als für die Erfüllung des Vertrags erforderlich gewesen wären, wurde dem Kläger nicht vorgeworfen und von dem Beklagten nicht behauptet.

Da sich der Vertragszweck durch die Forderungsabtretung nicht geändert hat, ist Art. 6 Abs. 4 DS-GVO nicht einschlägig (vgl. Schulz, in: Gola, DS-GVO, 2. Aufl. (2018), Art. 6, Rn. 136; Abel/Djagani, ZD 2017, 114 [117]). Schließlich soll auch nach der Abtretung die vertragliche Hauptleistungspflicht des Tierhalters durchgesetzt und nicht etwa neue Ziele, wie zum Beispiel Werbezwecke, verfolgt werden.

b) Jedenfalls ist die Datenübermittlung hier (auch) gemäß Art. 6 Abs. 1 Satz 1 lit. f DS-GVO rechtmäßig. Danach ist die Verarbeitung von Daten zulässig, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Auf

dieser Grundlage müssen die berechtigten Interessen des Verantwortlichen mit den Interessen der betroffenen Person miteinander abgewogen werden.

Die Interessenabwägung fällt hier zugunsten des Klägers aus. Die Übermittlung der Daten an die VTX war hier zur Wahrung seiner berechtigten Interessen erforderlich. Der Kläger hat als Tierarzt ein berechtigtes – rechtliches und wirtschaftliches – Interesse daran, dass seine tierärztlichen Leistungen von den jeweiligen Tierhaltern vergütet werden. Sofern ein Tierhalter seiner vertraglichen Leistungspflicht nicht nachkommt, hat der Tierarzt darüber hinaus ein berechtigtes Interesse daran, seine vertragliche Forderung auch unter Zuhilfenahme Dritter durchzusetzen. Dies stellt eine übliche Reaktion des Verantwortlichen auf ein vertragswidriges Verhalten eines Dritten dar (vgl. Wolff, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 668).

Überwiegende Interessen des von der Datenübermittlung betroffenen Tierhalters stehen diesem Interesse des Tierarztes nicht entgegen: Schließlich hat der Tierhalter durch die Verletzung seiner vertraglichen Zahlungspflicht selbst dazu beigetragen, dass die Datenübermittlung zur Forderungseinziehung erforderlich wurde (vgl. Conrad/Dovas, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil IX, Kapitel 2, Rn. 105; Schulz, in: Gola, DS-GVO, 2. Aufl. (2018), Art. 6, Rn. 136).

3. Ob die Datenübermittlung hier gemäß Art. 9 DS-GVO rechtmäßig ist, kann offenbleiben. Die Kammer geht davon aus, dass es sich bei den hier vom Kläger übermittelten Daten nicht um Gesundheitsdaten i.S.d. § 4 Nr. 15 DS-GVO handelt. Danach sind „Gesundheitsdaten“ solche personenbezogenen 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.

Vorliegend geht es um „Gesundheitsdaten“ der vom Kläger tierärztlich behandelten Tiere. Aus der Honorarrechnung, die der Kläger der VTX zur Forderungseinziehung übermittelt hat, ergeben sich auch Rückschlüsse auf die Gesundheit der Tiere. Dabei handelt es sich jedoch nicht um Daten, die die Gesundheit einer natürlichen Person betreffen, sodass sie auch nicht besonders durch die Regelung in Art. 9 DS-GVO geschützt werden. Dass es sich im hier vorliegenden Fall um Erkrankungen der Tiere gehandelt hat, die auf den Menschen und damit den betroffenen Tierhalter übergehen und seine Gesundheit berühren können, oder Krankheiten betroffen waren, die vom Menschen auf Tiere übertragen werden (sog. „Zoonosen“), haben die Beteiligten nicht vorgetragen. Allein aufgrund der abstrakten Möglichkeit, dass aus Informationen über Tierbehandlungsverträge – wie Abrechnungsunterlagen – in besonderen Fällen Rückschlüsse auf die Gesundheit des Tierhalters gezogen werden können, werden diese noch nicht zu Gesundheitsdaten (vgl. LG Dortmund, Urteil vom 9. Februar 2006 – 4 S 176/05 –, juris, Rn. 16 ff.; a.A. LG Bochum, Urteil vom 25. November 1992 – 10 S 42/92 – beck-online).

Sofern andererseits Informationen über den Schuldner – Tierhalter – übermittelt wurden, weil diese für die Forderungsdurchsetzung relevant sind (bspw. Name und Adresse), handelt es sich nicht um besonders sensible Daten nach Art. 9 DS-GVO.

Im Übrigen wird die Berufung gemäß § 124a Abs. 1 Satz 1 VwGO i.V.m. § 124 Abs. 2 Nr. 3 VwGO zugelassen, weil die Rechtssache nach Auffassung der Kammer grundsätzliche Bedeutung hat. Es gilt insofern die nachfolgend abgedruckte Rechtsmittelbelehrung.



Mitarbeiter schulen via E-Learning

kosteneffizient - flexibel - einfach

TV-Studioqualität

E-LEARNING-KURSE:

- Antidiskriminierung
- Einführung in die IT-Sicherheit
- Einführung in den Datenschutz
- Haftungsrisiken in der Entgeltabrechnung

Jetzt informieren: datakontext.com/eLearning

Berichte, Informationen, Sonstiges

LfD S-H: Plötzlich im Homeoffice – und der Datenschutz?

Aufgrund der Corona-Pandemie sollen alle Menschen ihre direkten Kontakte einschränken. Das bedeutet auch, dass die meisten nun zu Hause bleiben. Wann immer es geht, schicken Unternehmen und Behörden ihre Mitarbeiterinnen und Mitarbeiter ins Homeoffice. Auf was muss man achten, um auch zu Hause die Datenschutzerfordernisse zu erfüllen? Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein, berichtet von zahlreichen Anfragen zum Thema Homeoffice: „Für viele Mitarbeiterinnen und Mitarbeiter heißt es gerade: Ab sofort Homeoffice! Viele Unternehmen und Behörden kannten dies bisher gar nicht oder nur in Ausnahmefällen. Deswegen wird vielerorts gerade improvisiert, um den Betrieb am Laufen zu halten und dabei die Bedürfnisse aller Beschäftigten möglichst gut zu erfüllen.“

Die Unternehmen und Behörden, die bereits über die technische Ausstattung und die organisatorischen Anweisungen für Homeoffice-Arbeitsplätze verfügen, haben meist nur noch geringen Anpassungsbedarf. Für die anderen stellen sich nun aber viele Fragen. An was müssen Mitarbeiterinnen und Mitarbeiter denken, damit ihr Homeoffice nicht zu einem Datenschutzrisiko wird? Aus diesem Grund veröffentlicht Hansens Dienststelle, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), die wichtigsten Regeln und Maßnahmen für das Arbeiten im Homeoffice auf der Webseite:

„Datenschutz: Plötzlich im Homeoffice – was nun?“, <https://www.datenschutz-zentrum.de/uploads/it/uld-plotzlich-homeoffice.pdf>

Hansen betont die Wichtigkeit: „Wer spontan ins Homeoffice geschickt wird, hat oft nicht im Blick, wie sich die personenbezogenen Daten vor unbefugten Zugriffen zu Hause, beim Transport oder bei der Datenübertragung schützen las-

sen. Technische und organisatorische Sicherheitsmaßnahmen sind wichtig für das Arbeiten am Computer, mit Papierdokumenten oder auch beim Telefonieren. Und für den Fall, dass doch einmal eine Datenpanne passiert, müssen alle Beschäftigten wissen, wem sie dies melden. Achtung: Nicht alle Tätigkeiten dürfen im Homeoffice geleistet werden – beispielsweise schließen dies einige Auftragsverarbeitungsverträge aus.“

Die Hilfestellungen des ULD sollen für die nächste Zeit Orientierung geben. Hansen rät dazu, dass diejenigen Unternehmen und Behörden, die noch keine schriftlichen Regeln für das Arbeiten von zu Hause aus erstellt haben, dies nun nachholen.

Die Informationen der Landesbeauftragten für Datenschutz zu Themen der Corona-Pandemie werden unter dem folgenden Link bereitgestellt und regelmäßig aktualisiert: <https://www.datenschutz-zentrum.de/corona/>

BayLfD: Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder erreichen vermehrt Anfragen von Arbeitgebern/Dienstherren, ob und wie personenbezogene Daten von Mitarbeitern sowie Gästen und Besuchern bei im Zusammenhang mit der Corona-Pandemie stehenden Maßnahmen verarbeitet werden können. Dazu einige allgemeine Hinweise:

Werden im Zusammenhang mit der Corona-Pandemie personenbezogene Daten erhoben, werden in den meisten Fällen Bezüge zwischen Personen und deren Gesundheitszustand hergestellt.

Ab diesem Zeitpunkt handelt es sich um Gesundheitsdaten, die nach Art. 9 Datenschutz-Grundverordnung (DS-GVO) besonders geschützt sind.

Auch wenn eine Verarbeitung von Gesundheitsdaten grundsätzlich nur restriktiv möglich ist, können für verschiedene Maßnahmen zur Eindämmung der Corona-Pandemie oder zum Schutz von Mitarbeiterinnen und Mitarbeitern datenschutzkonform Daten erhoben und verwendet werden. Dabei ist der Grundsatz der Verhältnismäßigkeit und der gesetzlichen Grundlage stets zu beachten.

Beispielsweise können die folgenden Maßnahmen zur Eindämmung und Bekämpfung der Corona-Pandemie als datenschutzrechtlich legitimiert betrachtet werden:

- Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Beschäftigten durch den Arbeitgeber oder Dienstherren, um eine Ausbreitung des Virus unter den Beschäftigten bestmöglich zu verhindern oder einzudämmen. Hierzu zählen insbesondere Informationen zu den Fällen:
 - in denen eine Infektion festgestellt wurde oder Kontakt mit einer nachweislich infizierten Person bestanden hat.
 - in denen im relevanten Zeitraum ein Aufenthalt in einem vom Robert-Koch-Institut (RKI) als Risikogebiet eingestuftes Gebiet stattgefunden hat.
- Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Gästen und Besuchern, insbesondere um festzustellen, ob diese
 - selbst infiziert sind oder im Kontakt mit einer nachweislich infizierten Person standen.
 - sich im relevanten Zeitraum in einem vom RKI als Risikogebiet eingestuftes Gebiet aufgehalten haben.
- Die Offenlegung personenbezogener Daten von nachweislich infizierten oder unter Infektionsverdacht stehenden Personen zur Information von

Kontaktpersonen ist demgegenüber nur rechtmäßig, wenn die Kenntnis der Identität für die Vorsorgemaßnahmen der Kontaktpersonen ausnahmsweise erforderlich ist.

Rechtliche Hintergrundinformationen:

Die vorstehenden Maßnahmen lassen sich rechtlich auf Grundlage der DS-GVO und des BDSG (ggf. in Verbindung mit Landesdatenschutz- und weiteren Fachgesetzen) legitimieren. Je nach Maßnahme können die einschlägigen Rechtsgrundlagen dabei leicht variieren. Ungeachtet dessen gelten aber die folgenden allgemeinen Grundsätze: Die Berechtigung zur Verarbeitung personenbezogener Mitarbeiterdaten ergibt sich in diesen Fällen für öffentlich-rechtliche Arbeitgeber grundsätzlich aus Art. 6 Abs. 1 Satz 1 lit. e) DS-GVO und für Arbeitgeber im nicht-öffentlichen Bereich aus § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO jeweils i.V.m. den einschlägigen beamtenrechtlichen sowie tarif-, arbeits- und sozialrechtlichen Regelungen des nationalen Rechts. Soweit Gesundheitsdaten verarbeitet werden, sind zudem auch § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b) DS-GVO einschlägig. Bei Art. 9 Abs. 2 lit. b) DS-GVO umfasst der Begriff "Arbeitsrecht" nach Auffassung der Datenschutzaufsichtsbehörden auch das deutsche Beamtenrecht. Zugunsten des öffentlich-rechtlichen Arbeitgebers könnte zusätzlich Art. 9 Abs. 2 lit. g) DS-GVO herangezogen werden, da die Fürsorgepflicht im Sinne der Gesundheitsvorsorge hier auch einem wichtigen öffentlichen Interesse dient.

Maßnahmen gegenüber Dritten können bei öffentlichen Stellen auf Art. 6 Abs. 1 Satz 1 lit. c) und e) ggf. in Verbindung mit den jeweiligen Landesdatenschutzgesetzen gestützt werden. Im nicht-öffentlichen Bereich kann Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO als Rechtsgrundlage herangezogen werden. Soweit besonders sensible Daten wie Gesundheitsdaten betroffen sind, findet zudem Art. 9 Abs. 2 lit. i) i.V.m. § 22 Abs. 1 Nr. 1 lit. c) BDSG Anwendung.

Die Fürsorgepflicht der Arbeitgeber bzw. der Dienstherrn verpflichtet diese, den Gesundheitsschutz der Gesamtheit ihrer Beschäftigten sicherzustellen. Hierzu zählt nach Ansicht der unabhängigen Datenschutzaufsichtsbehörden auch die angemessene Reak-

tion auf die epidemische bzw. inzwischen pandemische Verbreitung einer meldepflichtigen Krankheit, die insbesondere der Vorsorge und im Fall der Fälle der Nachverfolgbarkeit (also im Grunde nachgelagerte Vorsorge gegenüber den Kontaktpersonen) dient. Diese Maßnahmen müssen dabei natürlich immer auch verhältnismäßig sein. Die Daten müssen vertraulich behandelt und ausschließlich zweckgebunden verwendet werden. Nach Wegfall des jeweiligen Verarbeitungszwecks (regelmäßig also spätestens dem Ende der Pandemie) müssen die erhobenen Daten unverzüglich gelöscht werden.

Eine Einwilligung der von Maßnahmen Betroffenen allein sollte hingegen vorliegend nur als datenschutzrechtliche Verarbeitungsgrundlage in Betracht gezogen werden, wenn die Betroffenen über die Datenverarbeitung informiert sind und freiwillig in die Maßnahme einwilligen können.

Zusätzlich zu den bestehenden Rechtsgrundlagen für die Datenverarbeitung auf Seiten des Arbeitgebers ergeben sich aus dem Beamtenrecht, aus dem Tarifrecht bzw. dem Arbeitsrecht für Beschäftigte verschiedene Nebenpflichten, unter anderem auch Rücksichts-, Verhaltens- und Mitwirkungspflichten gegenüber ihrem Arbeitgeber und Dritten. Vorliegend stellt nach Auffassung der Datenschutzaufsichtsbehörden beispielsweise die Pflicht zur Information des Dienstherrn bzw. des Arbeitgebers über das Vorliegen einer Infektion mit dem Corona-Virus eine solche Nebenpflicht zum Schutz hochrangiger Interessen Dritter dar, aus der unter gewissen Voraussetzungen auch eine Offenlegungsbefugnis gemäß Art. 6 Abs. 1 lit. c) und f) DS-GVO bezüglich personenbezogener Daten der Kontaktpersonen folgt.

Whitepaper zu rechtlichen Risiken bei der Nutzung internationaler Cloudanbieter

Viele Unternehmen in Deutschland erwägen die Nutzung internationaler Cloudanbieter. Neben den großen Playern aus den USA werden sich auch

asiatische Anbieter als Alternativen in diesem Umfeld etablieren. Aus rechtlicher Perspektive wird hier ein „Clash of Cultures“ zu managen sein.

Bei der Auswahl des richtigen Cloudanbieters gilt es rechtliche Fallstricke zu beachten, die weit über die Schlagworte „internationaler Datentransfer“ und „EU-US-Privacy-Shield“ hinausgehen.

Zusammen mit dem Kölner IaaS- und PaaS-Hersteller gridscale hat Heuking Kühn Lüer Wojtek ein Whitepaper zum rechtssicheren Umgang mit internationalen Cloudanbietern herausgegeben. Das praxisnahe Kompendium richtet sich an Business- und IT-Entscheider im Mittelstand. Erstellt wurde der Ratgeber von Dominik Eickemeier und Dr. Lutz M. Keppeler aus dem Kölner Standort von Heuking Kühn Lüer Wojtek.

Das Kompendium gibt einen checklistenartigen Überblick über die wichtigsten Themen, um Managern und IT-Experten in deutschen Unternehmen die Entscheidung über die Auswahl des für sie passenden Cloudanbieters zu erleichtern.

Das Kompendium können Sie hier herunterladen:

<https://gridscale.io/Rechtsrisiken-bei-Hyperscalern><https://gridscale.io/Rechtsrisiken-bei-Hyperscalern/?utm_source=PM_Heuking&utm_medium=referral&utm_campaign=ePaper_Heuking>

Bitkom-Befragung: Der Chief Digital Officer bleibt die Ausnahme

– Nicht einmal jedes fünfte Unternehmen hat einen CDO oder Leiter Digitalisierung –

In den wenigsten deutschen Unternehmen gibt es einen Leiter Digitalisierung oder einen Chief Digital Officer (CDO). Wo diese Position geschaffen wurde, ist sie allerdings ganz oben, d.h. auf Vorstands- bzw. Geschäftsführungsebene oder direkt darunter angesiedelt. Das ist das Ergebnis einer repräsentativen Umfrage unter 603 Unternehmen aller Branchen im Auftrag des Digitalverbands Bitkom. Demnach gibt nicht einmal jedes fünfte Unternehmen (19 Prozent) an, einen Leiter Digitalisierung oder CDO berufen zu

haben. Damit steigt die Zahl gegenüber dem Vorjahr (15 Prozent) zwar leicht, vor allem kleine Unternehmen sind aber weiterhin sehr zurückhaltend. So geben nur 14 Prozent der Unternehmen mit 20 bis 99 Mitarbeiter an, dass sie eine entsprechende Position geschaffen haben. Bei jenen mit 100 bis 499 Mitarbeiter sind es dagegen 36 Prozent, bei 500 bis 1.999 Mitarbeiter 56 Prozent und bei Unternehmen mit 2.000 oder mehr Beschäftigten sogar

70 Prozent. „Unternehmen mit einem Leiter Digitalisierung oder CDO haben die Funktion in 4 von 10 Fällen (43 Prozent) auf Vorstands- bzw. Geschäftsführungsebene angesiedelt. Noch etwas häufiger (50 Prozent) wurde die Rolle auf der Ebene direkt unter Vorstand bzw. Geschäftsführung etabliert. Nur in 5 Prozent der Fälle ist der CDO Teil des mittleren Managements. „Wichtig ist, dass der CDO mit den erforderlichen Ressourcen ausgestattet und die Rückendeckung der Unternehmensleitung

hat. Der CDO muss nicht nur disruptiv denken dürfen, sondern auch handeln können. Es reicht nicht, digitale Konzepte zu entwerfen, man muss sie auch in die Praxis bringen.“

Weitere Ergebnisse der Befragung finden sich hier: www.bitkom.org/Presse/Presseinformation/Deutsche-Unternehmen-geben-sich-eine-Drei-im-Fach-Digitales

(Pressemitteilung vom 14. April 2020)

Literaturhinweise

Louisa Specht-Riemenschneider/Nikola Werry/Susanne Werry (Hrsg.), **Datenrecht in der Digitalisierung**, Beck-Verlag, München 2019, 1008 S., 134,- €

Internet der Dinge, Big Data, Künstliche Intelligenz, Blockchain, Clouds, internationale Datentransfers: Der rechtliche Umgang mit Daten im digitalen Zeitalter zählt zu den facettenreichsten Herausforderungen unserer Generation. Dieses Buch definiert erstmals das neu entstehende "Datenrecht" in seinen wichtigsten Ausprägungen. Es ist erfasst als Praxisbuch die aktuellen neuen Rechtsfragen im Kontext der digitalen, global vernetzten Geschäfts- und Alltagswelt. Dabei geht es um

- Aktuelles Datenschutzrecht im Zukunft-Check – z.B. zum Status und Grenzen von DS-GVO und ePrivacy-VO, dem Umgang mit Virtual Reality, Automatisierung oder im Onlinemarketing
- Herausforderungen datensensibler Praxisbereiche – z.B. zu Vermögensrechten an Daten, Rechtspositionen in EU/USA/China, vertragsrechtlichen Vorgaben für die Weitergabe und Nutzung von Daten, Kartellrecht, Insolvenzrecht

- Neue Haftungsfragen – z.B. mit Blick auf Gesundheitsdaten oder autonomes Fahren
- Kommunikation und Psychologie – z.B. zum Privacy Paradox als Widerspruch zwischen Wahrnehmung (Sorge um Privatsphäre) und Verhalten (sorglose Datenpreisgabe) oder zu innovativer Informationsvisualisierung. Damit umfasst das Buch einen hochaktuellen Querschnitt neuartiger datenbezogene Rechtsfragen und den gelungenen Versuch, sie praktikabel zu lösen.

(Redaktion)

Robert Kreyßing, **Öffentliche Stellen in den Sozialen Medien – Die primären Rechtsfragen in der Praxis**, Deutscher Fachverlag GmbH, Frankfurt/M. 2020, 152 S., 59,90 €

Wie darf bzw. sollte sich eine öffentliche Stelle in den Sozialen Medien verhalten? Welche praktischen Fallstricke gibt es und was muss stets beachtet werden?

Auf diese Fragen gibt die neue Schrift Juristen und Nicht-Juristen praxisorientierte Hilfestellungen und liefert Lösungsansätze. So werden am

Beispiel von Facebook elementare datenschutzrechtliche Vorgaben beleuchtet, die maßgeblich für die Bestimmung der grundsätzlichen Zulässigkeit von Sozialen Medien in der Arbeit von öffentlichen Stellen sind.

Zielgruppen innerhalb von öffentlichen Stellen sind: Social-Media-Redaktionen, Beauftragte für Öffentlichkeitsarbeit, Entscheidungsträgerinnen und -träger oder auch Datenschutzbeauftragte in der öffentlichen Verwaltung.

(Redaktion)

Florian Sackmann, **Datenschutz bei der Digitalisierung der Mobilität**, Nomos-Verlag, Baden-Baden 2020, 211 S., brosch., 54,- €

Die Entwicklung zu einer „Mobilität 4.0“ hat großes Potential. Dem wirtschaftlichen und gesellschaftlichen Mehrwert steht jedoch das steigende Risiko eines „gläsernen Menschen“ gegenüber, dessen tägliche Bewegungen nachvollziehbar werden. Auf dieses Risiko muss das Recht zeitnah zur technischen Entwicklung Antworten geben.

Die Arbeit identifiziert zunächst in einer Realweltanalyse die besonderen Herausforderungen für den Schutz der

Privatsphäre, die sich durch eine datengetriebene Mobilität stellen. Auf der Basis des geltenden Rechts werden Lösungsmöglichkeiten entwickelt und Defizite der geltenden Datenschutzordnung herausgearbeitet.

Daraus wird schließlich der aktuelle legislative Handlungsbedarf ermittelt. Da die Mobilität als Querschnittsphänomen eine Vielzahl von Lebensbereichen betrifft, können die Erkenntnisse auch für andere Teilaspekte der Digitalisierung nutzbar gemacht werden.

(Redaktion)

Rolf Schwartmann/Heinz-Joachim Pabst (Hrsg.), Landesdatenschutzgesetz Nordrhein-Westfalen, Nomos Verlag, Baden-Baden 2020, 1. Aufl., 672 S., 98,- €

Einem Datenschutzgesetz, das nach der europaweit einheitlichen Neuordnung dieses Rechtsgebietes besondere Vorschriften für den Bereich nur eines Bundeslandes enthält, so dass seine Geltung auf 1/16 Bruchteil Deutschlands als eines von 27 Mitgliedsstaaten der Europäischen Union beschränkt ist, sollte – so meint man auf den ersten Blick – nur eingeschränkte Relevanz zukommen. Bei näherer Betrachtung indes wird deutlich, welche hohe Bedeutung gerade diesen Normen zukommt: NRW ist das bevölkerungsreichste Land der Bundesrepublik mit einer riesigen Vielfalt an öffentlichen Stellen, zu denen allein 396 Kommunen zählen. Aufgrund des erheblichen Grades an Abstraktheit und der beträchtlichen – je nach Zählweise 3-stelligen – Anzahl von Öffnungsklauseln der Datenschutzgrundverordnung war das Bedürfnis der Praxis nach Konkretisierung und Ausfüllung der nicht europarechtlich zwingend vorgegebenen Bereiche außerordentlich groß. Doch die landesgesetzlichen Regelungen, die zeitgleich mit der DS-GVO Mitte 2018 wirksam wurden, sind komplex. Mit dem DSGVO NRW wurde neben dem Erlass von Durchführungsbestimmungen zur Datenschutzgrundverordnung auch die sog. JI-Richtlinie in deutsches Recht umgesetzt.

Hier setzt der Handkommentar zum Landesdatenschutzgesetz NRW an. Er verfolgt das Ziel, dem anwendenden

Praktiker einfach und leicht den Sinn der Vorschriften zu erklären, auf die dazu ergangenen Papiere der Aufsichtsbehörden und Akteure im Datenschutzbereich hinzuweisen sowie Literatur und Rechtsprechung – soweit bereits vorhanden – entsprechend einzuordnen. Dies trägt wesentlich dazu bei, dass Rechtssicherheit bei der Gesetzesanwendung einkehren kann. Mit seinem kompakten Format gibt die Kommentierung die von zahlreichen Datenschutzbeauftragten und Juristen in den Rechtsabteilungen und Ämtern herbeigesehnte Hilfe und schließt endlich die Lücke in diesem erläuterungsintensiven Bereich. Das Werk erfüllt damit alle Voraussetzungen, ein unentbehrlicher Begleiter für alle Datenschutzpraktiker des öffentlichen Sektors zu werden.

An frühere Kommentierungen zum DSGVO NRW – die Jahrzehnte alt waren, aus dem Ressortministerium stammten und sich auf ein früheres Recht bezogen – konnte nicht angeknüpft werden. Umso verdienstvoller ist es, dass sich kompetente Hochschullehrer dieser Aufgabe angenommen haben, die dieses Thema seit langem in Ihrem Portfolio haben. Eine kluge arbeitsteilige Konzeption hat es möglich gemacht, sowohl Wissenschaftler als auch ausgewiesene Praktiker als Autoren zu gewinnen. So ist eine umfassende und vertiefende Erläuterung entstanden, die den gesamten Kontext hilfreich und umfassend erläutert. Vor jeder Vorschrift wird in einer Kurzübersicht das Verhältnis der kommentierten Norm zu DS-GVO und BDSG synoptisch dargestellt, was den systematischen Zusammenhang deutlich macht. Hinzu kommt jeweils ein Hinweis auf die bisherige Gesetzeslage, der sofort klarstellt, ob und inwiefern sich eine Neuerung ergeben hat. Den Erläuterungen ist jeweils eine Gliederung vorangestellt, die den Leser in aller Kürze zu der gesuchten Information führt. Die zu einer Bemerkung gehörende Fundstelle ist übersichtlich in einer Fußnote auf derselben Seite abgelegt, um den Sinnzusammenhang des Textflusses nicht zu stören. Die Nummerierung der Fußnoten beginnt bei jeder kommentierten Norm neu von vorn. Die Zitierge nauigkeit wird durch Randnummern erleichtert. Die verwendete Literatur wird der Kommentierung der Norm vorangestellt. So sind formal alle

Voraussetzungen erfüllt, die eine moderne, den Nutzer zuverlässig unterstützende Kommentierung heute erfüllen muss.

Inhaltlich kommt das Werk zu einem frühen Zeitpunkt, so dass die Hinweise, die es geben kann, sich in überschaubarem Rahmen halten. Gleichwohl ist nahezu sämtliches vorhandene aktuelle Material verarbeitet. Divergierende Auffassungen in der Auslegung von Normen sind in der bisherigen Literatur eher selten, weshalb eine Stellungnahme zu Meinungsstreitigkeiten nicht erforderlich ist. Der Umgang mit unbestimmten Rechtsbegriffen, der gerade bei Datenschutzpraktikern ohne spezifisch juristische Ausbildung oft Fragen aufwirft, könnte in einer Folgeauflage noch intensiviert werden. Gerade so schwierige Vorschriften wie beispielsweise diejenige zur Videoüberwachung (§ 20 DSGVO NRW), die zuletzt noch im Gesetzgebungsverfahren eine Änderung erfahren hat und von Parallelnormen in anderen Landesgesetzen abweicht, ist in der Fallsubsumtion nicht immer einfach; hier wünscht sich der Praktiker verstärkt eine Hilfe des Kommentators. Systematisch Fragen, die sich Anwendern zur Konzeption von Normenkatalogen stellen können (Z.B. Datengeheimnis in Teil 3 (§ 41), nicht jedoch in Teil 2), können ergänzt werden, wenn die Praxis ein Bedürfnis dazu entwickelt.

Bei einer Gesamtbewertung darf mit Lob nicht gespart werden: Das Werk ist eine gelungene, sehr umfassende und gleichwohl noch handlich gebliebene, optisch ansprechende Hilfe, die absolut jedem Praktiker, der in NRW mit öffentlichem Datenschutzrecht befasst ist, unentbehrlich werden wird. Darüber hinaus wird sie zweifellos in der Datenschutzwissenschaft ihren Platz finden und im Kreise von Kommentierungen anderer Landesdatenschutzgesetze namhaft hervortreten. Eine hilfreiche Ergänzung bildet das Buch allen Juristen in Rechtsberatung, Wirtschaft und Verwaltung, die in ihrer täglichen Arbeit datenschutzrechtliche Fragen lösen müssen. Der Kommentator weist insofern wesentliche Alleinstellungsmerkmale auf und ist ohne jede Einschränkung zu empfehlen.

*(Dr. Martin Zilkens
Mitglied des Vorstandes der Gesellschaft
für Datenschutz und Datensicherheit e.V.)*

Neuerscheinungen

Aufsätze

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

Düwell, Franz-Josef, Rechtsfragen zur Arbeitsunfähigkeit bei COVID-19, BB 2020, S. 891

Die Coronavirus SARS-CoV-2-Pandemie hat zwar nicht die bestehenden arbeits- und sozialrechtlichen Bestimmungen außer Kraft gesetzt. Das trifft auch für das Recht der krankheitsbedingten Arbeitsunfähigkeit zu. Jedoch treten bei der Corona-Krankheit neue Rechtsfragen zur Erhebung von Krankheitsdaten auf.

Grambow, Tobias, Kein Initiativrecht des Betriebsrats zur Abberufung der Fachkraft für Arbeitssicherheit, DB 2010, S. 511

Der Beitrag bespricht LAG Berlin-Brandenburg, Beschluss vom 05.11.2019 – 7 TaBV 1728/19 – wonach der Arbeitgeber gem. § 9 Abs. 3 Satz 1 ASiG bestellte Fachkräfte für Arbeitssicherheit und Betriebsärzte mit Zustimmung des Betriebsrats bestellt; entsprechendes gilt für die Abberufung. Ein Initiativrecht des Betriebsrats besteht nicht.

Härtling, Niko, Externe Lohnbuchhaltung: ein Fall der gemeinsamen Verantwortlichkeit i.S.d. Art. 26 DS-GVO, DB 2020, S. 490

Viele Unternehmen beauftragen externe Steuerberater oder Lohnbüros mit der Erstellung der Lohn- und Gehaltsabrechnung. Seit langem umstritten ist die Frage, ob dies als Auftragsverarbeitung gem. Art. 28 DS-GVO zu qualifizieren ist. Während der DStV und die BStBK zumindest mit Blick auf Steuerberater eine Auftragsverarbeitung ablehnen, sehen dies einzelne Landesdatenschutzbehörden anders. Der Gesetzgeber hat im Jahressteuergesetz 2019 nun § 11 StBerG zur Verarbeitung personenbezogener Daten neu gefasst. Ob und inwieweit die Neuregelung die Streitfrage löst und welche datenschutzrechtlichen Anforderungen beim Outsourcing der Lohn- und Gehaltsabrechnung zu beachten sind, erörtert der Beitrag.

Krois, Christopher, Maßnahmen zur Sicherung der Funktionsfähigkeit der Betriebsverfassung während der Covid-19-Pandemie, DB 2020, S. 674

Die Covid-19-Pandemie stellt auch die Betriebspartner vor nie gekannte Herausforderungen. Der Beitrag zeigt auf, vor welchen Aufgaben die Betriebspartner aktuell stehen und wie sie diese mit dem vorhandenen gesetzlichen Instrumentarium bestmöglich meistern können.

Krusche, Jan, Kumulation von Rechtsgrundlagen zur Datenverarbeitung, ZD 2020, S. 232

Der Beitrag geht noch einmal der Frage nach, ob eine gesetzlich zulässige Datenverarbeitung, die auch noch durch eine Einwilligung abgesichert ist, nach Rücknahme der Einwilligung gleichwohl fortgesetzt werden darf und befürwortet dies.

Roßnagel, Alexander, Evaluation der Datenschutz-Grundverordnung, DuD 2020, S. 287

Art. 97 Abs. 1 DS-GVO gibt der Kommission den Auftrag, bis zum 25.05.2020 eine Bewertung der DS-GVO und ggf. als notwendig erkannte Änderungsvorschläge vorzulegen. Der Autor gibt hierzu Anregungen.

Schrief, Dorothee/Potthoff, Tobias S., Zusammenarbeit von Datenschutz und weiteren Kontrollfunktionen im Unternehmen, ZD 2020, S. 229

Für große Unternehmen bietet es sich an, dass die ihnen gesetzlich oder auch sich freiwillig auferlegten Kontrollfunktionen bei dem Datenschutz, der Datensicherheit, der Compliance oder Revision in Zusammenarbeiten (combined assurances) wahrgenommen werden, wobei jedoch Personalunionen häufig an Interessenkollisionen scheitern werden.

Schulz, Sebastian, Die Evaluation der DS-GVO, DuD 2020, S. 302

Heft 5/20 der DuD widmet sich in mehreren Beiträgen mit der Notwendigkeit der DS-GVO und den hierbei sich anbietenden Aspekten, wobei Schulz sich mit wünschenswerten Erleichterungen der praktischen Umsetzung der Verordnung befasst.

Stähler, Thomas, Sonderkündigungsschutz des betrieblichen Beauftragten für den Datenschutz, DB 2010, S. 680

Wann endet der Sonderkündigungsschutz des betrieblichen Datenschutzbeauftragten? Wann beginnt der nachwirkende Sonderkündigungsschutz? Hiermit setzt sich das BAG zwar noch unter der alten Gesetzeslage auseinander, doch gelten die Feststellungen in gleicher Weise bei Zugrundelegung neuen Rechts, d.h. nach DS-GVO i.V.m dem BDSG in der jetzt geltenden Fassung.

Straßmeyer, Karl, Die Transparenzvorgaben der DS-GVO für algorithmische Verarbeitungen, K&R 2020, S. 176

Personenbezogene Daten werden zunehmend mit immer komplexeren technischen Systemen verarbeitet, wie beispielsweise künstlichen neuronalen Netzen. Dies erschwert die Einhaltung von Transparenzanforderungen der DS-GVO fortlaufend. Als Konsequenz droht der zurzeit praktizierte Darstellungsansatz zu versagen. Nachzuvollziehen, was mit Daten „über einen“ geschieht, ist indes eines der Kernelemente von Transparenz.



KI erobert Toiletten

Corona Tracking-Apps sollen die Pandemie bekämpfen. Smarte Technik wird aber auch unabhängig davon zur Gesundheitsvorsorge erprobt. In den USA haben Forscher an der Stanford-Universität eine Toilette entwickelt, die Fäkalien medizinisch analysiert und ihre Benutzer erkennen soll. Mittels Kameras, Druck- und Bewegungssensoren soll man Prostata-Krebs oder Nierenkrankheiten diagnostizieren können. Ausgewertet werden Durchflussrate und Druck des Urinstahls, ebenso wie dessen molekulare Eigenschaften aber auch die Konsistenz des Stuhls. Das smarte Klo soll bis zu 10 Biomarker messen können. Die Ge-

sundheitsdaten werden dann automatisiert zum Zugriff für Mediziner in einer Cloud gespeichert. Wenn mehrere Personen die smarte Toilette medizinisch sinnvoll benutzen sollen, müssen diese voneinander unterschieden werden können. Dazu nimmt der Abspülknopf einen Fingerabdruck vom jeweiligen Benutzer ab. Aber versagt die Technik, wenn die Spülung von jemand anderem gedrückt wird, etwa weil ein anderer Nutzer nicht abgezogen hat? Dieses Problem umgeht man über eine Kamera, die anstelle eines Iris-Scans eine Art Scan der Analregion vornimmt. Das ist möglich, denn Studien ergaben deren Einzigartigkeit.

Um den Datenschutz zu wahren, werden diese Bilder aber nicht gespeichert und verlassen das Gerät nicht. Sie dienen allein der Authentifizierung der Nutzer. Gut, dass der Datenschutz gewahrt ist.

<https://www.nature.com/articles/s41551-020-0534-9>



Ab sofort für jeden Praktiker unentbehrlich



Landesdatenschutzgesetz Nordrhein-Westfalen

Handkommentar

Herausgegeben von Prof. Dr. Rolf Schwartmann
und Prof. Dr. Heinz-Joachim Pabst
2020, 672 S., geb., 98,- €
ISBN 978-3-8487-6308-5

Das nordrhein-westfälische Landesdatenschutzgesetz ist wesentlich geprägt von der DS-GVO und der Umsetzung der JI-RL. Die Abweichungen zum bisherigen LDSG sind erheblich, vieles ist umstritten.

Der neue Kommentar erleichtert das Verständnis und schafft Struktur, indem er

- die parallelen Vorschriften der DS-GVO und des BDSG stets berücksichtigt
- die landesrechtliche Umsetzung der JI-RL, auch in ihren Parallelen zur DS-GVO, aufgreift
- die Unterschiede zwischen neuem und altem LDSG deutlich macht, und
- die Spielräume herausarbeitet, die die DS-GVO und die JI-RL den operativen Landesvorschriften lässt.

Für die Anwendungspraxis sind konkrete Beispiele aus der Landesverwaltung einbezogen.

Landesdatenschutzgesetz Rheinland-Pfalz

Handkommentar

Herausgegeben von Prof. Dr. Dieter Kugelmann
2020, 608 S., geb., 98,- €
ISBN 978-3-8487-5428-1

Das neue rheinland-pfälzische Landesdatenschutzgesetz wirft viele praktische Anwendungsfragen auf.

Der Handkommentar ermöglicht eine rechtssichere Handhabung der Vorschriften. Schwerpunkte liegen auf

- den Unterschieden zwischen neuem und altem LDSG
- den Spielräumen, die die DS-GVO den operativen Landesvorschriften lässt
- der Auslegung der besonderen Regelungen des LDSG.

Verständlich in der Darstellung:

- paragrafengenaue Gegenüberstellung LDSG neu/alt
- durchgängige Quervergleiche DS-GVO, Bundes- wie Landes-DSG
- europarechtsorientierte Gesamtdarstellung der geltenden Regeln
- typische Querbezüge zu Fachgesetzen des Landes und auch den LDSG anderer Bundesländer.

Bestellen Sie im Buchhandel oder
versandkostenfrei online unter [nomos-shop.de](https://www.nomos-shop.de)

Alle Preise inkl. Mehrwertsteuer



Nomos

Otto Schmidt online

NEU

Beratermodul
Otto Schmidt
IT-Recht



Umfassend, hochaktuell, hilfreich – das neue Beratermodul IT-Recht. Alles relevante zum IT-Recht in Ihrer Online-Datenbank.

- Alle Ausgaben der Zeitschriften Computer und Recht (CR) und IT-Rechtsberater (ITRB)
- Dreimal jährlich Updates von *Redeker* Handbuch der IT-Verträge
- Bewährte Handbücher wie Härtling Internetrecht und *Schneider* Handbuch EDV-Recht
- Volltexte zu Gesetzen und Entscheidungen tagesaktuell
- Inklusive Selbststudium mit Zertifikat nach § 15 FAO

Nur 49,- € monatlich für 3 Nutzer.

Jetzt 4 Wochen gratis nutzen!

www.otto-schmidt.de/bmitr

ottoschmidt