

Zeitschrift für
Datenschutz-,
Informations- und
Kommunikationsrecht

RDV

6/2021

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

GOLA, Gilt das Fernmeldegeheimnis am Arbeitsplatz?
– Anwendung des neuen TTDSG im Beschäftigungsverhältnis

HELLMICH/ÉLES, DS-GVO Bußgelder in der Praxis:
Wer muss den Rückgriff fürchten?

CONRAD/SEITER, Zur inhaltlichen Ausgestaltung der
Auftragsverarbeitung nach Art. 28 DS-GVO – Teil 2

Kurzbeiträge

CLAUS/REIF, Praxisfälle zum Datenschutzrecht XIII:
Der Verlust eines USB-Sticks

GOLA, Aus den aktuellen Berichten und Informationen der
Aufsichtsbehörden (57): LDI NRW. 26. Bericht 2021 LDI
S. 122: Betriebliche DSB und Kurzarbeit

GMEINER, Nochmals: Zur Statthaftigkeit der Anfechtungsklage
im kirchengerichtlichen Datenschutzverfahren

Rechtsprechung Aus dem Inhalt

EUGH, Grenzen einer nationale Regelung, die den Zugang
der Öffentlichkeit zu personenbezogenen Daten über
Strafpunkte für Verkehrsverstöße vorsieht

NOWAK/GARIR, Besprechung der BGH-Entscheidung vom 15.06.2021,
VI ZR 576/19 zum Umfang des Auskunftsanspruchs
nach Art. 15 Abs 1 DS-GVO

BAG, Erschütterung des Beweiswerts einer Arbeitsunfähigkeits-
bescheinigung (Ls)

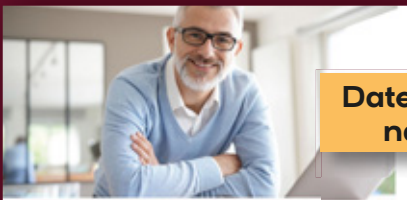
BAG, Keine namentliche Benennung der Mitglieder einer Gewerkschaft
bei der gerichtlichen Geltendmachung von Ansprüchen

37. Jahrgang
Dezember 2021
Seiten 303–356



Gesellschaft für Datenschutz
und Datensicherheit e.V.

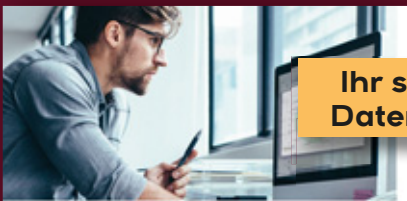

DATAKONTEXT
www.rdv-online.de



Datenschutzorganisationen prüfen und bewerten nach der Systematik der Aufsichtsbehörden



Datenschutzorganisationen prüfen und beurteilen mit begrenztem Zeitaufwand



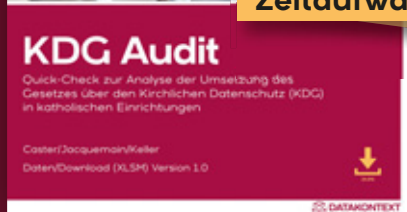
Ihr ständiger Begleiter im Datenschutz-Management



Ihre DS-GVO Umsetzung smart auditiert und visualisiert ab 249 €.



Kirchliche Stellen mit begrenztem Zeitaufwand zum Datenschutz auditieren



Wie DS-GVO-konform arbeitet Ihr Unternehmen?

Machen Sie den Test mit unseren Excel-Tools!

Bestellen Sie direkt unter: datakontext.com

Inhaltsverzeichnis

Editorial	303		
Veranstaltungen	304		
Aufsätze			
Prof. Peter GOLA Gilt das Fernmeldegeheimnis am Arbeitsplatz? – Anwendung des neuen TTDSG im Beschäftigungsverhältnis	305	Zum Auskunftsanspruch bei fehlender Datenspeicherung (OLG Dresden, Urteil vom 31.08.2021)	344
Dr. Stefanie HELLMICH/Kata ÉLES DS-GVO Bußgelder in der Praxis: Wer muss den Rückgriff fürchten?	308	Arbeitgeber darf Rückkehr aus Homeoffice anordnen (Ls) (LAG München, Urteil vom 26.08.2021)	347
Conrad Sebastian CONRAD/Stefan R. SEITER Zur inhaltlichen Ausgestaltung der Auftragsverarbeitung nach Art. 28 DS-GVO – Teil 2	316	Kündigung wegen Verwendung einer gefälschten Entgelt- abrechnungen bei Kreditbeantragung (Ls) (LAG Hamm, Urteil vom 19.08.2021)	347
Kurzbeiträge		Initiativrecht des Betriebsrats bei Einführung einer elektronischen Zeiterfassung (LAG Hamm, Beschluss vom 27.07.2021)	347
Miriam CLAUS, LL.M./RAIN Yvette REIF, LL.M. Praxisfälle zum Datenschutzrecht XIII: Der Verlust eines USB-Sticks	325	Äußerungen im WhatsApp-Chat als Kündigungsgrund (Ls) (LAG Berlin-Brandenburg, Urteil vom 19.07.2021)	349
Prof. Peter GOLA Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (57): LDI NRW. 26. Bericht 2021 LDI S. 122: Betriebliche DSB und Kurzarbeit	328	Kein Anspruch auf Bedauern des Ausscheidens oder (gute) Wünsche für die Zukunft im Arbeitszeugnis (LAG München, Urteil vom 15.07.2021)	349
Robert GMEINER Nochmals: Zur Statthaftigkeit der Anfechtungsklage im kirchengerichtlichen Datenschutzverfahren	329	Keine Ansprüche aus der DS-GVO bei Sicherheitsakten (Ls) (OVG Münster, Beschluss vom 28.07.2021)	349
Rechtsprechung		Zur Abtretung des Anspruchs aus Art. 82 DS-GVO wegen USB-Stick-Verlust (n. rk.) (LG Essen, Urteil vom 23.09.2021)	349
Grenzen einer nationale Regelung, die den Zugang der Öffentlichkeit zu personenbezogenen Daten über Strafpunkte für Verkehrsverstöße vorsieht (EuGH, Urteil vom 22.06.2021)	332	Berichte, Informationen, Sonstiges	
Besprechung der BGH-Entscheidung vom 15.06.2021, VI ZR 576/19 zum Umfang des Auskunftsanspruchs nach Art. 15 Abs 1 DS-GVO (Entscheidung veröffentlicht in RDV 5/21, 272 und RDV 4/21, 224) (Jaroslaw Norbert Nowak, LL.M./Nadine Garir)	340	BSI-Lagebericht der IT-Sicherheit in Deutschland 2021 – Bitkom – Stellungnahme	353
Erschütterung des Beweiswerts einer Arbeitsunfähigkeits- bescheinigung (Ls) (BAG, Urteil vom 08.09.2021)	344	Notwendigkeit voller Cloud-Kontrolle	353
Keine namentliche Benennung der Mitglieder einer Gewerkschaft bei der gerichtlichen Geltendmachung von Ansprüchen (BAG, Urteil vom 29.04.2021)	344	Literaturhinweise	
		<i>Buchbesprechungen</i>	
		<i>Kosmider, Thomas</i> , Die Verantwortlichkeit im Datenschutz – Die Zuordnung zum Verantwortlichen und deren Bedeutung für Rechtfertigung, Geldbußen und Schadensersatz (WEIB)	354
		<i>Steinbach, Kathrin</i> , Regulierung algorithmenbasierter Entscheidungen – Grundrechtliche Argumentation im Kontext von Artikel 22 DSGVO (REDAKTION)	354
		<i>Walker, Matthias</i> , Die Kosten kostenloser Dienste – Personenbezogene Daten als neues Zahlungsmittel Internetrecht und Digitale Gesellschaft (IDG) (REDAKTION)	354
		<i>Neuerscheinungen</i>	
		Aufsätze	355
		Nachgefasst	356

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

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

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

in Kooperation mit der

Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

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

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

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

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

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

Prof. Dr. Karl LINNENKOHL, Universität Kassel

Prof. Dr. Boris P. PAAL, M. Jur. (Oxford), Universität Leipzig

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 6/2021

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 € 155,-

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

HRB 337678

Satz

alka mediengestaltung gmbh

Willmuthstraße 30, 53332 Bornheim-Secktem

Druck

Grafisches Centrum Cuno GmbH & Co. KG

Gewerbering West 27, 39240 Calbe (Saale)

Anzeigenverwaltung

DATAKONTEXT GmbH, Frechen

Wolfgang Scharf

Telefon: (0 22 34) 9 89 49-60

wolfgang.scharf@datakontext.com

www.datakontext.com

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
37. Jahrgang 2021 Heft 6
Seiten 303-356

RDV

Recht der Datenverarbeitung

37. Jahrgang · Dezember 2021 · Seiten 303–356

Editorial

Koalitionsvertrag mit realistischen Ankündigungen?

Im Koalitionsvertrag werden SPD, Bündnis 90/Die Grünen und FDP Regelungen zum Beschäftigtendatenschutz zur Rechtsklarheit für Arbeitgeber und Beschäftigte angekündigt. Wieder einmal. Eine solche Ankündigung gab schon in den Koalitionsvereinbarungen seit den 80er Jahren. Diese wurden jedoch nie umgesetzt. Das BAG hat in seiner unter betrieblichen Datenschützern legendären Entscheidung vom 11.11.1997 auf die Notwendigkeit eines Beschäftigtendatenschutzgesetzes zur Regelung der Kontrolle des Betriebsrates hingewiesen, um Kontrolllücken im Unternehmen zu verhindern. Diese Kontrolllücke ist nach 24 Jahren durch § 79a BetrVG gesetzlich geschlossen werden. Er unterstellt durch eine Erweiterung der Verschwiegenheitsverpflichtung des betrieblichen Datenschutzbeauftragten dessen Kontrollrecht bei der Mitarbeitervertretung. Damit ist aber ein entscheidender Handlungsdruck für ein eigenes Beschäftigtendatenschutz genommen. Es bleiben die umstrittenen Themen wie das Zusammenwirken von Complianceanforderungen und Beschäftigtendatenschutz oder der Einsatz von KI im Beschäftigungsverhältnis. Ob diese tatsächlich auch zu einer gesetzgeberischen Detaillösung geführt werden

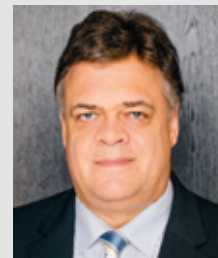
kann, bleibt angesichts der diametralen Positionen von Arbeitgeberverbänden und Gewerkschaften sehr zweifelhaft.

Die Koalitionäre setzen sich auch für eine bessere Kohärenz des Datenschutzes ein. Dazu soll die europäische Zusammenarbeit verbessert und der Datenschutzkonferenz im Bundesdatenschutzgesetz rechtlich verbindliche Beschlüsse ermöglicht werden. Die Kohärenz ist in der Auslegung des Datenschutzrechts für eine rechtssichere und verbindliche Datenschutzpraxis ein wichtiges Anliegen für die Datenschutzpraxis. Unterschiedliche Bewertungsmaßstäbe der Aufsichtsbehörden des Bundes und der Länder sollten künftig vermieden werden. Dazu kann die geplante rechtliche Verbindlichkeit der Beschlüsse der Datenschutzkonferenz einen Beitrag leisten. Gleichzeitig ist die verbesserte Kohärenz auf deutscher Seite auch bedeutsam für die Zusammenarbeit der Aufsichtsbehörden im Europäischen Datenschutzausschuss.

Positiv bewertet werden kann, was nicht Gegenstand einer Ankündigung im Koalitionsvertrag ist. Das bewährte Instrument der betrieblichen Selbstkontrolle durch betriebliche Datenschutzbeauftragte steht nicht im Zusammenhang mit einem Bürokratieabbau. Hierzu be-

steht auch keine Veranlassung. So führt der Evaluationsbericht des Bundesinnenministeriums zu dem Ergebnis, dass Datenschutzbeauftragte eine wichtige Rolle als Ansprechpartner für Aufsichtsbehörden und bei der wirksamen operativen Umsetzung des Datenschutzrechts übernehmen. Eine weitere Anhebung der Bestellungspflichtgrenze könne zu Problemen und Umsetzungsdefiziten bei Vereinen und kleineren und mittleren Unternehmen führen, während der Entlastungseffekt vielfach nicht wahrgenommen werde. Dem ist nur zuzustimmen.

RA Andreas Jaspers



RA Andreas Jaspers

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

Termine	Thema	Ort	Kontakt
16.03.2022	Compliance-Tests und Schwachstellenscannen	Köln	GDD e.V. und DATAKONTEXT
21.03.2022	Planung und Umsetzung der Überwachungsaufgabe des DSB	Berlin	GDD e.V. und DATAKONTEXT
22.03.2022	Datenschutz-Management light	Frankfurt/M.	GDD e.V. und DATAKONTEXT
23.03.2022	Kundendatenschutz aktuell: Kunden datenschutzkonform gewinnen und binden	Frankfurt/M.	GDD e.V. und DATAKONTEXT
28.03.2022	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
30.03.2022	IT-Sicherheitsmanagement aus Sicht der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
31.03.2022	Teleworking unter Beachtung von Datenschutz und Sicherheit	Frankfurt/M.	GDD e.V. und DATAKONTEXT
05.04.2022	Einführung in die ISO 27701	Berlin	GDD e.V. und DATAKONTEXT
06.-07.04.2022	Datenschutz-Management nach der DS-GVO – Teil 3	Köln	GDD e.V. und DATAKONTEXT
11.04.2022	Hacker-Tools für Datenschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
12.04.2022	Datenschutz International	Frankfurt/M.	GDD e.V. und DATAKONTEXT
12.04.2022	Mobile Endgeräte im Zeitalter von DS-GVO und ePrivacy-Verordnung	München	GDD e.V. und DATAKONTEXT
25.04.2022	ISO 27001 und Datenschutz	Online	GDD e.V. und DATAKONTEXT
26.04.2022	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Köln	GDD e.V. und DATAKONTEXT
27.-28.04.2022	Datenschutz kompakt	Berlin	GDD e.V. und DATAKONTEXT
02.-06.05.2022	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
03.05.2022	Datenschutzverletzungen richtig behandeln	Köln	GDD e.V. und DATAKONTEXT
04.05.2022	Websites datenschutzkonform gestalten	Online	GDD e.V. und DATAKONTEXT
10.05.2022	Datenschlösschung und andere SAP-Funktionen für den Datenschutz	Berlin	GDD e.V. und DATAKONTEXT
11.05.2022	Löschen nach DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
12.05.2022	Strategischer Umgang mit Bußgeldbescheiden und Verbandssanktionengesetz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
17.05.2022	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
17.05.2022	Konzerndatenschutz	Köln	GDD e.V. und DATAKONTEXT
19.05.2022	Verzeichnis von Verarbeitungstätigkeiten	Online	GDD e.V. und DATAKONTEXT
24.05.2022	DS-GVO-konforme Verarbeitung personenbezogener Daten mit SAP-Systemen	Frankfurt/M.	GDD e.V. und DATAKONTEXT
08.06.2022	Strafverfolgung, Whistleblowing, International Investigations – Datenschutz und Strafrecht	Frankfurt/M.	GDD e.V. und DATAKONTEXT

Prof. Peter Gola

Gilt das Fernmeldegeheimnis am Arbeitsplatz? Anwendung des neuen TTDSG im Beschäftigungsverhältnis

Das vom Bundestag am 20.05.2021 verabschiedete Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)¹ ist am 01.12.2021 in Kraft getreten. Das Gesetz ist Teil des auch eine Neufassung des Telekommunikations-

gesetzes (TKG) enthaltenden Telekommunikation-Modernisierungsgesetzes (TKModG). Inwieweit das nunmehr im TTDSG verankerte Fernmeldegeheimnis (§ 3 TTDSG) auch gegenüber Beschäftigten Anwendung findet, lässt das Gesetz weiter offen.

I. Die Neuregelung des TTDSG

Mit dem Inkrafttreten der DS-GVO stellte sich die Frage, ob das für den Datenschutz beim Einsatz elektronischer Medien bis dato bestehende datenschutzrechtliche Trio aus Telekommunikationsgesetz (TKG), Telemediengesetz (TMG) und Bundesdatenschutzgesetz trotz der grundsätzlich vorrangigen europäischen Regelung fortbestehen könnte. Der Gesetzgeber sah nunmehr zumindest klarstellenden Regelungsbedarf. Alle Anbieter von Telemedien und Telekommunikationsdiensten unterliegen ab dem 01.12.2021 dem neuen Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG).² Typische Telemedien sind Internetangebote wie Chatrooms, Soziale Medien und Blogs. Als Telekommunikationsdienste werden digitale Produkte definiert, deren Informationsübertragung über eine Kabel- oder Funktechnik realisiert wird. Mobilfunknetze, Glasfaserkabel und Kabelnetze zur Übertragung von Rundfunk und Fernsehen gehören zu den bekanntesten Telekommunikationsdiensten.

Daneben besteht auch das Telekommunikationsgesetz (TKG) in novellierter Fassung fort.

II. Das Fernmeldegeheimnis

1. Allgemeines

In § 2 TKG werden die Ziele der Regulierung des Telekommunikationsmarktes dargestellt, die ebenso vom TTDSG aufgegriffen werden. Diese bestehen unter anderem aus der fortbestehenden Wahrung des Fernmeldegeheimnisses, d.h. der Vertraulichkeit bei Telekommunikationsdiensten, wie sie auch nach wie vor verfassungs- (Art. 12 GG), straf- (§ 206 StGB) und kommunikationsrechtlich (§ 3 Abs. 1 TTDSG) abgesichert ist.

Die zur Achtung des Fernmeldegeheimnisses Verpflichteten ergeben sich aus § 3 Abs. 2 TTDSG. Neben Anbietern von öffentlich zugänglichen Telekommunikationsdiensten (§ 3 Abs. 2 S. 1 Nr. 1 TTDSG) gehören hierzu auch ansonsten ganz oder teilweise geschäftsmäßig tätige Anbieter solcher Dienste (§ 3 Abs. 2 S. 1 Nr. 2 TTDSG). Wenn also – wie das bei einem Hotelier gegenüber seinen Gästen geschieht – je-

mand Dritten Telekommunikation ermöglicht, ist ein solches Anbieter-Nutzerverhältnis gegeben. Von Geschäftsmäßigkeit ist auszugehen, wenn ein erforderliches nachhaltiges Angebot für Dritte mit oder ohne Gewinnerzielungsabsicht vorliegt. Dem Hotelier, d.h. dem Diensteanbieter, ist untersagt, sich oder anderen Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation im Betrieb zu verschaffen, soweit sie über die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme hinausgehen.

Damit greift, wenn die Beschäftigten innerbetriebliche Kommunikationstechniken oder Unternehmensnetze ausschließlich im Rahmen ihrer Arbeit nutzen, das Fernmeldegeheimnis des § 3 TTDSG nicht.³ Das Bereitstellen der betrieblichen Infrastruktur und i.d.R. die Pflicht zu ihrer aufgabenerforderlichen Nutzung ist kein geschäftsmäßiges „Angebot“ an die Beschäftigten⁴, und der Arbeitgeber tritt nicht in die Funktion eines Diensteanbieters.⁵

2. Dienstliche Nutzung

Die Kontrolle der Verarbeitung personenbezogener Daten im Falle der rein dienstlichen Nutzung⁶ richtet sich nach dem Bundesdatenschutzgesetz (§ 26 BDSG). Maßgebend für den Umfang der Kontrolle sind deren „Erforderlichkeit“, die im Rahmen einer durch das Verhältnismäßigkeitsprinzip bestimmten Interessenabwägung festzustellen ist.⁷ Eine Registrierung und Kontrolle dienstlicher Telekommunikation ist daher zunächst erlaubt, soweit sie durch den technischen Ablauf bedingt ist. Des Weiteren hat der Arbeitgeber

1 TTDSG, BGBl. I, 2021, Nr. 35 v. 28.06.2021.

2 Schwartmann/Benedikt/Reif, Entwurf zum TTDSG: Für einen zeitgemäßen Datenschutz?, MMR 2021, 99.

3 Thüsing/Thüsing, Beschäftigtendatenschutz und Compliance, 3. Aufl. § 3 Rn. 63; aber ebenso bei privater Nutzung wegen der vom Gesetzgeber nicht beabsichtigten Folgen für den Arbeitgeber, § 3 Rn. 88 ff.

4 Däubler, Gläserne Belegschaften, § 6 Rn. 337 m.w.N.

5 Baumgartner, in: Wert/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl., B IX Rn. 73 ff.; ebenso jedoch auch bei privater Nutzungseröffnung, Rn. 84 f.

6 Zum Begriff der dienstlichen Nutzung Däubler, Digitalisierung und Arbeitsrecht, § 11 Rn. 7.

7 Gola, Handbuch Beschäftigtendatenschutz, Rn. 141 ff., 746 f., 1764 f.

zunächst ein berechtigtes Interesse an einer „Telefondatenerfassung“⁸ zumindest bei Ferngesprächen allein schon wegen der Kostenkontrolle oder an dem Festhalten der „äußeren“ Daten des E-Mail Verkehrs und der Internetnutzung.⁹ Inhaltliche Kontrollen hängen von der Art der Kommunikation ab. Während dienstliche Telefonate¹⁰ schon im Hinblick auf den Persönlichkeitsschutz der Gesprächspartner i.d.R. nicht aufgezeichnet oder mitgehört werden dürfen,¹¹ ist das bei der E-Mail-Korrespondenz hinsichtlich der Aufzeichnung und der u.a. dienstlich notwendigen Kenntnisnahme durch z.B. Kollegen und Vorgesetzte anders.

3. Private Nutzung

Umstritten ist jedoch, ob der Schutz des Fernmeldegeheimnis für Beschäftigte dann gilt, wenn sie die betriebliche Kommunikationstechnik – erlaubter oder geduldeter Weise – für private Zwecke nutzen und in diesem Falle von dem oben aufgezeigten Angebot des Arbeitgebers Gebrauch machen. Trifft dies zu, so unterliegt der Arbeitgeber dem Fernmeldegeheimnis (§ 3 Abs. 3 TTDSG), wobei dann zu differenzieren ist, ob die Kommunikation mit Dritten und per Telefon, E-Mail oder Internet erfolgt.

Eine besondere Problematik ergibt sich im Falle sog. „Mischnutzung“, d.h. wenn dienstliche und private Nutzung nicht getrennt ablaufen,¹² mit der Folge, dass der Arbeitgeber, wenn er nicht erkennen kann, welche Daten ggf. unter das Fernmeldegeheimnis fallen, alle als besonders geschützt zu behandeln hat.

III. Der Arbeitgeber als Adressat des Fernmeldegeheimnisses

1. Das unterschiedliche Meinungsbild

Vor Inkrafttreten des TTDSG gab es kein einheitliches Meinungsbild,¹³ ob das damals in § 88 TKG mit identischem Inhalt geregelte Fernmeldegeheimnis auch im Arbeitsverhältnis bei der „privaten“ Nutzung der betrieblichen Kommunikationstechnik Wirkung entfaltet.¹⁴ Daran hat sich mit Inkrafttreten des TTDSG nichts geändert.

Eine Ursache dafür ist, dass das BAG noch keine Gelegenheit hatte, sich mit der in dieser Frage unterschiedlichen Instanzrechtsprechung¹⁵ zu beschäftigen.

Eine andere Ursache der Rechtsunsicherheit ist, dass eine einschlägige Zuordnungsregelung auch im TTDSG fehlt: Wenn also der Arbeitgeber zur Kenntnisnahme dienstlicher E-Mails – wozu er zweifelsohne befugt ist – auf das auch private Nachrichten enthaltene E-Mail-Postfach eines Beschäftigten zugreift, besteht nach wie vor ein nicht unerhebliches Risiko, dass dies als eine strafbewehrte Verletzung des Fernmeldegeheimnisses bewertet wird,¹⁶ wengleich der EGMR¹⁷ Unternehmen jedenfalls gestattet, auch die private Internetkommunikation ihrer Beschäftigten zu überwachen, sofern die Überwachung verhältnismäßig ist, was u.a. verlangt, dass der Beschäftigte vorab über die Möglichkeit, die Art und das Ausmaß von Kontrollen informiert wurden. Der EGMR sieht ansonsten eine Verletzung des Rechts auf Achtung des Privatlebens und der Korrespondenz (Art. 8 EMRK).

2. Bewertung der E-Mail-Kommunikation

Aktuell hat auch das LG Erfurt¹⁸ geurteilt, dass die private Nutzung betrieblicher E-Mail-Accounts den Arbeitgeber nicht zum Diensteanbieter werden lässt und ein Zugriff auf die E-Mails daher unter besonderen Voraussetzungen auch ohne Einwilligung des Betroffenen zulässig sei. Ebenso entschieden bereits zuvor eine Reihe von Instanzgerichten.¹⁹ Ein Teil der Literatur folgt dieser Rechtsprechung. Nach wie vor vertreten die Aufsichtsbehörden eine andere Ansicht.²⁰

3. Reichweite des Fernmeldegeheimnisses

Auch wenn man bei der Eröffnung privater Telekommunikation eine Telekommunikationsleistung beim Arbeitgeber annehmen würde, so ist zu beachten, dass der Schutz des Fernmeldegeheimnisses beim Telefonat oder E-Mail-Eingang in dem Moment endet, in dem die E-Mail im „Herrschaftsbereich“ des Empfängers ankommt und der Übertragungsvorgang beendet ist.²¹ Der Zugriff des Arbeitgebers auf die im Posteingang oder -ausgang liegenden E-Mails unterliegt daher nicht den Beschränkungen des Fernmeldegeheimnisses, sondern denen des informationellen Selbstbestimmungsrechts²² und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme²³ und damit konkret denen der DS-GVO bzw. des § 26 BDSG.²⁴

8 Gola, Handbuch Beschäftigtendatenschutz, Rn. 1319 ff. mit Nachweis der Rechtsprechung.

9 Vgl. Däubler, Gläserne Belegschaften, Rn. 1311

10 Zur insoweit bestehenden Kontrollbefugnis vgl. Gola, Handbuch Beschäftigtendatenschutz, Rn. 1319 ff.

11 BVerfG, Beschl. v. 19.12.1991 – 1 BvR 382/85 und 09.10.2002 – 1 BvR 1611/96 sowie BAG, Urt. v. 30.08.1995 – 1 ABR 4/95.

12 Zur Organisation einer technischen Trennung, Däubler, Gläserne Belegschaften, § 9 Rn. 340 b und 378 a.

13 Ausführlich z.B. Byers, Mitarbeiterkontrolle, Rn. 31 ff.

14 Vgl. zum unterschiedlichen Meinungsstand, auch Gola, Handbuch Beschäftigtendatenschutz, Rn. 82 ff.; Rucker, in: Moos, Datenschutz und Datennutzung, § 23 Rn. 23.14 ff.; Baumgarten, in: Weth/Herberger/Wächter/Sorge (Fn. 5) Kap. IX; Telefon-, Internet- und E-Mail Nutzung einschließlich Privatnutzung, Rn. 88.

15 Vgl. nachstehend Fn. 19

16 Aufhäuser, Die übersehene DS-GVO: Zur Verdrängung des Fernmeldegeheimnisses bei betrieblichen E-Mail-Systeme, PinG 2021, 188.

17 EGMR vom 05.09.2017 Beschwerde-Nr. 61496/08.

18 Urt. v. 28.04.2021 – 1 HK O 43/20.

19 LAG Berlin-Brandenburg, Urt. v. 14.01.2016 – 5 Sa 657/15 und v. 16.02.2011 – 4 Sa 2132/10; VG Karlsruhe, Urt. v. 27.05.2013 – 2 K 3249/12; LAG Hamm, Urt. v. 10.07.2012 – 14 Sa 1711/10; LAG Niedersachsen, Urt. v. 31.05.2010 – 12 Sa 875/09; VGH Hessen, Urt. v. 19.05.2009 – 6 A 2672/08.Z; ArbG Düsseldorf, Urt. v. 29.10.2007 – 3 Ca 1455/07.

20 DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, S. 8.

21 Vgl. bei Däubler, Gläserne Belegschaften, § 6 Rn. 340a; zur Ausdehnung des Fernmeldegeheimnisses, vgl. ausführlich bei Rucker, in: Moos, Datenschutz und Datennutzung, § 23 Rz. 23. 29 ff., Aufhäuser (Fn. 16) PinG 2021; 188 (190), der ein Ankommen im „Herrschaftsbereich“ des Mitarbeiters verneint.

22 HessVG, Beschl. v. 19.05.2009 – 6 A 2672/08.

23 BVerfG, Beschl. v. 16.06.2009 – 2 BvR 902/06.

24 Vgl. ausführlich bei Rucker, in: Moos, Datenschutz und Datennutzung, § 23 Rz. 23.29 ff.

4. Der Schutz des externen Dritten

Das Fernmeldegeheimnis schützt zwar einerseits auch den Dritten, mit dem der Beschäftigte kommuniziert,²⁵ andererseits steht es dem Beschäftigten aber auch grundsätzlich frei, anderen und damit auch den Arbeitgeber vom Inhalt der Kommunikation, jedenfalls nach deren Beendigung, in Kenntnis zu setzen, so dass er auch dem Arbeitgeber gestatten kann, Einblick in private E-Mails zu nehmen, oder ihm über ein privates Telefonat unterrichten kann. Ein Mithörenlassen wäre ohne Erlaubnis des Gesprächspartners aber unzulässig.²⁶

IV. Kompetenz zur Regelung durch den nationalen Gesetzgeber

Dass es an einer Regelung zum Schutz von mit dienstlicher Technik geführter privater Kommunikation im TTDSG fehlt, mag seine Ursache darin haben, dass es fraglich ist, ob der nationale Gesetzgeber überhaupt befugt ist, Anbieter von geschäftsmäßig angebotenen Telekommunikationsdiensten speziellen Regelungen zu unterwerfen, da weder Art. 95 DS-GVO noch die ePrivacy-Richtlinie das Merkmal der Geschäftsmäßigkeit kennen. In der Literatur mehren sich insofern Stimmen,²⁷ die die Datenverarbeitung von Arbeitgebern, welche die Privatnutzung von Telefon, Internet und/oder E-Mail gestatten, ausschließlich an der DS-GVO messen. Zentraler Unterschied ist insbesondere die Möglichkeit, Datenverarbeitungen auch auf eine Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f DS-GVO) stützen zu können. Insofern ist dann auch für das Tatbestandsmerkmal „unbefugt“ in § 206 Abs. 1 StGB auf die Erlaubnisnormen der DS-GVO abzustellen. Nach Aufhäuser²⁸, soll § 3 Abs. 2 TTDSG mit seiner umfangreichen Normadressierung über die Vorgaben des Art. 5 Abs. 1 ePrivacy-RLi.V: m. Art. 2 Nr. 4 TK-Kodex sowie die Öffnungsklausel der Art. 95 DS-GVO hinausgehen und insoweit von den Regeln der DS-GVO verdrängt werden.

V. Regelung durch Betriebsvereinbarung und Einwilligung

Eingriffe in das Fernmeldegeheimnis können durch Einwilligung gerechtfertigt werden, wobei wiederum ungeklärt ist, ob bei kenntlich gemachter privater Kommunikation dem „Eingriff“ nicht nur der Beschäftigte,²⁹ sondern auch der externe Partner³⁰ zustimmen muss.

Die Kontrolle der privaten Nutzung der betrieblichen Kommunikationstechnik kann auch aufgrund kollektiver und individueller Erlaubnis gestattet sein, d.h. es bietet sich für den Arbeitgeber die Möglichkeit an, die private Nutzung durch Beschäftigte zu gestatten, hierzu aber Regelungen in einer internen Richtlinie bzw. Betriebsvereinbarung aufzustellen und

gleichzeitig eine datenschutzrechtliche Einwilligung³¹ mit dem Verzicht auf das Fernmeldegeheimnis einzuholen.³²

Die individuelle Einwilligung ist auch bei Abschluss einer zwingend abzuschließenden Betriebsvereinbarung (§ 87 Abs. 1 Nr. 1 und 6 BetrVG)³³ geboten, da Betriebsvereinbarungen keine gesetzlichen Vorschriften sind, die zur Durchbrechung des Fernmeldegeheimnisses erforderlich wären.³⁴

VI. Fazit

Festzuhalten ist, dass eine Klärung zur Geltung des Fernmeldegeheimnisses bei privater Nutzung betrieblicher Kommunikationstechnik durch höchstrichterliche Rechtsprechung bislang nicht herbeigeführt wurde und es der Gesetzgeber bei der Neufassung des Fernmeldegeheimnisses im TTDSG versäumte, eine nicht nur klarstellende, sondern auch praxisgerechte Lösung zu schaffen.

Wenn die Privatnutzung dienstlicher Endgeräte und Infrastruktur im Unternehmen gestattet werden soll, sollte deren notwendige Kontrolle angesichts der ungeklärten Rechtslage eine dem Verhältnismäßigkeitsgrundsatz Rechnung tragende kollektiv- und individualrechtliche Basis haben.



Prof. Peter Gola

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

25 Brink/Wirtz, ArbRAktuell 2016, 255 (257).

26 Gola, Handbuch Beschäftigtendatenschutz, Rn. 1338 ff.

27 Zeh, <https://jowecon.de/duerfen-unternehmen-die-privaten-e-mails-ihrer-beschaeftigten-einsehen>; Bürger/Nelder, <https://seitzblog.de/privatnutzung-von-smartphone-verbot-nach-neuen-ttdsg-fuer-beschaeftigte>.

28 Das Fernmeldegeheimnis für Arbeitgeber unter dem TTDSG; PinG 2021, 224.

29 So Jenny, in: Plath, DS-GVO/BDSG; 3. Aufl., § 88 TKG Rn. 11.

30 Zur Zustimmung aller Beteiligten Henn, in: Auernhammer, DS-GVO/BDSG, § 88 TKG Rn. 43 f.; Spindler/Schuster/Eckhardt, Recht der elektronischen Medien, 4. Aufl., § 88 TKG Rn. 25.

31 Gola, Handbuch Beschäftigtendatenschutz. Rn. 513 ff. und 1375 ff.

32 Heun, in: Auernhammer, TKG § 88 Rn. 60; Rücker, in: Moos, Datenschutz und Datennutzung, Rz. 23.45 mit dem Muster einer entsprechenden Erklärung in Rz. 23.119.

33 Gola, Handbuch Beschäftigtendatenschutz, Rn. 1381 ff.

34 Däubler, Gläserne Belegschaften, § 6 Rn. 340; Rücker, in: Moos, Datenschutz und Datennutzung, Rz. 23.41.

Dr. Stefanie Hellmich/Kata Éles

DS-GVO Bußgelder in der Praxis: Wer muss den Rückgriff fürchten?¹

Die Datenschutz-Grundverordnung (DS-GVO) dient dem Schutz von natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten. Um diesen Schutz effektiv durchsetzen zu können, wurde durch den europäischen Gesetzgeber ein umfassendes Sanktionsregime eingeführt. Dieses ermöglicht den Aufsichtsbehörden, bei bestimmten Verstößen Geldbußen von bis zu 20 Mio. Euro oder bei Unternehmen von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres zu verhängen (Art. 83 Abs. 5 und 6 DS-GVO) – je nachdem, welcher der Beträge höher ist. Der Jahresumsatz meint dabei den des gesamten Unternehmensverbundes.² Jüngst verhängte die Landesbeauftragte für den Datenschutz Niedersachsen ein Bußgeld von über 10,4 Mio. Euro gegen ein Unternehmen aufgrund von schwerwiegenden Verstößen im Zusammenhang mit der Videoüberwachung.³ Wegen eines Verstoßes gegen die Pflichten betreffend die Datensicherheit verhängte die Bußgeldstelle des LfDI Baden-Württemberg gegen die AOK Baden-Württemberg eine Geldbuße von 1,24 Mio. EUR.⁴ Bei derart hohen Beträgen stellt sich die Frage, inwieweit ein Regress zwischen den an der Verarbeitung Beteiligten möglich ist oder in zulässiger Weise vertraglich ausgeschlossen oder beschränkt werden kann. So mag in Vereinbarungen zwischen Verantwortlichem und Auftragsverarbeiter versucht werden, die Haftung abweichend zur gesetzlichen Rechtslage zu regeln. Gleichmaßen mögen Beschäftigte in Vereinbarun-

gen mit Unternehmen versuchen, sich vor Haftungsrisiken zu schützen, die als unangemessen erachtet werden. Vertragliche Vereinbarungen über Haftungsbegrenzungen oder den Ausschluss einer Haftung sind aufgrund der Privatautonomie im Grundsatz zulässig. Gleichwohl ergeben sich bereits aus dem Gesetz Vorgaben für vertragliche Haftungsbegrenzungen. So verbietet § 276 Abs. 3 BGB den Ausschluss der Haftung für Vorsatz. Darüber hinaus existieren spezialgesetzlich Verbote, etwa § 52 BRAO oder § 67 StBerG.⁵ Gemäß § 309 Nr. 7 lit. b) BGB sind ein Ausschluss oder eine Begrenzung der Haftung für Schäden, die auf einer grob fahrlässigen Pflichtverletzung des Verwenders oder auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung eines gesetzlichen Vertreters oder Erfüllungsgehilfen des Verwenders beruhen, in allgemeinen Geschäftsbedingungen unwirksam. Entsprechendes gilt für Schäden, die aus der Verletzung des Lebens, Körpers oder der Gesundheit resultieren. Für die leicht fahrlässige Verletzung vertragswesentlicher Pflichten kann die Haftung nur auf die vorhersehbaren Schäden beschränkt werden. Diese Regelungen sagen allerdings nichts dazu aus, ob ein mit einem Bußgeld belegtes Unternehmen gegen einen anderen an der Verarbeitung Beteiligten – etwa wegen der Verletzung von Pflichten aus einem Vertragsverhältnis – Rückgriff nehmen kann und ein verhängtes Bußgeld ein ersatzfähiger Schaden im Sinne der §§ 249 ff. BGB wäre.

I. Gerichtliche Entscheidungen im Kartellrecht

Gerichtliche Entscheidungen zu Rückgriffsansprüchen bei datenschutzrechtlichen Bußgeldern nach der DS-GVO existieren noch nicht. Bei den vorhandenen arbeits- und kartellrechtlichen Entscheidungen zu Rückgriffsansprüchen geht es um den Rückgriff eines mit einem Bußgeld belegten Beschäftigten gegen das Unternehmen, bei dem der Mitarbeiter beschäftigt ist, (Fallgruppe 1) und den Rückgriff des bußgeldbelegten Unternehmens gegen einen Beschäftigten wegen schuldhafter Verletzung von Pflichten (Fallgruppe 2). Es finden sich zu diesen Fallgruppen einige Entscheidungen, die Rückgriffsansprüche im Grundsatz ablehnen. In einer Sonderkonstellation und bei einem Ausgleich innerhalb einer Unternehmensgruppe wurde ein Rückgriff hingegen zugelassen (Fallgruppe 3).

1. Kein Regress des Beschäftigten gegen das Unternehmen (Fallgruppe 1)

Das Bundesarbeitsgericht (BAG) lehnte in einer Entscheidung aus dem Jahr 2001 einen Rückgriffsanspruch des Beschäftigten ab. In dem konkreten Fall ging es um einen Arbeitnehmer, gegen den ein Bußgeld wegen eines während

der Arbeitszeit begangenen Verstoßes gegen die Straßenverkehrsordnung verhängt wurde und der dieses von seinem Arbeitgeber ersetzt haben wollte. Nach Auffassung des BAG sei ein solches Bußgeld grundsätzlich vom Arbeitnehmer selbst zu tragen; ein Regress beim Arbeitgeber sei nur in Ausnahmefällen möglich. Im Vorfeld erteilte Zusagen des Arbeitgebers, dem Arbeitnehmer auferlegte Bußgelder zu übernehmen, seien regelmäßig als Verstoß gegen § 138 BGB anzusehen. Sie würden dem Zweck von Straf- und Bußgeldvorschriften zuwiderlaufen und seien geeignet, die Hemmschwelle des Arbeitnehmers, Straftaten oder Ordnungswidrigkeiten zu begehen, herabzusetzen. Geldbußen sind vom

1 Literatur und Rechtsprechungen wurden bis Mai 2021 berücksichtigt.

2 Sog. „funktionaler Unternehmensbegriff“, vgl. LG Bonn, Urteil v. 11.11.2020 – 29 OWi 1/20, NRWE Rn. 92 f.

3 Pressemitteilung abrufbar unter: <https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html>.

4 https://www.baden-wuerttemberg.datenschutz.de/lfDI_Baden-Wuerttemberg_verhaengt_Bu%C3%9Fgeld_gegen_AOK_Baden-Wuerttemberg_-_Wirksamer_Datenschutz_erfordert_regelm%C3%A4%C3%9Fige_Kontrolle_und_Anpassung_|_Der_Landesbeauftragte_f%C3%BCr_den_Datenschutz_und_die_Informationsfreiheit_Baden-Wuerttemberg.

5 Palandt/Grüneberg, § 276 BGB Rn. 35.

Arbeitnehmer grundsätzlich persönlich aus dem eigenen Vermögen zu tragen.⁶ Die Geldbuße könne allenfalls freiwillig vom Arbeitgeber übernommen werden.⁷

Das Landesarbeitsgericht (LAG) Rheinland-Pfalz ließ die Frage offen, ob ein Bußgeld ein ersatzfähiger Schaden nach §§ 249 ff. BGB ist. Ein Bußgeld als Schaden solle seiner Natur nach grundsätzlich nicht ersatzfähig sein. Es entspricht der herrschenden Auffassung in der Rechtsprechung⁸ und in der versicherungsrechtlichen Kommentarliteratur, dass Geldbußen keine versicherungsfähigen Vermögensschäden sind, weil eine vorherige Erstattungszusage das Sanktionsprinzip des Straf- und Ordnungswidrigkeitenrechts verletzen würde.⁹ Das Gericht argumentierte auch hier – ähnlich wie das BAG – mit dem Sinn und Zweck von Bußgeldern. Es führte in seiner Entscheidung aus, dass, wenn die Rechtsordnung dem Täter einen Anspruch darauf zubilligen würde, von den finanziellen Belastungen, die mit der Verhängung eines Bußgeldes verbunden sind, freigestellt zu werden, die Geldbuße den mit ihr verfolgten Zweck verfehlen würde.¹⁰

2. Kein Regress des Unternehmens gegen den Geschäftsführer (Fallgruppe 2)

Das Landesarbeitsgericht (LAG) Düsseldorf lehnte in einer Entscheidung aus dem Jahre 2015 einen Regress des Unternehmens gegen einen Geschäftsführer wegen eines durch das Bundeskartellamt verhängten Bußgeldes ab.¹¹ Das Urteil des LAG Düsseldorf wurde durch das BAG allerdings aufgehoben.¹² Das Verfahren ruht aktuell beim Landgericht Dortmund. Ob das BAG der Auffassung des LAG im Übrigen folgt, ließ es in seiner Entscheidung ausdrücklich offen.¹³ Das LAG Düsseldorf stützte die Ablehnung des Regressanspruchs im Wesentlichen auf folgende Punkte: Der Normgeber habe explizit den Adressaten des Bußgeldes bestimmt (im Kartellrecht in § 81 GWB) und daher auch eine Entscheidung darüber getroffen, wer das Bußgeld letztlich tragen müsse. Wäre es dem Unternehmen gestattet, die Geldbuße im Innenverhältnis zu regressieren, würde die gewollte Sanktionswirkung nicht eintreten und die Entscheidung des Gesetzgebers ins Leere laufen, dass ein Unternehmen zur Verantwortung gezogen werden soll. Es würde vielmehr eine – vom Gesetzgeber nicht gewollte – Korrektur der ordnungsrechtlichen Entscheidung durch das Zivilrecht erreicht werden. Diese Wertung sei im Zivilrecht zu berücksichtigen und ein Regress im Rahmen der Innenhaftung daher zu verneinen. Ansonsten könne der mit einem Bußgeld verbundene Zweck, eine bestimmte Ordnung zu garantieren, nicht wirksam erreicht werden.¹⁴

Wenn ein Regress einer natürlichen Person gegen eine juristische Person regelmäßig nicht möglich sei, könne auch andersherum nichts anderes gelten. Insbesondere sei auch gegenüber juristischen Personen der Grundsatz der individuellen Straf- und Sanktionsfestsetzung zu berücksichtigen. Der in dem Bußgeld enthaltene Vorwurf sei der eines Organisationsverschuldens in Gestalt einer nicht ausreichenden Kontrolle der Organe. Unternehmen und Unternehmensträger sollen durch fühlbare Einbußen zu einer angemessenen Kontrolle angehalten werden. Nur durch die finale Bußgeldbelastung bei dem Unternehmen sei dem Sinn und Zweck

des Kartellbußgeldrechts mit der Aufteilung der innergesellschaftlichen Verantwortungssphären Rechnung getragen.¹⁵ Im Kartellrecht existiere eine Unterscheidung zwischen Bußgeldern, die gegen Unternehmen verhängt werden können (bis zu 10% des Gesamtjahresumsatzes), und Bußgeldern, die gegenüber natürlichen Personen (Begrenzung auf 1 Mio. Euro) verhängt werden können. Diese Unterscheidung würde ins Leere laufen, wenn ein Regress des Unternehmens gegen die Geschäftsleitung möglich wäre.¹⁶ Bestünde ein Regressanspruch des Unternehmens gegen die Geschäftsleitung, würde dies dazu führen, dass die von der Behörde beabsichtigte Abschöpfung des unrechtmäßig erwirtschafteten Mehrerlöses beim Unternehmen (§ 81 Abs. 5 GWB) letztlich vom Geschäftsführer getragen werden würde.¹⁷ Dieser Linie folgend halten zahlreiche Stimmen in der Kommentarliteratur bei Kartellrechtsverstößen Regressansprüche des Unternehmens gegen die handelnden Personen einschließlich der Geschäftsleitung grundsätzlich für ausgeschlossen.¹⁸

Abweichende Auffassungen in der Literatur wollen Regress – ausgenommen den Gewinnabschöpfungsanteil – gegen die Geschäftsleitung zumindest beschränkt zulassen, um unbillige Entlastungen der Geschäftsleitung zu vermeiden.¹⁹ Auch fehle es an den Voraussetzungen der dafür not-

6 BAG, Urt. v. 25.01.2001 – 8 AZR 465/00 (Hamm), NZA 2001, 653 f.; so auch LAG Köln, Urt. v. 29.02.2012 – 9 Sa 1464/11, BeckRS 2012, 69448; LAGE § 670 BGB Nr. 11; LAG Schleswig-Holstein, Urt. v. 30.03.2000 – 4 Sa 450/99, BeckRS 2000, 30468364; LAG Hamm, Urt. v. 20.12.1991 – 18 Sa 506/91, BeckRS 1991, 30983102; NJW 1991, 861.

7 BAG, Urt. v. 25.01.2001 – 8 AZR 465/00 (Hamm), NZA 2001, 653 f.; zur strafrechtlichen Zulässigkeit der nachträglichen Erstattung durch den Arbeitgeber trotz fehlenden zivilrechtlichen Anspruchs des Arbeitnehmers Holly/Friedhofen NZA 1992, 145; im Einzelfall einen nachträglichen Aufwendungsersatzanspruch aus § 670 BGB bei Geldstrafen und -bußen bejahend Kapp NJW 1992, 2796, 2800.

8 BGH, NJW 1997, 518 (519).

9 Langheid/Wandt, 2. Teil. Systematische Darstellungen 3. Kapitel. Versicherungssparten 320. Directors & Officers-Versicherung Rn. 213, beck-online; Bruck/Möller/Johannsen, 8. Aufl., Bd. IV, Anm. B 8 geht von Sittenwidrigkeit aus. Zur Nichtigkeit von vorherigen Erstattungszusagen des Unternehmens gemäß § 134 BGB vgl. KölnKommAktG/Mertens § 84 Rn. 82; Bastuck S. 135, 136, 140.

10 LAG Rheinland-Pfalz Urt. v. 26.01.2010 – 3 Sa 497/09, BeckRS 2010, 68132, beck-online.

11 LAG Düsseldorf, Teilurt. v. 20.01.2015 – 16 Sa 459/14, NJOZ 2015, 782, BAG, NJW 2018, 184, 187.

12 Grund dafür war die Unzuständigkeit des LAG, da es sich in der Sache um eine kartellrechtliche Vorfrage im Sinne von § 87 Satz 2 GWB handelte, welche die Zuständigkeit des Landgerichts begründete. Vgl. Dux-Wenzel/Janssen, CB 2021, 87.

13 BAG, NJW 2018, 184, 187.

14 LAG Düsseldorf, Teilurt. v. 20.01.2015 – 16 Sa 459/14, NJOZ 2015, 782, 790.

15 LAG Düsseldorf, Teilurt. v. 20.01.2015 – 16 Sa 459/14 = NJOZ 2015, 782, 790, in einem obiter dictum gleicher Auffassung LG Saarbrücken, v. 15.09.2020, NZKart 2021, 64-65.

16 LAG Düsseldorf, Teilurt. v. 20.01.2015 – 16 Sa 459/14, NJOZ 2015, 782, 791.

17 Ebenda.

18 Bachmann, BB 2015, 911; Dreher, FS Konzen, 2006, 84, 104 ff.; Gaul, AG 2015, 109, 110 f.; Goette, ZHR 176, 588, 603 f.; Grunewald, NZG 2016, 1121, 1122; 76, 588, 603 Horn, ZIP 1997, 1129, 1136; Kapp/Gärtner, CCZ 2009, 168; Kollmann/Aufdermauer, BB 2015, 1024; Krause, BB Beilage 2007 Nr. 7, S. 2, 13; Labusga, VersR 2015, 634; Lotze/Smolinski, NZKart 2015, 254, 255 f., 258; Thomas, NZG 2015, 1409, 1416.

19 MüKoAktG/Spindler, 5. Aufl. 2019, AktG § 93 Rn. 194; Hüffer/Koch/Koch, 15. Aufl. 2021, AktG § 93 Rn. 48; Backhaus/Brand, jurisPR-HaGesR 4/2021 Anm. 5; a.A. ausdrücklich LAG Düsseldorf, Teilurt. v. 20.01.2015 – 16 Sa 459/14, NJOZ 2015, 782, 789; Stancke, BB 2020, 1667-1672.

wendigen teleologischen Reduktion der haftungsrechtlichen Vorschriften in § 93 Abs. 2 S. 1 AktG. Die Regelungen zur Verhängung eines Bußgeldes könnten auch nicht als derart abschließend angesehen werden, als dass sie jegliche Regressnahmen gegenüber der Geschäftsleitung ausschließen. Jedoch sei aufgrund der Treu- und Fürsorgepflicht der Gesellschaft die Regresshöhe zu beschränken.²⁰

3. Einen Regress in Ausnahmefällen zulassende Urteile (Fallgruppe 3)

In der Rechtsprechung wurde ein Regress bei Bußgeldern allerdings in bestimmten Ausnahmefällen bejaht.²¹ So soll ein Regress etwa dann möglich sein, wenn sich der Adressat des Bußgeldes bei einem sachkundigen Dritten Rat einhole, um der Gefahr einer Sanktionierung zu begegnen und aufgrund der nicht sachgerechten Beratung ein Bußgeld verhängt werde. So könne ein Steuerberater, der es durch einen von ihm erteilten Rat oder durch die von ihm veranlasste unzutreffende Darstellung steuerlich bedeutsamer Vorgänge verschuldet habe, dass gegen seinen Mandanten wegen leichtfertiger Steuerverkürzung ein Bußgeld verhängt wird, verpflichtet sein, jenem den darin bestehenden Vermögensschaden zu ersetzen.²² Dem Bebußten wird demnach ein Regressanspruch zugebilligt, wenn sein Vertragspartner gerade verpflichtet ist, die Verwirklichung des Bußgeldtatbestandes abzuwenden.²³

Eine Geldbuße kann ausnahmsweise auch zu einem nach § 826 BGB zu ersetzenden Schaden gehören. Demnach ist ein Regress des Arbeitnehmers beim Arbeitgeber möglich, wenn es dem Arbeitnehmer trotz seiner rechtlichen Verpflichtung im Einzelfall nicht zumutbar gewesen ist, sich den Anordnungen seines Arbeitgebers zu widersetzen.²⁴

Für eine gegen zwei Unternehmen als Gesamtschuldner verhängte kartellrechtliche Geldbuße entschied der EuGH, dass eine privatautonome Regressregelung bzgl. des Bußgeldes wirksam getroffen werden kann und dies dem Sanktionszweck von Bußgeldern nicht entgegensteht.²⁵ Der BGH stellte dazu fest, dass der interne Ausgleich zwischen Gesamtschuldnern bei dieser von der Kommission festgesetzten Geldbuße sich nach § 426 BGB richtet und in Ermangelung einer Vereinbarung über die Ausgleichsansprüche die individuellen Verursachungs- und Verschuldensbeiträge der Beteiligten heranzuziehen sind.²⁶ Diese Entscheidungen werden teilweise allgemein dahingehend interpretiert, dass eine vertragliche Regressregelung für Bußgelder rechtlich wirksam getroffen werden könne.²⁷ Allerdings hat der BGH ausdrücklich festgehalten, dass Ansprüche auf Erstattung einer gezahlten Geldbuße auf der Grundlage eines Schadensersatzanspruchs schon deshalb nicht in Betracht kommen, weil das Wettbewerbsrecht der Union nicht dazu diene, einzelne Unternehmenseinheiten eines gegen dieses Recht verstoßenden Unternehmens vor der Belastung mit einer Geldbuße zu schützen.²⁸ Ansprüche dieser Art seien weder zur effektiven Durchsetzung der Wettbewerbsregeln der Union notwendig noch förderlich.²⁹

II. Übertragung der Rechtsprechung auf DS-GVO-Bußgelder

Die dargestellte Rechtsprechung bezieht sich nicht auf das Datenschutzrecht. Es stellt sich daher die Frage, ob die Argumentation auch auf die verschiedenen datenschutzrechtlichen Akteure und ihre Rechtsbeziehungen zueinander übertragen werden kann.

1. Grundlagen der Verhängung von Bußgeldern gegen das Unternehmen

Gemäß § 41 Abs. 1 S. 1 BDSG sind die Vorschriften des OWiG für die Verhängung von Bußgeldern nach Art. 83 DS-GVO „sinngemäß“ anwendbar. Die Zurechnungsvorschrift in § 30 OWiG, nach der eine in dem Katalog des § 30 OWiG genannte Leitungsperson die jeweilige Straftat oder Ordnungswidrigkeit begangen haben muss, damit die juristische Person oder Personenvereinigung sanktioniert werden kann, ist von dem Verweis – anders als andere OWiG Vorschriften – gerade nicht ausdrücklich ausgenommen worden. Offen bleibt, inwieweit diese Regelung den Täterkreis gegenüber Art. 83 DS-GVO abändern kann.³⁰ Das Abstellen auf die Leitungspersonen wird damit begründet, dass Inhaber von Betrieben und Unternehmen nach § 130 Abs. 1 OWiG verantwortlich sind, wenn sie ihre Aufsichtspflicht hinsichtlich der Einhaltung der DS-GVO schuldhaft verletzen. Zu ihren Aufsichtspflichten gehöre u.a. die Bestellung, die sorgfältige Auswahl und Überwachung von Aufsichtspersonen.³¹

Das Landgericht Bonn hat in einer aktuellen Entscheidung ausdrücklich festgestellt, dass ein Bußgeld entgegen § 30 OWiG nicht nur dann gegenüber einem Unternehmen verhängt werden kann, wenn ein schuldhaftes Fehlverhalten bestimmter Personen in Führungs- oder Aufsichtspersonen vorliegt, sondern auch dann, wenn ein sonstiger Mitarbeiter Datenschutzverstöße begeht. Nach Auffassung des Gerichts

20 Petersen, in: van Kann, Vorstand der AG, 3. Aufl. 2021, Kapitel III: Verantwortlichkeit und Haftung, Rn. 104; Bayer/Scholz, NZG 2014, 926 ff.; Hoffmann, NJW 2012, 1393 ff.; Koch, AG 2012, 429 ff.; Koch, AG 2014, 513 ff., m.w.N.; Koch, in: Hüffer/Koch, AktG, § 93, Rn. 51, m.w.N.; Vetter, NZG 2014, 921 ff.

21 BGH, NJW 1997, 518, NJW-RR 1997, 565 Ls.; BGHZ 23, 222, NJW 1957, 586; RG, Urt. v. 10.06.1942 – III 14/42.

22 BGH, NJW 1997, 518, NJW-RR 1997, 565, Ls.; Entscheidung u.a. bestätigt durch BGH, Urt. v. 15.04.2010 – IX ZR 189/09, DStR 2010, 1695 sowie LAG Düsseldorf, Teilurt. v. 20.01.2015 – 16 Sa 459/14, NJOZ 2015, 782; BAG, NJW 2001, 1962, NZA 2001, 653.

23 LAG Düsseldorf, Teilurt. v. 20.01.2015 – 16 Sa 459/14, NJOZ 2015, 782.

24 BAG, NJW 2001, 1962, NZA 2001, 653.

25 EuGH, Urt. v. 10.04.2014 – C-247/11 P und C-253/11 P, NZKart 2014, 181, 184, Rn. 152 und 157 – Areva.

26 BGH, Urt. v. 18.11.2014 – WRP 2015, 201-208, GRUR-RS 2015, 00033.

27 Taeger/Gabel/Moos/Schefzig, 3. Aufl. 2019, DS-GVO Art. 83 Rn. 83.

28 BGHZ 190, 145, – ORWI; BGH, Urt. v. 18.11.2014 – KZR 15/12, NJW 2015, 1763.

29 EuGH, EuZW 2006, 529, Rn. 60, 91 ff. – Manfredi (Rs C 295/4); EuGH, EuZW 2001, 715 Rn. 25 ff. – Courage (Rs. 453/99).

30 Nolde PinG 2017, 114 (118 f.); Eckhardt/Menz DuD 2018, 139 (143); BeckOK-Brodowski/Nowak § 41 BDSG 2018 Rn. 13.

31 Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 83, Rn. 17.

sei insoweit nicht das OWiG, sondern es seien vielmehr die Grundsätze des supranationalen Kartellsanktionsrechts anwendbar. Dass dies gewollt sei, habe der europäische Gesetzgeber etwa in Erwägungsgrund 150 zur DS-GVO zum Ausdruck gebracht. Denn darin heißt es, dass im Fall einer Geldbuße gegen Unternehmen der Begriff „Unternehmen“ i.S.d. Art. 101 und 102 AEUV verstanden werden solle. Das supranationale europäische Kartellrecht gehe bei Verstößen gegen Art. 101 und 102 AEUV von einer unmittelbaren Verantwortlichkeit der Unternehmen aus. Danach hafte der Verband unmittelbar für den Verstoß, gleichgültig, welche natürliche Person für ihn gehandelt habe. Eine Kenntnis oder Anweisung der Geschäftsführung oder die Verletzung der Aufsichtspflicht sei nicht erforderlich.³²

Ebenso wies auch die Datenschutzkonferenz (DSK) in einer Entschließung vom 03. April 2019 darauf hin, dass Unternehmen im Rahmen von Art. 83 DS-GVO für schuldhaftige Datenschutzverstöße ihrer Beschäftigten haften. Dabei sei nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Zurechnungseinschränkende Regelungen im nationalen Recht würden dem widersprechen.³³

Das Landgericht (LG) Berlin hingegen erachtet die Vorschriften des OWiG für anwendbar. Im konkreten Fall ging es um einen Bußgeldbescheid in Höhe von rund 14,5 Mio. Euro, den die Berliner Beauftragte für den Datenschutz und Informationsfreiheit (BerlBfDI) gegen die Deutsche Wohnen SE wegen eines Verstoßes gegen die DS-GVO, namentlich eines unzureichenden Löschkonzepts, verhängt hatte. Auf den hiergegen eingelegten Einspruch des Unternehmens hat das Landgericht Berlin das Verfahren mit Beschluss vom 18.02.2021 eingestellt.³⁴ Der Bußgeldbescheid sei mangels Angaben zu konkreten Tathandlungen eines Organs des Unternehmens unwirksam. Das LG Berlin setzt sich damit in Widerspruch zu der Auffassung sämtlicher deutscher Datenschutzaufsichtsbehörden sowie zum Urteil des LG Bonn. Die Staatsanwaltschaft Berlin hat nunmehr im Einvernehmen mit der BerlBfDI Beschwerde gegen den Beschluss eingelegt.³⁵

Gegen die Auffassung des LG Berlin lässt sich anführen, dass die DS-GVO zwar in Art. 83 Abs. 8 die Anwendung nationalen Rechts ermöglicht. Um allerdings die Ziele der DS-GVO effektiv erreichen zu können, sind die nationalen Vorschriften europarechtskonform auszulegen. Wären hier die nationalen Regelungen, namentlich § 30 OWiG anwendbar, würde das strenge Sanktionssystem, das die DS-GVO vorsieht, erheblich abgeschwächt werden. Demnach müssen die Grundsätze des supranationalen Kartellsanktionsrechts anwendbar sein, sodass die Verhängung eines Bußgeldes gegen das Unternehmen wegen eines Datenschutzverstoßes von sonstigen Mitarbeitern grundsätzlich möglich sein dürfte.³⁶

2. Verhängung von Bußgeldern gegen die Leitungsperson/ den Mitarbeiter

Ausnahmsweise ist nach Auffassung der DSK das Verhalten eines Beschäftigten dem Unternehmen nicht zuzurechnen, sofern es sich um einen Exzess des Beschäftigten handele. Denn der Beschäftigte lege bei einem Exzess die Zwecke der

Verarbeitung selbst fest, sodass er sich selbst zum Verantwortlichen für die Datenverarbeitung mache.³⁷ In solchen Fällen ist die Verhängung eines Bußgeldes direkt gegenüber dem Beschäftigten denkbar. Derartige Mitarbeiterexzesse wurden durch die Aufsichtsbehörden bereits geahndet. So verhängte der Landesbeauftragte für den Datenschutz und die Informationssicherheit Baden-Württemberg ein Bußgeld gegen einen Polizeibeamten, der im Dienst erlangte Daten zu privaten – und damit von ihm selbst festgelegten – Zwecken verarbeitete.³⁸

In der Literatur wird unter Berufung auf den Wortlaut von Art. 83 DS-GVO, dass als Adressat der Geldbuße ausschließlich Verantwortliche und Auftragsverarbeiter genannt seien, vertreten, dass ein Bußgeld gegen den betrieblichen Datenschutzbeauftragten grundsätzlich ausgeschlossen sei.³⁹ Dem Datenschutzbeauftragten werde in der DS-GVO gerade keine eigene Verantwortlichkeit zugewiesen.⁴⁰ Dies ergebe sich aus Art. 39 Abs. 1 lit. b) DS-GVO; denn der Schutzzweck der Vorschrift sei so ausgestaltet, dass nicht jeder Verstoß verhindert werden soll, der Datenschutzbeauftragte also grundsätzlich nicht haften dürfe.⁴¹ Anders könnte dies bei einem Exzess des Datenschutzbeauftragten zu beurteilen sein, da sich auch der Datenschutzbeauftragte somit zum Verantwortlichen machen würde und so auch nach Art. 83 DS-GVO selbst möglicher Adressat des Bußgeldes wäre.

Nach einer Auffassung soll im Übrigen die Verhängung eines Bußgeldes gegen eine natürliche Person nur bei Verstoß gegen die Pflichten in Art. 83 Abs. 5 und 6 DS-GVO in Betracht kommen.⁴² Andere lehnen die Verhängung eines

32 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20, NRWE Rn. 49 ff.; so auch Taeger/Gabel/Moos/Schefzig, 3. Aufl. 2019, DS-GVO Art. 83 Rn. 81-90; es genüge, dass irgendein Mitarbeiter des Unternehmens gehandelt hat, der nicht einmal namentlich bekannt sein muss. Faust/Spittka/Wybitul, ZD 2016, 120, 121; vgl. Bayerisches Landesamt für Datenschutzaufsicht, Kurzpapier 7 zur DS-GVO – Sanktionen nach der DS-GVO.

33 Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20190405_Entschliessung_Unternehmenshaftung.pdf.

34 526 OWi LG) 212 Js-OWi 1/20 (1/20), Pressemitteilung der Deutsche Wohnen SE vom 23.02.2021, abrufbar unter: <https://www.deutsche-wohnen.com/ueber-uns/presse-news/pressemitteilungen/landgericht-berlin-stellt-bussgeldverfahren-gegen-deutsche-wohnen-ein/>

35 Pressemitteilung des BerlBfDI vom 03.03.2021, abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210303-PM-Deutsche_Wohnen.pdf.

36 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20, NRWE Rn. 49 ff.; Taeger/Gabel/Moos/Schefzig, 3. Aufl. 2019, DS-GVO Art. 83 Rn. 81-90; Faust/Spittka/Wybitul, ZD 2016, 120, 121; Paal, RDV 2021, 71, 73; Bayerisches Landesamt für Datenschutzaufsicht, Kurzpapier 7 zur DS-GVO – Sanktionen nach der DS-GVO.

37 Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20190405_Entschliessung_Unternehmenshaftung.pdf.

38 Pressemitteilung des Landesbeauftragten für Datenschutz und Informationssicherheit Baden-Württemberg vom 18.06.2019, abrufbar unter: <https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-erstes-bussgeld-gegen-polizeibeamten/>

39 Eßer/Steffen, CR 2018, 289 (290 f.); Nils Steffen, Zivilrechtliche Haftung von Datenschutzbeauftragten für Bußgelderhaftung für „durchge-reichte“ Bußgelder nach der DS-GV, DuD 2018, 145-150.

40 Thiel/Wybitul/Zimmer-Helfrich (Interview): Bußgelder wegen Datenschutzverstößen – aus Sicht von Aufsichtsbehörden und Unternehmen, ZD 2020 3, (4); Eßer/Steffen, CR 2018, 289 (290 f.).

41 BeckOK DatenschutzR/Holländer, 35. Ed. 01.08.2020, DS-GVO Art. 83 Rn. 8.1; Steffen, DuD 2018, 145 (150); Eßer/Steffen, CR 2018, 289 (290 f.).

42 Bergt, in: Kühling/ Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 83 Rn. 11.

Bußgeldes gegen die für das Unternehmen handelnde Person grundsätzlich ab,⁴³ andere halten dies nur im Anwendungsbereich von § 130 OWiG, d.h. gegenüber Leitungspersonen, für zulässig.⁴⁴ Eine Pflichtverletzung i.S.d. §§ 93 Abs. 2 AktG, 43 Abs. 2 GmbHG kann vorliegen, wenn Geschäftsleitungsmitglieder selbst gegen datenschutzrechtliche Bußgeldvorschriften verstoßen, oder wenn sie gem. §§ 130, 30, 9 OWiG eine Aufsichtspflichtverletzung begehen, indem sie zulassen, dass in ihrem Verantwortungsbereich Verstöße gegen datenschutzrechtliche Bestimmungen vorgenommen werden.⁴⁵

3. Regress der Gesellschaft gegen die Geschäftsleitung oder Beschäftigte

Art. 83 DS-GVO regelt die Voraussetzungen, nach denen Aufsichtsbehörden Geldbußen verhängen können. Darin sind auch die mögliche Höhe eines Bußgeldes sowie Anhaltspunkte für die Faktoren, die bei der Bemessung der Höhe zu berücksichtigen sind, genannt. Die Vorschrift enthält keine Regelungen zu möglichen Rückgriffsansprüchen. Vielmehr betrifft Art. 83 DS-GVO das Verhältnis zwischen den Adressaten eines Bußgeldes, den Aufsichtsbehörden und dem Verantwortlichen bzw. Auftragsverarbeiter.⁴⁶

Demgegenüber regeln Art. 82 Abs. 1 ff. DS-GVO die Voraussetzungen, unter denen Verantwortliche oder ein Auftragsverarbeiter gegenüber Betroffenen auf Schadensersatz haften, sowie ihre Regressansprüche untereinander. Ausweislich der systematischen Stellung der Absätze bezieht sich dieser Innenregress nicht auf Bußgelder. Art. 83 DS-GVO fehlt eine entsprechende Regelung, was dafür spricht, dass der Gesetzgeber für Bußgelder eine abweichende interne Haftungsverteilung durch die Beteiligten als nicht sachgerecht erachtet hat.

Im dargestellten Urteil des LAG Düsseldorf wurde der Regress des Unternehmens gegen die Geschäftsleitung aufgrund eines Bußgeldes wegen eines Kartellrechtsverstößes abgelehnt. Die vom Gericht getroffenen Erwägungen sind auf DS-GVO-Bußgelder übertragbar. In vergleichbarer Weise trifft im Datenschutzrecht der Normgeber in Art. 83 DS-GVO (und §§ 30, 130 OWiG) eine ausdrückliche Entscheidung über den möglichen Bußgeldadressaten. Demnach kann das Bußgeld gegen das Unternehmen als Verantwortlichen oder Auftragsverarbeiter oder eben – nach nicht unumstrittener Auffassung – zumindest für bestimmte Verstöße gegen eine für diese handelnde Person verhängt werden.⁴⁷ Würde man einen zivilrechtlichen Regress des Unternehmens gegen den Mitarbeiter uneingeschränkt zulassen, würde die Entscheidung des Normgebers jedenfalls unterlaufen, bestimmtes Fehlverhalten auf der Ebene des Bußgeldadressaten zu sanktionieren.

Gegenüber Unternehmen ist ausweislich des Wortlautes der Vorschrift eine Bemessung des Bußgeldes anhand des Jahresumsatzes möglich; bei natürlichen Personen ist – theoretisch – ein Bußgeld bis zu 20 Mio. Euro möglich. Hier ist die gesetzliche „Privilegierung“ der natürlichen Person zwar nicht so offensichtlich wie im Kartellrecht. Nach § 81 Abs. 1 S.1 GWB dürfen kartellrechtliche Geldbußen gegen natürliche Personen maximal EUR 1 Mio. erreichen. Es wird auch nicht deutlich, ob die natürliche Person hier nicht nur

als eigenverantwortlich und im Unternehmenskontext ggf. im Exzess zu den ihr obliegenden Verantwortlichkeiten handelnd oder als paralleler Bußgeldadressat neben dem Unternehmen angesehen wird.

Es findet aber auf der Ebene der Festsetzung des Bußgeldes durch die Aufsichtsbehörde eine Differenzierung statt. Bei Unternehmen ist die Bemessung nach dem Umsatz aufgrund des Bußgeldkonzepts der DSK gängige Praxis; bei natürlichen Personen ist die Aufsichtsbehörde aufgrund von Erwägungsgrund Nr. 150 zur DS-GVO verpflichtet, die wirtschaftliche Lage der jeweiligen Person zu berücksichtigen, wenn diese nicht als Unternehmen agiert.⁴⁸ Die Aufsichtsbehörde bestimmt also den Adressaten des Bußgeldes und die Höhe des auf den Adressaten ausgerichteten Bußgeldes. Dieser Gedanke spiegelt sich im Bußgeldkonzept der Datenschutzkonferenz (DSK)⁴⁹ wider. Darin ist festgelegt, dass bei der Bemessung des Bußgeldes gegenüber einem Unternehmen stets die konkreten, tatbezogenen Umstände des Einzelfalls, wie etwa der Grad der Verantwortung (vgl. Art. 83 Abs. 2 Satz 2 DS-GVO) als Faktoren zur Bemessung der Höhe der Geldbuße berücksichtigt werden. Das – nach hier vertretener Auffassung – überzeugendste Argument gegen einen Regress ist allerdings der Sinn und Zweck von Geldbußen, der auch in der genannten Rechtsprechung immer wieder aufgegriffen wird und auf DS-GVO-Bußgelder übertragen werden kann.⁵⁰ Auch durch Geldbußen wegen DS-GVO-Verstößen soll der durch die Aufsichtsbehörde identifizierte Täter durch eine eindringliche Pflichtenmahnung davon abgehalten werden, die geahndeten bzw. gleichartige Zuwiderhandlungen künftig erneut zu begehen. Die bisherige Praxis der Bußgeldverhängung zeigt zudem, dass Bußgeldern gegen Einzelpersonen bislang nur in den Ausnahmefällen des Mitarbeiterexzesses und auch keine parallelen Bußgelder gegen Unternehmen und Beschäftigte oder Leistungspersonen verhängt wurden. Entsprechend bewegen sich die gegen Privatpersonen wegen DS-GVO Verstößen verhängten Geldbußen in anderen Größenordnungen.⁵¹

43 Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 1. Aufl. 2019, Art. 83 Rn. 47 f.

44 Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 83, Rn. 17.

45 Für kartellrechtliche Pflichtverletzungen, vgl. Stancke, BB 2020, 1667, 1668.

46 Bußgelder gegen Zertifizierungs- und Überwachungsstellen i.S.v. Art. 83 Abs. 4 lit. b) und c) werden im Folgenden nicht behandelt.

47 Bergt, in: Kühling/ Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 83 Rn. 11 für die Pflichten in Art. 83 Abs. 5 und 6; Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 83, Rn. 17 soweit § 130 OWiG einschlägig ist, im Übrigen eine Haftung des gegen die Verordnung verstoßenden Mitarbeiters selbst ablehnend; eine Haftung von Personen ablehnend Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 1. Aufl. 2019, Art. 83 Rn. 47 f.; in Bezug auf den betrieblichen Datenschutzbeauftragten eine Haftung desselben ablehnend Eßer/Steffen, CR 2018, 289 (290 f.); Nils Steffen, Zivilrechtliche Haftung von Datenschutzbeauftragten für Bußgelder – Haftung für „durchgereichte“ Bußgelder nach der DS-GV, DuD 2018, 145-150.

48 LG Bonn, Urteil v. 11.11.2020 – 29 OWi 1/20, NRW Rn. 66.

49 Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf.

50 Ausführlich: Eßer/Steffen, CR 2018, 289 (292 f.) zum Regress gegen den betrieblichen Datenschutzbeauftragten mit dem Argument, dass es für eine zivilrechtliche Haftung des Datenschutzbeauftragten regelmäßig an einem kausalen Schaden fehle, da ein Bußgeld nicht vom Schutzzweck des Art. 39 DS-GVO erfasst sei.

51 <https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-erstes-bussgeld-gegen-polizeibeamten/>.

Die gesetzgeberische Wertung, dass Normadressat der Geldbuße das Unternehmen und nicht die für das Unternehmen handelnde Person ist, ist daher im Zivilrecht zu berücksichtigen.⁵² Ein zivilrechtlicher Regress, der den Adressaten des Bußgeldes von der Pflichtenmahnung befreit, würde diesen Zweck unterlaufen.⁵³ Auch bei datenschutzrechtlichen Bußgeldern liegt der Vorwurf häufig in einem Organisationsverschulden in Gestalt einer nicht ausreichenden Kontrolle der handelnden Personen durch das Unternehmen. Nur durch die finale Bußgeldbelastung bei dem Unternehmen wird dem Sinn und Zweck des Sanktionsregimes mit der Aufteilung der Verantwortungssphären Rechnung getragen.⁵⁴ Sollte ein Regress für DS-GVO-Bußgelder dennoch für zulässig erachtet werden, dürfte vor dem Hintergrund der auf die konkrete Gesellschaft ausgerichteten Höhe der Bußgelder und der Treue- und Fürsorgepflicht der Gesellschaft aber eine Beschränkung der Regresshöhe – ähnlich wie im Kartellrecht durch Teile der Literatur gefordert⁵⁵ – auch im Datenschutzrecht unverzichtbar sein.

Überträgt man die aus dem Kartellrecht stammende Rechtsprechung auf die nach Art. 83 DS-GVO gegenüber einem Unternehmen verhängten Geldbußen, wäre ein Regress gegenüber Beschäftigten nicht, gegenüber Leitungspersonen nur ausnahmsweise möglich. In Ausnahmefällen, in denen eine abschließende Klärung des Sachverhalts und der Verursachungsbeiträge im Rahmen des Bußgeldverfahrens nicht erfolgte,⁵⁶ mögen Szenarien denkbar sein, in denen ein Bußgeld als erstattungsfähiger Schaden angesehen werden könnte.

Dies deckt sich mit dem Sinn und Zweck von DS-GVO-Bußgeldern, denn diese sollen gemäß Art. 83 Abs. 1 DS-GVO wirksam, verhältnismäßig und abschreckend sein. Abschreckend wären sie gleichwohl nicht, wenn sich der Bebußte schadlos halten könnte. Vielmehr soll eine Geldbuße speziellpräventiv wirken und so den jeweiligen, durch die Aufsichtsbehörde identifizierten Täter davon abhalten, in Zukunft die geahndete oder gleichartige Zuwiderhandlungen gegen Rechtsvorschriften zu begehen.⁵⁷ Ihm soll also eine nachdrückliche Pflichtenmahnung erteilt und das finanzielle Risiko einer Zuwiderhandlung bewusst gemacht werden. Eine zivilrechtliche Vereinbarung, die den Bebußten von der Pflichtenmahnung befreit, würde diesen Zweck unterlaufen.⁵⁸

4. Regress der Leitungsperson/ des Beschäftigten gegen das Unternehmen

In Fällen des Mitarbeiterexzesses ist die Aufsichtsbehörde angehalten, das Bußgeld nicht gegenüber dem Unternehmen, sondern direkt gegenüber dem Mitarbeiter zu verhängen.

Für diese Fälle kann ein Regress gegen das Unternehmen nicht in Betracht kommen, um den Zweck der eindringlichen Pflichtenmahnung nicht in Frage zu stellen, die den Täter davon abhalten soll, die geahndeten bzw. gleichartige Zuwiderhandlungen künftig erneut zu begehen. Pauschale Freistellungsvereinbarungen bezogen auf gegen eine Person verhängte Bußgelder zugunsten von Leitungspersonen wären vor dem Hintergrund unwirksam.

5. Regress des Verantwortlichen gegen den Auftragsverarbeiter

Durch die Auftragsverarbeitung ermöglicht die DS-GVO dem Verantwortlichen, Datenverarbeitungsvorgänge auszulagern, um sich durch die Aufteilung der Verarbeitungsfunktionen Effizienzvorteile zu erschließen.⁵⁹ Dies kann beispielsweise durch ein IT-Outsourcing geschehen. In der Konstellation stellt der Auftragsverarbeiter insoweit keinen anderen Verantwortlichen dar, vielmehr verarbeitet er die Daten im Namen des Verantwortlichen.⁶⁰ Die Verarbeitung wird dem Verantwortlichen zugerechnet, daher ist der Auftragsverarbeiter gegenüber dem Verantwortlichen auch weisungsgebunden.⁶¹ Der Verantwortliche kann allerdings die Entscheidung über die technisch-organisatorischen Fragen der Verarbeitung auf den Auftragsverarbeiter delegieren.⁶² Dies ist sinnvoll, da der Auftragsverarbeiter regelmäßig weitreichendere informationstechnische Kenntnisse hat. Nach Art. 28 Abs. 1 DS-GVO ist der Verantwortliche verpflichtet, nur mit Auftragsverarbeitern zu arbeiten, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen⁶³ – hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen umgesetzt werden, damit die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet.

Gleichwohl normiert die DS-GVO auch ausdrücklich eigene gesetzliche Pflichten und damit eine eigene Verantwortlichkeit des Auftragsverarbeiters. So ist er beispielsweise verpflichtet, die Weisungen des Verantwortlichen zu befolgen (Art. 29 DS-GVO), ein Verarbeitungsverzeichnis zu führen (Art. 30 Abs. 2 DS-GVO) sowie geeignete technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung zu gewährleisten (Art. 32 DS-GVO). Ferner trifft ihn die Pflicht zur Zusammenarbeit mit den Aufsichtsbehörden (Art. 31 DS-GVO) und zur Meldung von sogenannten „Datenpan-

52 LAG Düsseldorf Schlussurt. v. 27.11.2015 – 14 Sa 800/15, BeckRS 2016, 65558 Rn. 164, beck-online.

53 LAG Rheinland-Pfalz Ur. v. 26.01.2010 – 3 Sa 497/09, BeckRS 2010, 68132, beck-online; kritisch u.a.: Backhaus/Brand, jurisPR-HaGesR 4/2021 Anm. 5.

54 So für Verstöße im Kartellrecht argumentierend: LAG Düsseldorf, Teilurt. v. 20.01.2015 – 16 Sa 459/14, NJOZ 2015, 782, 790.

55 MüKoAktG/Spindler, 5. Aufl. 2019, AktG § 93 Rn. 194; Hüffer/Koch/Koch, 15. Aufl. 2021, AktG § 93 Rn. 48, vgl. Fn 19.

56 Vgl. die Ausführungen von Stancke, BB 2020, 1667, 1668, dass die kartellrechtliche Bußgeldentscheidung nicht zwingend eine präjudizielle Wirkung für den Zivilrechtsstreit haben muss.

57 Sinngemäß Thiel/Wybitul/Zimmer-Helfrich (Interview): Bußgelder wegen Datenschutzverstößen – aus Sicht von Aufsichtsbehörden und Unternehmen, ZD 2020, 3; ausdrücklich so bezüglich StVO-Bußgeld: LAG Rheinland-Pfalz Ur. v. 26.01.2010 – 3 Sa 497/09, BeckRS 2010, 68132, beck-online.

58 So bezüglich StVO-Bußgeld: LAG Rheinland-Pfalz Ur. v. 26.01.2010 – 3 Sa 497/09, BeckRS 2010, 68132, beck-online, a.A. Taeger/Gabel/Moos/Schefzig, 3. Aufl. 2019, DS-GVO Art. 83 Rn. 83 für die Wirksamkeit einer vertraglichen Regressklausel im Verhältnis Auftragsverarbeiter und Verantwortlichem und gemeinsam Verantwortlichen.

59 Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 28 DS-GVO Rn. 8.

60 Erwägungsgrund 81 zur DS-GVO.

61 Kurzpapier Nr. 13 der DSK, S. 1, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.

62 Kurzpapier Nr. 13 der DSK, S. 2, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.

63 Erwägungsgrund 81 zur DS-GVO.

nen“ an den Verantwortlichen (Art. 33 Abs. 2 DS-GVO). Verletzt der Auftragsverarbeiter diese eigenen gesetzlichen Pflichten, treffen ihn die Haftungs- und Bußgeldvorschriften nach Art. 82, 83 DS-GVO unmittelbar selbst. Dies kommt im Vergleich zur früheren Rechtslage einem „Paradigmenwechsel“ gleich⁶⁴ und bedeutet in Zeiten der Verlagerung von Prozessen und Daten in die Cloud und der zunehmenden Gefährdung durch Cyberisiken auch für Auftragsverarbeiter ein erheblich gesteigertes Risikopotential.

Da das Konstrukt der Auftragsverarbeitung nicht den oben genannten Fallgruppen zuzuordnen ist, kann die aufgefundene Rechtsprechung nicht uneingeschränkt übertragen werden. So sieht das Gesetz den Auftragsverarbeiter bei Verstößen gegen seine datenschutzrechtlichen Pflichten als möglichen Bußgeldadressaten vor, Art. 83 Abs. 4 ff. DS-GVO, Erwägungsgrund 79 zur DS-GVO betont, dass es bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter – auch mit Blick auf die Überwachungsmaßnahmen und die sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuordnung der Verantwortlichkeiten bedarf. Anhand der Zuweisung der Verantwortungsbereiche soll die Aufsichtsbehörde in die Lage versetzt werden, den richtigen Bußgeldadressaten zu identifizieren. Ebenso spricht die an die individuellen Verhältnisse des Adressaten angepasste Höhe des Bußgeldes dafür, dass es sich um eine abschließende Entscheidung der Aufsichtsbehörde handelt. Daher würde das Zivilrecht die Ermessensentscheidung der Aufsichtsbehörde „korrigieren“, was nach dem Sinn und Zweck von Bußgeldern nicht gewollt sein kann. Zudem legt das Gesetz fest, dass die Bemessung des Bußgeldes anhand des Umsatzes und unter Berücksichtigung der individuellen Verhältnisse zu erfolgen hat, wozu etwa eine drohende Zahlungsunfähigkeit des Adressaten zählt.⁶⁵ Daher könnte der Auftragsverarbeiter in Anbetracht der enormen Höhe eines gegen einen Verantwortlichen verhängten und auf dessen Verhältnisse angepassten Bußgeldes in die Gefahr der Insolvenz geraten, wenn er verpflichtet wäre, die Geldbuße zu übernehmen. Eine drohende Zahlungsfähigkeit von Dritten wird bei Festsetzung der Bußgeldhöhe durch die Aufsichtsbehörde nicht berücksichtigt. Auch dies kann vom Gesetzgeber nicht gewollt sein, sodass von einer persönlichen Sanktionierung, die nicht im Wege zivilrechtlicher Vereinbarungen übertragen werden kann, auszugehen sein dürfte.

Ist der Verantwortliche also der Auffassung, dass den Auftragsverarbeiter eine wesentliche Verantwortung trifft, ist im Rahmen der vorherigen Anhörung durch die Aufsichtsbehörde auf die entsprechende Verantwortlichkeit des Auftragsverarbeiters hinzuweisen und das Risiko einer Nicht-Erstattungsfähigkeit des Bußgeldes im Rahmen der Abstimmungen im Vorfeld zu berücksichtigen. Die Aufsichtsbehörde hat in die Aufteilung der Verantwortungsbereiche von „außen“ nur eingeschränkt Einblick.

Anders als im Kartellrecht wurde für die DS-GVO-Bußgelder bislang nicht darauf abgestellt, dass sich der Ermittlungsaufwand für die Aufsichtsbehörden durch die Anordnung einer gesamtschuldnerischen Haftung mehrerer (Gruppen-) Gesellschaften verringert und die Kommission eine persönliche Beteiligung (der Vertreter der Muttergesellschaft) nicht nach-

weisen muss.⁶⁶ Bei der Verhängung einer Geldbuße gegen den Verantwortlichen oder den Auftragsverarbeiter muss sich die Aufsichtsbehörde gerade Gedanken über den Tatbeitrag des jeweiligen Unternehmens machen. Die kartellrechtlichen Überlegungen können daher auf das Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter nicht eins zu eins übertragen werden. Eine gesamtschuldnerische Haftung ordnet die DS-GVO ausdrücklich nur für die Ansprüche eines Betroffenen auf Schadensersatz gegen Verantwortlichen und Auftragsverarbeiter (vgl. Art. 84 Abs. 4 DS-GVO), nicht aber für die Verhängung von Bußgeldern an. Gleichwohl könnte nach nicht unumstrittener Auffassung der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) die Muttergesellschaft für Datenschutzverstöße ihrer Tochtergesellschaften belangt werden.⁶⁷

Denkbar wäre, ausnahmsweise einen Regress zuzulassen, wenn der Verantwortliche einen in informationstechnischer Hinsicht sachkundigen Auftragsverarbeiter beauftragt und aufgrund eines Fehlers des Auftragsverarbeiters ein Bußgeld gegen den Verantwortlichen verhängt wird. Hat der Verantwortliche alles ihm Zumutbare getan, um seinen oben genannten datenschutzrechtlichen Pflichten nachzukommen, wie etwa eine ausreichende Vereinbarung getroffen und den Auftragsverarbeiter objektiv sorgfältig und gewissenhaft ausgewählt und kontrolliert, und kommt es dennoch zu einem Datenschutzverstoß, wäre dem Verantwortlichen insoweit kein Vorwurf zu machen.

Die Aufsichtsbehörde wäre in einem solchen Fall gehalten, die Verursachungsbeiträge aufzuklären und mit dem Bußgeld den Auftragsverarbeiter und nicht den Verantwortlichen zu adressieren. Sollte dies nicht geschehen, ist zweifelhaft, ob ein Regress zugelassen werden sollte. Der Verantwortliche müsste zunächst jedenfalls die Bußgeldentscheidung mit den zulässigen Rechtsmitteln angreifen. Es ist nicht ohne weiteres ersichtlich, welche Verteidigungsmittel ein Verantwortlicher nicht vorbringen könnte oder dürfte, um von der behördlichen Einschätzung abweichende Verursachungs- oder Verschuldensbeiträge von Verantwortlichem und Auftragsverarbeiter geltend zu machen. Um eine reibungslose Kommunikation mit den Aufsichtsbehörden sowie den Gerichten zu gewährleisten, sollten vertragliche Geheimhaltungspflichten so ausgestaltet werden, dass die Offenlegung von Informationen gegenüber den Aufsichtsbehörden und Gerichten möglich bleibt. Die Bußgeldandrohung ist zentral, um beim Verantwortlichen die pflichtgemäße Wahrnehmung seiner Kontroll- und Überwachungspflichten durchzusetzen. Das Verhältnis von Verantwortlichem und Auftragsverarbeiter ist nur bedingt mit der Fallgestaltung vergleichbar,

64 Ingold, in Sydow: DS-GVO, 2. Aufl., 2018, Art (Fußn. 7), Art. 28 Rn. 13.

65 Thiel/Wybitul/Zimmer-Helfrich (Interview): Bußgelder wegen Datenschutzverstößen – aus Sicht von Aufsichtsbehörden und Unternehmen, ZD 2020 3, (4).

66 Vgl. EuGH, EUZW 2009, S. 816, Rn 59 f. – Akzo Nobel (C 97/08 P).

67 Art.-29-Datenschutzgruppe, WP 253, S. 6; Datenschutzkonferenz, Kurzpapier Nr. 2 – Aufsichtsbefugnisse/Sanktionen, S. 2, vgl. Moos/Schefzig, in: Taeger/Gabel, 3. Aufl. 2019, DS-GVO Art. 83 Rn. 86 zu der Aussage, dass gesamtschuldnerische Haftung nach ständiger Rechtsprechung des EuGH möglich ist, z.B. EuGH, Urt. v. 20.1.2011 – C-90/09 P, Slg. 2011, I-1, Rn. 85, 89; zur Durchgriffs-Haftung ausführlich Holländer, in: Wolff/Brink, BeckOK DatenschutzR, Art. 83 Rn. 12.

dass sich der Bußgeldadressat fachkundigen Rat bei einem Berater einholt, um der Gefahr einer Sanktionierung zu begegnen und aufgrund der nicht sachgerechten Beratung ein Bußgeld verhängt wird. Zwar kann es im Fall einer Auftragsverarbeitung sein, dass der Verantwortliche gerade deshalb einen Auftragsverarbeiter beauftragt, weil er selbst nicht ausreichende informationstechnische Kenntnisse, beispielsweise bezüglich der Datensicherheit, besitzt. Daher verlässt sich auch hier der Bebußte gewissermaßen berechtigterweise auf die Fachkunde eines anderen. Der Schwerpunkt der Leistung wird regelmäßig aber nicht auf der Beratungsleistung liegen und die Kontroll- und Überwachungspflicht bleibt kraft gesetzlicher Anordnung beim Verantwortlichen.

6. Regress zwischen gemeinsam Verantwortlichen

Die gemeinsame Verantwortlichkeit ist eine Konstellation, die aufgrund ihrer Besonderheit im Datenschutzrecht nicht mit den in der Rechtsprechung behandelten Sachverhalten vergleichbar ist. Art. 26 DS-GVO bestimmt, dass gemeinsam Verantwortliche in einer Vereinbarung in transparenter Form festlegen müssen, wer von ihnen welche Pflichten nach der DS-GVO erfüllt. Die Vereinbarung soll also einer klaren Zuteilung der Verantwortlichkeiten dienen, womit zugleich der zunehmend komplexeren Realität von informationstechnischen Vorgängen Rechnung getragen wird. Sie soll dadurch Rechtssicherheit bezüglich Verantwortung und Haftung gewährleisten.⁶⁸ Die Verantwortungsbereiche müssen nachvollziehbar, also ohne weiteres erkennbar und verifizierbar sein.⁶⁹ Diesbezüglich kann der Erwägungsgrund 79 zur DS-GVO herangezogen werden; die Aufsichtsbehörde soll anhand der Vereinbarungen feststellen können, welche Zuteilung der Verantwortlichkeiten die Beteiligten gewählt haben, um anhand dessen den zutreffenden Bußgeldadressaten zu identifizieren. Erforderlich ist, dass die Vereinbarung die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen widerspiegeln.

Sofern die aufsichtsbehördliche Entscheidung als final anzusehen ist, dürfte hier ein Regress regelmäßig unzulässig sein. Denn Sinn des Bußgeldes ist es, genau den durch die Aufsichtsbehörde identifizierten Täter für sein Fehlverhalten zu sanktionieren; es kann nicht gewollt sein, diese abschließende Entscheidung durch zivilrechtliche Vereinbarungen auszuhebeln.⁷⁰ Dies verdeutlicht, dass eine detaillierte, die tatsächlichen Umstände widerspiegelnde Vereinbarung zwischen den gemeinsam Verantwortlichen unverzichtbar ist, um nicht für das Fehlverhalten der anderen Partei sanktioniert zu werden. Sollten die Parteien dies allerdings versäumt haben, ist in dieser Konstellation noch am ehesten denkbar, dass ein berechtigtes Interesse besteht, eine Bußgeldentscheidung im Innenverhältnis zwischen den Parteien zivilrechtlich zu überprüfen.

7. Vertragliche Regelungsmöglichkeiten

Daraus folgt, dass pauschale Freistellungsvereinbarungen bezogen auf Bußgelder nach hier vertretener Auffassung unwirksam wären. In Ausnahmefällen, in denen eine ab-

schließende Klärung des Sachverhalts und der Verursachungsbeiträge im Rahmen des Bußgeldverfahrens nicht oder fehlerhaft erfolgte, könnte ein Bußgeld als erstattungsfähiger Schaden angesehen werden. Aus Sicht anderer Beteiligter als Beschäftigter, die einen Regress fürchten, bestünde insoweit ein Bedürfnis für eine von der gesetzlichen Regelung abweichende vertragliche Haftungsregelung. Im Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter oder von gemeinsam Verantwortlichen hätte eine vertragliche Klarstellung, dass unter die vereinbarte Haftungsgrenze auch Ansprüche auf Erstattung von Bußgeldern fallen, den Nachteil, dass man sich vor dem Hintergrund der bisherigen Rechtsprechung eine Argumentation zur Nicht-Erstattungsfähigkeit von Bußgeldern abschneidet und die Haftungsregelung im Übrigen dem Risiko der Gesamtwirksamkeit aussetzt. Es verbleibt im Übrigen die praktische Herausforderung, dass eine für die vertragliche Leistungsbeziehung ansonsten als interessengerecht angesehene Haftungsbegrenzung angesichts der unterschiedlichen Höhe der potentiellen Bußgeldandrohungen zu verhandeln wäre und eine unterschiedliche wirtschaftliche Leistungsfähigkeit der Beteiligten zu berücksichtigen hätte.

Auch handelt es sich bei einem auf § 280 BGB basierenden Anspruch wegen der schuldhaften Verletzung vertraglicher Pflichten eines Unternehmens als Verantwortlicher gegen einen Auftragsverarbeiter um keine mit dem Innenausgleich nach § 426 BGB als Folge einer gesamtschuldnerischen Bußgeld-Haftung mehrerer Gruppenunternehmen vergleichbare Konstellation.

Dies spricht dagegen, in die vertragliche Regelung zur Haftung für Schäden ausdrückliche Aussagen zur (Höhe der) Erstattungsfähigkeit von Bußgeldern aufzunehmen.⁷¹

III. Fazit

Vieles spricht dafür, dass Geldbußen wegen DS-GVO-Verstößen von dem – von der Aufsichtsbehörde ausgewählten – Adressaten des Bußgeldes selbst zu tragen sind und eine Korrektur der Entscheidung der Aufsichtsbehörde über das Zivilrecht unzulässig ist. Denn die von den Gerichten in kartellrechtlichen Sachverhalten angeführten Argumente lassen sich im Grundsatz auf Geldbußen wegen Datenschutzverstößen übertragen.

Sieht man sich den grundlegenden Zweck von Bußgeldern an, müssen diese den von den Aufsichtsbehörden identifizierten Täter treffen, um dessen zukünftiges Verhalten zu beeinflussen. Die generalpräventive Wirkung der Geldbuße würde entfallen, wenn sich der eigentliche Adressat bei seinen Organmitgliedern, Beschäftigten oder Vertragspartnern ohne Weiteres entlasten könnte.⁷²

68 BeckOK Datenschutzrecht/Spoerr, Art. 26 Rn. 2.

69 BeckOK Datenschutzrecht/Spoerr, Art. 26 Rn. 5.

70 Beispielsweise Tribess, in: Beck'sches Formularbuch IT-Recht, Weitnauer/Mueller-Stöfen, 5. Aufl. 2020, 4. Vereinbarung zwischen gemeinsamen Verantwortlichen – Joint Controller Agreement, Anm. 1-30.

71 A.A. Moos/Schefzig, in: Taeger/Gabel/ 3. Aufl. 2019, DS-GVO Art. 83 Rn. 83, „eine vertragliche Regressklausel für Bußgelder erscheine wirksam“.

72 LAG Düsseldorf, Teilurt. v. 20.01.2015 – 16 Sa 459/14, NJOZ 2015, 782.

Auch würde die als grundsätzlich abschließend anzusehende Entscheidung der Aufsichtsbehörden über den Adressaten untergraben werden, wenn durch zivilrechtliche Regelungen eine Korrektur erreicht werden könnte. Eine Kontrolle und Korrektur der Bußgeld-Entscheidung ist in erster Linie den für die Überprüfung der Behördenentscheidung zuständigen Gerichten vorbehalten.⁷³ Dies gilt jedenfalls für das Verhältnis zwischen Auftragsverarbeiter und Verantwortlichem sowie zwischen mehreren gemeinsam Verantwortlichen. Hinsichtlich der Auftragsverarbeitung und der Verarbeitung in gemeinsamer Verantwortlichkeit zeigt dies die Notwendigkeit, in den getroffenen Vereinbarungen zutreffend und detailliert die Aufgaben- und Verantwortungsbereiche darzustellen, damit die Aufsichtsbehörden den richtigen Bußgeldadressaten anhand der Vereinbarung identifizieren können. Ohne eine solche Abgrenzung der Verantwortungsbereiche laufen die Parteien Gefahr, bei einem Verstoß auch ohne tatsächliche Verantwortung sanktioniert zu werden.

Es bleibt im Übrigen abzuwarten, ob und in welchen Ausnahmefällen die Gerichte in Abweichung von diesen Grundsätzen für DS-GVO-Bußgeldentscheidungen einen zivilrechtlichen Regress dennoch zulassen. Pauschale Frei-

stellungsvereinbarungen bezogen auf Bußgelder empfehlen sich vor diesem Hintergrund nicht. Diese wären unwirksam.



Dr. Stefanie Hellmich

ist Rechtsanwältin und Partner bei der Luther Rechtsanwaltsgesellschaft mbH in Frankfurt.



Kata Èles

ist Rechtsreferendarin am Landgericht Darmstadt und war bis März 2021 als wissenschaftliche Mitarbeiterin bei der Luther Rechtsanwaltsgesellschaft mbH tätig.

⁷³ Korrektur hinsichtlich der Höhe: LG Bonn, Urt. v. 11.11.2020 – 29 OWI 1/20.

Conrad Sebastian Conrad/Stefan R. Seiter

Zur inhaltlichen Ausgestaltung der Auftragsverarbeitung nach Art. 28 DS-GVO – Teil 2*

Der nur scheinbar erschöpfende Anforderungskatalog des Art. 28 DS-GVO bietet Konfliktpotenzial in gleich mehrerlei Hinsicht. So sind neben eher „formalen“ Gesichtspunkten (wie z.B. der Einheitlichkeit des Vertragswerks durch Verweis auf externe Dokumentationen) auch ganz praktisch und bisweilen wirtschaftlich elementar bedeutsame Erwä-

gungen (wie z.B. die Möglichkeit, die vertragliche Haftung einzuschränken) zu beachten. Ergänzend wird die Frage beleuchtet, wer auf Seiten des Verantwortlichen die Kontrollen gegenüber Auftragsverarbeitern durchzuführen hat und ob insbesondere der betriebliche Datenschutzbeauftragte diese Aufgabe übernehmen kann.

I. Ausschluss oder Begrenzung der Haftung

Gewissermaßen ein „Evergreen“ der Vertragsgestaltung sind – auch beim Datenschutz, ähnlich wie in anderen Rechtsgebieten – Bestimmungen, welche das rechtliche (und finanzielle) Entstehen müssen einer Partei für die Verletzung einer vertraglichen Pflicht zum Inhalt haben. Demgemäß weit verbreitet sind Versuche der Vertragsparteien, dieses Vorhaben in sprachlich entsprechende, vorteilhafte Klauseln zu gießen. Immer dort, wo aber eine mögliche Verlagerung

der juristischen Verantwortlichkeiten im Raum steht, sind auch hier wiederum gesetzliche Grenzen zu beachten.

* Wie bereits im ersten Teil (Conrad/Seiter, RDV 2021, 186) dieser Beitragsreihe ausführlich besprochen, sind der Ausgestaltung von Auftragsverarbeitungs-Verträgen (AV-Verträgen) nach Art. 28 DS-GVO in der Praxis trotz Vertragsfreiheit der Parteien gewisse Grenzen gesetzt. Diese können sich zum einen aus der AGB-Kontrolle gem. §§ 305 ff. BGB ergeben. Doch auch aus der Deutung der DS-GVO lassen sich mittelbare Vorgaben bei der Anwendung des Rechts ableiten, die es zu berücksichtigen gilt.

1. Vorgaben durch das Datenschutzrecht

Ausgangspunkt für die Beurteilung, welchen Inhalt einzelne Regelungen zur Haftung innerhalb eines AV-Verhältnisses i.S.v. Art. 28 DS-GVO haben dürfen, ist Art. 82 DS-GVO. Dieser eröffnet der betroffenen Person einen Anspruch auf Ersatz des durch eine unrechtmäßige Verarbeitung ihrer Daten verursachten Schadens¹ gegen den Verantwortlichen oder gegen den Auftragsverarbeiter (Art. 82 Abs. 1 DS-GVO), d. h. sie kann sich grds. an beide Unternehmen wenden. Die Absätze 2 und 3 präzisieren diesen Anspruch dahingehend, dass die Vertragsparteien nur in dem Umfang haften, in dem sie für den Umstand, durch den der Schaden eingetreten ist, verantwortlich sind. Dies dient wiederum einer weitgehenden Sicherung und umfassenden Durchsetzung der Rechte der betroffenen Person.²

Damit legt die Verordnung (bis hierhin) hauptsächlich den Fokus auf das sog. Außenverhältnis, also das Verhältnis zwischen Verantwortlichem oder Auftragsverarbeiter auf der einen und betroffener Person auf der anderen Seite. Darauf aufbauend bestimmt nun Abs. 4, wie sich die Vertragsparteien untereinander – also im Innenverhältnis – über den zu leistenden Schadenersatz auseinanderzusetzen haben. In der Praxis dürfte es häufig darauf hinauslaufen, dass sich die betroffene Person an ausschließlich eine der beiden Parteien aus dem AV-Vertrag wendet, mutmaßlich den – sei es regional bedingt oder kraft Sachzusammenhangs – am nächsten Greifbaren. Für diesen Fall bestimmt Abs. 5 in Art. 82 DS-GVO, dass für den Innenausgleich eine Partei berechtigt ist, von der anderen den Teil des Schadenersatzes zurückzufordern, der ihrem spezifischen Anteil an der Verantwortung für den konkreten Schaden entspricht.³ Der Innenausgleich ist in der Regel von wirtschaftlich größerer Bedeutung und wird von den Vertragsparteien selbst ausgehandelt.

Soweit die Vorschrift davon spricht, dass der Verantwortliche oder der Auftragsverarbeiter für einen durch die Verarbeitung „verursachten Schaden verantwortlich“ sein muss, darf dies nicht gleichgesetzt werden mit der Verantwortlichkeit gemäß Art. 4 Nr. 7 DS-GVO. Entgegen der missverständlichen deutschen Sprachfassung der Verordnung ist damit tatsächlich das Verschulden der Beteiligten gemeint.⁴ Im Ergebnis handelt es sich dabei um eine „spezielle deliktische Haftungsnorm“, welche durch die entsprechenden Regelungen im BGB (speziell die §§ 831 ff.) ergänzt wird.⁵ Damit sieht die DS-GVO wohl vor, dass eine anteilige Haftung der Vertragsparteien gemessen an dem konkret verursachten Schaden eintreten soll.

2. Abdingbarkeit von Art. 82 DS-GVO

Mit Verweis auf den Willen des Ordnungsgebers wird vereinzelt vertreten, dass Ausschlüsse oder Beschränkungen der Haftung auf vertraglicher Grundlage auch für leichte Verstöße generell unzulässig seien. Dies gebiete zum einen der Wortlaut von Art. 82 Abs. 3 DS-GVO, der eine Befreiung von der Haftung für den Beteiligten nur dann zulässt, wenn er nachweist, dass er in „keinerlei Hinsicht“ für den Umstand, durch den der Schaden eingetreten ist, verantwort-

lich ist.⁶ Zudem entfele ansonsten die abschreckende Wirkung, welche die Verpflichtung zum Schadenersatz entfalten soll, auch zur Einhaltung der Rechtmäßigkeit der Verarbeitung im Übrigen. Diese Vorgaben würden ausgehebelt, wenn einem Verantwortlichen oder Auftragsverarbeiter von vornherein die Haftung auch ohne speziellen Nachweis erlassen würde.⁷

Der Gegenmeinung folgend,⁸ sei zunächst und mangels spezialgesetzlicher Regelungen in der DS-GVO kein generelles Freizeichnungsverbot anzunehmen. Vielmehr seien die einzelnen vertraglichen Regelungen im Lichte der europäischen Grundrechte-Charta auszulegen. Demgemäß könnte es zulässig sein, zumindest in einem direkt mit der betroffenen Person geschlossenen (Nicht-AV-)Vertrag bestimmte verhältnismäßige Beschränkungen zur Haftung niederzulegen. Solange also der Vertrag weiterhin eine effektive Durchsetzung der Betroffenenrechte gewährleistet, sei z.B. eine Einschränkung für den Grad des Verschuldens durchaus zulässig.⁹

Mag man eine die Haftung beschränkende Regelung im AV-Vertrag an sich billigen, so dürfte dies in erster Linie dann zulässig sein, wenn die fragliche Vereinbarung unmittelbar mit den betroffenen Personen geschlossen worden ist. Da diese jedoch in den seltensten Fällen selbst Partei des AV-Vertrages sind, haben sie folglich in dieser Hinsicht keine Möglichkeit, auf die Ausgestaltung ihrer Rechte unmittelbar Einfluss zu nehmen. Die Schutzwirkung von gesetzlichen Vorschriften (hier: Art. 82 DS-GVO) muss daher ihre Geltung erst recht in einer solchen Konstellation beanspruchen. Ob der – zwischen Verantwortlichem und Auftragsverarbeiter – durch entsprechend gestalterischer Vereinbarungen vermittelte Schutz dann jedoch vom Niveau her prinzipiell höher ausfallen müsse, als wenn die betroffene Person selbst an diesem Gestaltungsprozess unmittelbar beteiligt wäre, darf bezweifelt werden. Zumindest findet eine solche Erwägung keine gesetzliche Stütze.

Unter der zuvor genannten Prämisse, dass die betroffene Person infolge transparenter Information in gewissem verhältnismäßigem Rahmen über die Geltendmachung ihrer persönlichen Rechte disponieren kann, muss es daher auch zwischen den Parteien des AV-Vertrages möglich sein, spezifische Vereinbarungen über Modalitäten der Haftung niederzulegen, sofern dadurch kein faktischer Ausschluss des Schadenersatzes (zu Lasten anderer, insbesondere der betroffenen Personen) erfolgt.

1 Vgl. Bleckat, RDV 2020, 11.

2 Siehe Frenzel, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 82 Rn. 15; Gola, in: Gola, DS-GVO Art. 82 Rn. 15.

3 Siehe Boehm, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 1. Aufl. 2019, Art. 82 Rn. 35.

4 Siehe Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Rn. 22.

5 Siehe Piltz, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, DS-GVO, Art. 82 Rn. 9.

6 Bergt, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 82 Rn. 49.

7 Siehe Spiecker, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 1. Aufl. 2019, DS-GVO Art. 82 Rn. 25.

8 Siehe Schefzig, in: Taeger/Gabel/DS-GVO BDSG, 3. Aufl. 2019, Art. 82 Rn. 53 f.

9 Siehe Schefzig, in: Taeger/Gabel/Moos, ebenda.

3. Einbeziehung des AGB-Rechts

Nach der hier vertretenen Meinung wird also grds. eine die Haftung modifizierende, d.h. auch begrenzende Regelung innerhalb eines AV-Vertrages für zulässig erachtet. Die allgemeinen zivilrechtlichen Regelungen zur Zulässigkeit von vertraglichen Bestimmungen ergänzen hier die spezialgesetzlichen (vor allem die datenschutzrechtlichen) Vorgaben. Als Maßstab für die Inhaltskontrolle ist in der Folge § 307 Abs. 2 Nr. 1 BGB auszuspähen, wonach eine Klausel unzulässig ist, wenn die Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist. Denn nach hiesigem Standpunkt würde durch eine vertragsgestaltende Maßnahme gerade nicht von einer feststehenden (also nicht-dispositiven) Regelung abgewichen.

Es steht indes nicht zu befürchten, dass die verbleibenden Vorschriften als Kontrollmaßstab unangemessene Lücken für allzu kreative Vertragsgestaltungen entstehen lassen. Insbesondere bietet § 307 Abs. 2 Nr. 2 BGB die Möglichkeit, die Erreichung des Zwecks eines AV-Vertrages dahingehend auszulegen, dass die weitgehende Gewährleistung bzw. effektive Umsetzung der Betroffenenrechte als in diesem Kontext „wesentlich“ erachtet wird. Demgemäß würden vertragliche Bestimmungen, welche dieses Ziel zu unterlaufen drohen, gleichsam als unwirksam bewertet. Und selbst Vertreter der konträren Auffassung – wonach Art. 82 DS-GVO nicht dispositiv sei – räumen mitunter ein, dass ein Abrücken von diesem gesetzlichen Grundgedanken unter Berücksichtigung allgemeiner zivilrechtlicher Erwägungen zulässig sein könne; immerhin sei denkbar, dass jedenfalls leichte Fahrlässigkeit ausgeschlossen werde und nur die vorhersehbaren Schäden umfasst seien.¹⁰

Die vor diesem Hintergrund denkbaren Vereinbarungen müssen dabei jedoch stets dem unionsrechtlichen Äquivalenz- und Effektivitätsprinzip¹¹ Genüge tun. Im Gegensatz zu den recht ausführlich gestalteten Anforderungen an die Verhängung von Bußgeldern in Art. 83 DS-GVO¹² hat der Schadensbegriff keine nähere Konkretisierung erfahren. Demnach ist es Aufgabe des innerstaatlichen Rechts eines jeden Mitgliedstaats, die Einzelheiten zur Durchsetzung der entsprechenden Ansprüche festzulegen, wobei die betreffenden Vorschriften nicht weniger günstig ausgestaltet sein dürfen als die für Schadensersatzklagen wegen Verstoßes gegen rein nationale Vorschriften. In diesem Zusammenhang sind insbesondere die AGB-rechtlichen Regelungen zur Inhaltskontrolle von Bedeutung.

Im geschäftlichen Verkehr sind – anders als bei der Beteiligung von Verbrauchern – zwischen Unternehmen zwar keine so strengen Maßstäbe bei der hiernach vorzunehmenden Beurteilung anzulegen. Dennoch werden der Vertragsfreiheit insoweit durch die Rechtsordnung Grenzen gesetzt, als das Gleichgewicht von Leistung und Gegenleistung bedroht ist. Im unternehmerischen Umfeld ist hier vor allem an § 307 BGB zu denken. Hier dürfte auch die Monopolstellung oder Marktmacht von großen Dienstleistern zu berücksichtigen sein.

Daneben sind einzelne Klauseln möglicherweise nach § 305c BGB so ungewöhnlich, dass der Vertragspartner

des Verwenders mit ihnen nicht zu rechnen braucht. Dies kann beispielsweise dadurch hervorgerufen werden, dass der AV-Vertrag auf eine Bestimmung zur Haftung aus dem Hauptleistungsvertrag verweist, bspw. durch eine Formulierung wie „Es gelten die Haftungsregelungen aus dem Hauptvertrag“. Zwar wird ein solcher Verweis auf externe Unterlagen und sonstige Vertragsdokumente von der Rechtsordnung durchaus gebilligt¹³ und deshalb nicht zwangsläufig zur Unzulässigkeit der gesamten Regelung führen. Es ist aber dennoch auf den Erwartungshorizont des für diesen (AV-) Vertrag typischen Kundenkreises und dessen Geschäftserfahrung sowie auf die drucktechnische Gestaltung der Klausel abzustellen.¹⁴ So kann auch im unternehmerischen Umfeld ein wirksamer Verweis auf den Hauptvertrag u. U. daran scheitern, dass dieses weitere Dokument nicht konkret genug bezeichnet oder gar nicht bekannt ist. Es sollte daher sichergestellt sein, dass die betreffenden Unterlagen eindeutig erkennbar (z.B. durch direktes Beifügen, sei es in Papierform oder eingescannt als PDF) oder anderweitig hinreichend präzise benannt werden, etwa durch Angabe einer Auftrags- oder Vorgangsnummer, notfalls durch Zitieren der Überschrift des jeweiligen Vertrages mit Angabe des Zeichnungsdatums und der Revision oder des Änderungsdatums.

Was im Einzelfall darüber hinaus für die jeweilige Vertragspartei im Sinne der obigen Vorschriften überraschend oder unangemessen ist, eröffnet hinreichenden Spielraum, um z.B. branchenübliche Gepflogenheiten – so diese im Rahmen von AV-Verträgen überhaupt Platz finden können – zu berücksichtigen.

4. Zulässige Regelungen im Innenverhältnis (zwischen den AV-Vertragsparteien)

Dabei ist zu unterscheiden, ob eine Haftungsregelung unmittelbar mit der betroffenen Person vereinbart wird (z.B. über einen entsprechenden Servicevertrag oder innerhalb von Nutzungsbedingungen) oder ob diese ihren Ursprung in dem AV-Vertrag zwischen Verantwortlichem und Auftragsverarbeiter hat.

Soweit in der Literatur darauf verwiesen wird, eine Regelung zur Haftung entziehe sich der Vertragsfreiheit der Parteien, so wird dies primär im Hinblick auf den zu leistenden Schadensersatz in seiner Außenwirkung zu werten sein.¹⁵ Daher wird eine solche Regelung also allenfalls im Verhältnis zwischen dem Verantwortlichen und der betroffenen Person in Betracht zu ziehen sein. Mit Recht wird in diesem Zusammenhang auf ErwG 146 der DS-GVO hingewiesen, welcher den betroffenen Personen „einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden“ zuspricht.

Ausgangspunkt für die Betrachtung, was im Innenverhältnis – zwischen Verantwortlichem und Auftragsverarbeiter

10 Siehe Spindler/Horváth, in: Spindler/Schuster, DS-GVO, Art. 82 Rn. 11.

11 EuGH, Urteil vom 13.07.2006, C-295/04 (Manfredi).

12 Vgl. dazu auch die ErwG 148 und 150 der DS-GVO.

13 Vgl. Ulmer/Schäfer, in: Ulmer/Brandner/Hensen, ErwG. 148 und 150 der DSGVO AGB-Recht, 12. Aufl. 2016, § 305c BGB Rn. 48.

14 Siehe Grüneberg, in: Palandt, Bürgerliches Gesetzbuch, § 305c Rn. 4.

15 Siehe Schefzig, in: Taeger/Gabel DS-GVO BDSG, 3. Aufl. 2019, Art. 82 Rn. 56.

ter – an haftungsbegründenden Vereinbarungen zulässig sein mag, ist also gleichwohl der Anspruch auf Schadensersatz, den eine betroffene Person geltend macht und ohne den eine Diskussion um etwaige Beschränkungen oder Verschiebungen des finanziellen Geradestehens obsolet ist.

In Bezug auf eine graduelle Abstufung der Haftung zwischen den Parteien des AV-Vertrages gilt es hingegen genauer zu differenzieren. Denn der Umstand, dass nach außen hin der Schadensersatzanspruch (weitestgehend) unbegrenzt gewährleistet sein muss, bedingt für sich genommen noch nicht die rechtliche Notwendigkeit, das Innenverhältnis gleichermaßen von jeglichen Modifikationen auszunehmen.

Es sind dabei verschiedene Ausprägungen denkbar – angefangen bei dem vollständigen Ausschluss jeglicher Haftung über die teilweise Verlagerung hin zu einer Partei (z.B. was bestimmte Schäden dem Grund oder der Höhe nach angeht) bis hin zu einer bloßen Übernahme der gesetzlichen Bestimmungen (in der Regel durch einen schlichten Verweis auf Art. 82 DS-GVO).

5. Vollständiger Ausschluss der Haftung

Letztgenanntem (etwa in der Form: „Auf Art. 82 DS-GVO wird verwiesen.“) ist freilich nichts entgegenzuhalten, außer dem möglichen Einwand, dass – wenn auch in überschaubarem Maße – der Vertragstext ausgedehnt werde und man sich durch bloßes Zitieren des Gesetzes (letztlich) unnötig wiederhole, ohne einen Mehrwert zu schaffen. Rein rechtlich ist eine klarstellende Bezugnahme auf die einschlägige Norm jedoch als unkritisch zu betrachten.

Ebenso unproblematisch dürfte die „Extremposition“ des vollständigen und bedingungslosen Ausschlusses jeglicher Haftung für den Auftragsverarbeiter sein (z.B. durch eine Formulierung wie „Die Haftung des Auftragsverarbeiters ist ausgeschlossen“). Hierbei tritt der Widerspruch zur Rechtslage, wie sie vom Ordnungsgeber beabsichtigt ist, ohne weiteres zu Tage, wenn man nur den Wortlaut betrachtet. Sowohl nach den differenzierten Regelungen in Art. 82 DS-GVO selbst wie auch durch eine Wertung anhand von § 307 BGB ist ein Abweichen von dem gesetzlichen Grundgerüst offensichtlich, wodurch die Klausel zu solch einem schlichten und pauschalen Haftungsausschluss – wie oben exemplarisch zitiert – unzulässig ist.

6. Teilweise Beschränkung der Haftung

Soweit unter den zuvor geäußerten Bedingungen¹⁶ immerhin eine teilweise Begrenzung der (vertraglichen) Haftung vorgenommen werden darf, ist freilich auch hier desto eher von einer unzulässigen Gestaltung auszugehen, je stärker sich das finanzielle Risiko in Richtung einer der beiden Parteien verlagert. Wird also im Falle des Falles der Verantwortliche berechtigt, den weit überwiegenden Anteil – von etwa 90% – der Ersatzsumme pauschal auf den Vertragspartner abzuwälzen, setze dies das gesetzlich gewollte Regime zum Innenausgleich faktisch außer Kraft.¹⁷ Dem ist insofern vom Ergebnis her zuzustimmen, als sich diese Wertung auch mit dem vorliegend vertretenen Standpunkt, dass alternativ für die Inhaltskontrolle im Kern § 307 Abs. 2 Nr. 2 BGB heranzuziehen ist, herleiten lässt.

Systematisch kann es dabei vorrangig um zwei Szenarien gehen, die gewissermaßen von außen auf die Vertragsparteien einwirken: (1) ein Anspruchsteller macht Schadensersatz oder Schmerzensgeld geltend; oder (2) eine Aufsichtsbehörde verfügt entweder bestimmte Sanktionen, welche sich mittelbar monetär auswirken (z.B. durch Produktions- oder Dienstausschfallzeiten), oder verhängt auch direkt ein Bußgeld. In beiden Szenarien kann sich prinzipiell die Frage stellen, inwieweit eine vertragliche Verlagerung der Haftung statthaft sei.

In Bezug auf den Schadensersatz kommt ein teilweiser Verzicht auf Innenausgleich – nichts anderes wäre in der Praxis die Übernahme eines darauf gerichteten Haftungsrisikos – vorliegend in Betracht, sofern sich die Vereinbarungen im Rahmen der einschlägigen nationalen Vorschriften, insbesondere derer zur AGB-rechtlichen Inhaltskontrolle nach den §§ 305 ff. BGB bewegen. Schwierigkeiten dabei bereitet die nach wie vor offene und daher strittige Auslegung, in welchem Umfang die Möglichkeit zur Exkulpation gemäß Art. 82 Abs. 3 DS-GVO greift.¹⁸ Insbesondere Fragen nach der Kausalität einzelner Verfehlungen als schadensauslösendes Moment wären im Einzelfall zu klären.¹⁹

Selbst diejenigen Stimmen in der Literatur, welche den Regelungen in Art. 82 DS-GVO ihren dispositiven Charakter absprechen, tendieren dazu, in engen Grenzen Ausnahmen zuzulassen.²⁰ So könnten in den überwiegenden Fällen zumindest bestimmte, leichte Verstöße bzw. überschaubare Schadensverläufe aus dem Verantwortungsbereich des jeweils Verpflichteten (sprich: desjenigen Beteiligten, der von der betroffenen Person in Anspruch genommen wird und darauffolgend den anderen Vertragspartner in Regress nimmt) ausgeklammert werden.

Vor dem Hintergrund der Bestimmungen in Art. 83 DS-GVO, die vergleichsweise strikt und detailliert daher kommen, wird die Übernahme von Bußgeldern zwischen den Parteien eines AV-Vertrages hingegen schwerlich begründbar sein. Insbesondere die ausdrückliche Vorgabe, dass die verhängten Geldbußen „wirksam, verhältnismäßig und abschreckend sein“ sollen – so Art. 83 Abs. 9 S. 2 DS-GVO – lässt keinen ersichtlichen Raum für vertragliche Dispositionen in diesem Kontext.²¹ Diese Erwägungen dürften in wesentlichen Teilen auch auf das Ergreifen anderweitiger Sanktionen, die von der zuständigen Aufsichtsbehörde explizit gegenüber einem der Beteiligten ergriffen werden, zu übertragen sein. Folglich dürfte es – unabhängig von den tatsächlichen Möglichkeiten – mit Sinn und Zweck dieser Sanktionen unvereinbar sein, wenn die eine Partei des AV-Vertrages sich zur Übernahme von verwaltungsrechtlichen Verpflichtungen der jeweils anderen aus einer behördlichen Auseinandersetzung bereit erklärt.

16 Siehe oben 2.b.

17 Siehe Haumann, DSRITB 2020, 101, 102.

18 Siehe Frenzel, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 82 Rn. 15.

19 Siehe Conrad, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, Rn.706; Schefzig, in: Taeger/Gabel/Moos, DS-GVO, Art. 82 Rn. 22.

20 Vgl. Nemitz, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 28.

21 So auch Haumann, DSRITB 2020, 101, 107.

II. Einbeziehung externer Dokumente und Webseiten

Ein ebenso mannigfaltiges Thema ist die Einbeziehung von externen Dokumenten oder auch Webseiten innerhalb des AV-Vertrages bzw. der Verweis auf andere Quellen außerhalb des zu besprechenden Vertragswerks. Das bekannteste Beispiel hierfür ist sicherlich der Verweis auf ein zusätzliches Dokument, das losgelöst vom AV-Vertrag die technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO bzw. ein entsprechendes Sicherheitskonzept darstellt. Doch auch ein Link oder Hinweis im Vertrag auf eine Webseite mit entsprechenden Darstellungen taucht in der Beratungspraxis immer wieder auf. Vor allem internationale Anbieter bedienen sich dieses Handgriffs, um einerseits die Aktualität der relevanten Angaben und Informationen zu gewährleisten, andererseits den „DPA“ (Data Processing Agreement) relativ kurz und abstrakt zu auszugestalten. Das ist sogar ressourcenschonender, als seitenweise Anhänge mitzuschicken.

1. Verweis auf externe Dokumentation

Die technischen und organisatorischen Maßnahmen (kurz: TOMs) werden bisweilen mit Checklisten, bisweilen auch als „IT-Konzept“ auf Seiten des Auftragsverarbeiters skizziert und dem Verantwortlichen zur Prüfung vorgelegt. Dabei gilt es zu berücksichtigen, dass diese Prüfung oder Kontrolle einerseits vor bzw. bei Vertragsabschluss stattfinden, andererseits aber auch im Zuge der regelmäßigen Nach-Kontrolle gem. Art. 28 Abs. 3 S. 2 lit. h) DS-GVO innerhalb der laufenden Vertragsbeziehung erfolgen kann.

a) Vorgaben aus der DS-GVO

Das führt zur vorgelagerten Frage: Sind die TOMs überhaupt zwingender Bestandteil des AV-Vertrages? Aus Art. 28 Abs. 3 S. 2 lit. c) DS-GVO ergibt sich nur die Vorgabe, dass der Auftragsverarbeiter „alle gemäß Art. 32 erforderlichen Maßnahmen ergreift“.²² Daher wird diese Regelung in der Rechtswissenschaft teilweise für deklaratorisch erachtet.²³

Hier wurde vom Ordnungsgeber das „Ergreifen“ dieser Maßnahmen, nicht jedoch die „Dokumentation“ oder das „Festlegen“²⁴ derselben (wie im alten BDSG, bis 2018) in den Wortlaut der Vorschrift aufgenommen, woraus sich deuten lässt, dass eine Dokumentation der TOMs gem. Art. 32 DS-GVO nicht zwingend erforderlich ist und insbesondere im Geltungsbereich der DS-GVO nicht innerhalb des AV-Vertrages zu erfolgen hat. Die Verordnung verweist an dieser Stelle lediglich auf den Art. 32 DS-GVO, der diese Pflicht ohnehin aus den Absätzen 1 und 4 von Art. 28 DS-GVO dem Auftragsverarbeiter unmittelbar auferlegt; d.h. sie würde per se greifen und von jedem Unternehmen auch unabhängig einer Auftragsverarbeitung umzusetzen sein.

Bereits aus den allgemeinen Anforderungen, wonach der Verantwortliche zu prüfen hat, dass er nur mit Auftragsverarbeitern arbeitet, „die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und

den Schutz der Rechte der betroffenen Person gewährleistet“ (Art. 28 Abs. 1 DS-GVO), werden die TOMs einbezogen.²⁵ Deshalb muss der Verantwortliche in die Lage versetzt werden, den Auftragsverarbeiter vorab prüfen und jederzeit kontrollieren²⁶ zu können, was auch die Überprüfung der bereits ergriffenen TOMs mit umfasst (vgl. auch Art. 28 Abs. 3 S. 2 lit. h) DS-GVO). Dies gilt ebenso für den Nachweis der insgesamt sachgerechten Auswahl des Auftragsverarbeiters nach Art. 28 Abs. 1 S. 1 DS-GVO²⁷ und sollte wiederum aus Gründen der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO dokumentiert werden.²⁸ Diesbezüglich gilt es zu beachten, dass sich in den AV-Verträgen regelmäßig Klauseln wiederfinden, die eine Anzeige oder Zustimmung des Verantwortlichen bei der Veränderung, zumindest bei der Verschlechterung des Sicherheitsniveaus bzw. der TOMs regeln. Eine derartige Klausel erscheint grundsätzlich sinnvoll, setzt aber voraus, dass sich diese Veränderungen abbilden, respektive durch Gegenüberstellung des Status-Quo prüfen lassen.

Diese Aspekte lassen den Schluss zu, dass eine „klassische“ Dokumentation der TOMs auf Papier bzw. in einer eigenen Datei (vgl. dazu Art. 28 Abs. 9 DS-GVO) die gestellten Anforderungen problemlos erfüllen können. Im Gegensatz zu einem Vertrag, der per E-Mail oder Briefpost verschickt wird, stellen sich bei einem Online-Dokument jedoch Folgefragen: Wie können Zugang und Vertragsschluss (etwa durch einen elektronischen Zeitstempel) verlässlich vermerkt werden? Auf welche Weise können die Vertragsparteien eine rechtsgültige Kopie des Dokuments erlangen? Und wie lässt sich beweisen, dass genau dieses besagte Dokument beiden Vertragsparteien vorgelegen hat?

b) Rechtssicherheit

Zudem bestehen ganz offenkundige Risiken, denn es ist möglich, dass die Webseite, auf die solcherart verwiesen wird, technische Störungen hat, so dass die Inhalte vorübergehend oder gar nicht mehr abrufbar wären. Damit könnte letztlich eine Kontrolle der TOMs wie auch die Prüfung von Veränderungen zumindest erschwert, bisweilen gar unmöglich gemacht werden. Die zuvor aufgeworfenen Fragen zu ausschließlich online verlinkten Inhalten mögen überdies problematisch werden, wenn es darum geht, deren wirksame Einbeziehung gegenüber externen Kontrolleuren

22 Vgl. Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 28 Rn. 45.

23 Bertermann, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 28 Rn. 25; Vgl. Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 28 Rn. 45.

24 Vgl. hierzu: Gabel/Lutz, in: Taeger/Gabel, DS-GVO BDSG, 3. Aufl. 2019, Art. 28 Rn. 51.

25 Zum Wortlaut und dem alten Recht aus § 11 Abs. 2 S. 1 BDSG a.F.: Hartung, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 28 Rn. 57; Gabel/Lutz, in: Taeger/Gabel, DS-GVO BDSG, 3. Aufl. 2019, Art. 28 Rn. 51.

26 Mehr hierzu: Conrad/Seiter, RDV 2021, 186, 189 ff.

27 Petri, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 1. Aufl. 2019, Art. 28 Rn. 68.

28 Hartung, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 28 Rn. 58; Petri, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 1. Aufl. 2019, Art. 28 Rn. 68; Gabel/Lutz, in: Taeger/Gabel, DS-GVO BDSG, 3. Aufl. 2019, Art. 28 Rn. 51.

oder der Aufsichtsbehörde zu beweisen (so auch nach Art. 5 Abs. 2 DS-GVO).

Beschreibungen der TOMs auf einer Webseite genießen zwar den Vorteil, sich im stetigen Wandel der Anpassungen und Verbesserungen zu befinden, und könnten durch verknüpfte Erklärungen, FAQs und Zertifikate einen Mehrwert bieten, ermöglichen allerdings keine beweissichere Dokumentation des konkreten „Ist-Zustands“ bei Vertragsverhandlungen. Zudem könnte die Verbindlichkeit der ergriffenen Maßnahmen infrage gestellt werden, würden sich diese lediglich als allgemeingültige Inhalte einer Webseite darstellen, die jederzeit geändert werden kann. Möglicherweise leidet deshalb auch die Nachvollziehbarkeit im Ganzen darunter, wenn etwa Texte innerhalb des Onlineauftritts bearbeitet werden können, ohne hinreichend dem Aspekt der Revisionsicherheit Rechnung zu tragen. Man könnte gar erwägen, ob der Auftragsverarbeiter vor diesem Hintergrund zusätzlich verpflichtet wäre, wiederum spezifische ergänzende Angaben in Bezug auf die TOMs zur Webseite selbst zu tätigen.

Daher dürften wegen den Rechenschaftspflichten und dem Erfordernis zur verbindlichen Dokumentation die Darstellungen der TOMs vorab und im Rahmen des AV-Vertrages (unter Umständen als Anhang) vorzugswürdig erscheinen. Sie sollten daher als notwendiger Bestandteil des Vertragsinhaltes verstanden werden, was durch einen dynamischen Verweis auf ein externes Dokument oder einer Webseite, die ggf. auch durch dritte Personen verwaltet wird, nicht gewährleistet wird.

2. Verweis auf eine externe Liste der „Unterauftragnehmer“

Die vergleichbare Fragestellung besteht bei der Benennung von weiteren Auftragsverarbeitern. Auch hier begegnen einem in der Praxis teilweise Vertragsmodelle, wonach die einbezogenen Dienstleister oder Tochtergesellschaften in ihrer Rolle als weitere Auftragsverarbeiter (Unterauftragnehmer) lediglich auf einer hierfür geschaffenen Webseite bzw. in einer verlinkten Datei abrufbar sein sollen und deshalb nicht im Vertragstext selbst aufgeführt und festgehalten werden.

a) Vorgaben aus der DS-GVO

Zunächst lässt sich konstatieren, dass die DS-GVO keine konkreten Vorgaben aufweist, wie die Unterauftragnehmer abzubilden sind. Solche gehören offenbar nicht zum Pflichtenkatalog aus Art. 28 Abs. 3 S. 1 DS-GVO, der die Eckpfeiler der konkreten Auftragsverarbeitung festhält.²⁹

Nach Art. 28 Abs. 3 S. 2 lit. d) DS-GVO haben der AV-Vertrag oder das vergleichbare Rechtsinstrument insbesondere vorzusehen, dass der Auftragsverarbeiter „die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält“, womit auch Bezug genommen wird auf die vorherige oder allgemeine Genehmigung des Verantwortlichen zur Hinzuziehung oder Änderung von weiteren Auftragsverarbeitern, welche es hiermit zu regeln gilt.³⁰ Solche

weiteren Auftragsverarbeiter können bekanntermaßen eine mehrstufige Kette der Datenverarbeitung bilden und in dieser Ausprägung das Durchführen von Kontrollen wie auch überhaupt die vollumfängliche Kenntnisnahme der Datenverarbeitung bis zum letzten Glied in der IT-Infrastruktur (z.B. dem Webhoster) erschweren.³¹

Denklogisch bedarf es für die Kontrolle und Einhaltung der datenschutzrechtlichen Vorgaben überhaupt der Kenntnis über solche weiteren Auftragsverarbeiter. Zum Bestandteil des Vertrages sollte deshalb nach Art. 28 DS-GVO auch die Darstellung von „Unterauftragnehmern“ zählen. Denn zum einen sind diese weiteren Auftragsverarbeiter und deren Einsatz je nach Umsetzung der Alternativen aus Art. 28 Abs. 2 DS-GVO genehmigungspflichtig, zum anderen müssen spätere Änderungen dieser „Unter-Auftragsverarbeiter“ ebenso bekannt gegeben werden.³² Daraus lässt sich die Pflicht ableiten, die weiteren Auftragsverarbeiter bereits direkt im AV-Vertrag aufzuführen. Vor allem wegen eines etwaigen Drittlandtransfers und angesichts der „Schrems II“-Problematik³³ hat dieses Kriterium noch weiter an Bedeutung zugenommen.

b) Ausgestaltungsmöglichkeiten und Grenzen

Der Verweis auf eine Webseite bietet die Vorteile der Aktualität, insbesondere bei sich verändernden Gegebenheiten, ist jedoch wie auch bei Abbildung der TOMs wegen vielerlei Gesichtspunkten zu kritisieren. Als alleiniges und abschließendes Mittel wäre es mit der DS-GVO unvereinbar, die tatsächlich eingesetzten Dienstleister lediglich auf einer Webseite anzuzeigen. Andernfalls müsste der Verantwortliche in der Konsequenz praktisch jeden Tag auf diese Online-Liste schauen, um seine Zustimmung ausüben zu können.

Ohnehin kann darüber hinaus die Transparenz der Datenverarbeitung angezweifelt werden, wenn die „Sub-Dienstleister“ erst über mehrere Klicks bzw. in anderen Quellen einsehbar sind, und damit in keiner Weise bei Vertragsschluss sofort erkennbar. Dies kollidiert mit dem Genehmigungs- bzw. Zustimmungskarakter der Vorschrift aus Art. 28 Abs. 2 DS-GVO. Schließlich würde es auch die Kontrollmöglichkeiten unterlaufen.³⁴

Dieser Problematik könnte zwar eine „Benachrichtigungsfunktion“, beispielsweise automatisch per E-Mail, entgegenkommen. Ein Folgeproblem könnte sich aber daraus ergeben, wie detailliert (oder im Gegensatz: allgemein gehalten) diese Benachrichtigung ausfällt. Immerhin muss von vornherein sichergestellt sein, dass der Verantwortliche unmittelbar alle für ihn nötigen Informationen an die Hand bekommt, um von

²⁹ Conrad/Seiter, RDV 2021, 186, 189.

³⁰ Vgl. Hartung, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 28 Rn. 73.

³¹ Conrad/Seiter, RDV 2021, 186, 191; vgl. Petri, in: Simitis/Hornung/Spi-ecker gen. Döhm, Datenschutzrecht, 1. Aufl. 2019, Art. 28 Rn. 85.

³² Vgl. Klug, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 28 Rn. 13; Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 28 Rn. 60 ff.

³³ Siehe EuGH v. 16.07.2021 – C-311/18; mehr hierzu: Eichmann/Nowak, RDV 2021, 194, 194 ff.

³⁴ Zur Reichweite der Kontrollmöglichkeiten: Conrad/Seiter, RDV 2021, 186, 191.

seinem Genehmigungs- oder Widerspruchsrecht fachkundig Gebrauch zu machen. Andernfalls wäre die offenkundige Notwendigkeit eines aktiven Handelns mittelbar als eine Beschränkung zur Ausübung der Kontrolle und somit eine Benachteiligung des Verantwortlichen zu vermuten.

Ähnlich wie schon für die TOMs bewertet,³⁵ besteht insgesamt die Gefahr, dass sich hier ebenso wenig der Vertragsgegenstand belegen, respektive die dazugehörigen Umstände der konkreten Datenverarbeitung und eingesetzten weiteren Auftragsverarbeiter zum Zeitpunkt des Vertragsschlusses fixieren lassen. Schließlich setzt die Genehmigung die eindeutige Kenntnis, d. h. die belegbare, schriftliche bzw. textliche Fixierung der weiteren Auftragsverarbeiter voraus.

Entsprechende Regelungen sind daher streng danach zu beurteilen, ob sie transparent und in leicht verständlicher Weise es zulassen, schnell und beweissicher die notwendigen Inhalte aufzufinden. Vereinbarungen bzw. Verlinkungen, die diesen Anforderungen nicht genügen, dürften an die Grenzen nach § 307 Abs. 2 oder § 305c BGB stoßen, und es spricht vieles für die Unzulässigkeit eines derartigen Vertragsmodells. Im Ergebnis und wie üblich im europäischen Rechtsraum sollten die weiteren Auftragsverarbeiter im AV-Vertrag (ggf. in einem Anhang) festgehalten und damit direkt einbezogen werden.

III. Dokumentation der Weisung

Ähnlich wie der beweissicheren Einbeziehung von Regelungen zu Unterauftragnehmern ist die Folgefrage zu beleuchten: Wie müssen Weisungen im Sinne von Art. 28 Abs. 3 S. 2 lit. a) DS-GVO, die neben der ursprünglichen bzw. anfänglichen Festlegung des Vertragsinhalts die Auftragsverarbeitung während ihrer Laufzeit signifikant ausgestalten und bestimmen können, ausgesprochen und dokumentiert werden? Ferner wäre zu erörtern, ob diese Weisungen des Verantwortlichen auch (fern)mündlich erfolgen können.

1. Vorgaben aus der DS-GVO

Die Verordnung lässt in Art. 28 Abs. 3 S. 2 lit. a) DS-GVO erkennen, dass die Textform oder Schriftform anzuraten ist, um dem Merkmal der „Dokumentation“ zu entsprechen.³⁶ Ohnehin ist zumeist in der Praxis innerhalb des AV-Vertrages die Schriftform geregelt, allerdings zumeist nicht, wer die Weisungen zu dokumentieren hat.³⁷

Dabei ist die Weisung noch nicht einmal als solche definiert. Was als Weisung im gesetzlichen Sinne zu verstehen ist, gilt es daher zunächst einmal einzugrenzen. Rein praktisch könnte unter einer solchen „Weisung“ auch die „Ablehnung“ des Einsatzes weiterer Auftragsverarbeiter oder die „Beendigung“ der Auftragsverarbeitung bzw. die „vollständige Rückgabe“ der Daten fallen. Derartige Forderungen können erheblich vertragsrelevant sein und sollten daher beiden Parteien deutlich vor Augen geführt werden. Insofern sollten sich die Parteien einig sein, wie die Weisungen zu erteilen, respektive zu dokumentieren sind.

2. Handlungsspielraum der Vertragsparteien

Dabei können die Vertragsparteien auch regeln bzw. aushandeln, wer diese Weisungen zu dokumentieren hat. Diese Aufgabe könnte entweder gänzlich dem Verantwortlichen oder aber primär dem Auftragsverarbeiter zukommen.

Ferner wäre im nächsten Schritt zu klären, ob und inwiefern dies zusätzliche Kosten verursacht und wie die Befolgung einer Weisung im Einzelfall ohnehin zu gewährleisten ist. Könnte beispielsweise die weisungsempfangende Stelle, in der Regel der Auftragsverarbeiter im Massengeschäft, dem Verantwortlichen konkrete Vorgaben zur Darstellung/Übermittlung der Weisung machen, wie z.B. die zwingende Nutzung eines bestimmten Formularblatts oder Meldekanals? Die Erfahrung in der Praxis zeigt, dass eine telefonisch oder elektronisch gegenüber Beschäftigten des Vertragspartners erklärte Weisung, z.B. gegenüber dem Kundensupport, häufig nicht mit der notwendigen Beachtung behandelt und dokumentiert werden mag. Die beachtete Weisung droht dann ggf. ins Leere zu laufen, wenn nicht eine spezielle Anlaufstelle (etwa per E-Mail an ein dafür vorgesehenes Funktionspostfach) oder eine bestimmte Form der Übermittlung (etwa durch ein Formular) vertraglich fixiert sind. Ohnehin dürfte eine dergestalt offen und unspezifisch kommunizierte Weisung wegen des ggf. dann kollidierenden Direktionsrechts im Arbeitsverhältnis kritisch zu werten sein.³⁸ Wird hingegen die Weisung ausschließlich an die Geschäftsleitung adressiert, kann dies zu Verzögerungen in der Wahrnehmung und Umsetzung durch die jeweiligen operativen Bereiche im Unternehmen³⁹ führen. Es besteht gar die Gefahr, dass die auf diesem Wege übermittelten Weisungen in Unkenntnis der konkret für die Verarbeitung relevanten Einzelheiten durch die Geschäftsleitung fälschlicherweise abgelehnt bzw. zurückgewiesen werden.

Ein für jede Weisung zu ergänzender/abzuändernder Annex zum Vertrag hingegen wäre zwar deutlich rechtssicherer, aber von weiteren Nachteilen geprägt. Mitunter wäre ein solches Konstrukt in der praktischen Handhabung gleichsam zeitintensiv und aufwendig. Insbesondere bei Weisungen, die Absprachen bzw. Mitwirkungsanfragen bei der Prüfung von Datenschutzvorfällen im Sinne von Art. 33 DS-GVO betreffen, können weitere haftungsbegründende Risiken zu Tage treten. Bedürfte es hierzu einer konkreten Weisung, wäre diese mutmaßlich zu langsam für die Meldefrist gegenüber der Aufsichtsbehörde und daher nicht ratsam. Und ein solcher Vertragsanhang dürfte dann auch nur von vertretungsberechtigten Personen unterzeichnet bzw. geändert werden, was ebenso schnelle Abstimmungen hemmen kann.

³⁵ Siehe oben 3.a.

³⁶ Petri, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 1. Aufl. 2019, Art. 28 Rn. 59.

³⁷ Vgl. Spoerr, in: Wolff/Brink, BeckOK Datenschutzrecht, 37. Ed. 2021, Art. 28 DS-GVO, Rn. 59.

³⁸ Gabel/Lutz, in: Taeger/Gabel, DS-GVO BDSG, 3. Aufl. 2019, Art. 28 Rn. 45.

³⁹ Abgesehen von kleinen inhabergeführten Betrieben dürfte die Geschäftsführung in den seltensten Fällen unmittelbar in die alltäglichen Entscheidungsabläufe im Rahmen der Auftragsverarbeitung einbezogen sein.

Je nach Überlegenheit einer Partei droht daher das Instrument der Weisung durch den Verantwortlichen eingeschränkt zu werden, wäre dieses an allzu hohe Hürden geknüpft. Entsprechende Ausgestaltungen des AV-Vertrages, die Weisungen von strengen Vorgaben anhängig zu machen, könnten eine unangemessene Benachteiligung des Verantwortlichen im Sinne von § 307 Abs. 2 BGB darstellen und daher für unzulässig befunden werden. Gleichwohl dürfte eine konkrete Festlegung von Weisungen für alle Parteien am rechtssichersten sein. Als ausreichend erachtet wird jedenfalls die Dokumentation auf Seiten des Auftragsverarbeiters;⁴⁰ auch um nicht eine eigene Verantwortlichkeit (nach Art. 28 Abs. 10 DS-GVO) durch ein Abweichen von den vertraglichen Vereinbarungen und den Weisungen des Verantwortlichen zu begründen.⁴¹ Denn insgesamt drohen als Folgen etwaiger Unklarheiten neben den Beweisproblemen unter Umständen auch unvorhersehbare Kosten sowie Sanktionen der Aufsichtsbehörden bzw. Schadensersatz nach Art 82 DS-GVO.⁴²

IV. Auftragskontrolle des Datenschutzbeauftragten

In Art. 28 Abs. 3 S. 2 lit. h) DS-GVO sind die Kontrollrechte des Verantwortlichen geregelt,⁴³ die entweder von ihm selbst oder „einem anderen von diesem beauftragten Prüfer“ durchgeführt werden. Es steht zur Diskussion, ob sich hieraus eine sog. Auftragskontrolle des Datenschutzbeauftragten (DSB) ergibt, falls dieser als ein solcher „Prüfer“ gilt. Es stellt sich insbesondere die Frage, ob er bereits von Amts wegen vorab den Auftragsverarbeiter zu kontrollieren hat.

Legt man den Wortlaut dieser Norm zu Grunde, handelt es sich hierbei um einen „beauftragten“ Prüfer. Da der DSB ohnehin von Gesetzes wegen nach Art. 39 DS-GVO seine Aufgabe wahrzunehmen hat und überdies „benannt“ werden muss, erscheint die Formulierung „beauftragter Prüfer“ hier auf eine andere Person abzielen. Ferner spricht die DS-GVO ganz explizit an vielen Stellen vom „Datenschutzbeauftragten“ (z.B. in Art. 13 Abs. 1 lit. b) oder in Art. 30 Abs. 1 S. 1 lit. a)), womit dieses Amt bzw. dessen Funktion eindeutig einbezogen wird. Der Begriff des „Prüfers“ wird hingegen nicht näher definiert und mutmaßlich in anderen Rechtsvorschriften anders interpretiert.

Anforderungen, welche an die Kontrolle der Auftragsverarbeiter gestellt werden, können aus unterschiedlichen Richtungen formuliert sein. So sehen bspw. einige Standards und Prüfkataloge der Wirtschaftsprüfer (IDW) Fragen zur Einhaltung des Datenschutzes vor. Auch aus Richtung des Qualitätsmanagements (ISO 9001) im Unternehmen und erst recht durch Compliance-Abteilungen werden mitunter Prüfungen vorgenommen. Eine Person, die also allgemein – in einer noch zu bestimmenden Art und Weise – auf Seiten des Verantwortlichen prüfend tätig wird, kann daher verschiedene Aufgaben mit Bezug zum Datenschutz wahrnehmen. Vom Verständnis her ist diese Funktion also zunächst im Vergleich weiter gefasst, so dass hierzu möglicherweise auch, aber nicht nur der DSB zählen mag.

Immerhin sind dessen Aufgaben konkret in Art. 39 DS-GVO ausgestaltet, die auch die „Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters“ (Art. 39 Abs. 1 lit. a) DS-GVO) sowie die „Überwachung der Einhaltung dieser Verordnung“ (Art. 39 Abs. 1 lit. b) DS-GVO) vorsehen. Unter diesem relativ weit gefassten Regelungsgehalt und den damit einhergehenden Befugnissen lassen sich auch Kontrollen von Auftragsverarbeitern subsumieren. Dennoch stellt sich die Frage, ob dies zum Kreis an originären Aufgaben für den DSB gehört. Immer vorausgesetzt, die Person verfügt über das notwendige Fachwissen, insbesondere zur IT-Sicherheit, sowie die erforderliche Zeit (gerade für den internen „Teilzeit-DSB“ eine Herausforderung) oder die tatsächliche Zugriffsmöglichkeit (möglicherweise bei großen und/oder internationalen Dienstleistern ein Problem), lässt sich eine derartige Obliegenheit nicht per se ausschließen.

Es könnte zusätzlich argumentiert werden, dass die „Überwachung der Einhaltung der Verordnung“ auf Seiten des Verantwortlichen umso mehr und unmittelbar der Auftragsverarbeitung gilt, als in diesem Fall die „eigenen“ Daten bei einem externen Dienstleister verarbeitet werden. Diesen zu überwachen, stellt in der Regel aufgrund der mangelnden Vertrautheit mit der konkreten Umgebung der Verarbeitung eine größere Herausforderung dar, als wäre lediglich die eigene Sphäre beim Verantwortlichen betroffen. Daher mögen erhöhte Anforderungen an diese Kontrolle zu stellen sein, derer sich ein hierfür ausgewählter Experte bedienen sollte.

Zunächst liegt es nahe, dass der DSB auch ein Prüfer im Sinne von Art. 28 Abs. 3 S. 2 lit. h) DS-GVO sein kann, obwohl hier gewissermaßen ein Interessenkonflikt droht, indem der DSB diese Kontrollen nicht als unabhängiges Organ wahrnimmt, sondern in der Realität im Lager des Verantwortlichen steht und dadurch ggf. „interessengesteuert“ agieren könnte. Ähnlich wie auch bei einer Vertragsverhandlung lässt sich nicht verheimlichen, dass der DSB tendenziell mittelbar zu Gunsten „seiner“ Firma handelt. Würde er also durch selbstständiges Kontrollieren des Auftragsverarbeiters direkt einen Teil der Aufgaben des Verantwortlichen übernehmen, käme seine Überwachungsfunktion einer Situation gleich, in der er seine eigene Arbeit kontrollieren würde.

Ferner muss der DSB gem. Art 38, 39 DS-GVO weisungsfrei und objektiv in seiner Rolle agieren, wird daher gerade nicht zur Prüfung zusätzlich erst „beauftragt“, wie es aber der Wortlaut in Art. 28 Abs. 3 S. 2 lit. h) DS-GVO nahelegt. So kann der jeweiligen Beauftragung im Allgemeinen – mangels entgegenstehender zwingender Vorgaben – auch die Festlegung oder Beschränkung auf einzelne Bestandteile der zu prüfenden Verarbeitungstätigkeit innewohnen. Es ist beispielsweise denkbar, dass der Verantwortliche besonde-

40 Gabel/Lutz, in: Taeger/Gabel, DS-GVO BDSG, 3. Aufl. 2019, Art. 28 Rn. 44; vgl. Spoerr, in: Wolff/Brink, BeckOK Datenschutzrecht, 37. Ed. 2021, Art. 28 DS-GVO, Rn. 59.

41 Hartung, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 28 DS-GVO Rn. 33.

42 Vgl. Hartung, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 28 DS-GVO Rn. 33.

43 Conrad/Seiter, RDV 2021, 186, 189 ff.

res Augenmerk auf eine starke Zutrittskontrolle (zur Absicherung des Gebäudes nach außen hin) legt, diese daher entsprechend umfangreich geprüft haben möchte, und demgegenüber jedoch die Verfügbarkeit von Daten (etwa das Bestehen von Backups betreffend) nur marginal und vergleichsweise oberflächlich betrachtet – oder auch umgekehrt. Wie dem auch sei: In einer solchen Konstellation wird eine auf die konkrete Tätigkeit gerichtete Abhängigkeit vom Auftraggeber deutlich, was jedoch im klaren Widerspruch zur ausgiebig definierten, weitgehende Unabhängigkeit mahnende Rolle des DSB steht. Immerhin ist sicherzustellen, dass „der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält“ (Art. 38 Abs. 3 S. 1 DS-GVO), was den drohenden Konflikt im Falle der Wahrnehmung der Funktion als „beauftragten Prüfer“ untermauern dürfte.

Wegen der Zielrichtung dieser Vorschrift dürfte vieles dagegensprechen, dass der DSB die Rolle des Prüfers gegenüber dem Auftragsverarbeiter wahrnimmt. Überdies trifft die Pflicht zur Kontrolle und Auswahl des geeigneten Auftragsverarbeiters nur den Verantwortlichen (Art. 28 Abs. 1 DS-GVO) und ist als solche auch Bestandteil von dessen Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO. All jenes wird vom bestellten DSB lediglich überwacht – jedoch gerade, ohne eigenständig operativ tätig zu werden.

V. Neue EU-Standardvertragsklauseln

Mit Beschluss vom 4. Juni 2021⁴⁴ hat die Europäische Kommission erstmalig von der in Art. 28 Abs. 7 DS-GVO niedergelegten Möglichkeit Gebrauch gemacht, einen eigenen „AV-Mustervertrag“ in Form entsprechender Standardvertragsklauseln zu erlassen. Ob dadurch schlichtweg die Anzahl an für die Öffentlichkeit verfügbaren Mustern – und aus Sicht mancher Anwender vielleicht ein Stück rechtlicher Beliebigkeit – steigt, oder ob dies zu mehr rechtlicher Verbindlichkeit in der Praxis sorgen wird, bleibt dabei zu beobachten.

Was die inhaltliche Ausgestaltung betrifft, so werden sich womöglich einige der in dem vorliegenden Beitrag (und seinem Vorgänger-Teil⁴⁵) angestellten Erwägungen auf das neue EU-Vertragswerk übertragen lassen. Auf der anderen Seite wird es sicher auch neue oder geänderte Streitfragen geben, die mit den aufgestellten Regelungen einhergehen mögen. Insofern wird zukünftig noch zu untersuchen sein, welchen Einfluss die Gestaltung der neuen EU-Standardvertragsklauseln auf die hier vorgenommene Bewertung nehmen wird und inwiefern Abweichungen überhaupt zulässig sind.

VI. Fazit

Viele Fragen, die sich letztlich für beide Seiten des AV-Vertrages stellen, dürften durch belegbare Dokumentation im Rahmen der datenschutzrechtlichen Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) beantwortet werden können, andernfalls Unklarheiten zu haftungsrechtlichen Lasten der jeweils handelnden Akteure gehen. Den Vertragsparteien sollte daher vieles an einer möglichst beweissicheren Dokumentation und dem Abfassen von klaren Regelungen gelegen sein. Dies betrifft sowohl die Einbeziehung externer Quellen (wie für den Verweis auf TOMs oder zur Benennung von Unter-Auftragsverarbeitern) als auch das Vereinbaren von Weisungen und Meldewegen.

Vieles ist jedoch nach wie vor unklar: Die praktisch bedeutsame Überlegung, ob der Datenschutzbeauftragte Kontrollen beim Auftragsverarbeiter durchführen darf, gehört mit dazu und wird vorliegend im Ergebnis zurückhaltend bewertet. Diese und weitere Fragen, so auch die Zulässigkeit von Haftungsausschlüssen bei der Geltendmachung von Schadenersatzansprüchen betreffend, werden zunehmend sicher auch durch die Rechtsprechung thematisiert werden.



Conrad Sebastian Conrad

Senior Berater Datenschutz bei der datenschutz nord GmbH, Büro Hamburg



Stefan R. Seiter

Rechtsanwalt und Senior Berater Datenschutz bei der datenschutz nord GmbH, Büro Bremen

⁴⁴ Siehe <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=DE>.

⁴⁵ Conrad/Seiter, RDV 2021, 186.

Kurzbeiträge

Praxisfälle zum Datenschutzrecht XIII: Der Verlust eines USB-Sticks

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

I. Sachverhalt

Der Datenschutzbeauftragte (DSB) des Unternehmens (U) besteht darauf, dass der nicht mehr eindeutig aufzuklärende Verlust eines USB-Sticks mit Gehaltsabrechnungen und Mitarbeiterbewertungen mehrerer Dutzend Mitarbeiter/-innen diesen bekannt gegeben wird. Auch die Datenschutzaufsichtsbehörde soll nach Auffassung des DSB informiert werden. Bei dem USB-Stick handelt es sich um einen einfachen mobilen Datenträger. Die enthaltenen Informationen waren weder verschlüsselt, noch lag ein Zugriffsschutz vor. Der Mitarbeiter, dem der USB-Stick abhandengekommen ist, nimmt an, dass ihm dieser im Mitarbeiterparkhaus auf dem Weg zu seinem Auto heruntergefallen ist. Eine ausführliche Suche nach dem USB-Stick verlief ohne Erfolg.

Neben der Information von Beschäftigten und zuständiger Aufsichtsbehörde verlangt der DSB von der Geschäftsleitung, dass diese eine von ihm vorgelegte Richtlinie zum sicheren Umgang mit mobilen Datenträgern in Kraft setzt.

Wie sind die Forderungen des Datenschutzbeauftragten zu bewerten?

II. Musterfalllösung

1. Vorüberlegungen

Im vorliegenden Fall stellt sich zunächst die Frage, ob das Unternehmen zur Vornahme der vom DSB geforderten Maßnahmen verpflichtet ist, also Behörde bzw. betroffene Personen informieren muss und eine Richtlinie zum Umgang mit mobilen Datenträgern in Kraft setzen sollte. Unabhängig von der inhaltlichen Richtigkeit der vom DSB verlangten Maßnahmen stellt sich zudem die Frage, inwiefern dieser Forderungen gegenüber der Unternehmensleitung zur Umsetzung des Datenschutzes aufstellen darf. Zu beantworten ist also, welche Rolle dem Datenschutzbeauftragten im Hinblick auf die Gewährleistung des Datenschutzes bei der benennenden Stelle zukommt.

2. Meldepflicht gegenüber der zuständigen Aufsichtsbehörde, Art. 33 DS-GVO

Nach Art. 33 Abs. 1 S. 1 DS-GVO hat der Verantwortliche Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der zuständigen Datenschutzaufsichtsbehörde zu melden, es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich

nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

Voraussetzung für die Verpflichtung aus Art. 33 DS-GVO ist zunächst das Vorliegen einer „Verletzung des Schutzes personenbezogener Daten“. Dieser Begriff ist in Art. 4 Nr. 12 DS-GVO legaldefiniert. Danach handelt es sich um eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Hier steht eine Verletzung der Vertraulichkeit personenbezogener Daten im Raum, denn aufgrund der fehlenden technischen Schutzmaßnahmen ist nicht ausgeschlossen, dass unbefugte Personen von den auf dem Stick gespeicherten Informationen Kenntnis nehmen. Verletzungen der Vertraulichkeit fallen unproblematisch unter den Begriff der Verletzung des Schutzes personenbezogener Daten.¹ Auf ein Verschulden, also darauf, ob die Vertraulichkeitsverletzung vorsätzlich oder zumindest fahrlässig verursacht wurde, kommt es nicht an.

Fraglich ist, welche Konsequenzen sich daraus ergeben, dass der Datenschutzvorfall nicht vollständig aufgeklärt ist und unklar bleibt, ob die Daten auf dem Stick tatsächlich unbefugt zur Kenntnis genommen wurden. Konkret stellt sich die Frage, ob ein Bekanntwerden der Datenschutzverletzung i.S.v. Art. 33 f. DS-GVO nur bei positiver Feststellung der Datenschutzverletzung anzunehmen ist oder ob ein bestimmter Grad an Wahrscheinlichkeit genügt.

Für letztere Interpretation spricht der Schutzzweck der Pflichten nach Art. 33 f. DS-GVO: Schutzzweck der Pflichten ist insbesondere, betroffene Personen rechtzeitig vor einem Datenmissbrauch zu warnen und mögliche Folgeschäden abzuwenden. Wird abgewartet, bis absolute Gewissheit hinsichtlich der Datenschutzverletzung besteht und alle Details bekannt sind, sind Folgeschäden ggf. nicht mehr zu verhindern. Nach Auffassung des EDSA ist anzunehmen, dass eine Datenschutzverletzung bekannt wurde, wenn der betreffende Verantwortliche eine hinreichende Gewissheit darüber hat, dass ein Sicherheitsvorfall aufgetreten ist, der zu einer Beeinträchtigung des Schutzes personenbezogener Daten geführt hat.² Bei Verlust eines nicht gegen unbefugten Zugriff geschützten Datenträgers in einem von diversen Perso-

1 Kühling/Buchner/Jandt, DS-GVO Art. 4 Nr. 12 Rn. 6 ff.

2 Art.-29-Datenschutzgruppe, WP 250 rev.01 (Stand: 06.02.2018), S. 12, bestätigt durch den EDSA am 25.05.2018.

nen frequentierten Bereich wird von einer hinreichenden Gewissheit im vorgenannten Sinne auszugehen sein. Vorliegend ist U damit eine Verletzung des Schutzes personenbezogener Daten bekanntgeworden.

Während eine Benachrichtigungspflicht nach Art. 34 DS-GVO nur besteht, wenn aufgrund der Schutzverletzung voraussichtlich ein hohes Risiko für die betroffenen Personen besteht, begründet bei Art. 33 DS-GVO jedes nicht auszuschließende Risiko die Meldepflicht gegenüber der Behörde. Die Meldepflicht ist damit der Regelfall.³ Nur die Meldung von Bagatellfällen soll nach Art. 33 DS-GVO ausgeschlossen sein.⁴ Bei der Entscheidung, ob voraussichtlich kein Risiko für die betroffenen Personen besteht, handelt es sich um eine Prognoseentscheidung, für deren Richtigkeit der für die Verarbeitung Verantwortliche die Verantwortung trägt.⁵ Hier spricht nichts dafür, dass aus dem Vorfall keine Risiken für die betroffenen Beschäftigten entstehen. Im Gegenteil: Aufgrund der Sensibilität der auf dem verlorenen Datenträger enthaltenen Informationen und der naheliegenden Möglichkeit sozialer und beruflicher Nachteile liegt vorliegend sogar ein hohes Risiko für die Betroffenen nahe. Vgl. dazu nachfolgend unter 3.

Mithin ist hier die Meldepflicht gegenüber der zuständigen Datenschutzaufsichtsbehörde nach Art. 33 Abs. 1 DS-GVO zu bejahen.

Die Meldung nach Art. 33 DS-GVO hat „unverzüglich“ (englische Fassung „without undue delay“) zu erfolgen. Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sind die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person zu berücksichtigen (Erwägungsgrund 87). Je gravierender der Vorfall ist, desto kürzer ist also der Zeitraum für die unverzügliche Meldung bemessen.⁶ Was regelmäßig als angemessene und nicht schuldhaftige Verzögerung anzusehen ist, wird durch die DS-GVO selbst konkretisiert, die davon ausgeht, dass die Information der Behörde „möglichst binnen 72 Stunden“ zu erfolgen hat. Wird die 72-Stunden-Frist überschritten, löst dies gemäß Art. 33 Abs. 1 S. 2 DS-GVO eine Begründungspflicht gegenüber der Aufsichtsbehörde aus.

Vorgaben zum (Mindest-)Inhalt der Meldung des Verantwortlichen an die Behörde enthält Art. 33 Abs. 3 DS-GVO. Die Verpflichtung zur Meldung entfällt nicht allein deshalb, weil noch nicht alle Mindestinhalte zur Meldung vorliegen. Dies zeigt Art. 33 Abs. 4 DS-GVO, der in solchen Fällen eine schrittweise Information der Behörde fordert.

Eine bestimmte Form der Meldung an die Aufsichtsbehörde ist nicht vorgeschrieben. Die Meldung kann danach im Grundsatz auf alle erdenklichen Arten erfolgen, also (fern-) mündlich, per Fax, Email oder Brief, allerdings trägt der Meldepflichtige das Risiko des Zugangsnachweises. Viele Aufsichtsbehörden stellen inzwischen Onlinemeldeformulare zum Ausfüllen im Browser bereit und präferieren im Sinne der Verwaltungsvereinfachung eine Meldung über diesen Kanal. Teilweise werden auch nur Formulare zum Download und anschließendem Versand per Post, Fax oder Email angeboten.

3. Verpflichtung zur Benachrichtigung der Beschäftigten, Art. 34 DS-GVO

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche gemäß Art. 34 DS-GVO außerdem die betroffenen Personen, hier also die Beschäftigten, bezüglich des Datenschutzvorfalls zu informieren.

Das Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten i.S.v. Art. 4 Nr. 12 DS-GVO wurde bereits oben unter 2. bejaht. Entscheidend ist damit, ob im vorliegenden Fall von einem voraussichtlich hohen Risiko für die persönlichen Rechte und Freiheiten der vom Verlust des USB-Sticks betroffenen Beschäftigten auszugehen ist.

Als Risiken für die Rechte und Freiheiten natürlicher Personen sind alle drohenden physischen, materiellen oder immateriellen Schäden zu berücksichtigen, wie etwa Verlust der Kontrolle über die personenbezogenen Daten oder Einschränkung der Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile (vgl. Erwägungsgrund 85).

Bei der Risikobewertung sollen aus Sicht des EDSA insbesondere folgende Faktoren Berücksichtigung finden:⁷ Art der Datenschutzverletzung, Art/Sensibilität/Umfang der personenbezogenen Daten, Identifizierbarkeit betroffener Personen, Schwere der Folgen für die betroffenen Personen, besondere Eigenschaften der betroffenen Person oder des Verantwortlichen sowie Zahl der betroffenen Personen. Zu prüfen sei die Schwere der möglichen Folgen für die Rechte und Freiheiten der betroffenen Personen in Verbindung mit der Eintrittswahrscheinlichkeit dieser Folgen, so der EDSA. Das Risiko steige dabei zum einen mit zunehmender Schwere und zum anderen mit steigender Eintrittswahrscheinlichkeit der Folgen einer Datenschutzverletzung. In Zweifelsfällen rät der EDSA, sicherheitshalber eine Meldung vorzunehmen.

Unter Zugrundelegung vorgenannter Kriterien ist hier von einem voraussichtlich hohen Risiko i.S.v. Art. 34 Abs. 1 DS-GVO auszugehen. Nachdem der USB-Stick nicht durch einen ehrlichen Finder zurückgebracht wurde und nicht mehr auffindbar ist, spricht einiges dafür, dass ein/-e andere/-r Mitarbeiter/-in diesen im Mitarbeiterparkhaus an sich ge-

3 Laue/Kremer/Laue, Das neue Datenschutzrecht in der betrieblichen Praxis, § 7 Rn. 45.

4 Franck, GDD-Ratgeber Datenpannen – Melde- und Benachrichtigungspflichten nach DS-GVO und BDSG, 3. Aufl. 2021, S. 42. Um den Umgang mit den Meldungen noch beherrschen zu können, filtern die Datenschutzaufsichtsbehörden im Rahmen ihrer Onlinemeldeverfahren für Datenschutzverletzungen allerdings teilweise auch oberhalb der Bagatellschwelle aus.

5 Ehmann/Selmayr/Hladjk, DS-GVO Art. 33 Rn. 11 f.

6 Kühling/Buchner/Jandt, DS-GVO Art. 33 Rn. 15.

7 Art.-29-Datenschutzgruppe, WP 250 rev. 01 (Stand: 06.02.2018), S. 27 ff., bestätigt durch den ED-SA am 25.05.2018.

nommen hat und auch auf diesen zugegriffen hat bzw. dies noch tun wird. Bei den Gehaltsabrechnungen und Mitarbeiterbewertungen handelt es sich um sensible Informationen. So können Gehaltsabrechnungen z.B. Informationen zu Lohnpfändungen enthalten und damit Rückschlüsse auf die finanzielle Lage der betroffenen Beschäftigten zulassen. Auch sind über die Abrechnung Rückschlüsse auf die familiäre Situation (Steuerklasse, Freibeträge) und die Religionszugehörigkeit möglich. Letztere zählt zu den besonders geschützten besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO. Ein hohes Risiko i.S.v. Art. 34 DS-GVO wird regelmäßig u.a. dann angenommen, wenn die Vertraulichkeit besonderer Kategorien personenbezogener Daten oder von Bankverbindungs- oder Kreditkartendaten verletzt wird.⁸ Lohn- und Gehaltsabrechnungen enthalten sowohl Daten nach Art. 9 DS-GVO als auch Bankverbindungsdaten.

Besonders in nicht tarifgebundenen Unternehmen eröffnen öffentlich gewordene Gehaltsinformationen außerdem erhebliches Konfliktpotenzial, da Gerechtigkeitsdiskussionen drohen. Vermeintlich zu gut entlohnte Beschäftigte laufen Gefahr, Zielscheibe kollegialer Missgunst und schlimmstenfalls sogar von Mobbing zu werden. Wer schlechter verdient als vergleichbare Kollegen/-innen, läuft Gefahr, den Respekt der anderen zu verlieren. Bei einem Bekanntwerden von Mitarbeiterbewertungen drohen ähnliche Folgen. Es besteht zudem die Gefahr, dass bekanntgewordene Informationen aus den Bewertungen zweckentfremdet werden, um andere Karrieren zu behindern und selbst beruflich voranzukommen. Ganz generell lässt sich festhalten, dass die auf dem USB-Stick enthaltenen Informationen brisanten Gesprächsstoff für die Belegschaft bieten und für potenziell viel Klatsch und Tratsch und einigen betrieblichen Unfrieden sorgen dürften, so sie sich verbreiten.

Eine Benachrichtigung der betroffenen Personen ist damit nur dann nicht erforderlich, wenn eine Ausnahme des Art. 34 Abs. 3 DS-GVO einschlägig ist. Wären die Informationen auf dem Stick entsprechend dem Stand der Technik verschlüsselt, käme eine Ausnahme von der Benachrichtigungspflicht nach Art. 34 Abs. 3 lit. a DS-GVO in Betracht. Möglich ist eine Hardware- oder Software-basierte-Verschlüsselung von USB-Sticks. Nach dem Sachverhalt waren aber weder Verschlüsselung noch auch nur ein einfacher Zugriffsschutz vorhanden. Auch für eine Ausnahme nach Art. 34 Abs. 3 lit. b DS-GVO bestehen keine Ansatzpunkte. Hierüber könnte man ggf. diskutieren, wenn es sich um einen USB-Stick gehandelt hätte, der auch eine Fernlöschung ermöglicht. Auch an einem unverhältnismäßigen Aufwand i.S.v. Art. 34 Abs. 3 lit. c DS-GVO fehlt es. Als Arbeitgeber kann der Verantwortliche die Beschäftigten ohne großen Aufwand kontaktieren. Sofern nicht klar ist, welche konkreten Mitarbeiter betroffen sind, kommt ein Rundschreiben an alle Beschäftigten in Frage.

U muss also auch die von dem Datenschutzvorfall betroffenen Beschäftigten nach Art. 34 DS-GVO benachrichtigen. Die Benachrichtigung muss unverzüglich, also ohne schuld-

haftes Zögern erfolgen. Bezüglich des Inhalts der Benachrichtigung ist Art. 34 Abs. 2 DS-GVO maßgeblich. Es ist insbesondere auf eine klare und einfache Sprache zu achten.

4. Rolle des DSB

Die Aufgaben des DSB ergeben sich aus Art. 39 DS-GVO. Danach hat der DSB den Verantwortlichen sowie die dort konkret mit der Datenverarbeitung Beschäftigten hinsichtlich ihrer datenschutzrechtlichen Pflichten zu unterrichten und beraten (Art. 39 Abs. 1 lit. a DS-GVO). Unterrichtung meint insofern die allgemeine Information über die bestehenden datenschutzrechtlichen Verpflichtungen, Beratung die Unterstützung bei der Lösung von konkreten datenschutzrechtlichen Fragestellungen.⁹ Weitere Kernaufgabe neben der Unterrichtung und Beratung ist die Überwachung der Einhaltung des Datenschutzes (Art. 39 Abs. 1 lit. b DS-GVO). Zu überwachen ist im Einzelnen die Einhaltung der DS-GVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien („policies“) der benennenden Stelle für den Schutz personenbezogener Daten. Sicherzustellen und nachzuweisen, dass durchgeführte Datenverarbeitungen im Einklang mit den datenschutzrechtlichen Anforderungen stehen, ist Aufgabe des Verantwortlichen bzw. – in abgeleiteter Verantwortlichkeit – der Fachabteilung.¹⁰ Die Verantwortung für die Einhaltung des Datenschutzes kann dem DSB auch nicht übertragen werden, da sich dieser dann selbst überwachen müsste und es ihm insofern als internem Überwachungsorgan an der notwendigen Unabhängigkeit (ErwGr 97 S. 3 DS-GVO) fehlen würde.¹¹ Weitere Aufgaben des DSB sind gemäß Art. 39 DS-GVO die Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) sowie die Zusammenarbeit mit der Datenschutzaufsichtsbehörde und die Tätigkeit als deren Anlaufstelle.

Auch wenn der DSB hier also zu Recht annimmt, dass bezüglich des konkreten Datenschutzvorfalls eine Meldung an die Aufsichtsbehörde wie auch eine Information der betroffenen Beschäftigten vorzunehmen ist, ist er gleichwohl nicht in der Position, entsprechende Maßnahmen von der Unternehmensleitung zu verlangen, denn, wie dargestellt, hat er lediglich beratende Funktion. Die Entscheidung, ob eine Meldung bzw. Benachrichtigung tatsächlich vorgenommen wird, verbleibt bei der Leitung.

Inhaltlich richtig ist auch, eine Richtlinie zum Umgang mit mobilen Datenträgern in Kraft zu setzen. Unternehmen sind nach der DS-GVO verpflichtet, jederzeit nachweisen zu können, dass und wie sie die geltenden Datenschutzerfordernungen umsetzen (Rechenschaftspflicht oder Accountabi-

⁸ Kühling/Buchner/Jandt, DS-GVO Art. 34 Rn. 5; Simitis/Hornung/Spietker/Dix, DS-GVO Art. 34 Rn. 5.

⁹ GDD-Praxishilfe: Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung, Stand: Juli 2019, S. 12 ff.

¹⁰ GDD-Praxishilfe: Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung, Stand: Juli 2019, ebenda.

¹¹ GDD-Praxishilfe: Verantwortlichkeiten und Aufgaben nach der DS-GVO, Stand: Aug. 2021, S. 14.

lity, Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO). In der Praxis hat sich die Erstellung und Einführung von Datenschutzrichtlinien bewährt, um die Umsetzung des Datenschutzes und den diesbezüglichen kontinuierlichen Verbesserungsprozess zu dokumentieren. Während Leitlinien zum Datenschutz die Datenschutzziele einer Organisation in Grundzügen beschreiben, geben Richtlinien den Rahmen zur Umsetzung konkreter Maßnahmen zur Erreichung dieser Ziele vor.¹² Der hier zu beurteilende Datenschutzvorfall selbst zeigt die Sinnhaftigkeit entsprechender interner Vorgaben. Gäbe es bei U bereits eine entsprechende Richtlinie, hätte sich der Vorfall in dieser Form gar nicht ereignet, bzw. dieser hätte zumindest einen – per Ermahnung, ggf. sogar Abmahnung – sanktionierbaren Verstoß gegen die Richtlinie dargestellt. Denn unter Geltung einer sachgerecht gestalteten Richtlinie zum Umgang mit mobilen Datenträgern hätten die hier relevanten Daten nicht ohne Verschlüsselung und Zugriffsschutz auf dem USB-Stick transportiert werden dürfen.

Neben Regelungen zum Umgang mit mobilen Datenträgern sollten auch interne Vorgaben zum Umgang mit potenziell meldepflichtigen Datenschutzvorfällen existieren. Besonders für größere und international agierende Unternehmen kann die Einhaltung der 72-Stunden-Vorgabe aus Art. 33 Abs. 1 S. 1 DS-GVO eine nicht zu unterschätzende Herausforderung dar-

stellen.¹³ Eine unverzügliche Meldung ist nur möglich, wenn bereits vor dem Ernstfall entsprechende prozessuale Vorkehrungen getroffen wurden und sich vorausplanend mit Inhalt und Form der Meldung befasst wurde. Die konkret mit der personenbezogenen Datenverarbeitung befassten Mitarbeiter/-innen in den Fachabteilungen müssen wissen, was bei einem potenziellen Datenschutzvorfall zu tun ist.

Die Inkraftsetzung entsprechender interner Regelungen bzw. die Entscheidung über deren konkreten Inhalt fällt aber wieder ausschließlich in den Verantwortungsbereich der Unternehmensleitung bzw. von dieser hiermit betrauter Personen. Der DSB ist beratend einzubeziehen bei der Erstellung datenschutzrelevanter interner Regelwerke. Er kann Empfehlungen machen und z.B. Formulierungsvorschläge oder Muster liefern.

Der DSB sollte die Unternehmensleitung über deren Pflichten informieren und auf mögliche Risiken bei Nichteinhaltung hinweisen. Sofern die Leitung seinen Empfehlungen nicht nachkommt, sollte der DSB dies entsprechend dokumentieren.

¹² Zum Ganzen ausführlich GDD-Praxishilfe DS-GVO, Die Datenschutzrichtlinie.

¹³ Vgl. Sydow/Wilhelm, Art. 33 Rn. 15; Simits/Hornung/Spiecker/Dix, DS-GVO Art. 33 Rn. 17.

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (57): LDI NRW, 26. Bericht 2021, S. 122: Betriebliche DSB und Kurzarbeit

Zusammengestellt und erläutert von Prof. Peter Gola*

Die Zahl der Corona-Neuinfektionen in Deutschland geht zurück. Doch noch immer bestimmt die COVID-19-Pandemie das Geschehen in der Wirtschaft und damit auch die Arbeit der Datenschutz-Aufsichtsbehörden. Das belegen die aktuellen Tätigkeitsberichte. So verzeichnete der HambBfDI im Pandemiejahr 2020 rund 3000 datenschutzrechtliche Beschwerden, etwa 500 mehr als im Vorjahr. Das ULD Schleswig-Holstein erreichte eine um 300 Fälle erhöhte Zahl von Eingaben. Nicht dokumentiert, aber naheliegend und im Grunde zwingend musste coronabedingte Mehrbeschäftigung auch bei betrieblichen Datenschutzbeauftragten anfallen. Die Einbindung der Datenschutzexperten in die aktuellen Fragestellungen war und ist fast unerlässlich und für eine Vielzahl von Unternehmen sogar verpflichtend.

Die Corona-Pandemie bleibt nämlich nicht ohne Auswirkung auf die Tätigkeit der betrieblichen Datenschutzbeauftragten. Diese sind mit vielen neuen datenschutzrechtlichen Fragestellungen konfrontiert, die sich aus der Corona-bedingten Änderung bisheriger Arbeitsabläufe in einem Unter-

nehmen ergeben. Die Neuorganisation von Arbeitsprozessen, die Zunahme der elektronischen Datenverarbeitung, das Arbeiten im Homeoffice, in Tele-Arbeit und mittels Videokonferenzsystemen sowie nicht zuletzt Fragen des Gesundheitsdatenschutzes bei Beschäftigten und Kunden erfordern die Einbindung der betrieblichen Datenschutzbeauftragten.

Andererseits waren und sind – u.a. durch coronabedingte Lieferengpässe – Unternehmen gezwungen, auf Kurzarbeit zurückzugreifen. Im umfassendsten Fall kann Kurzarbeit bedeuten, dass Mitarbeiter von ihrer Arbeitspflicht vollständig befreit werden, wobei sich dann die Frage stellt, ob ein interner Datenschutzbeauftragter im Fall von Kurzarbeit berücksichtigt werden kann.

Die LDI NRW hat sich in einer Kurzmeldung (vom 27. 05. 2020) und in ihrem aktuellen Tätigkeitsbericht (26. Bericht 2021, S. 123) zu dieser Frage geäußert. Ihr Fazit lautet:

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

betriebliche Datenschutzbeauftragte sind auch bei Corona-bedingter Kurzarbeit unverzichtbar: Ihnen ist auch in dieser Zeit die Wahrnehmung der Kontroll- und Beratungsaufgaben zu ermöglichen (Art. 38 Abs. 2 DS-GVO): Das gilt insbesondere für den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen. Daran ändert die Einführung von Kurzarbeit nichts.

Meistens arbeitet ein Unternehmen in verringertem Umfang weiter. Und selbst wenn ein Unternehmen für bestimmte Zeit seine Tätigkeit einstellt, besteht es weiter, hat Beziehungen zu Beschäftigten, Kunden etc. und verarbeitet deren Daten. Deshalb werden Datenschutzbeauftragte weiter gebraucht und müssen ihre Aufgaben erfüllen können.“

Auch an der Benennungspflicht nach dem Bundesdatenschutzgesetz (BDSG) ändere sich nichts. Zwar komme es nach § 38 Abs. 1 BDSG darauf an, dass Personen „in der Regel (...) ständig“ mit der Verarbeitung personenbezogener Daten beschäftigt sind. Mit dieser Formulierung ist aber gerade nicht gemeint, dass kurzzeitige Veränderungen berücksichtigt werden, sondern dass es auf eine langfristige Betrachtung ankommt. Wenn also vor und voraussichtlich auch nach der zeitlich begrenzten Kurzarbeit mindestens 20 Personen gezählt werden, bleibt es auch während der Kurzarbeit bei der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten.

Die LDI akzeptiert, dass es nach den jeweiligen Umständen geboten sein kann, den Arbeitsumfang des DSB zu reduzieren, weil vorübergehend weniger Zeit für die Aufgabe als Datenschutzbeauftragter erforderlich ist. Andererseits stellt sie wie folgt fest: „Das Arbeitsfeld der oder des Datenschutzbeauftragten darf jedoch keinesfalls vollständig

„brach liegen“. Vielmehr ist zu prüfen, unter welchen Voraussetzungen Datenschutzbeauftragte in der aktuellen Situation ihre Pflichten weiterhin wahrnehmen können. Datenschutzbeauftragte müssen nach wie vor seitens des Verantwortlichen bzw. des Auftragsverarbeiters ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden; sie müssen die Möglichkeit haben, regelmäßig ihre Posteingänge sichten zu können, sowie telefonisch und/oder per E-Mail als Ansprechpartner*in für die Beschäftigten, Kund*innen oder andere betroffene Personen erreichbar sein. Um dies sicherzustellen, sollten geeignete Maßnahmen ergriffen werden, beispielsweise regelmäßiger Zugang zum Büro oder Einrichtung eines Tele-Arbeitsplatzes, Bereitstellen eines Diensthandys, Vereinbarung bestimmter „Sprechzeiten“. Wie viel Zeit Datenschutzbeauftragte unter den aktuellen Umständen benötigen und welche Maßnahmen sachgerecht sind, sollten Arbeitgeber*innen mit ihren Datenschutzbeauftragten abstimmen.“

Fazit ist also: „Trotz Kurzarbeit in einem Unternehmen müssen die betrieblichen Datenschutzbeauftragten weiter in der Lage sein, ihre gesetzlichen Aufgaben wahrzunehmen und als Ansprechpartner für Betroffene zur Verfügung zu stehen. Die Verantwortlichen sind gesetzlich verpflichtet, die Datenschutzbeauftragten auch während der Kurzarbeit bei der Erfüllung ihrer Aufgaben zu unterstützen und die entsprechenden Rahmenbedingungen zu schaffen. Geboten ist eine bewusste und dokumentierte Entscheidung. Verfehlt wäre es, den internen Datenschutzexperten im Rahmen von Kurzarbeitsmaßnahmen vorschnell von seinen Aufgaben zu entbinden, vielmehr kann sogar die Nicht-Einbeziehung in die Kurzarbeit geboten sein.“

Nochmals: Zur Statthaftigkeit der Anfechtungsklage im kirchengerichtlichen Datenschutzverfahren

Robert Gmeiner*

I. Einleitung

Nur wenige Wochen, nachdem in dieser Zeitschrift ein Aufsatz zur Praxis des erstinstanzlichen Interdiözesanen Datenschutzgerichts (IDSG) bezüglich der Statthaftigkeit von Anfechtungsanträgen im kirchlichen Datenschutzverfahren erschien,¹ hat sich das zweit- und letztinstanzliche Datenschutzgericht der Deutschen Bischofskonferenz (DBK-DSG; nachfolgend: Datenschutzgericht) zu der Thematik geäußert und die Praxis des Interdiözesanen Datenschutzgerichts bestätigt.² Da der Beschluss in dem Aufsatz noch nicht berücksichtigt werden konnte, sei er an dieser Stelle besprochen.

II. Entscheidung des DBK-DSG

Die Antragstellerin beehrte im erstinstanzlichen Verfahren die Feststellung, dass ihre Maßnahmen zur Überprüfung der Einhaltung des Corona-Schutzkonzepts entgegen einem Bescheid des Katholischen Datenschutzzentrums keine Datenschutzverletzung darstelle. Diesem Antrag hat das Interdiöze-

* Der Autor ist Rechtsreferendar am LG Ellwangen (Jagst) und wissenschaftliche Hilfskraft am Lehrstuhl für Öffentliches Recht, Finanz- und Steuerrecht (Prof. Dr. Hellermann) an der Universität Bielefeld.

1 Gmeiner, RDV 2021, 148-150.

2 DBK-DSG, Beschl. v. 12.07.2021 – DBK-DSG 01/2021, Rn. 17.

sane Datenschutzgericht entsprochen.³ Dagegen hat das Katholische Datenschutzzentrum als Antraggeber Beschwerde zum zweitinstanzlichen Datenschutzgericht erhoben und beantragte die Aufhebung des erstinstanzlichen Beschlusses.

Obwohl die Antragstellerin vom Gericht lediglich eine gerichtliche Feststellung begehrte,⁴ hat das Datenschutzgericht⁵ zur Statthaftigkeit eines Anfechtungsantrags im kirchengerichtlichen Datenschutzverfahren ausgeführt: Die Konstellation, wonach sich ein Antragsteller gegen einen datenschutzrechtlichen Bescheid wende, sei von § 14 Abs. 2 KDSGO nicht unmittelbar erfasst. Es gehöre indes gem. § 2 Abs. 1 KDSGO zu den Aufgaben des Kirchengerichts, Entscheidungen der Datenschutzaufsicht zu überprüfen. Weise der kirchliche Gesetzgeber dem Gericht diese Aufgabe zu, müsse es nicht nur bei unbegründeten, sondern auch bei begründeten Anträgen entsprechende Tenorierungsmöglichkeiten haben, da das gerichtliche Ergebnis nicht vorab terminiert sein könne. § 14 Abs. 2 KDSGO könne deshalb nicht abschließend sein. Das Datenschutzgericht teile daher die Rechtsauffassung des erstinstanzlichen Interdiözesanen Datenschutzgerichts, wonach Anfechtungsanträge auch ohne Nennung in § 14 Abs. 2 KDSGO statthaft seien. Als Minus dazu seien daher auch Feststellungsanträge statthaft, wenn die Datenschutzaufsicht ein Vorgehen in einem Bescheid für datenschutzrechtlich unzulässig halte. Diese könnten auf § 14 Abs. 2 lit. c) KDSGO gestützt werden, der nur auf das Vorliegen eines Datenschutzverstoßes anwendbar sei.⁶

III. Bewertung der Entscheidung

1. Anwendungsbereich des § 14 Abs. 2 KDSGO

Zunächst hat das Datenschutzgericht ausgeführt, dass die Konstellation des Vorliegens eines datenschutzrechtlichen Bescheids von § 14 Abs. 2 KDSGO nicht unmittelbar erfasst sei. Wie es zu dieser Einschätzung gelangt, erläutert es indes nicht. Diese Aussage liegt auch nicht auf der Hand, schließlich zeigte das Interdiözesane Datenschutzgericht in einer – wenn auch singulären gebliebenen – Entscheidung keine Bedenken, auch beim Vorliegen eines Bescheids ausschließlich einen Feststellungsantrag nach § 14 Abs. 2 lit. c) KDSGO für statthaft zu erachten.⁷ Mit dem Argument, dass Rechtsschutz gegen Bescheide außerhalb des Anwendungsbereichs des § 14 Abs. 2 lit. c) KDSGO liege, übernimmt das Datenschutzgericht zwar die überwiegende Rechtsprechung des Interdiözesanen Datenschutzgerichts.⁸ Das erstinstanzliche Gericht ging aber dennoch zunächst vom Leitbild des Feststellungsantrags auch in dieser Konstellation aus. Die Statthaftigkeit eines Anfechtungsantrags begründete es mit einem Interesse an der Rechtsklarheit.⁹ Das zweitinstanzliche Datenschutzgericht verkürzt diese Argumentation dahingehend, dass es aufgrund der fehlenden Anwendbarkeit des § 14 Abs. 2 lit. c) auf datenschutzrechtliche Bescheide die Möglichkeit eines Anfechtungsantrags geben müsse. Das eigentliche Hauptargument des Interdiözesanen Datenschutzgerichts, die Anfechtung diene (primär) der Rechtsklarheit, übergeht das Datenschutzgericht hingegen.¹⁰

Ungeachtet dessen, dass das Datenschutzgericht die Argumentation des Interdiözesanen Datenschutzgerichts verkürzt, bleibt des Weiteren offen, weshalb der Anwendungs-

bereich des § 14 Abs. 2 lit. c) KDSGO nicht eröffnet sein soll, wenn sich die Klage gegen einen Bescheid richtet. Der Normwortlaut steht dem jedenfalls nicht entgegen. Danach erkennt das Gericht auf Feststellung des Vorliegens und Umfangs einer Datenschutzverletzung. Wie sich aus § 8 Abs. 2 S. 1 KDSGO ergibt, kann eine gerichtlich rügefähige Datenschutzverletzung auch in einer rechtsfehlerhaften Entscheidungen der Datenschutzaufsicht zulasten des datenschutzrechtlich Verantwortlichen liegen.¹¹ Eine begriffliche Einschränkung der Rechtsnatur der Entscheidung der Datenschutzaufsicht unter Ausschluss seiner Bescheide in § 2 Abs. 1 S. 1, § 8 Abs. 2 S. 1 KDSGO erfolgt hingegen nicht.¹² Eine Datenschutzverletzung i.S.v. § 14 Abs. 2 lit. c) KDSGO liegt daher nicht nur dann vor, wenn das subjektive Datenschutzrecht einer natürlichen Person (§ 4 Nr. 1 KDG, Art. 4 Nr. 1 DS-GVO)¹³ durch einen Verantwortlichen verletzt wurde. Vielmehr kann auch eine rechtsfehlerhafte Beurteilung des Datenschutzrechts durch die Datenschutzaufsicht mittels eines Bescheids eine Verletzung des Datenschutzrechts und damit eine Datenschutzverletzung darstellen.

2. Fehlende Tenorierungsmöglichkeit

Als zweites Argument für die Statthaftigkeit der Anfechtungsanträge nennt das Datenschutzgericht die ansonsten fehlende Tenorierungsmöglichkeit für begründete Anträge. Zunächst ist der Gedanke zwar richtig, dass es sinnvoll ist, wenn dem Gericht die prozessualen Mittel zur Verfügung stehen, die es benötigt, um die Entscheidungen der Datenschutzaufsicht zu überprüfen und Datenschutzrechte durchzusetzen, wie es in § 2 Abs. 1 KDSGO beschrieben ist. Ob dies allerdings dazu führen darf, dass im Prozessrecht eine Vermischung von Aufgaben- und Befugnisnormen zulässig ist,¹⁴ kann letztendlich dahinstehen. Selbst wenn man aus § 2 Abs. 1 KDSGO die Befugnis herausliest, geeignete gerichtliche Maßnahmen zur Rechtsdurchsetzung gegen rechtswidrige Bescheide zu ergreifen, bedeutet dies nicht, dass

3 IDSG, Beschl. v. 01.03.2021 – IDSG 27/2020.

4 DBK-DSG, Beschl. v. 12.07.2021 – DBK-DSG 01/2021, Rn. 3, 16 sowie IDSG, Beschl. v. 01.03.2021 – IDSG 27/2020, Rn. 14.

5 Siehe bereits die erstinstanzliche Entscheidung: IDSG, Beschl. v. 01.03.2020 – IDSG 27/2020, Rn. 22-24.

6 DBK-DSG, Beschl. v. 12.07.2021 – DBK 01/2021, Rn. 17.

7 IDSG, Beschl. v. 05.05.2020 – IDSG 02/2018, Rn. 17.

8 IDSG, Beschl. v. 15.05.2019 – IDSG 01/2018, Rn. 23; Beschl. v. 01.03.2021 – IDSG 27/2020, Rn. 22 m.w.N.

9 IDSG, Beschl. v. 15.05.2019 – IDSG 01/2018, Rn. 23.

10 Ebenfalls verkürzt: IDSG, Beschl. v. 19.04.2021 – IDSG 14/2020, Rn. 24; Beschl. v. 12.07.2021 – IDSG 21/2020, Rn. 58.

11 IDSG, Beschl. v. 14.12.2020 – IDSG 01/2020, Rn. 31; Beschl. v. 01.03.2021 – IDSG 27/2020, Rn. 27; Beschl. v. 19.04.2021 – IDSG 14/2020, Rn. 28; Beschl. v. 12.07.2021 – IDSG 21/2020, Rn. 62.

12 So die Beschlüsse des IDSG in der vorhergehenden Fußnote. Aus den Begründungen ist nicht ersichtlich, ob sich der Einschluss der Bescheide in den Anwendungsbereich unmittelbar aus § 8 Abs. 2 S. 1 KDSGO ergibt oder nur, weil die Anfechtungsklage statthaft ist.

13 Die Verarbeitung von Daten juristischer Personen unterfällt nicht der DS-GVO: ErwGr 14 S. 2; Gola, in: ders. (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 23-25; für das kirchliche Datenschutzrecht ergeben sich für § 4 Nr. 1 KDG keine Besonderheiten, sodass der Begriff inhaltsgleich mit Art. 4 Nr. 1 DS-GVO ist: Herrlein, in: Sydow (Hrsg.), Kirchliches Datenschutzrecht, 2021, § 4 Rn. 3.

14 Zur Trennung von Aufgaben- und Befugnisnormen im Verwaltungsrecht: Bull/Mehde, Allgemeines Verwaltungsrecht mit Verwaltungslehre, 9. Aufl. 2015, Rn. 550, 552; relativierend noch: Knemeyer, DÖV 1978, 11-17.

dazu gedanklich zwingend eine Kassationsbefugnis gehören müsste. Eine Feststellung der Rechtswidrigkeit eines Bescheids würde ausreichen, um begründeten Anträgen zum Erfolg zu verhelfen.¹⁵ In der Rechtsprechung des Bundesverwaltungsgerichts ist anerkannt, dass von einem Verwaltungsakt, dessen Rechtswidrigkeit gem. § 113 Abs. 1 S. 4 VwGO verwaltungsgerichtlich rechtskräftig festgestellt wurde, keine Rechtswirkungen mehr ausgehen können.¹⁶ Dem folgt auch das Interdiözesane Datenschutzgericht.¹⁷ Freilich ist das Datenschutzgericht nicht an die Rechtsprechung des Bundesverwaltungsgerichts gebunden, sodass es einem Feststellungsbeschluss nach § 14 Abs. 2 lit. c) KDSGO andere Rechtswirkungen zuerkennen kann.¹⁸ Das Datenschutzgericht hat aber in einem anderen Verfahren, jedoch in derselben personellen Besetzung wie in dem vorliegend besprochenen Beschluss, selbst angenommen, dass allgemeine Wertungen der VwGO auf das kirchliche Datenschutzverfahren übertragbar seien. Dort vertrat es die Ansicht, dass das Erfordernis des Feststellungsinteresses in § 43 Abs. 1 Hs. 2 VwGO ein allgemeines Prinzip sei, welches auch im kirchengerichtlichen Verfahren gelte. Dies ergebe sich daraus, dass auch das kirchengerichtliche Verfahren der Rechtsdurchsetzung und nicht der abstrakten Klärung von Rechtsfragen diene.¹⁹

Ebenso wie das Feststellungsinteresse,²⁰ kann auch die Rechtsprechung des Bundesverwaltungsgerichts zu den fehlenden Rechtswirkungen eines nach § 113 Abs. 1 S. 4 VwGO als rechtswidrig festgestellten Verwaltungsaktes auf ein allgemeines Rechtsprinzip zurückgeführt werden; nämlich auf Treu und Glauben.²¹ Der Grundsatz von Treu und Glauben ist dem kanonischen Recht seinerseits nicht fremd.²² Aufgrund des Primats des kirchlichen Heildienstes muss dieser Grundsatz die gesamte kirchliche Rechtspflege beherrschen.²³ Daher verfolgt das kirchliche Prozessrecht in can. 221 § 2, can. 1446 § 2 CIC das Ziel, eine billige Entscheidung durch das Kirchengericht herbeizuführen.²⁴ Wenn der allgemeine Grundsatz des allgemeinen Rechtsschutzbedürfnisses aus dem staatlichen Prozessrecht in die kirchliche Gerichtsordnung übertragen werden kann, stellt sich die Frage, weshalb dies nicht auch für den – noch zudem kirchenrechtlich selbst anerkannten – Grundsatz von Treu und Glauben mit den damit verbundenen prozessualen Konsequenzen gelten sollte.

3. Problematik des Wahlrechts

Unterstellt man dagegen die Richtigkeit der Argumentation des Datenschutzgerichts, dann stellt sich die Frage nach der Konsistenz seiner Rechtsprechung. Das Interdiözesane Datenschutzgericht hat im vorliegend besprochenen Rechtsstreit ein Wahlrecht des Antragstellers zwischen Anfechtungs- und Feststellungsantrag angenommen. Ein Antragsteller könne wählen, ob er einen rechtsschutzintensiveren Anfechtungsantrag oder einen weniger rechtsschutzintensiven Feststellungsantrag stelle.²⁵ Dies wurde vom Datenschutzgericht im vorliegend besprochenen Beschluss nicht in Frage gestellt.²⁶ Eine mit § 43 Abs. 2 S. 1 VwGO vergleichbare Subsidiarität besteht demnach im kirchengerichtlichen Verfahren nicht.

Die Subsidiaritätsregel in § 43 Abs. 2 S. 1 VwGO lässt sich ebenfalls auf das allgemeine Rechtsschutzbedürfnis zurückführen²⁷ – das nach der Rechtsprechung des Datenschutzgerichts auch im kirchengerichtlichen Verfahren gelte²⁸ –, so-

dass sie grundsätzlich auch im Verfahren nach der KDSGO anwendbar wäre. Folge wäre, dass ein Antragsteller nicht zwischen verschiedenen Verfahrensarten wählen dürfte; ein Feststellungsantrag anstelle eines Anfechtungsantrags wäre unzulässig.²⁹ Dies würde auch folgerichtig der vom Datenschutzgericht aufgestellten Prämisse entsprechen, dass es zu seiner Aufgabenwahrnehmung nach § 2 Abs. 1 KDSGO auf die Statthaftigkeit eines Anfechtungsantrags angewiesen sei. Wenn einem Antragsteller jedoch ein Wahlrecht hinsichtlich der Verfahrensarten zusteht und er sein Anliegen genauso gut mit einem Feststellungsantrag anstelle eines Anfechtungsantrags erreichen kann, stellt sich die Frage, ob die Anfechtungsmöglichkeit tatsächlich erforderlich ist. Letztendlich dürfte das Datenschutzgericht damit die Grundlage seiner Argumentation selbst negieren.

IV. Fazit

Das Datenschutzgericht der Deutschen Bischofskonferenz hat nunmehr die Praxis des Interdiözesanen Datenschutzgerichts abgesegnet, wonach über den Wortlaut des § 14 Abs. 2 lit. c) KDSGO hinaus auch Anfechtungsanträge statthaft seien. Dieser Beschluss enthält jedoch keine neuen substantiellen Argumente zur Klärung der Frage nach der Statthaftigkeit der Anfechtungsklage im kirchengerichtlichen Datenschutzverfahren, sondern wiederholt lediglich verkürzt die Argumente des Interdiözesanen Datenschutzgerichts. Die bereits zuvor formulierten Bedenken gegen die Statthaftigkeit der Anfechtungsklage³⁰ können durch diesen Beschluss des Datenschutzgerichts der Deutschen Bischofskonferenz nicht ausgeräumt werden. Stattdessen werden neue Fragen aufgeworfen. Daher ist nach wie vor davon ausgehen, dass einem Antragsteller prozessual allein die Möglichkeit zur Feststellung der Datenschutzverletzung nach § 14 Abs. 2 lit. c) KDSGO bleibt.

15 IDSG, Beschl. v. 05.05.2020 – IDSG 02/2018, Rn. 17; Gmeiner, RDV 2021, 148 (150); ohne die prozessualen Konsequenzen daraus zu ziehen, angenommen von IDSG, Beschl. v. 15.05.2019 – IDSG 01/2018, Rn. 23.

16 BVerwGE 105, 370 (373); 116, 1 (2 f.); aus der Literatur zur Thematik: W.-R. Schenke, JZ 2003, 31-36.

17 IDSG, Beschl. v. 01.03.2021 – IDSG 27/2020, Rn. 24 mit Verweis auf Beschl. v. 05.05.2020 – IDSG 02/2018, wobei das Gericht im letztgenannten Beschluss gerade nicht von der Statthaftigkeit eines Anfechtungsantrags ausgeht.

18 Krit. zur Vergleichbarkeit kirchlichen und staatlichen Rechtsschutzes: Gmeiner, ZevKR 65 (2020), 325 (331 f.); ders. RDV 2021, 148 (149 f.).

19 DBK-DSG, Beschl. v. 20.05.2021 – DBK-DSG 02/2020, Rn. 15.

20 BVerwGE 112, 253 (255); W.-R. Schenke, in: Kopp/Schenke (Hrsg.), Verwaltungsgerichtsordnung, 27. Aufl. 2021, § 43 Rn. 23: Feststellungsinteresse als Ausdruck des allgemeinen Rechtsschutzbedürfnisses.

21 W.-R. Schenke, JZ 2003, 31 (35).

22 Als aequitate in: can. 19, can. 122, 1°, 2°, can. 221 § 2, can. 271 § 3, can. 686 § 3, can. 1148 § 3, can. 1446 § 2, can. 1560, can. 1752 CIC.

23 Socha, in: Lüdicke (Hrsg.), Münsterischer Kommentar zum Codex Iuris Canonici, Stand: 47. Erg.-Lfg. 2012, can. 19 Rn. 16.

24 Dazu: Reinhardt, in: Lüdicke (Hrsg.), Münsterischer Kommentar zum Codex Iuris Canonici, Stand: 6. Erg.-Lfg. 1987, can. 221 Rn. 7; Lüdicke, ebd., Stand: 7. Erg.-Lfg. 1988, can. 1446 Rn. 3.

25 IDSG, Beschl. v. 01.03.2021 – IDSG 27/2021, Rn. 24.

26 DBK-DSG, Beschl. v. 12.07.2021 – DBK-DSG 01/2021, Rn. 16 f.

27 Sodan, in: ders./Ziekow (Hrsg.), Verwaltungsgerichtsordnung, 5. Aufl. 2018, § 43 Rn. 114; Glaser, in: Gärditz (Hrsg.), Verwaltungsgerichtsordnung, 2. Aufl. 2018, § 43 Rn. 68; Hufen, Verwaltungsprozessrecht, 12. Aufl. 2021, § 18 Rn. 5.

28 DBK-DSG, Beschl. v. 20.05.2021 – DBK-DSG 02/2020, Rn. 15.

29 Siehe nur: BVerwG, Buchholz 236.1 § 10 Nr. 2, S. 2.

30 Gmeiner, RDV 2021, 148-150.

Rechtsprechung

Grenzen einer nationalen Regelung, die den Zugang der Öffentlichkeit zu personenbezogenen Daten über Strafpunkte für Verkehrsverstöße vorsieht

(Europäischer Gerichtshof (Große Kammer), Urteil vom 22. Juni 2021 – C-439/19 –)

- 1. Art. 10 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) ist dahin auszulegen, dass er auf die Verarbeitung personenbezogener Daten über Strafpunkte, die gegen Fahrzeugführer wegen Verkehrsverstößen verhängt wurden, anwendbar ist.**
- 2. Die Bestimmungen der Verordnung (EU) 2016/679, insbesondere ihr Art. 5 Abs. 1, ihr Art. 6 Abs. 1 Buchst. e und ihr Art. 10, sind dahin auszulegen, dass sie einer nationalen Regelung entgegenstehen, die die mit dem Register, in das die gegen Fahrzeugführer wegen Verkehrsverstößen verhängten Strafpunkte eingetragen werden, betraute öffentliche Einrichtung verpflichtet, diese Daten der Öffentlichkeit zugänglich zu machen, ohne dass die Person, die den Zugang beantragt, ein besonderes Interesse am Erhalt dieser Daten nachzuweisen hat.**
- 3. Die Bestimmungen der Verordnung (EU) 2016/679, insbesondere ihr Art. 5 Abs. 1, ihr Art. 6 Abs. 1 Buchst. e und ihr Art. 10, sind dahin auszulegen, dass sie einer nationalen Regelung entgegenstehen, die es der mit dem Register, in das die gegen Fahrzeugführer wegen Verkehrsverstößen verhängten Strafpunkte eingetragen werden, betrauten öffentlichen Einrichtung erlaubt, diese Daten Wirtschaftsteilnehmern zur Weiterverwendung zu übermitteln.**
- 4. Der Grundsatz des Vorrangs des Unionsrechts ist dahin auszulegen, dass er es dem Verfassungsgericht eines Mitgliedstaats, bei dem ein Rechtsbehelf gegen eine nationale Regelung anhängig ist, die im Licht einer Vorabentscheidung des Gerichtshofs mit dem Unionsrecht unvereinbar ist, verwehrt, in Anwendung des Grundsatzes der Rechtssicherheit zu entscheiden, dass die Rechtswirkungen dieser Regelung bis zum Zeitpunkt der Verkündung des Urteils, mit dem es endgültig über diesen verfassungsrechtlichen Rechtsbehelf entscheidet, aufrechterhalten werden.**

Ausgangsverfahren und Vorlagefragen

B ist eine natürliche Person, gegen die wegen einer oder mehrerer Verkehrsverstöße Strafpunkte verhängt wurden.

Gemäß dem Straßenverkehrsgesetz und der Verordnung Nr. 551 vom 21. Juni 2004 hat die Ceļu satiksmes drošības direkcija (Direktion für Straßenverkehrssicherheit, Lettland, im Folgenden: CSDD) diese Strafpunkte in das nationale Register für Fahrzeuge und Fahrzeugführer eingetragen.

Da die in diesem Register enthaltenen Informationen über Strafpunkte öffentlich zugänglich sind und zudem nach den Angaben von B mehreren Wirtschaftsteilnehmern zur Weiterverwendung übermittelt wurden, erhob B Verfassungsbeschwerde bei der Latvijas Republikas Satversmes tiesa (Verfassungsgericht), damit diese die Vereinbarkeit von Art. 141 Abs. 2 des Straßenverkehrsgesetzes mit dem in Art. 96 der lettischen Verfassung verankerten Grundrecht auf Achtung des Privatlebens prüft.

Die Latvijas Republikas Satversmes tiesa (Verfassungsgericht) hat das Verfahren ausgesetzt und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorgelegt:

1. Ist der in Art. 10 der DS-GVO verwendete Begriff „Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln“ dahin auszulegen, dass er auch die in der in Rede stehenden Vorschrift vorgesehene Verarbeitung von Informationen über die Punkte umfasst, die wegen Verkehrsordnungswidrigkeiten gegen Fahrzeugführer verhängt worden sind?

2. Können – unabhängig von der Beantwortung der ersten Frage – die Bestimmungen der DS-GVO, insbesondere der in Art. 5 Abs. 1 Buchst. f genannte Grundsatz der „Integrität und Vertraulichkeit“, dahin ausgelegt werden, dass sie es den Mitgliedstaaten verbieten festzulegen, dass Informationen über die wegen Verkehrsordnungswidrigkeiten gegen Fahrzeugführer verhängten Punkte jedermann zugänglich sind, und die Verarbeitung der entsprechenden Daten durch deren Offenlegung zu gestatten?

3. Sind die Erwägungsgründe 50 und 154, Art. 5 Abs. 1 Buchst. b und Art. 10 der DS-GVO sowie Art. 1 Abs. 2 Buchst. cc der Richtlinie 2003/98 dahin auszulegen, dass sie der Regelung eines Mitgliedstaats entgegenstehen, die die Übermittlung von Informationen über wegen Verkehrsordnungswidrigkeiten gegen Fahrzeugführer verhängte Punkte zum Zweck der Weiterverwendung gestattet?

4. Sollte eine der vorstehenden Fragen bejaht werden, sind dann der Grundsatz des Vorrangs des Unionsrechts und der Grundsatz der Rechtssicherheit dahin auszulegen, dass es zulässig sein könnte, die in Rede stehende Norm anzuwenden und ihre rechtlichen Wirkungen bis zum Eintritt der Rechtskraft der abschließenden Entscheidung des Verfassungsgerichts aufrechtzuerhalten?

Zu den Vorlagefragen

Zur ersten Frage

Mit seiner ersten Frage möchte das vorliegende Gericht wissen, ob Art. 10 der DS-GVO dahin auszulegen ist, dass er auf die in der Offenlegung entsprechender Daten gegenüber der

Öffentlichkeit bestehende Verarbeitung personenbezogener Daten über Strafpunkte, die gegen Fahrzeugführer wegen Verkehrsverstößen verhängt wurden, anwendbar ist.

Nach Art. 10 der DS-GVO darf die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen aufgrund von Art. 6 Abs. 1 nur unter behördlicher Aufsicht vorgenommen werden, oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist.

Daher ist zunächst zu prüfen, ob die nach der im Ausgangsverfahren in Rede stehenden Regelung an Dritte übermittelten Informationen über Strafpunkte „personenbezogene Daten“ im Sinne von Art. 4 Nr. 1 der DS-GVO sind und ob diese Übermittlung eine „Verarbeitung“ solcher Daten im Sinne von Art. 4 Nr. 2 der DS-GVO darstellt, die in den sachlichen Anwendungsbereich dieser Verordnung fällt, wie er in ihrem Art. 2 definiert ist.

Hierzu ist erstens festzustellen, dass aus der Vorlageentscheidung hervorgeht, dass die lettische Regelung die Verhängung von Strafpunkten gegen Fahrzeugführer vorsieht, die einen (Straßen-)Verkehrsverstoß begangen haben und gegen die eine finanzielle oder andere Sanktion verhängt wurde. Diese Punkte werden von einer öffentlichen Einrichtung, der CSDD, am Tag des Ablaufs der Frist für die Einlegung eines Rechtsbehelfs gegen die Entscheidung, mit der diese Sanktion verhängt wird, in das nationale Register für Fahrzeuge und Fahrzeugführer eingetragen.

Aus der Vorlageentscheidung geht auch hervor, dass die Verkehrsverstöße und die Sanktionen, um sie zu ahnden, in Lettland unter das Verwaltungsrecht fallen und dass die Verhängung von Strafpunkten nicht die Verhängung einer zusätzlichen Sanktion zum Ziel hat, sondern die betroffenen Fahrzeugführer sensibilisieren soll, indem sie dazu veranlasst werden, eine sicherere Fahrweise anzunehmen. Wird eine bestimmte Zahl von Strafpunkten erreicht, kann dem Betroffenen für eine bestimmte Zeit ein Fahrverbot auferlegt werden.

Aus dieser Entscheidung geht ferner hervor, dass die im Ausgangsverfahren in Rede stehende Regelung die CSDD verpflichtet, allen Personen, die Zugang zu diesen Informationen beantragen, die Informationen über die gegen einen bestimmten Fahrzeugführer verhängten Strafpunkte zu übermitteln. Die CSDD verlangt zu diesem Zweck lediglich, dass der Antragsteller den betreffenden Fahrzeugführer unter Angabe seiner nationalen Identifikationsnummer gebührend identifiziert.

Somit ist festzustellen, dass die Informationen über Strafpunkte, die sich auf eine bestimmte natürliche Person beziehen, „personenbezogene Daten“ im Sinne von Art. 4 Nr. 1 der DS-GVO sind und dass ihre Übermittlung durch die CSDD an Dritte eine „Verarbeitung“ im Sinne von Art. 4 Nr. 2 der DS-GVO darstellt.

Zweitens ist festzustellen, dass die Übermittlung dieser Informationen unter die sehr weite Definition des sachlichen Anwendungsbereichs der DS-GVO gemäß ihrem Art. 2 Abs. 1 fällt und nicht zu den Verarbeitungen personenbezogener

Daten gehört, die nach Art. 2 Abs. 2 Buchst. a und d der DS-GVO von diesem Anwendungsbereich ausgenommen sind.

Was nämlich zum einen Art. 2 Abs. 2 Buchst. a der DS-GVO betrifft, so findet diese Verordnung danach keine Anwendung auf die Verarbeitung personenbezogener Daten „im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt“. Diese Ausnahme vom Anwendungsbereich der DS-GVO ist, wie die anderen in ihrem Art. 2 Abs. 2 vorgesehenen Ausnahmen, eng auszulegen (vgl. in diesem Sinne Urteile vom 9. Juli 2020, Land Hessen, C 272/19, EU:C:2020:535, Rn. 68, und vom 16. Juli 2020, Facebook Ireland und Schrems, C 311/18, EU:C:2020:559, Rn. 84).

Art. 2 Abs. 2 Buchst. a der DS-GVO ist insoweit in Verbindung mit ihrem Art. 2 Abs. 2 Buchst. b und ihrem 16. Erwägungsgrund zu lesen, wonach diese Verordnung nicht für die Verarbeitung personenbezogener Daten im Zusammenhang mit „Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, wie etwa die nationale Sicherheit betreffende Tätigkeiten“, sowie Tätigkeiten „im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der Union“ gilt.

Daraus folgt, dass Art. 2 Abs. 2 Buchst. a und b der DS-GVO teilweise an Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 anknüpft. Folglich kann Art. 2 Abs. 2 Buchst. a und b der DS-GVO nicht dahin ausgelegt werden, dass er weiter gefasst ist als die Ausnahme nach Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46, wonach bereits diese Richtlinie keine Anwendung fand u. a. auf die Verarbeitung personenbezogener Daten, „die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des [EU]Vertrags [in seiner Fassung vor dem Vertrag von Lissabon], und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates ...“

Wie der Gerichtshof wiederholt entschieden hat, waren indessen nur Verarbeitungen personenbezogener Daten im Rahmen einer in Art. 3 Abs. 2 ausdrücklich genannten spezifischen Tätigkeit des Staates oder staatlicher Stellen oder einer Tätigkeit, die derselben Kategorie zugeordnet werden kann, vom Anwendungsbereich der Richtlinie 95/46 ausgeschlossen (vgl. in diesem Sinne Urteile vom 6. November 2003, Lindqvist, C 101/01, EU:C:2003:596, Rn. 42 bis 44, vom 27. September 2017, Puškár, C 73/16, EU:C:2017:725, Rn. 36 und 37, sowie vom 10. Juli 2018, Jehovan todistajat, C 25/17, EU:C:2018:551, Rn. 38).

Daraus folgt, dass Art. 2 Abs. 2 Buchst. a der DS-GVO im Licht des 16. Erwägungsgrundes dieser Verordnung so zu verstehen ist, dass damit vom Anwendungsbereich dieser Verordnung allein Verarbeitungen personenbezogener Daten ausgenommen werden sollen, die von staatlichen Stellen im Rahmen einer Tätigkeit, die der Wahrung der nationalen Sicherheit dient, oder einer Tätigkeit, die derselben Kategorie zugeordnet werden kann, vorgenommen werden, so dass der bloße Umstand, dass eine Tätigkeit eine spezifische Tätigkeit des Staates oder einer Behörde ist, nicht dafür ausreicht, dass diese Ausnahme automatisch für diese Tätigkeit gilt (vgl. in diesem Sinne Urteil vom 9. Juli 2020, Land Hessen, C 272/19, EU:C:2020:535, Rn. 70).

Die auf die Wahrung der nationalen Sicherheit abzielenden Tätigkeiten, auf die Art. 2 Abs. 2 Buchst. a der DS-GVO abstellt, umfassen, wie auch der Generalanwalt in den Nrn. 57 und 58 seiner Schlussanträge im Wesentlichen ausgeführt hat, insbesondere solche, die den Schutz der grundlegenden Funktionen des Staates und der grundlegenden Interessen der Gesellschaft bezwecken.

Mit den Tätigkeiten, die die Straßenverkehrssicherheit betreffen, wird jedoch kein solches Ziel verfolgt, so dass sie nicht der Kategorie der auf die Wahrung der nationalen Sicherheit abzielenden Tätigkeiten zugeordnet werden können, auf die Art. 2 Abs. 2 Buchst. a der DS-GVO abstellt.

Was zum anderen Art. 2 Abs. 2 Buchst. d der DS-GVO betrifft, so findet diese Verordnung danach keine Anwendung auf die Verarbeitung personenbezogener Daten „durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“. Wie sich aus dem 19. Erwägungsgrund dieser Verordnung ergibt, beruht diese Ausnahme darauf, dass für die Verarbeitung personenbezogener Daten zu solchen Zwecken und durch die zuständigen Behörden ein spezifischerer Rechtsakt der Union gilt, nämlich die Richtlinie 2016/680, die am selben Tag wie die DS-GVO erlassen wurde und in ihrem Art. 3 Nr. 7 definiert, was unter „zuständige Behörde“ zu verstehen ist, wobei diese Definition auf Art. 2 Abs. 2 Buchst. d entsprechend anzuwenden ist.

Aus dem zehnten Erwägungsgrund der Richtlinie 2016/680 geht hervor, dass der Begriff „zuständige Behörde“ im Zusammenhang mit dem Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit zu verstehen ist, unter Berücksichtigung der spezifischen Regelungen, die sich insoweit aufgrund der Besonderheiten dieser Bereiche als erforderlich erweisen können. Außerdem heißt es im elften Erwägungsgrund dieser Richtlinie, dass die DS-GVO für die Verarbeitung personenbezogener Daten gilt, die von einer „zuständigen Behörde“ im Sinne von Art. 3 Nr. 7 der Richtlinie 2016/680, aber zu anderen als den in ihr vorgesehenen Zwecken vorgenommen wird.

In Anbetracht der dem Gerichtshof vorliegenden Informationen ist nicht ersichtlich, dass die CSDD bei der Ausübung der im Ausgangsverfahren in Rede stehenden Tätigkeiten, die in der Übermittlung personenbezogener Daten über Strafpunkte an die Öffentlichkeit zu Zwecken der Straßenverkehrssicherheit bestehen, als „zuständige Behörde“ im Sinne von Art. 3 Nr. 7 der Richtlinie 2016/680 angesehen werden könnte und diese Tätigkeiten somit unter die in Art. 2 Abs. 2 Buchst. d der DS-GVO vorgesehene Ausnahme fallen könnten.

Daher fällt die von der CSDD vorgenommene Übermittlung personenbezogener Daten über Strafpunkte, die gegen Fahrzeugführer wegen Verkehrsverstößen verhängt wurden, in den sachlichen Anwendungsbereich der DS-GVO.

Was die Anwendbarkeit von Art. 10 der DS-GVO auf eine solche Übermittlung betrifft, geht es um die Frage, ob die so übermittelten Informationen personenbezogene Daten

„über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen“ im Sinne dieser Bestimmung darstellen, deren Verarbeitung „nur unter behördlicher Aufsicht vorgenommen werden [darf]“, es sei denn, sie ist „nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig“.

Insoweit ist darauf hinzuweisen, dass Art. 10 einen verstärkten Schutz gegen Verarbeitungen gewährleisten soll, die aufgrund der besonderen Sensibilität der betreffenden Daten einen besonders schweren Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen können (vgl. in diesem Sinne Urteil vom 24. September 2019, GC u. a. [Auslistung sensibler Daten], C 136/17, EU:C:2019:773, Rn. 44).

Da nämlich die Daten, auf die sich Art. 10 der DS-GVO bezieht, Verhaltensweisen betreffen, die zur Missbilligung durch die Gesellschaft führen, kann die Gewährung eines Zugangs zu solchen Daten die betroffene Person stigmatisieren und damit einen schweren Eingriff in ihr Privat- oder Berufsleben darstellen.

Im vorliegenden Fall werden zwar die Entscheidungen der lettischen Behörden zur Ahndung von Verkehrsverstößen, wie die lettische Regierung in ihren Antworten auf die Fragen des Gerichtshofs hervorgehoben hat, in das Register der Verurteilungen eingetragen, zu dem die Öffentlichkeit nur in begrenzten Fällen Zugang hat, und nicht in das Register der Fahrzeuge und Fahrzeugführer, zu dem Art. 141 Abs. 2 des Straßenverkehrsgesetzes freien Zugang gewährt. Wie jedoch das vorlegende Gericht hervorhebt, ermöglicht die Übermittlung der in diesem Register enthaltenen personenbezogenen Daten über Strafpunkte durch die CSDD der Öffentlichkeit die Feststellung, ob eine bestimmte Person Verkehrsverstöße begangen hat, und, falls dies der Fall ist, den Schluss auf die Schwere und die Häufigkeit dieser Verstöße. Eine solche Regelung über die Mitteilung von Strafpunkten läuft daher darauf hinaus, Zugang zu personenbezogenen Daten über Verkehrsverstöße zu gewähren.

Um zu bestimmen, ob ein solcher Zugang eine Verarbeitung personenbezogener Daten über „Straftaten“ im Sinne von Art. 10 der DS-GVO darstellt, ist erstens darauf hinzuweisen, dass sich dieser Begriff ausschließlich auf Straftaten im Sinne des Strafrechts bezieht, wie sich insbesondere aus der Entstehungsgeschichte der DS-GVO ergibt. Das Europäische Parlament hatte nämlich vorgeschlagen, die Wendung „verwaltungsrechtliche Sanktionen“ (ABL 2017, C 378, S. 430) ausdrücklich in diese Bestimmung aufzunehmen, doch wurde dieser Vorschlag nicht angenommen. Dieser Umstand ist umso bemerkenswerter, als die Vorgängerbestimmung zu Art. 10 der DS-GVO, d.h. Art. 8 Abs. 5 der Richtlinie 95/46, der sich in Unterabs. 1 auf „Straftaten“ und „strafrechtliche Verurteilungen“ bezog, den Mitgliedstaaten in Unterabs. 2 die Möglichkeit gab, vorzusehen, „dass Daten, die administrative Strafen... betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen“. Aus einer Gesamtbetrachtung dieses Art. 8 Abs. 5 ergibt sich somit eindeutig, dass sich der Begriff „Straftaten“

ausschließlich auf Straftaten im Sinne des Strafrechts bezog.

Unter diesen Umständen ist davon auszugehen, dass der Unionsgesetzgeber, indem er bewusst davon abgesehen hat, das Adjektiv „administrativ“ in Art. 10 der DS-GVO aufzunehmen, den in dieser Bestimmung vorgesehenen verstärkten Schutz allein dem strafrechtlichen Bereich vorbehalten wollte.

Diese Auslegung wird, wie der Generalanwalt in den Nrn. 74 bis 77 seiner Schlussanträge ausgeführt hat, dadurch bestätigt, dass mehrere Sprachfassungen von Art. 10 der DS-GVO ausdrücklich auf „Straftaten“ im Sinne des Strafrechts Bezug nehmen, wie z.B. die deutsche (Straftaten), die spanische (*infracciones penales*), die italienische (*reati*), die litauische (*nusikalstamas veikas*), die maltesische (*reati*) und die niederländische (*strafbare feiten*).

Zweitens ist der Umstand, dass Verkehrsverstöße in Lettland als Ordnungswidrigkeiten eingestuft werden, für die Beurteilung, ob diese Verstöße unter Art. 10 der DS-GVO fallen, nicht entscheidend.

Insoweit ist darauf hinzuweisen, dass die Begriffe einer Vorschrift des Unionsrechts, die für die Ermittlung ihres Sinnes und ihrer Tragweite nicht ausdrücklich auf das Recht der Mitgliedstaaten verweist, in der Regel in der gesamten Union eine autonome und einheitliche Auslegung erhalten müssen (Urteile vom 19. September 2000, *Linster*, C 287/98, EU:C:2000:468, Rn. 43, und vom 1. Oktober 2019, *Planet49*, C 673/17, EU:C:2019:801, Rn. 47).

Im vorliegenden Fall ist zunächst festzustellen, dass die DS-GVO hinsichtlich der Tragweite der in ihrem Art. 10 verwendeten Begriffe, insbesondere der Begriffe „Straftaten“ und „strafrechtliche Verurteilungen“, nicht auf die nationalen Rechtsordnungen verweist.

Sodann geht aus dem zehnten Erwägungsgrund der DS-GVO hervor, dass diese zur Verwirklichung eines Raums der Freiheit, der Sicherheit und des Rechts beitragen soll, indem ein gleichmäßiges und hohes Schutzniveau für natürliche Personen bei der Verarbeitung personenbezogener Daten gewährleistet wird, was voraussetzt, dass dieses Schutzniveau in allen Mitgliedstaaten gleichwertig und homogen ist. Einem solchen Zweck liefe es zuwider, wenn der in dieser Bestimmung vorgesehene verstärkte Schutz nur in einigen Mitgliedstaaten für die Verarbeitung personenbezogener Daten über Verkehrsverstöße gilt, nicht aber in anderen, nur weil diese Verstöße in den letztgenannten Mitgliedstaaten nicht als Straftaten eingestuft werden.

Schließlich wird diese Feststellung, wie der Generalanwalt in Nr. 84 seiner Schlussanträge ausgeführt hat, durch den 13. Erwägungsgrund der Richtlinie 2016/680 bestätigt, wo-nach „[e]ine Straftat im Sinne dieser Richtlinie... ein eigenständiger Begriff des Unionsrechts in der Auslegung durch den Gerichtshof der Europäischen Union... sein [sollte]“.

Daraus folgt, dass der Begriff „Straftat“, der für die Bestimmung der Anwendbarkeit von Art. 10 der DS-GVO auf personenbezogene Daten über Verkehrsverstöße wie die im Ausgangsverfahren in Rede stehenden entscheidend ist, in der gesamten Union einer autonomen und einheitlichen

Auslegung bedarf, die unter Berücksichtigung des mit dieser Bestimmung verfolgten Ziels und des Kontexts, in den sie sich einfügt, gefunden werden muss, ohne dass es insoweit darauf ankommt, wie der betreffende Mitgliedstaat diese Verstöße einstuft; diese Einstufung kann in den einzelnen Staaten unterschiedlich sein (vgl. in diesem Sinne Urteil vom 14. November 2013, *Baláz*, C 60/12, EU:C:2013:733, Rn. 26 und 35).

Drittens ist zu prüfen, ob Verkehrsverstöße wie die, die zur Eintragung von Strafpunkten in das Register für Fahrzeuge und Fahrzeugführer führen, deren Mitteilung an Dritte in der streitigen Bestimmung vorgesehen ist, eine „Straftat“ im Sinne von Art. 10 der DS-GVO darstellen.

Nach der Rechtsprechung des Gerichtshofs sind für die Beurteilung des strafrechtlichen Charakters einer Zuwiderhandlung drei Kriterien maßgebend: erstens die rechtliche Einordnung der Zuwiderhandlung im innerstaatlichen Recht, zweitens die Art der Zuwiderhandlung und drittens der Schweregrad der dem Betroffenen drohenden Sanktion (vgl. in diesem Sinne Urteile vom 5. Juni 2012, *Bonda*, C 489/10, EU:C:2012:319, Rn. 37, vom 20. März 2018, *Garlsson Real Estate u. a.*, C 537/16, EU:C:2018:193, Rn. 28, und vom 2. Februar 2021, *Consob*, C 481/19, EU:C:2021:84, Rn. 42).

Auch für Zuwiderhandlungen, die im innerstaatlichen Recht nicht als „strafrechtlich“ eingestuft werden, kann sich ein solcher Charakter nichtsdestoweniger aus der Art der Zuwiderhandlung und dem Schweregrad der dem Betroffenen drohenden Sanktion ergeben (vgl. in diesem Sinne Urteil vom 20. März 2018, *Garlsson Real Estate u. a.*, C 537/16, EU:C:2018:193, Rn. 28 und 32).

Das Kriterium, das sich auf die Art der Zuwiderhandlung bezieht, erfordert die Prüfung, ob mit der fraglichen Sanktion u. a. eine repressive Zielsetzung verfolgt wird, ohne dass der bloße Umstand, dass mit ihr auch eine präventive Zielsetzung verfolgt wird, ihr ihre Einstufung als strafrechtliche Sanktion nehmen kann. Es liegt nämlich in der Natur strafrechtlicher Sanktionen, dass sie sowohl auf die Repression als auch auf die Prävention rechtswidriger Verhaltensweisen abzielen. Dagegen ist eine Maßnahme, die nur den durch die Zuwiderhandlung entstandenen Schaden ersetzen soll, nicht strafrechtlicher Natur (vgl. in diesem Sinne Urteile vom 5. Juni 2012, *Bonda*, C 489/10, EU:C:2012:319, Rn. 39, und vom 20. März 2018, *Garlsson Real Estate u. a.*, C 537/16, EU:C:2018:193, Rn. 33). Es steht indessen fest, dass mit der Verhängung von Strafpunkten für Verkehrsverstöße ebenso wie mit Bußgeldern oder anderen Sanktionen, die die Begehung dieser Verstöße nach sich ziehen kann, nicht nur der Ersatz von Schäden bezweckt wird, die durch diese Verstöße möglicherweise verursacht werden, sondern auch ein repressiver Zweck verfolgt wird.

Was das Kriterium des Schweregrads der Sanktionen betrifft, zu denen die Begehung dieser Verstöße führen kann, ist zunächst darauf hinzuweisen, dass nur Verkehrsverstöße von gewisser Schwere zur Verhängung von Strafpunkten führen und dass solche Verstöße daher zu Sanktionen von bestimmter Schwere führen können. Sodann kommt die Verhängung von Strafpunkten im Allgemeinen zu der im Fall eines solchen Verstoßes verhängten Sanktion hinzu. Wie in

Rn. 58 des vorliegenden Urteils ausgeführt, ist dies im Übrigen bei der im Ausgangsverfahren in Rede stehenden Regelung der Fall. Schließlich hat die Kumulierung dieser Punkte als solche rechtliche Folgen, wie etwa die Verpflichtung, eine Prüfung abzulegen, oder ein Fahrverbot.

Diese Analyse wird bestätigt durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, wonach Verkehrsverstöße trotz einer Tendenz zur „Entkriminalisierung“ dieser Verstöße in einigen Staaten angesichts des zugleich präventiven und repressiven Zwecks der verhängten Sanktionen und des Schweregrads, den diese erreichen können, im Allgemeinen als Verstöße strafrechtlicher Natur anzusehen sind (vgl. in diesem Sinne Europäischer Gerichtshof für Menschenrechte, 21. Februar 1984, Öztürk/Deutschland, CE:ECHR:1984:0221JUD000854479, Nrn. 49 bis 53, vom 29. Juni 2007, O'Halloran und Francis/Vereinigtes Königreich, CE:ECHR:2007:0629JUD001580902, Nrn. 33 bis 36, und vom 4. Oktober 2016, Rivard/Schweiz, CE:ECHR:2016:1004JUD002156312, Nrn. 23 und 24).

Die Einstufung von Verkehrsverstößen, die zur Verhängung von Strafpunkten führen können, als „Straftaten“ im Sinne von Art. 10 der DS-GVO entspricht auch dem Zweck dieser Bestimmung. Die Übermittlung personenbezogener Daten über Verkehrsverstöße, einschließlich der für ihre Begehung verhängten Strafpunkte, an die Öffentlichkeit ist nämlich angesichts dessen, dass solche Verstöße die Straßenverkehrssicherheit beeinträchtigen, geeignet, zu einer Missbilligung durch die Gesellschaft und zur Stigmatisierung der betreffenden Person zu führen, insbesondere wenn diese Punkte eine bestimmte Schwere oder eine bestimmte Häufigkeit dieser Verstöße zeigen.

Daraus folgt, dass Verkehrsverstöße, die zur Verhängung von Strafpunkten führen können, unter den Begriff „Straftaten“ im Sinne von Art. 10 der DS-GVO fallen.

Nach alledem ist auf die erste Vorlagefrage zu antworten, dass Art. 10 der DS-GVO dahin auszulegen ist, dass er auf die Verarbeitung personenbezogener Daten über Strafpunkte, die gegen Fahrzeugführer wegen Verkehrsverstößen verhängt wurden, anwendbar ist.

Zur zweiten Frage

Mit seiner zweiten Frage möchte das vorlegende Gericht wissen, ob die Bestimmungen der DS-GVO dahin auszulegen sind, dass sie einer nationalen Regelung entgegenstehen, die die mit dem Register, in das die gegen Fahrzeugführer wegen Verkehrsverstößen verhängten Strafpunkte eingetragen werden, betraute öffentliche Einrichtung verpflichtet, diese Daten jeder Person zu übermitteln, die dies beantragt, ohne dass sie ein besonderes Interesse am Erhalt dieser Daten nachzuweisen hat.

Insoweit ist darauf hinzuweisen, dass jede Verarbeitung personenbezogener Daten zum einen mit den in Art. 5 der DS-GVO aufgestellten Grundsätzen für die Verarbeitung der Daten im Einklang stehen und zum anderen einem der in Art. 6 der DS-GVO aufgeführten Grundsätze in Bezug auf die Rechtmäßigkeit der Verarbeitung entsprechen muss (vgl. in diesem Sinne Urteil vom 16. Januar 2019, Deutsche Post, C

496/17, EU:C:2019:26, Rn. 57 und die dort angeführte Rechtsprechung).

Was die Grundsätze für die Verarbeitung personenbezogener Daten betrifft, bezieht sich das vorlegende Gericht zwar speziell auf die in Art. 5 Abs. 1 Buchst. f der DS-GVO verankerten Grundsätze der „Integrität“ und der „Vertraulichkeit“. Allerdings ergibt sich aus den Fragen des vorlegenden Gerichts, dass es allgemeiner feststellen möchte, ob die im Ausgangsverfahren in Rede stehende Verarbeitung personenbezogener Daten im Hinblick auf alle Bestimmungen dieser Verordnung, insbesondere im Hinblick auf den Grundsatz der Verhältnismäßigkeit, als rechtmäßig angesehen werden kann.

Folglich sind in der dem vorlegenden Gericht zu gebenden Antwort auch andere in Art. 5 Abs. 1 der DS-GVO genannte Grundsätze und insbesondere der in Buchst. c dieser Bestimmung enthaltene Grundsatz der „Datenminimierung“ zu berücksichtigen, wonach personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen, womit der Grundsatz der Verhältnismäßigkeit zum Ausdruck gebracht wird (vgl. in diesem Sinne Urteil vom 11. Dezember 2019, Asociația de Proprietari bloc M5A-ScaraA, C 708/18, EU:C:2019:1064, Rn. 48).

Hinsichtlich der Grundsätze in Bezug auf die Rechtmäßigkeit der Verarbeitung sieht Art. 6 der DS-GVO eine erschöpfende und abschließende Liste der Fälle vor, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann. Daher muss eine Verarbeitung unter einen der in Art. 6 vorgesehenen Fälle subsumierbar sein, um als rechtmäßig angesehen werden zu können (vgl. in diesem Sinne Urteil vom 11. Dezember 2019, Asociația de Proprietari bloc M5A-ScaraA, C 708/18, EU:C:2019:1064, Rn. 37 und 38). Insoweit kann die im Ausgangsverfahren in Rede stehende Verarbeitung personenbezogener Daten, d.h. die von der CSDD vorgenommene Übermittlung der Daten über für Verkehrsverstöße verhängte Strafpunkte an die Öffentlichkeit, unter Art. 6 Abs. 1 Buchst. e der DS-GVO fallen, wonach die Verarbeitung rechtmäßig ist, wenn und soweit sie „für die Wahrnehmung einer Aufgabe erforderlich [ist], die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“.

Da, wie in Rn. 94 des vorliegenden Urteils festgestellt wurde, die personenbezogenen Daten über Strafpunkte, die gegen Fahrzeugführer wegen Verkehrsverstößen verhängt wurden, unter Art. 10 der DS-GVO fallen, unterliegt ihre Verarbeitung zudem den in dieser Bestimmung vorgesehenen zusätzlichen Beschränkungen. Danach darf die Verarbeitung dieser Daten „nur unter behördlicher Aufsicht vorgenommen werden“, es sei denn, sie ist „nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig“. In dieser Bestimmung heißt es im Übrigen, dass „[e]in umfassendes Register der strafrechtlichen Verurteilungen... nur unter behördlicher Aufsicht geführt werden [darf]“.

Im vorliegenden Fall steht fest, dass die im Ausgangsverfahren in Rede stehende Verarbeitung personenbezogener Daten, d.h. die Übermittlung der Daten über für Verkehrsverstöße verhängte Strafpunkte an die Öffentlichkeit, durch eine öffentliche Einrichtung, die CSDD, erfolgt, die der für die Verarbeitung Verantwortliche im Sinne von Art. 4 Nr. 7 der DS-GVO ist (vgl. entsprechend Urteil vom 9. März 2017, Manni, C 398/15, EU:C:2017:197, Rn. 35). Es steht jedoch auch fest, dass diese Daten nach ihrer Übermittlung von den Personen eingesehen werden, die ihre Übermittlung beantragt haben, und von diesen Personen gegebenenfalls gespeichert oder verbreitet werden. Da diese Weiterverarbeitungen von Daten nicht mehr „unter [der] Aufsicht“ der CSDD oder einer anderen Behörde erfolgen, muss das nationale Recht, das die Übermittlung dieser Daten durch die CSDD erlaubt, „geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen“ vorsehen.

Daher ist die Vereinbarkeit einer nationalen Regelung wie der im Ausgangsverfahren in Rede stehenden mit der DS-GVO sowohl im Hinblick auf die allgemeinen Rechtmäßigkeitsvoraussetzungen, insbesondere die in Art. 5 Abs. 1 Buchst. c und Art. 6 Abs. 1 Buchst. e der DS-GVO aufgestellten, als auch im Hinblick auf die in Art. 10 der DS-GVO vorgesehenen besonderen Beschränkungen zu prüfen.

Hierzu ist festzustellen, dass keine dieser Bestimmungen es allgemein und absolut verbietet, dass eine Behörde durch eine nationale Regelung ermächtigt oder sogar gezwungen wird, personenbezogene Daten an Personen zu übermitteln, die dies beantragen.

Auch wenn Art. 5 Abs. 1 Buchst. c der DS-GVO die Verarbeitung personenbezogener Daten von der Einhaltung des Grundsatzes der „Datenminimierung“ abhängig macht, geht aus dem Wortlaut dieser Bestimmung nämlich klar hervor, dass mit ihr kein solches allgemeines und absolutes Verbot eingeführt werden soll und dass sie insbesondere der Übermittlung personenbezogener Daten an die Öffentlichkeit nicht entgegensteht, wenn diese Übermittlung im Sinne von Abs. 6 Abs. 1 Buchst. e der DS-GVO für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Dies gilt auch dann, wenn die fraglichen Daten unter Art. 10 DS-GVO fallen, sofern die Regelung, die diese Übermittlung gestattet, geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht (vgl. in diesem Sinne Urteil vom 24. September 2019, GC u. a. [Auslistung sensibler Daten], C 136/17, EU:C:2019:773, Rn. 73).

In diesem Zusammenhang ist darauf hinzuweisen, dass die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten keine uneingeschränkte Geltung beanspruchen, sondern im Hinblick auf ihre gesellschaftliche Funktion gesehen und gegen andere Grundrechte abgewogen werden müssen. Somit können Einschränkungen vorgesehen werden, sofern sie gemäß Art. 52 Abs. 1 der Charta gesetzlich vorgesehen sind und den Wesensgehalt der Grundrechte sowie den Grundsatz der Verhältnismäßigkeit wahren. Nach diesem Grundsatz dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl

dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Sie müssen sich auf das absolut Notwendige beschränken, und die den Eingriff enthaltende Regelung muss klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen (vgl. in diesem Sinne Urteil vom 16. Juli 2020, Facebook Ireland und Schrems, C 311/18, EU:C:2020:559, Rn. 172 bis 176).

Um festzustellen, ob eine Übermittlung personenbezogener Daten über Strafpunkte an die Öffentlichkeit, wie sie im Ausgangsverfahren in Rede steht, im Sinne von Art. 6 Abs. 1 Buchst. e der DS-GVO für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, und ob die Regelung, die eine solche Übermittlung gestattet, geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen im Sinne von Art. 10 dieser Verordnung vorsieht, ist somit insbesondere zu prüfen, ob diese Übermittlung angesichts der Schwere des durch sie bewirkten Eingriffs in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten im Hinblick auf die Verwirklichung der verfolgten Ziele gerechtfertigt und insbesondere verhältnismäßig ist.

Im vorliegenden Fall machen das lettische Parlament – in seinen Erklärungen vor dem vorlegenden Gericht – und die lettische Regierung – in ihren Erklärungen vor dem Gerichtshof – geltend, dass die Übermittlung von personenbezogenen Daten über Strafpunkte durch die CSDD an jede Person, die dies beantrage, zu der diesem Organ obliegenden Aufgabe im öffentlichen Interesse gehöre, die Straßenverkehrssicherheit zu verbessern, und in diesem Zusammenhang insbesondere die Identifizierung der Fahrzeugführer, die systematisch gegen die Straßenverkehrsregeln verstießen, ermöglichen und das Verhalten der Straßenverkehrsteilnehmer dahin gehend beeinflussen solle, dass sie zu einem den Straßenverkehrsregeln entsprechenden Verhalten veranlasst würden.

Insoweit ist darauf hinzuweisen, dass die Verbesserung der Straßenverkehrssicherheit ein von der Union anerkanntes Ziel im allgemeinen Interesse darstellt (vgl. in diesem Sinne Urteil vom 23. April 2015, Aykul, C 260/13, EU:C:2015:257, Rn. 69 und die dort angeführte Rechtsprechung). Die Mitgliedstaaten sind daher berechtigt, die Straßenverkehrssicherheit als „Aufgabe...“, die im öffentlichen Interesse liegt“, im Sinne von Art. 6 Abs. 1 Buchst. e der DS-GVO einzustufen.

Um die in dieser Bestimmung aufgestellten Voraussetzungen zu erfüllen, ist es jedoch erforderlich, dass die Übermittlung der in dem von der CSDD geführten Register eingetragenen personenbezogenen Daten über Strafpunkte tatsächlich dem im allgemeinen Interesse liegenden Ziel der Verbesserung der Straßenverkehrssicherheit entspricht, ohne über das hinauszugehen, was zur Erreichung dieses Ziels erforderlich ist.

Wie im 39. Erwägungsgrund der DS-GVO hervorgehoben wird, ist diese Anforderung der Erforderlichkeit nicht erfüllt, wenn das im allgemeinen Interesse liegende verfolgte Ziel in zumutbarer Weise ebenso wirksam mit anderen Mit-

teln erreicht werden kann, die weniger stark in die Grundrechte der betroffenen Personen, insbesondere die in den Art. 7 und 8 der Charta verbürgten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingreifen, wobei sich die Ausnahmen und Einschränkungen hinsichtlich des Grundsatzes des Schutzes solcher Daten auf das absolut Notwendige beschränken müssen (vgl. in diesem Sinne Urteil vom 11. Dezember 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C 708/18, EU:C:2019:1064, Rn. 46 und 47).

Wie sich aus der Praxis der Mitgliedstaaten ergibt, verfügt indessen jeder von ihnen über eine Vielzahl von Handlungsmöglichkeiten, zu denen u.a. die Möglichkeit einer abschreckenden Ahndung von Verkehrsverstößen gehört, insbesondere indem den betreffenden Fahrzeugführern das Recht zum Führen eines Kraftfahrzeugs genommen wird, wobei der Verstoß gegen ein solches Verbot seinerseits mit wirksamen Strafen geahndet werden kann, ohne dass es erforderlich wäre, den Erlass solcher Maßnahmen der Öffentlichkeit mitzuteilen. Aus dieser Praxis ergibt sich auch, dass darüber hinaus zahlreiche vorbeugende Maßnahmen ergriffen werden können, die von Kampagnen zur kollektiven Sensibilisierung bis zum Erlass individueller Maßnahmen dahin gehend reichen, einen Fahrzeugführer zur Teilnahme an Schulungen und zum Ablegen von Prüfungen zu zwingen, ohne dass es erforderlich wäre, den Erlass solcher individuellen Maßnahmen der Öffentlichkeit mitzuteilen. Aus den dem Gerichtshof vorliegenden Akten geht jedoch nicht hervor, dass solche Maßnahmen vom lettischen Gesetzgeber anstelle des Erlasses der im Ausgangsverfahren in Rede stehenden Regelung geprüft und bevorzugt worden wären.

Außerdem kann, wie in Rn. 92 des vorliegenden Urteils ausgeführt, die Übermittlung personenbezogener Daten über Verkehrsverstöße einschließlich der Daten über die für ihre Begehung verhängten Strafpunkte an die Öffentlichkeit einen schweren Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen, da sie zur Missbilligung durch die Gesellschaft und zur Stigmatisierung der betroffenen Person führen kann.

Unter Berücksichtigung zum einen der Sensibilität der fraglichen Daten und der Schwere dieses Eingriffs in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten der betroffenen Personen und zum anderen der Tatsache, dass in Anbetracht der Feststellungen in Rn. 111 des vorliegenden Urteils nicht ersichtlich ist, dass das Ziel der Verbesserung der Straßenverkehrssicherheit in zumutbarer Weise nicht mit anderen, weniger einschneidenden Mitteln ebenso wirksam erreicht werden kann, kann nicht davon ausgegangen werden, dass die Erforderlichkeit einer solchen Regelung der Übermittlung personenbezogener Daten über Strafpunkte für Verkehrsverstöße zur Gewährleistung dieses Zieles nachgewiesen ist (vgl. entsprechend Urteil vom 9. November 2010, *Volker und Markus Schecke und Eifert*, C 92/09 und C 93/09, EU:C:2010:662, Rn. 86).

Somit kann es zwar gerechtfertigt sein, die Fahrzeugführer, die systematisch und bösgläubig gegen die Straßenverkehrsregeln verstoßen, von den Fahrzeugführern zu unterscheiden, die gelegentlich Verstöße begehen, doch kann

nicht davon ausgegangen werden, dass die Identifizierung der ersten Kategorie von Fahrzeugführern für die Zwecke der Verbesserung der Straßenverkehrssicherheit von der breiten Öffentlichkeit vorgenommen oder mit der breiten Öffentlichkeit geteilt werden muss, so dass sogar an der Eignung der im Ausgangsverfahren in Rede stehenden Regelung, das erste der in Rn. 107 des vorliegenden Urteils genannten Ziele zu erreichen, Zweifel bestehen können.

Im Übrigen geht aus den dem Gerichtshof vorliegenden Akten hervor, dass die CSDD nicht nur die Daten über Strafpunkte, die gegen Fahrzeugführer verhängt wurden, die systematisch und bösgläubig gegen die Straßenverkehrsregeln verstoßen, sondern auch die über Strafpunkte, die gegen Fahrzeugführer verhängt wurden, die gelegentlich Verstöße begehen, an die Öffentlichkeit übermittelt. Somit geht die im Ausgangsverfahren in Rede stehende Regelung dadurch, dass sie einen generellen Zugang der Öffentlichkeit zu Strafpunkten vorsieht, jedenfalls über das hinaus, was erforderlich ist, um das Ziel sicherzustellen, die systematische und bösgläubige Missachtung der Straßenverkehrsregeln zu bekämpfen.

Was das zweite der mit der streitigen Regelung verfolgten Ziele betrifft, auf das in Rn. 107 des vorliegenden Urteils hingewiesen wurde, geht aus den Akten hervor, dass in Lettland zwar eine Tendenz zur Verringerung der Zahl von Verkehrsunfällen beobachtet werden konnte, dass aber nichts den Schluss zulässt, dass diese Tendenz mit der Offenlegung der Informationen über Strafpunkte und nicht mit der Einführung des Systems der Strafpunkte als solchen zusammenhängt.

Die in Rn. 113 des vorliegenden Urteils gezogene Schlussfolgerung wird nicht dadurch in Frage gestellt, dass die CSDD die Übermittlung der fraglichen personenbezogenen Daten in der Praxis von der Voraussetzung abhängig macht, dass der Antragsteller die nationale Identifikationsnummer des Fahrzeugführers angibt, über den er sich informieren möchte.

Selbst wenn die Mitteilung der nationalen Identifikationsnummern durch die öffentlichen Stellen, die die Bevölkerungsregister führen, entsprechend den Ausführungen der lettischen Regierung strengen Anforderungen unterliegt und damit Art. 87 der DS-GVO genügt, ändert dies nichts daran, dass die im Ausgangsverfahren in Rede stehende Regelung, wie sie von der CSDD angewandt wird, es jedem, der die nationale Identifikationsnummer eines bestimmten Fahrzeugführers kennt, erlaubt, die personenbezogenen Daten über die gegen diesen Fahrzeugführer verhängten Strafpunkte ohne weitere Voraussetzung zu erhalten. Eine solche Offenlegungsregelung kann zu einer Situation führen, in der diese Daten an Personen weitergegeben werden, die aus Gründen, die mit dem im allgemeinen Interesse liegenden Ziel der Verbesserung der Straßenverkehrssicherheit nichts zu tun haben, versuchen, sich über die gegen eine bestimmte Person verhängten Strafpunkte zu informieren.

Die in Rn. 113 des vorliegenden Urteils gezogene Schlussfolgerung wird auch nicht dadurch entkräftet, dass das nationale Register für Fahrzeuge und Fahrzeugführer ein amtliches Dokument im Sinne von Art. 86 der DS-GVO ist.

Zwar stellt der Zugang der Öffentlichkeit zu amtlichen Dokumenten, wie aus dem 154. Erwägungsgrund der DS-GVO hervorgeht, ein öffentliches Interesse dar, dass die Übermittlung von in solchen Dokumenten enthaltenen personenbezogenen Daten rechtfertigen kann, doch muss der entsprechende Zugang nichtsdestoweniger mit den Grundrechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten in Einklang gebracht werden, wie es im Übrigen in Art. 86 ausdrücklich verlangt wird. Angesichts insbesondere der Sensibilität der Daten über für Verkehrsverstöße verhängte Strafpunkte und der Schwere des Eingriffs in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, der mit der Offenlegung dieser Daten vorgenommen wird, ist indessen davon auszugehen, dass diese Rechte dem Interesse der Öffentlichkeit am Zugang zu amtlichen Dokumenten, insbesondere zum nationalen Register für Fahrzeuge und Fahrzeugführer, vorgehen.

Außerdem kann das in Art. 85 der DS-GVO verankerte Recht auf Informationsfreiheit aus demselben Grund nicht dahin ausgelegt werden, dass es die Übermittlung personenbezogener Daten über für Verkehrsverstöße verhängte Strafpunkte an jede Person rechtfertigt, die sie beantragt.

Nach alledem ist auf die zweite Frage zu antworten, dass die Bestimmungen der DS-GVO, insbesondere ihr Art. 5 Abs. 1, ihr Art. 6 Abs. 1 Buchst. e und ihr Art. 10, dahin auszulegen sind, dass sie einer nationalen Regelung entgegenstehen, die die mit dem Register, in das die gegen Fahrzeugführer wegen Verkehrsverstößen verhängten Strafpunkte eingetragen werden, betraute öffentliche Einrichtung verpflichtet, diese Daten der Öffentlichkeit zugänglich zu machen, ohne dass die Person, die den Zugang beantragt, ein besonderes Interesse am Erhalt dieser Daten nachzuweisen hat.

Zur dritten Frage

Mit seiner dritten Frage möchte das vorliegende Gericht wissen, ob die Bestimmungen der DS-GVO, insbesondere ihr Art. 5 Abs. 1 Buchst. b und ihr Art. 10, sowie Art. 1 Abs. 2 Buchst. cc der Richtlinie 2003/98 dahin auszulegen sind, dass sie einer nationalen Regelung entgegenstehen, die es der mit dem Register, in das die gegen Fahrzeugführer wegen Verkehrsverstößen verhängten Strafpunkte eingetragen werden, betrauten öffentlichen Einrichtung erlaubt, diese Daten Wirtschaftsteilnehmern zur Weiterverwendung zu übermitteln.

Wie das vorliegende Gericht ausführt, beruht diese Frage darauf, dass die CSDD mit Wirtschaftsteilnehmern Verträge schließt, nach denen sie die personenbezogenen Daten über die im nationalen Register für Fahrzeuge und Fahrzeugführer eingetragenen Strafpunkte an die betreffenden Wirtschaftsteilnehmer übermittelt, so dass u.a. jede Person, die sich über die gegen einen bestimmten Fahrzeugführer verhängten Strafpunkte informieren möchte, diese Daten nicht nur von der CSDD, sondern auch von diesen Wirtschaftsteilnehmern erhalten kann.

Aus der Antwort auf die zweite Frage ergibt sich, dass die Bestimmungen der DS-GVO, insbesondere ihr Art. 5 Abs. 1, ihr Art. 6 Abs. 1 Buchst. e und ihr Art. 10, dahin auszulegen

sind, dass sie einer nationalen Regelung entgegenstehen, die die mit dem Register, in das die gegen Fahrzeugführer wegen Verkehrsverstößen verhängten Strafpunkte eingetragen werden, betraute öffentliche Einrichtung verpflichtet, diese Daten der Öffentlichkeit zugänglich zu machen, ohne dass die Person, die den Zugang beantragt, ein besonderes Interesse am Erhalt dieser Daten nachzuweisen hat.

Diese Bestimmungen sind aus den gleichen Gründen, so wie sie in der Antwort auf die zweite Frage dargelegt wurden, dahin auszulegen, dass sie auch einer nationalen Regelung entgegenstehen, die es einer öffentlichen Einrichtung erlaubt, derartige Daten an Wirtschaftsteilnehmer zu übermitteln, damit diese sie weiterverwenden und an die Öffentlichkeit übermitteln können.

Schließlich ist zu Art. 1 Abs. 2 Buchst. cc der Richtlinie 2003/98, auf den sich die dritte Vorlagefrage ebenfalls bezieht, festzustellen, dass diese Bestimmung, wie der Generalanwalt in den Nrn. 128 und 129 seiner Schlussanträge ausgeführt hat, für die Feststellung, ob die unionsrechtlichen Vorschriften über den Schutz personenbezogener Daten einer Regelung wie der im Ausgangsverfahren in Rede stehenden entgegenstehen, nicht relevant ist.

Unabhängig davon, ob die gegen Fahrzeugführer wegen Verkehrsverstößen verhängten Strafpunkte in den Anwendungsbereich der Richtlinie 2003/98 fallen, ist der Umfang des Schutzes dieser Daten nämlich in jedem Fall auf der Grundlage der DS-GVO zu bestimmen, wie sich zum einen aus dem 154. Erwägungsgrund dieser Verordnung und zum anderen aus dem 21. Erwägungsgrund und Art. 1 Abs. 4 dieser Richtlinie in Verbindung mit Art. 94 Abs. 2 der DS-GVO ergibt. Art. 1 Abs. 4 der Richtlinie 2003/98 sieht nämlich im Wesentlichen vor, dass diese Richtlinie keinerlei Auswirkungen auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gemäß den Rechtsvorschriften u.a. der Union hat und insbesondere die Pflichten und Rechte gemäß der DS-GVO unberührt lässt.

Nach alledem ist auf die dritte Frage zu antworten, dass die Bestimmungen der DS-GVO, insbesondere ihr Art. 5 Abs. 1, ihr Art. 6 Abs. 1 Buchst. e und ihr Art. 10, dahin auszulegen sind, dass sie einer nationalen Regelung entgegenstehen, die es der mit dem Register, in das die gegen Fahrzeugführer wegen Verkehrsverstößen verhängten Strafpunkte eingetragen werden, betrauten öffentlichen Einrichtung erlaubt, diese Daten Wirtschaftsteilnehmern zur Weiterverwendung zu übermitteln.

Zur vierten Frage

Mit seiner vierten Frage möchte das vorliegende Gericht wissen, ob der Grundsatz des Vorrangs des Unionsrechts dahin auszulegen ist, dass er es dem Verfassungsgericht eines Mitgliedstaats, bei dem ein Rechtsbehelf gegen eine nationale Regelung anhängig ist, die im Licht einer Vorabentscheidung des Gerichtshofs mit dem Unionsrecht unvereinbar ist, verwehrt, in Anwendung des Grundsatzes der Rechtssicherheit zu entscheiden, dass die Rechtswirkungen dieser Regelung bis zum Zeitpunkt der Verkündung des Urteils, mit dem es endgültig über diesen verfassungsrechtlichen Rechtsbehelf entscheidet, aufrechterhalten werden.

Wie aus der Vorlageentscheidung hervorgeht, wird diese Frage aufgrund der großen Zahl der Rechtsverhältnisse gestellt, die von der im Ausgangsverfahren in Rede stehenden nationalen Regelung betroffen sind, und angesichts dessen, dass das vorlegende Gericht nach Art. 32 Abs. 3 des Gesetzes über das Verfassungsgericht und der dazu ergangenen Rechtsprechung bei der Wahrnehmung seiner Aufgabe, ein Gleichgewicht zwischen dem Grundsatz der Rechtssicherheit und den Grundrechten der betroffenen Personen zu gewährleisten, die Rückwirkung seiner Urteile beschränken kann, um zu verhindern, dass diese in schwerwiegender Weise die Rechte anderer beeinträchtigen.

Hierzu ist darauf hinzuweisen, dass durch die Auslegung einer Vorschrift des Unionsrechts, die der Gerichtshof in Ausübung seiner Befugnisse aus Art. 267 AEUV vornimmt, erläutert und verdeutlicht wird, in welchem Sinne und mit welcher Tragweite diese Vorschrift seit ihrem Inkrafttreten zu verstehen und anzuwenden ist oder gewesen wäre. Nur ganz ausnahmsweise kann der Gerichtshof aufgrund des allgemeinen unionsrechtlichen Grundsatzes der Rechtssicherheit die für die Betroffenen bestehende Möglichkeit beschränken, sich auf die Auslegung, die er einer Bestimmung gegeben hat, zu berufen, um in gutem Glauben begründete Rechtsverhältnisse in Frage zu stellen. Eine solche Beschränkung ist nur dann zulässig, wenn zwei grundlegende Kriterien erfüllt sind, nämlich guter Glaube der Betroffenen und die Gefahr schwerwiegender Störungen (Urteile vom 6. März 2007, Meilicke, C 292/04, EU:C:2007:132, Rn. 34 und 35, vom 22. Januar 2015, Balazs, C 401/13 und C 432/13, EU:C:2015:26, Rn. 49 und 50, sowie vom 29. September 2015, Gmina Wrocław, C 276/14, EU:C:2015:635, Rn. 44 und 45).

Eine solche Beschränkung kann nach der ständigen Rechtsprechung des Gerichtshofs nur in dem Urteil selbst vorgenommen werden, in dem über die erbetene Auslegung entschieden wird. Die zeitliche Wirkung der vom Gerichtshof auf ein Ersuchen hin vorgenommenen Auslegung einer Vorschrift des Unionsrechts muss nämlich notwendigerweise zu einem einzigen Zeitpunkt bestimmt werden. Der Grundsatz, dass eine Beschränkung nur in dem Urteil selbst erfolgen kann, mit dem über die erbetene Auslegung entschieden wird, stellt die Gleichbehandlung der Mitgliedstaaten und der Einzelnen in Ansehung des Unionsrechts sicher und erfüllt damit die Anforderungen, die sich aus dem Grundsatz der Rechtssicherheit ergeben (Urteil vom 6. März 2007, Meilicke, C 292/04, EU:C:2007:132, Rn. 36 und 37; vgl. in diesem Sinne auch Urteile vom 23. Oktober 2012, Nelson u.a., C 581/10 und C 629/10, EU:C:2012:657, Rn. 91, und vom 7. November 2018, O'Brien, C 432/17, EU:C:2018:879, Rn. 34).

Folglich können die zeitlichen Wirkungen einer Vorabentscheidung des Gerichtshofs weder vom Zeitpunkt der Verkündung des Urteils abhängen, mit dem das vorlegende Gericht endgültig über das Ausgangsverfahren entscheidet, noch von der Beurteilung der Notwendigkeit, die Rechtswirkungen der fraglichen nationalen Regelung aufrechtzuerhalten, durch dieses Gericht.

Nach dem Grundsatz des Vorrangs des Unionsrechts dürfen nämlich Vorschriften des nationalen Rechts, auch wenn sie Verfassungsrang haben, die einheitliche Geltung und die Wirksamkeit des Unionsrechts nicht beeinträchtigen (vgl. in

diesem Sinne Urteile vom 26. Februar 2013, Melloni, C 399/11, EU:C:2013:107, Rn. 59, und vom 29. Juli 2019, Pelham u.a., C 476/17, EU:C:2019:624, Rn. 78). Selbst wenn zwingende Erwägungen der Rechtssicherheit ausnahmsweise zu einer vorläufigen Aussetzung der Verdrängungswirkung führen können, die durch eine unmittelbar anwendbare Vorschrift des Unionsrechts gegenüber dem mit ihr unvereinbaren nationalen Recht ausgeübt wird, können die Voraussetzungen für eine solche Aussetzung nur vom Gerichtshof bestimmt werden (vgl. in diesem Sinne Urteil vom 8. September 2010, Winner Wetten, C 409/06, EU:C:2010:503, Rn. 61 und 67).

Da im vorliegenden Fall das Bestehen einer Gefahr schwerwiegender Störungen aufgrund der vom Gerichtshof im vorliegenden Urteil vorgenommenen Auslegung nicht dargetan ist, sind seine Wirkungen nicht zeitlich zu begrenzen, da die in Rn. 132 des vorliegenden Urteils genannten Kriterien kumulativ sind.

Nach alledem ist auf die vierte Frage zu antworten, dass der Grundsatz des Vorrangs des Unionsrechts dahin auszulegen ist, dass er es dem Verfassungsgericht eines Mitgliedstaats, bei dem ein Rechtsbehelf gegen eine nationale Regelung anhängig ist, die im Licht einer Vorabentscheidung des Gerichtshofs mit dem Unionsrecht unvereinbar ist, verwehrt, in Anwendung des Grundsatzes der Rechtssicherheit zu entscheiden, dass die Rechtswirkungen dieser Regelung bis zum Zeitpunkt der Verkündung des Urteils, mit dem es endgültig über diesen verfassungsrechtlichen Rechtsbehelf entscheidet, aufrechterhalten werden.

Besprechung der BGH-Entscheidung vom 15.06.2021, VI ZR 576/19 zum Umfang des Auskunftsanspruchs nach Art. 15 Abs 1 DS-GVO (Entscheidung veröffentlicht in RDV 4/21, 224)

Von Herrn Jaroslav Norbert Nowak, LL.M./Nadine Garir

Der Bundesgerichtshof (BGH) hat in seiner Entscheidung vom 15.06.2021, Az. VI ZR 576/19, entschieden, dass der Begriff der „personenbezogenen Daten“ im Rahmen eines Auskunftsanspruchs i.S.d. Art. 15 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) keiner teleologischen Reduktion dergestalt unterfällt, dass Auskunft nur über jene personenbezogenen Daten erteilt werden muss, bei denen es sich lediglich um signifikante biografische Informationen handelt. Vielmehr ist der Anspruch vollständig zu erfüllen.

Die Autoren setzen sich mit dieser BGH-Entscheidung und den daraus resultierenden Folgen für den Anspruch aus Art. 15 Abs. 3 DS-GVO auseinander.

I. Einleitung

Im Rahmen des Beitrags werden zunächst der zur Entscheidung stehende Fall und die Entscheidungsgründe vorgestellt, bevor das Urteil inhaltlich besprochen wird. Es wird

aufgezeigt, dass die Auslegung des BGHs erhebliche rechtliche und praktische Schwierigkeiten für das Zusammenspiel von Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO und Anspruch auf Herausgabe einer Kopie nach Art. 15 Abs. 3 DS-GVO mit sich bringt.

II. Die Entscheidung

1. Zum Sachverhalt

Der Kläger schloss im Jahr 1997 mit einer Rechtsvorgängerin der Beklagten einen Vertrag über eine kapitalbildende Lebensversicherung. Mit Schreiben vom 2016 widersprach der Kläger dem Zustandekommen des Lebensversicherungsvertrags. Auf Aufforderung des Klägers übersandte die Beklagte dem Kläger eine Datenauskunft über die vom Kläger gespeicherten Daten unter Hinweis darauf, dass die elektronisch gespeicherten Daten bei ihr ausschließlich dazu verwendet würden, den Lebensversicherungsvertrag des Klägers entsprechend ihrem Zweck als Auffanggesellschaft fortzuführen und ordnungsgemäß zu verwalten. Der Kläger war der Ansicht, dass die erteilten Auskünfte unvollständig seien.

Neben dem materiell-rechtlichen Anspruch auf Prämienrückzahlung, machte der Kläger gegen die Beklagte gerichtlich geltend,

- „3. dem Kläger eine vollständige [...] Datenauskunft durch Überlassen in Kopie – hilfsweise in Textform – zu erteilen;
4. hilfsweise zu 3., die Vollständigkeit und Richtigkeit ihrer bislang erteilten Datenauskunft an Eides statt zu versichern;
5. vorab gemäß § 256 Abs. 2 ZPO festzustellen, dass sich der Datenauskunftsanspruch des Klägers aus Art. 15 DS-GVO i.V.m. Art. 4 DS-GVO auf sämtliche bei der Beklagten tatsächlich über den Kläger vorhandene Daten erstreckt, einschließlich der intern zur Person des Klägers und der mit ihm gewechselten Korrespondenz (einschließlich E-Mails), der internen Telefon- und Gesprächsnotizen und sonstigen internen Vermerke der Beklagten zu dem zwischen den Parteien bestehenden Versicherungsverhältnis und auch der internen Bewertungen der Beklagten zu den Ansprüchen des Klägers aus der streitgegenständlichen Versicherungspolice.“

Im Laufe des Rechtsstreits erteilte die Beklagte weitere schriftliche Auskünfte zu den bei ihrem verarbeiteten personenbezogenen Daten des Klägers.

Das Berufungsgericht wies die Berufung des Klägers gegen das klagabweisende Urteil des Amtsgerichts als unzulässig zurück, ließ aber die Revision zu vorstehenden Anträgen zu.

Das Berufungsgericht begründete die Zurückweisung der Berufung damit, dass die Beklagte den Auskunftsanspruch (Anträge zu 3 und 4) nach Art. 15 DS-GVO vollständig erfüllt habe. Mit den von der Beklagten an den Kläger übermittelten Schreiben habe die Beklagte verschiedene Auskünfte gegenüber dem Kläger erteilt und darüber hinaus angegeben, dass weitere personenbezogene Daten des Klägers nicht gespeichert bzw. verarbeitet worden seien. Der

Kläger habe nicht konkret dargelegt, dass die bereits von der Beklagten erteilte Auskunft unvollständig gewesen sei und inwieweit er weitere Auskunft verlangt habe. Zurückliegende Korrespondenz der Parteien unterfalle dem Auskunftsanspruch ebenso wenig wie Datenauskünfte zu internen Bearbeitungsvermerken oder das Prämienkonto im Rahmen des Versicherungsverlaufs. Zu weiterer Korrespondenz mit Dritten habe die Beklagte erklärt, dass eine solche nicht geführt worden sei.

Für eine Zwischenfeststellungsklage (Antrag zu 5) sei kein Raum, da mit dem Urteil über die Hauptklage die Rechtsbeziehungen der Parteien erschöpfend geregelt würden.

2. Entscheidungsgründe

Die Revision des Klägers hatte Erfolg und führte zur teilweisen Aufhebung des Berufungsurteils und Zurückverweisung der Sache an das Berufungsgericht, soweit sich die Revision gegen die Anträge zu 3 und 4 richtet.

Der BGH führte aus, dass aus der Begründung des Berufungsgerichts nicht angenommen werden kann, dass die Beklagte den Auskunftsanspruch aus Art. 15 DS-GVO vollständig erfüllt hat.

Hierzu heißt es im Urteil:

„Nach Art. 15 Abs. 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen. Gemäß Art. 15 Abs. 3 Satz 1 DS-GVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.

[...]

Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH, Urteil vom 3. September 2020 – III ZR 136/18, GRUR 2021, 110 Rn. 43 m.w.N.). Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen [...].

[...]

Nach diesen Maßstäben tragen die Erwägungen des Berufungsgerichts die Annahme einer vollständigen Erfüllung des klägerischen datenschutzrechtlichen Auskunftsan-

spruchs nicht. Das Berufungsgericht hat zwar unangefochten festgestellt, dass die Beklagte dem Kläger bereits gewisse Auskünfte erteilt und angegeben hat, weitere personenbezogene Daten über den Kläger seien nicht gespeichert bzw. verarbeitet worden. Der Kläger hat jedoch, wie sich aus seinem Zwischenfeststellungsantrag und dem Sitzungsprotokoll der Berufungsverhandlung ergibt und worauf die Revision zu Recht hinweist, sein Auskunftsbegehren angesichts der bereits erteilten Auskünfte unter anderem dahingehend präzisiert, dass er weitergehende Auskünfte hinsichtlich der gesamten noch nicht mitgeteilten Korrespondenz der Parteien, einschließlich der Daten des vollständigen Prämienkontos und etwaig erteilter Zweitschriften und Nachträge zum Versicherungsschein, sowie Datenauskünfte bezüglich sämtlicher Telefon-, Gesprächs- und Bewertungsvermerke der Beklagten zum Versicherungsverhältnis fordere. Dass die Beklagte auch hinsichtlich dieser Gegenstände des Auskunftsbegehrens erklärt hätte, bereits vollständig Auskunft erteilt zu haben, hat das Berufungsgericht nicht festgestellt. Soweit das Berufungsgericht die Auffassung vertritt, diese Auskunftsgegenstände unterfielen bereits ihrer Art nach nicht dem Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO, beruht dies – jedenfalls teilweise – auf einem fehlerhaften Verständnis des Begriffs der personenbezogenen Daten im Sinne der DS-GVO und des Zwecks des datenschutzrechtlichen Auskunftsanspruchs.

[...]

Soweit die Revisionserwiderung meint, Art. 15 DS-GVO sei im Hinblick auf den Begriff der „personenbezogenen Daten“ teleologisch dahingehend zu reduzieren, dass der Personenbezug im Rahmen von Art. 15 DS-GVO voraussetze, dass es um „signifikante biografische Informationen“ gehe, die „im Vordergrund“ des fraglichen Dokuments stünden [...], ist diese Auffassung mit der zitierten Rechtsprechung des Gerichtshofs der Europäischen Union, die sich zweifelsfrei auf den Begriff der personenbezogenen Daten im Sinne des Art. 15 i.V.m. Art. 4 Nr. 1 Halbsatz 1 DS-GVO übertragen lässt, ersichtlich nicht zu vereinbaren“.

III. Bewertung der Autoren

1. Bewertung der BGH-Entscheidung

Das Urteil konkretisiert den Umfang des Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO weiter. Höchstrichterlich wurde nunmehr festgestellt, dass über verarbeitete personenbezogene Daten vollständig und umfänglich Auskunft nach Art. 15 Abs. 1 DS-GVO zu erteilen ist. Dieser Einschätzung des BGH ist zuzustimmen.

Gemäß Art. 15 Abs. 1 DS-GVO hat eine betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten.

Insofern ist ausschließlich maßgeblich, ob personenbezogene Daten vom Verantwortlichen verarbeitet werden.

Was personenbezogene Daten sind, richtet sich einzig nach Art. 4 Nr. 1 DS-GVO. Danach sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identi-

fizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, identifiziert werden kann.

Mithin geht die Definition davon aus, dass eine Einschränkung lediglich über die Frage des Rückschlusses auf eine natürliche Person erfolgen könne.¹ Ist ein Rückschluss möglich, liegt ein Personenbezug vor, und es handelt sich um personenbezogene Daten i.S.d. Art. 4 Nr. 1 DS-GVO. Ein solcher Rückschluss erfolgt über eine direkte respektive indirekte Bestimmbarkeit. Der Begriff der direkten Bestimmbarkeit drängt sich zunächst auf. Gemeint sind Faktoren und Kennzeichen, die eine natürliche Person kenntlich machen (z.B. Name, Anschrift, Geburtsdatum).² Weniger selbstverständlich ist die Identifizierung bei einer indirekten Bestimmbarkeit. In diesen Fällen ist eine Bestimmbarkeit zu bejahen, wenn die Informationen in Verbindung mit anderen Informationen eine Identifizierung ermöglichen.³ Hingegen fehlt es bei der absoluten Unmöglichkeit, einen Bezug herzustellen, an der Bestimmbarkeit.⁴ Liegt eine absolute Unmöglichkeit vor, ist das Vorliegen von personenbezogenen Daten daher grundsätzlich zu verneinen.

Insgesamt ist der Begriff der personenbezogenen Daten weit auszulegen.⁵ Insofern sind die Ausführungen des BGH zutreffend, wenn es in der Entscheidung heißt, dass personenbezogene Daten nicht auf sensible oder private Informationen beschränkt sind, sondern potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt, umfassen.⁶ Der BGH trifft es insofern auf den Punkt, wenn er im Hinblick auf den Personenbezug der Informationen darauf abstellt, ob diese „aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft“⁷ sind.

Folgerichtig gelangt der BGH damit auch zu der Auslegung, dass auch Schriftsätze zwischen den Parteien, das Prämienkonto sowie auch interne Vorgänge des datenschutzrechtlich Verantwortlichen unter den Begriff der personenbezogenen Daten i.S.d. Art. 4 Nr. 1 DS-GVO fallen, wenn sie einen – direkten oder indirekten – Personenbezug aufweisen. Daher kann der Auffassung des Berufungsgerichts in Bezug auf Art. 15 Abs. 1 DS-GVO nicht gefolgt werden, wenn es in der Entscheidung heißt:

„Nach Auffassung der Kammer bezieht sich der Auskunftsanspruch aber nicht auf sämtliche interne Vorgänge der Beklagten, wie z.B. Vermerke, oder darauf, dass die betreffende Person sämtlichen gewechselten Schriftverkehr, der dem Betroffenen bereits bekannt ist, erneut ausgedruckt und übersendet erhalten kann.“⁸

Bei den Schriftsätzen verweist der BGH darauf, dass die personenbezogene Information darin besteht, dass sich der Kläger dem Schreiben gemäß geäußert habe. Soweit es die Frage anbelangt, ob interne Vorgänge zu den personenbezogenen Daten gehören, verkennt das Berufungsgericht, dass die DS-GVO keine Einschränkung auf externe Vorgänge kennt.⁹ Ebenfalls unerheblich für das Vorliegen der personenbezogenen Daten und für den Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO ist, ob Schriftsätze, die personenbezogene Daten enthalten, der betroffenen Person bekannt sind. Der Umstand der Kenntnis ändert nichts an der Tatsache, dass personenbezogene Daten vorliegen (oder nicht).

Liegen personenbezogene Daten vor, gibt es keinen Anhaltspunkt innerhalb der DS-GVO dafür, den Begriff der personenbezogenen Daten nachträglich teleologisch zu reduzieren und schlussendlich zu verkürzen. Auch in diesem Fall ist der Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO zu erfüllen, da dieser andernfalls leerlaufen würde. Der betroffenen Person ist regelmäßig bekannt, dass sie personenbezogene Daten weitergegeben hat. Art. 15 Abs. 1 DS-GVO soll der betroffenen Person die Möglichkeit geben, sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können.¹⁰ Somit hat der Verantwortliche, will er den Anspruch aus Art. 15 DS-GVO erfüllen, sämtliche verarbeitete personenbezogene Daten der betroffenen Person in einem Antwortschreiben aufzuführen.¹¹

2. Die BGH-Entscheidung im Spannungsfeld zu Art. 15 Abs. 3 DS-GVO

So dogmatisch zutreffend die Beurteilung des BGHs in Bezug auf das Vorliegen der personenbezogenen Daten und auf die Erfüllung (§ 362 BGB) des Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO ist, so liefert diese doch erhebliches Konfliktpotential für den korrespondierenden Anspruch auf Erteilung einer Kopie, Art. 15 Abs. 3 DS-GVO.

Gemäß Art. 15 Abs. 3 DS-GVO stellt der Verantwortliche der betroffenen Person eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Dabei ist die „Kopie“ nicht ausschließlich im Sinne einer physikalischen Ablichtung der personenbezogenen Daten zu verstehen. Satz 4 des Erwägungsgrunds 63 nennt vielmehr den Fernzugriff als eine Möglichkeit, den Anspruch nach Art. 15 Abs. 3 DS-GVO zu erfüllen.

Das Verhältnis zwischen dem Anspruch auf Erteilung einer Auskunft über die verarbeiteten personenbezogenen Daten nach Art. 15 Abs. 1 DS-GVO und dem Anspruch aus Art. 15 Abs. 3 DS-GVO auf Herausgabe einer Kopie der Daten, ist umstritten.¹² Die – vermutlich herrschende – Literatur und Rechtsprechung erblickt in Art. 15 Abs. 3 DS-GVO einen eigenständigen Anspruch, der neben dem Anspruch auf Auskunft über die verarbeiteten personenbezogenen Daten nach Art. 15 Abs. 1 DS-GVO steht.

Leider trägt die Entscheidung des BGHs wenig dazu bei, dieses für die Praxis relevante Problem zu lösen. Dies ist zu bedauern. Erneut ist eine Chance vertan worden, Rechtssicherheit mit Blick auf Art. 15 Abs. 3 DS-GVO herzustellen. Auch das BAG¹³ ließ die Gelegenheit kürzlich ungenutzt.

Der BGH hätte vorliegend, zumindest obiter dictum, eine gute Möglichkeit gehabt, sich des Problems anzunehmen und Rechtssicherheit zu schaffen. Das obige Zitat aus dem Urteil des Berufungsgerichts zeigt, dass das Berufungsgericht neben dem Auskunftsanspruch aus Art. 15 Abs. 1 DS-GVO auch das Thema rund um die Kopie erkannt hat, da nach Ansicht des Berufungsgerichts die betroffene Person keinen Anspruch auf Ausdrucke der bekannten Schriftsätze habe. Auf diese Weise verwischt das Berufungsgericht die – zweifelsohne fließenden – Grenzen zwischen Art. 15 Abs. 1 und Art. 15 Abs. 3 DS-GVO.

Im Ergebnis verbleibt (lediglich) der Eindruck, dass der BGH dazu tendiert, den Anspruch auf Herausgabe der Kopien (aller) personenbezogenen Daten zu bejahen, wenn über diese personenbezogene Daten gemäß Art. 15 Abs. 1 DS-GVO Auskunft zu erteilen war. Hierdurch wird ein Gleichlauf geschaffen, der zu den Entscheidungsgründen des Urteils

passt und mit der Entscheidung des Bundesarbeitsgerichts (BAG)¹⁴ im Einklang steht.

Das BAG hielt in seiner Entscheidung vom 27. April 2021 fest, dass ein Antrag auf Erteilung einer Kopie i.S.v. § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmt ist, wenn er einen vollstreckungsfähigen Inhalt hat. Zudem fordert das BAG, dass im Vollstreckungsverfahren unzweifelhaft sein muss, auf welche Dokumente (in Form von E-Mails) sich die Verurteilung beziehen soll. Ein Klageantrag wird dem Bestimmtheitsgebot aus Sicht des BAG hingegen nicht gerecht, wenn er lediglich pauschal darauf gerichtet ist, dem Kläger eine Kopie des gesamten E-Mail-Verkehrs sowie von E-Mails, die den Kläger namentlich erwähnen, zur Verfügung zu stellen. Dies intendiert, dass der Anspruch nach Art. 15 Abs. 3 DS-GVO ohne Einschränkung begründet sein dürfte, sofern der Antrag hinreichend bestimmt ist und es sich um personenbezogene Daten handelt. Das BAG-Urteil stellt somit hohe Anforderungen an die Bestimmtheit des Anspruchs nach Art. 15 Abs. 3 DS-GVO, lässt diesen im Übrigen aber grundsätzlich gelten.

In der Praxis folgt daraus das Risiko, dass es zu einem hohen personellen, zeitlichen und monetären Aufwand auf Seiten des Verantwortlichen kommt, will er dem Anspruch auf Herausgabe einer Kopie gerecht werden.¹⁵ Gerade bei langjährigen Vertragsverhältnissen, wie etwa im Arbeitsverhältnis, dürfte der Anspruch aus Art. 15 Abs. 3 DS-GVO zunehmend als Druckmittel erhalten. Insbesondere in diesen Fällen dürfte die Erfüllung des Anspruchs aufgrund der kaum überschaubaren Anzahl an Dokumenten mit personenbezogenen Daten jedoch nahezu unmöglich sein.

Dem Berufungsgericht ist daher in dem Punkt zuzustimmen, dass es eines Korrektivs bedarf, damit sich die Erfüllung des Anspruchs auf Erteilung einer Kopie nicht lediglich zu einer arbeitsintensiven Förmelerei entwickelt. Vorzugswürdig erscheint es daher, den Anspruch aus Art. 15 Abs. 3 DS-GVO – ungeachtet eines bestehenden Anspruchs aus Art. 15 Abs. 1 DS-GVO – über den Einwand des unverhältnismäßigen Aufwands (vgl. Art. 14 Abs. 5 DS-GVO) unter Verweis auf die Grenze der Zumutbarkeit einzuschränken.¹⁶ Im Rahmen einer solchen Verhältnismäßigkeitsprüfung ist dann auch, die Kenntnis der betroffenen Personen zu berücksichtigen. Indes ist eine Anwendung des § 242 BGB, als nationale Vorschrift, auf die Bestimmungen der DS-GVO, abzulehnen.¹⁷

1 In diese Richtung auch BeckOK DatenschutzR/Schild, DS-GVO Art. 4 Rn. 16 ff.

2 BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn. 16.

3 BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn. 17.

4 Paal/Pauly/Ernst, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 9.

5 BeckOK DatenschutzR/Schild, 37. DS-GVO Art. 4 Rn. 21a.

6 BGH, Urte. v. 15.06.2021 – VI ZR 576/19, Rn. 22.

7 BGH, aaO.

8 LG Köln, Urte. v. 19.06.2019 – 26 S 13/18, Rn. 39.

9 BGH, aaO, Rn 27.

10 Erwägungsgrund 63 zur DS-GVO.

11 Nowak/Bornholdt, RDV 2020, 191, 192.

12 Statt vieler siehe Nowak/Bornholdt, aaO.

13 BAG, Urte. v. 27.04.2021 – 2 AZR 342/20.

14 BAG, aaO.

15 Wybitul/Brams, NZA 2019, 672, 674.

16 Härting, Mit der DS-GVO zum „Golden Handshake“ – von der Sprengkraft des „Rechts auf Kopie“, abrufbar unter: <https://www.cr-online.de/blog/2019/03/29/mit-der-dsgvo-zum-golden-handshake-von-der-sprengkraft-des-rechts-auf-kopie/>.

17 LG Wuppertal, Urte. v. 29.07.2021 – 4 O 409/20.

Erschütterung des Beweiswerts einer Arbeitsunfähigkeitsbescheinigung (Ls)

(Bundesarbeitsgericht, Urteil vom 8. September 2021 – 5 AZR 149/21 –)

1. Den Beweiswert einer Arbeitsunfähigkeitsbescheinigung kann der Arbeitgeber erschüttern, wenn er tatsächliche Umstände darlegt und ggf. beweist, die Anlass zu ernsthaften Zweifeln an der Arbeitsunfähigkeit geben. Gelingt das dem Arbeitgeber, muss der Arbeitnehmer substantiiert darlegen und beweisen, dass er arbeitsunfähig war. Der Beweis kann insbesondere durch Vernehmung des behandelnden Arztes nach entsprechender Befreiung von der Schweigepflicht erfolgen.
2. Kündigt ein Arbeitnehmer sein Arbeitsverhältnis und wird er am Tag der Kündigung arbeitsunfähig krankgeschrieben, kann dies den Beweiswert der Arbeitsunfähigkeitsbescheinigung insbesondere dann erschüttern, wenn die bescheinigte Arbeitsunfähigkeit passgenau die Dauer der Kündigungsfrist umfasst.

(Nicht amtliche Leitsätze)

Keine namentliche Benennung der Mitglieder einer Gewerkschaft bei der gerichtlichen Geltendmachung von Ansprüchen

(Bundesarbeitsgericht, Urteil vom 29. April 2021 – 8 AZR 276/20 –)

Eine Gewerkschaft, die ihren schuldrechtlichen Anspruch auf Durchführung eines geschlossenen Haustarifvertrags zu Gunsten ihrer Mitglieder durch Leistungsklage geltend macht, muss diese nicht namentlich benennen.

(Nicht amtlicher Leitsatz)

Aus den Gründen:

Der Beklagte hat gegen seine tarifliche Durchführungspflicht gegenüber der klagenden Gewerkschaft verstoßen. Die Vergütung der Tagesreporter hat vorrangig nach den speziellen Honorarkennziffern zu erfolgen. Der Anspruch auf Durchführung des Tarifvertrags ist allerdings auf die tarifgebundenen Beschäftigten beschränkt. Für die Zulässigkeit des auf die Gewerkschaftsmitglieder begrenzten Klageantrags war es entgegen der Auffassung des Landesarbeitsgerichts nicht erforderlich, diese bereits im Erkenntnisverfahren namentlich zu benennen.

Zum Auskunftsanspruch bei fehlender Datenspeicherung

(Oberlandesgericht Dresden, Urteil vom 31. August 2021 – 4 U 324/21 –)

Mit der Erklärung, einen eingesandten Datenträger nicht mehr in Besitz und die aufgespielten Daten nicht ausgelesen zu haben, hat der Datenverantwortliche den Auskunftsanspruch gemäß Art. 15 Datenschutz-Grundverordnung (DS-GVO) gegenüber dem Betroffenen erfüllt.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Der Kläger verlangt von der Beklagten Schadensersatz wegen behaupteter unzulässiger Verarbeitung seiner Daten, Auskunft über die Weitergabe dieser Daten in Form von Haupt- und Hilfsantrag, die Herausgabe einer Festplatte sowie Unterlassung des Einbehalts oder der Weitergabe bzw. Veröffentlichung der Daten auf dieser Festplatte.

Die Parteien schlossen im April 2018 einen Kaufvertrag über einen Laptop mit drei Jahren Garantie. Wegen eines Defekts übersandte der Kläger die Festplatte einschließlich der darauf befindlichen personenbezogenen Daten im April 2020 an die Beklagte zur Reparatur; die Beklagte hatte vor der Rücksendung in einer E-Mail vom 30.03.2020 (Anlage K 5) darauf hingewiesen, dass sie eine Datensicherung nicht vornehmen könne, hierfür vielmehr der Kunde selbst verantwortlich sei. Am 06.04.2020 übersandte sie dem Kläger eine Festplatte, bei der es sich unstreitig nicht um die von ihm eingesandte handelte. Personenbezogene Daten des Klägers waren auf dieser Festplatte nicht vorhanden, ob sie Dateien eines Dritten enthielt und ob es sich hierbei um eine neuwertige Festplatte gehandelt hat, ist zwischen den Parteien streitig. Das Landgericht hat nach Vernehmung von Zeugen zum Verbleib der Festplatte im Betrieb des Klägers die Klage abgewiesen. Wegen der Begründung wird auf die Entscheidungsgründe des angefochtenen Urteils verwiesen.

Mit seiner Berufung wiederholt der Kläger seine erstinstanzliche Rechtsauffassung. Er beantragt, die Beklagte zu verurteilen,

1.

a) Auskunft darüber zu erteilen, ob und welchen Dritten sie in die Daten auf der ihr von dem Kläger übersandten Festplatte Seagate mit der Seriennummer Einsicht gewährt hat, unter Auflistung der Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, samt Nennung der Rechtsgrundlage;

b) hilfsweise dem Kläger über die Ausführung des Reparaturauftrags vom 31.03.2020 der Festplatte Seagate mit der Seriennummer und deren Dateninhalte sowie einer etwaigen Weitergabe der Festplatte selbst Rechenschaft abzulegen;

2. die Festplatte Seagate mit der Seriennummer sowie die Daten-Inhalte der Festplatte, die sich zum Zeitpunkt des Versands der Festplatte an die Beklagte auf der Festplatte befunden haben, samt etwaig angefertigter Kopien, dem Kläger herauszugeben;

3. es bei Meldung eines Ordnungsgeldes von bis zu 250.000 €, ersatzweise Ordnungshaft bis zu 6 Monaten, die Ordnungshaft zu vollstrecken an dem Geschäftsführer der persönlich haftenden Gesellschafterin der Beklagten, zu unterlassen, die Festplatte Seagate mit der Seriennummer sowie die Daten-Inhalte der Festplatte, die sich zum Zeitpunkt des Versands der Festplatte an die Beklagte, auf der Festplatte befunden haben, samt etwaiger gefertigter Kopien, gleich ob in gedruckter oder digitaler Form, einzubehalten, an Dritte weiterzugeben oder zu veröffentlichen;

4. an den Kläger Schadensersatz, wie er sich anhand der Auskunft gemäß Ziffer I ergibt, mindestens jedoch in Höhe von 10.000 nebst Zinsen i.H.v. 5 Prozentpunkten über dem jeweiligen Basiszinssatz hieraus seit Rechtshängigkeit an den Kläger zu bezahlen,

5. an den Kläger die außergerichtlich entstandenen Rechtsanwaltskosten i.H.v. 1.029,35 € nebst Zinsen i.H.v. 5 Prozentpunkten über dem jeweiligen Basiszinssatz hieraus seit Rechtshängigkeit zu bezahlen.

Aus den Gründen:

Die zulässige Berufung des Klägers hat in der Sache keinen Erfolg.
1.

Der Kläger hat weder nach § 15 DS-GVO noch nach § 666 BGB einen Anspruch auf weitergehende Auskunft.

a) Nach Art. 15 DS-GVO hat der Verantwortliche dem Betroffenen zunächst Auskunft darüber zu erteilen, ob dessen personenbezogene Daten verarbeitet werden. Hieraus wird in der Literatur eine Einschränkung auf aktuell noch vorhandene personenbezogenen Daten abgeleitet, weil eine vergangenheitsbezogene Auskunftspflicht, die sich auch auf bereits gelöschte Daten erstreckte, Art. 5 Abs. 1 Buchst. e und den über Art. 15 Abs. 1 Buchst. d anzugebenden Speicherfristen widerspräche (Kamlah in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, Art. 15 DS-GVO, Rn. 5; BeckOK DatenschutzR/Schmidt-Wudy, Art. 15 DS-GVO Rz. 52; Kühling/Buchner/Bäcker, Art. 15 DS-GVO Rz. 9).

Der Senat lässt offen, ob dieser Auffassung, die dem Auskunftsanspruch des Klägers von vornherein die Grundlage entzöge, zu folgen ist. Jedenfalls steht im Anschluss an die erstinstanzliche Beweisaufnahme fest, dass die Beklagte über die eingesandte Festplatte nicht mehr im Besitz und auf die darauf möglicherweise enthaltenen Daten keinen Zugriff (mehr) hat, was sie dem Kläger auch bereits vorprozessual mitgeteilt hatte. Etwaige Auskunftspflichten nach Art. 15 DS-GVO hat sie damit jedenfalls gemäß § 362 BGB erfüllt.

Wie der Bundesgerichtshof zu Art. 15 DS-GVO bereits entschieden hat, ist ein Auskunftsanspruch erfüllt, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist allein die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH, Urteil vom 03.09.2020 – III ZR 136/18, GRUR 2021, 110 Rn. 43 m.w.N.). Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll (BGH, Urteil vom 15.06.2021 – VI ZR 576/19 –, Rn. 19-20, juris). Dies ist hier der Fall. Zwar mag im Ergebnis der Beweisaufnahme offengeblieben sein, ob die Festplatte bei der Beklagten vernichtet oder an den Hersteller zurückgesandt wurde; in jedem Fall ist die Beklagte zu weiteren Auskünften aber nicht mehr in der Lage, eine etwaige Unvollständigkeit der Auskunft steht einer Erfüllung mithin nicht entgegen.

b) Liegt – wie hier – eine negative Verarbeitungsbestätigung vor, kommt ein Anspruch auf weitergehende Auskunft hinsichtlich der in Art. 15 Abs. 1 Buchst. a-h beschriebenen Informationsbestandteile von vornherein nicht in Betracht (Kamlah in: Plath, a.a.O., Art. 15 DS-GVO, Rn. 3). Auch der unter b) geltend

gemachte Anspruch auf Rechenschaftslegung nach § 666 BGB scheidet aus. Ob § 666 BGB im Anwendungsbereich der Datenschutzgrundverordnung durch Art. 15 DS-GVO verdrängt wird, kann offenbleiben, weil auch dieser Anspruch erfüllt wäre. Eine weitergehende Rechenschaft als die hier allein mögliche Angabe, dass die Festplatte sich nicht mehr in ihrem Besitz befindet und sie keinen Zugriff auf die aufgespielten Daten genommen hat, schuldet die Beklagte auch nach dieser Vorschrift nicht. Dabei kommt es nicht darauf an, ob sie vernünftigerweise nach den Umständen des konkreten Falles und des Hinweises auf die Verantwortlichkeit des Kunden für die Datensicherheit in der E-Mail vom 30.3.2020 (K5) davon ausgehen durfte, dass der Kläger im Tausch gegen eine neue Festplatte auf den eingesandten Datenträger und die aufgespielten Daten verzichtet hatte. Wie das Landgericht auf der Grundlage der Zeugenaussagen ohne Fehler in der Beweiswürdigung festgestellt hat, hat die Beklagte jedenfalls auf die Festplatte und die aufgespielten Daten keinerlei Zugriff mehr, Aufzeichnungen hierüber hat sie ebenfalls nicht geführt. Weitere Rechenschaftspflichten sind ihr damit unmöglich geworden.

2.

Aus denselben Gründen kommt auch, ungeachtet des Vorliegens der sonstigen Voraussetzungen des § 985 BGB die Herausgabe der Festplatte wegen objektiver Unmöglichkeit nicht in Betracht. Ob die Unterlassung einer weiteren Verarbeitung der Daten, sofern sie auf einen Verstoß gegen Bestimmungen der DS-GVO gestützt wird, überhaupt mit einem zivilrechtlichen Unterlassungsanspruch durchgesetzt werden könnte, ist bereits im Ausgangspunkt fraglich. Nach dem Wortlaut des Art. 79 Abs. 1 DS-GVO bleiben nur andere verwaltungsrechtliche oder außergerichtliche Rechtsbehelfe „unbeschadet“, nicht aber gerichtliche Rechtsbehelfe. Hieraus wird teilweise gefolgert, dass über die in den Art. 12 bis 22 DS-GVO eingeräumten Auskunfts-, Berichtigungs- und Löschungsrechte (Art. 17 DS-GVO) sowie das Recht auf Einschränkung der Verarbeitung personenbezogener Daten hinaus dem Betroffenen keine Rechte zustünden, zu deren Durchsetzung ein wirksamer Rechtsbehelf nach Art. 79 DS-GVO zur Verfügung gestellt werden müsste; dies schließe auch Ansprüche nach §§ 823, 1004 BGB aus (VG Regensburg, Gerichtsbescheid vom 06.08.2020 – RN 9 K 19.1061 –, Rn. 19-20, juris; anders allerdings Senat, Beschluss vom 19.4.2021 – 4 W 243/21 –, juris).

Dies kann hier aber ebenfalls dahinstehen, weil es jedenfalls an der für einen solchen Unterlassungsanspruch erforderlichen Wiederholungsgefahr fehlt. Ebenso wenig wie der Beklagten eine Herausgabe der Festplatte möglich ist, ist ihr wegen Zerstörung oder Verlust des Datenträgers auch eine Weitergabe der darauf ggf. enthaltenen Daten möglich. Anhaltspunkte dafür, dass die Beklagte diese vor der Vernichtung gesichert oder an Dritte weitergegeben hätte, sind vom Kläger weder vorgetragen noch nach der Beweisaufnahme des Landgerichts ersichtlich.

3. Vertragliche Ansprüche auf den hier allein geltend gemachten immateriellen Schaden scheiden von vornherein aus. Der Kläger hat aber auch weder einen Anspruch auf eine Geldentschädigung nach Art. 2 Abs. 1 i.V.m. Art. 1 GG noch auf immateriellen Schadensersatz nach Art. 82 DS-GVO wegen des behaupteten Verlusts seiner personenbezogenen Daten, die sich auf der Festplatte befunden haben sollen.

a) Zwar läge in einem solchen Vorgang, seine Richtigkeit unterstellt, eine Verletzung seines Grundrechts auf informationelle Selbstbestimmung, die grundsätzlich auch Ansprüche auf

eine Geldentschädigung begründen kann. Die freie Entfaltung der Persönlichkeit setzt nach allgemeiner Auffassung unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Das Grundrecht gewährleistet damit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Das Recht auf informationelle Selbstbestimmung gilt im Wege der mittelbaren Drittwirkung auch im Verhältnis zwischen Privaten (BVerfG, Beschluss vom 06.11.2019 – 1 BvR 16/13 –, BVerfGE 152, 152 – 215, Rn. 84 – 85 Recht auf Vergessen I).

Der aus Art. 1, 2 Abs. 1 GG hergeleitete Anspruch auf eine immaterielle Geldentschädigung liegt aber nicht schon bei jeder Verletzung des allgemeinen Persönlichkeitsrechts, erst recht nicht bei jeder Vertragsverletzung vor. Er setzt vielmehr einen schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht voraus, dessen Beeinträchtigung nicht in anderer Weise befriedigend aufgefangen werden kann. Dabei hängt die Entscheidung, ob eine hinreichend schwerwiegende Verletzung des Persönlichkeitsrechts vorliegt, insbesondere von der Bedeutung und Tragweite des Eingriffs, ferner auch von Anlass und Beweggrund des Handelnden sowie von dem Grad seines Verschuldens ab (Senat, Beschluss vom 11.06.2019 – 4 U 760/19 –, Rn. 8, juris; Urteil vom 30.01.2018 – 4 U 1110/17 –, Rn. 4, juris mit weiteren Nachweisen). Vorliegend lässt sich die Bedeutung der behaupteten Datenlöschung für den Kläger mangels eines hierauf bezogenen Vorbringens schon nicht absehen. Der Kläger hat überdies nicht einmal behauptet, die nicht näher spezifizierten personenbezogenen Daten, die sich auf der Festplatte befunden haben sollen, seien nur dort gespeichert gewesen und nunmehr unwiederbringlich verloren. Der Anordnung des persönlichen Erscheinens zur mündlichen Anhörung durch den Senat gemäß § 141 ZPO hat er ohne Angabe von Gründen nicht Folge geleistet. Unabhängig hiervon liegt jedoch auch das für einen Anspruch auf eine Geldentschädigung erforderliche schwerwiegende Verschulden nicht vor, weil die Beklagte lediglich im Rahmen der von ihr eingeräumten Garantie und ohne Schädigungsvorsatz gehandelt hat.

b) Daneben scheidet auch ein Anspruch nach Art. 82 Abs. 1 DS-GVO wegen der zugunsten des Klägers unterstellten Datenvernichtung aus. Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat hiernach Anspruch auf Schadenersatz gegen den Verantwortlichen. Jeder an einer Verarbeitung beteiligte Verantwortliche haftet dabei für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein solcher Verstoß liegt hier aber nicht vor.

a. Allerdings hat die Beklagte die auf der Festplatte gespeicherten Daten des Klägers i.S.d. DS-GVO verarbeitet, unabhängig davon, ob die Festplatte vor Ort vernichtet oder zur Zerstörung an den Hersteller zurückgesandt wurde. Die damit in jedem Fall einhergehende Löschung der Daten stellt eine Datenverarbeitung nach Art. 4 Nr. 2 DS-GVO dar, auch soweit sie allein durch Zerstörung des Datenträgers erfolgt ist. (vgl. insoweit Kühling/Buchner/Herbst, 3. Aufl. 2020, DS-GVO Art. 17 Rn. 39). Die Zerstörung der Festplatte war auch nicht zur Erfül-

lung des Vertrags (Erwägungsgrund 44 DS-GVO), aufgrund einer rechtlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse (Erwägungsgrund 45 DS-GVO) oder um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen natürlichen Person zu schützen (Erwägungsgrund 46 DS-GVO) erforderlich.

b. Vorliegend hat der Kläger aber konkludent seine Einwilligung in die mit dem Austausch der Festplatte einhergehende Datenlöschung erteilt. Unstreitig hat er die Rücksendung nach Erhalt und in Kenntnis der E-Mail der Beklagte vom 30.3.2020 (K5) vorgenommen, in der ausdrücklich darauf hingewiesen wird, dass es vorkommen kann, dass „im Zuge der Reparatur die Festplatte gelöscht oder getauscht werden muss.“ In der Rücksendung der Festplatte lag angesichts dessen nach dem objektiven Empfängerhorizont die Zustimmung dazu, die eingeräumte Garantie entweder durch Reparatur oder Austausch unter gleichzeitigem Datenverlust vorzunehmen, zumal in diesem Kontext ebenfalls darauf hingewiesen wurde, dass die Beklagte Datensicherung und Datenrettung nicht anbietet und jeder Kunde „für die Sicherheit der Daten selbst verantwortlich“ sei (K 5).

Ob hierdurch der zwischen den Parteien bestehende Kaufvertrag und die damit einhergehenden vertraglichen Verpflichtungen wirksam nach §§ 305 ff. BGB abgeändert wurden, kann im Rahmen des Anspruchs nach Art. 82 DS-GVO dahinstehen. Entgegen der Auffassung des Klägers ist es auch ohne Belang, dass er nicht ausdrücklich in die Löschung seiner Daten eingewilligt hat. Wie sich aus Erwägungsgrund 32 der DS-GVO ergibt, ist eine solche ausdrückliche Einwilligung gerade nicht erforderlich (so auch Härting in: Härting, Internetrecht, 6. Aufl. 2017, Datenschutzrecht, Rn. 48). Ausreichend ist vielmehr „eine eindeutige bestätigende Handlung ..., mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert.“

Die DS-GVO stellt damit entscheidend darauf ab, dass die Einwilligung nicht aus der passiven Hinnahme der Datenverarbeitung abgeleitet wird, etwa durch ein voreingestelltes Ankreuzkästchen auf einer Internetseite, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss (vgl. hierzu EuGH, Urteil vom 01.10.2019 – C-673/17, GRUR 2019, 1198 – Verbraucherzentrale Bundesverband/Planet49 sowie nachfolgend BGH, Urteil vom 28.05.2020 – I ZR 7/16 –, Rn. 10, juris), sondern dass eine aktive, unmissverständliche Handlung des Betroffenen erforderlich ist, die vor Beginn der Datenverarbeitung liegt, freiwillig erfolgt und aus der sich ein Einverständnis mit der gebotenen Eindeutigkeit ableiten lässt (EuGH NJW 2019, 3433 Rn. 62; BeckRS 2020, 30027 Rn. 36, BeckOK DatenschutzR/Schild, 36. Ed. 1.5.2021, DS-GVO Art. 4 Rn. 124). Es genügt nicht, sich auf die Abwesenheit einer Erklärung oder Handlung zu berufen, die als Ausdruck der Verweigerung gedacht ist (Ehmann/Selmayr/Klabunde, 2. Aufl. 2018, DS-GVO Art. 4 Rn. 53). An diese Unmissverständlichkeit dürfen aber gerade bei Massengeschäften wie der Abwicklung von Gewährleistungsansprüchen im Internet bereits nach den aufgeführten Er-

wägungen des Ordnungsgebers keine überzogenen Anforderungen gestellt werden, die im Ergebnis doch wieder auf eine ausdrückliche Einwilligung hinauslaufen. Dies gilt im vorliegenden Fall umso mehr, als es der Kläger es in der Hand gehabt hätte, den Erklärungswert der in Kenntnis der E-Mail vom 30.03.2020 erfolgten Rücksendung zu präzisieren, indem er zugleich darauf hingewiesen hätte, dass sich auf der Festplatte personenbezogenen Daten befanden, die er aufgrund des Schadensfalls nicht mehr gesichert hatte oder nicht mehr hatte sichern können und dass in jedem Fall eine Rücksendung der Festplatte zur Datensicherung erbeten werde.

c. Ob der bloße Datenverlust überhaupt einen immateriellen Schaden i.S.d. Art. 82 DS-GVO darstellen kann oder ob hierfür eine erhebliche Beeinträchtigung erforderlich ist (vgl. Senat, Beschluss vom 11.6.2019 – 4 U 760/19 Rn. 13; zur Problematik der Geltendmachung von Bagatellschäden Wybitul, NJW 2020, 1190, 1193 unter Hinweis auf BVerfG NJW 2021, 1005; vgl. jetzt auch Vorlagebeschluss des ÖstOGH, Beschluss vom 15.04.2021, BeckRS 2021, 13879), kann angesichts dessen dahinstehen. Unabhängig hiervon steht dem Anspruch aber auch entgegen, dass es an jeglichem Vortrag des Klägers zu den Auswirkungen des behaupteten Datenverlusts fehlt. Der geltend gemachte immaterielle Schaden in Höhe von 10.000,00 € findet in seinem Vortrag keinerlei Stütze, sondern dient ersichtlich nur dazu, ein Drohpotential aufzubauen, um die Beklagte zu einer letztlich nicht gerechtfertigten Zahlung zu veranlassen.

III.

2. Gründe für die Zulassung der Revision sieht der Senat nicht. Auch eine Vorlage an den Europäischen Gerichtshof zur Auslegung des Begriffs der Einwilligung im Sinne der Art. 4 Nr. 11, 6 Abs. 1 lit a) DS-GVO ist nicht geboten. Nach der Rechtsprechung des EuGH (EuGH NJW 1983, 1257 Rn. 21 – C. I. L. F. I. T.; EuGH BeckRS 2005, 70935 Rn. 16; stRspr) kann von einer Vorlage abgesehen werden, wenn feststeht, dass die gestellte Frage nicht entscheidungserheblich ist, dass die betreffende unionsrechtliche Bestimmung bereits Gegenstand einer Auslegung durch den Gerichtshof war (*acte éclairé*) oder dass die richtige Anwendung des Unionsrechts derart offenkundig ist, dass für einen vernünftigen Zweifel keinerlei Raum bleibt (*acte clair*). Davon darf das innerstaatliche Gericht ausgehen, wenn es überzeugt ist, dass auch für die Gerichte der übrigen Mitgliedsstaaten und für den EuGH die gleiche Gewissheit bestünde (st. Rspr., vgl. zuletzt BVerfG NJW 2021, 1005 Rn. 10, beck-online).

So liegt der Fall hier. Der Senat geht angesichts der Formulierung in den Erwägungsgründen zur DS-GVO, die das Verständnis des normsetzenden europäischen Gesetzgebers wiedergeben und für die Auslegung durch die Gerichte der Mitgliedsstaaten maßgeblich sind, von einer eindeutigen Rechtslage („*acte clair*“) aus; abweichende Auffassungen zur Zulässigkeit einer konkludenten Einwilligung werden in Literatur und Rechtsprechung – soweit ersichtlich – nicht vertreten.

Arbeitgeber darf Rückkehr aus Homeoffice anordnen (Ls)

(Landesarbeitsgericht München, Urteil vom 26. August 2021 – 3 SaGa 13/21 –)

Ein Arbeitgeber, der seinem Arbeitnehmer gestattet hatte, seine Tätigkeit als Grafiker von zuhause aus zu

erbringen, ist gemäß § 106 Satz 1 GewO grundsätzlich berechtigt, seine Weisung zu ändern, wenn sich später betriebliche Gründe herausstellen, die gegen eine Erledigung von Arbeiten im Homeoffice sprechen.

(Nicht amtlicher Leitsatz)

Kündigung wegen Verwendung einer gefälschten Entgeltabrechnung bei Kreditbeantragung (Ls)

(Landesarbeitsgericht Hamm, Urteil vom 19. August 2021 – 8 Sa 1671/19 –)

1. Das Verfälschen von Entgeltabrechnungen zwecks Täuschung eines Kreditgebers kann die persönliche Eignung des Arbeitnehmers für die ihm übertragenen Aufgaben jedenfalls dann in Frage stellen, wenn im Rahmen einer kaufmännischen Tätigkeit gerade die Vertragsanbahnung zu den Arbeitsaufgaben gehört.
2. Das Herstellen verfälschter Abrechnungen und deren Verwendung im Rechtsverkehr verletzt zugleich die gegenüber dem Arbeitgeber begründete Rücksichtnahmepflicht aus § 241 Abs. 2 BGB. Ein derartiges Verhalten kann unter Berücksichtigung der Umstände des Einzelfalls eine außerordentliche Kündigung rechtfertigen.

(Nicht amtliche Leitsätze)

Initiativrecht des Betriebsrats bei Einführung einer elektronischen Zeiterfassung

(Landesarbeitsgericht Hamm, Beschluss vom 27. Juli 2021 – 7 TaBV 79/20 –)

Dem Betriebsrat steht bei der Einführung einer elektronischen Zeiterfassung ein Initiativrecht zu (Abweichung BAG, Beschl. v. 28.11.1989, 1 ABR 97/88).

Sachverhalt:

Die Beteiligten streiten vor dem Hintergrund eines ausgesetzten Einigungsstellenverfahrens um die Frage, ob dem antragstellenden Betriebsrat ein Initiativrecht bei der Einführung einer elektronischen Zeiterfassung zusteht.

Aus den Gründen:

II. Der Antrag des Betriebsrates ist begründet, da ihm gemäß § 87 Abs. 1 Nr. 6 BetrVG ein Initiativrecht bei der Einführung einer elektronischen Zeiterfassung zusteht.

1. Ausgangspunkt für die Annahme eines Initiativrechtes ist zunächst der Wortlaut des Gesetzes in § 87 Abs. 1 BetrVG (Eingangssatz) „mitzubestimmen“, ergänzt um die Eingangsformulierung des § 87 Abs. 1 Nr. 6 BetrVG „Einführung“. Mitbestim-

mung im Wortsinne beschreibt das Recht auf Mitgestaltung im Sinne gleichwertiger Verhandlungspartner. Diese gesetzliche Systematik wird nicht zuletzt durch den Konfliktregelungsmechanismus über das Einigungsstellenverfahren gemäß § 87 Abs. 2 BetrVG festgeschrieben (Fitting u.a. BetrVG 30. Aufl., § 87 Rn. 1). Die Ausübung der Mitbestimmung als „Vetorecht“, wie es in § 99 Abs. 2 und 3 BetrVG für die personelle Einzelmaßnahme beschrieben ist, kommt nicht in Betracht (BAG v. 29.01.2008, 3 AZR 42/06 Rn. 34). Daher entspricht es der übereinstimmenden Auffassung in Rechtsprechung und Literatur, dass im Sinne eines Mitgestaltungsrechtes grundsätzlich auch dem Betriebsrat die Initiative zukommen kann, in mitbestimmungspflichtigen Angelegenheiten Verhandlungen aufzunehmen und zu verlangen (so schon BAG, Beschl. v. 14.11.1974, 1 ABR 65/73).

Dem folgend hat das Bundesarbeitsgericht zutreffend im Beschluss vom 27.01.2004, 1 ABR 7/03 unter Rn. 28 ausdrücklich festgehalten, dass die Mitbestimmung bei der Einführung einer technischen Kontrolleinrichtung ausdrücklich auch das „ob“ der Anschaffung umfasst, ohne allerdings auf den Beschluss vom 18.11.1989 aaO zurückzugreifen.

2. Die Grundsätze zur Annahme eines Initiativrechtes sind auch auf die Mitbestimmung bei der Einführung einer technischen Kontrolleinrichtung i.S.d. § 87 Abs. 1 Nr. 6 BetrVG übertragbar.

a) Die Beschwerdekammer verkennt nicht, dass das Bundesarbeitsgericht im Beschluss vom 18.11.1989, 1 ABR 97/88, ein Initiativrecht des Betriebsrates bei der Einführung einer technischen Kontrolleinrichtung abgelehnt und zur Begründung unter Rn. 22 ausgeführt hat, dass ein Eingriff in den Persönlichkeitsbereich der Arbeitnehmer durch Verwendung anonymer technischer Kontrolleinrichtungen nur unter Wahrung der Mitbestimmung des Betriebsrates gem. § 87 Abs. 1 Nr. 6 BetrVG zulässig sei. Damit komme diesem Mitbestimmungsrecht des Betriebsrates eine Abwehrfunktion gegenüber der Einführung technischer Kontrolleinrichtungen zu. Dieser Zweckbestimmung widerspreche es, wenn der Betriebsrat selbst deren Einführung verlangen könne.

b) Abgesehen davon, dass die Entscheidung des BAG v. 18.11.1989 aaO Kritik erfahren hat (vgl. Wall, AiB 2021, 47 ff; Byers, RdA 2014, 37-41; Wiese/Gutzeit, GK/BetrVG 11. Aufl., § 87 Rdnr. 142, LAG Berlin-Brandenburg, Beschlüsse vom 22.01.2015, 10 TaBV 1812/14 und 10 TaBV 2124/14), erfordert der Rückgriff auf den Sinn und Zweck des Mitbestimmungsrechtes zur Eingrenzung des oben unter B. II. 1. beschriebenen Wortlautes die Auslegung mittels teleologischer Interpretation als Ermittlung des Gesetzeszweckes (hierzu MünchKomm BGB/Säcker, 8. Aufl., Einleitung BGB Rn. 143); die teleologische Reduktion ist richterliche Rechtsfortbildung.

aa) Die richterliche Rechtsfortbildung kann sich indessen nur innerhalb des vom Gesetzgeber gemeinten Sinn und Zwecks der Rechtsnorm bewegen (MünchKomm/Säcker a.a.O. Rn. 139 mwN.). Die Auslegung von Gesetzen und richterliche Rechtsfortbildung dürfen sich demnach von dem erkennbaren Willen des Gesetzgebers – namentlich von der gesetzgeberischen Grundentscheidung – nicht lösen (BVerfG, Beschlüsse v. 06.06.2018, 1 BvL 7/14 und 1 BvR 1375/14, Rn. 76 m.w. Nachw.; so auch LAG Berlin-Brandenburg, Beschlüsse v. 22.01.2015 a.a.O., Rn. 36 ff).

bb) Der erkennbare Wille des Gesetzgebers des BetrVG 1972 im Bereich der Mitbestimmung des § 87 Abs. 1 BetrVG ist im Gesetzgebungsverfahren dokumentiert.

Denn der Gesetzgeber hat bei der Schaffung des BetrVG 1972 bei der Mitbestimmung in sozialen Angelegenheiten bewusst nicht zwischen Mitbestimmungsrechten mit Initiativrecht und solchen ohne Initiativrecht unterschieden: der seinerzeitige Gesetzesentwurf der Bundestagsfraktion der CDU/CSU differenzierte zwischen Mitbestimmungsrechten des Betriebsrates in Form gemeinsamer Regelungsbefugnisse und solchen, die ohne Initiativrecht als Zustimmungsrecht ausgestaltet waren. Die gemeinsame Regelungsbefugnis sollte bei fehlender Einigung in ein Einigungsstellenverfahren münden, die als Zustimmungsrecht ausgestaltete Mitbestimmung sollte in ein Zustimmungseretzungsverfahren münden (BT-Drs. VI/1806). Der Ausschuss für Arbeits- und Sozialordnung lehnte diesen Vorschlag nach Beratung ab (dokumentiert zu BT-Drs. VI/2729, Seite 4) und führte u.a. an, dass eine Unterscheidung zwischen echten Mitbestimmungsrechten, die ein Initiativrecht erfassen und solchen, die ausschließlich von der Initiative des Arbeitgebers abhängen und lediglich der Zustimmung des Betriebsrates bedürften, abgelehnt würden. Der endgültige schriftliche Bericht des Ausschusses für Arbeit und Sozialordnung (BT-Drs. VI/2729) beinhaltete sodann im Entwurf eines Betriebsverfassungsgesetzes als einheitliche Vorschrift über die Mitbestimmung des Betriebsrates in sozialen Angelegenheiten die Norm des § 87 BetrVG in der Eingangsformulierung, wie er heute noch in Kraft ist; eine Aufspaltung der Mitbestimmungsrechte in solche mit und ohne Initiativrecht erfolgte ausdrücklich nicht. Vielmehr hat der Gesetzgeber den Weg gewählt, dass er Einschränkungen des Oberbegriffs der Mitbestimmung in § 87 Abs. 1 BetrVG (Eingangssatz) in der Weise vorgenommen hat, dass er einzelne Mitbestimmungsrechte wie z.B. § 87 Abs. 1 Nr. 8 BetrVG (betreffend Sozialeinrichtungen) so formuliert hat, dass dort lediglich Form-, Ausgestaltung und deren Verwaltung mitbestimmungspflichtig sind, woraus sich ohne weiteres ergibt, dass aufgrund dieser ausdrücklich gewählten Formulierung in § 87 Abs. 1 Nr. 8 BetrVG ein Initiativrecht nicht besteht. Genau eine solche Einschränkung findet sich in § 87 Abs. 1 Nr. 6 BetrVG nicht; vielmehr ist dort ausdrücklich die „Einführung“ beschrieben.

c) Nach alledem kam es für die Annahme eines Initiativrechtes zur Einführung der elektronischen Zeiterfassung gemäß § 87 Abs. 1 Nr. 6 BetrVG nicht auf die vom Betriebsrat vorgetragene Auffassung an, wonach durch den Wandel der Technik und des Verständnisses von technischen Kontrolleinrichtungen nicht (mehr) von einem reinen Abwehrrecht zum Schutze der Persönlichkeit der Arbeitnehmer im Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG auszugehen ist.

3. Europarechtliche Fragestellungen waren nicht entscheidungserheblich.

a) Da nach den vorstehenden Ausführungen das vom Betriebsrat für sich reklamierte Initiativrecht bereits vom Wortlaut des § 87 Abs. 1 Nr. 6 BetrVG erfasst wird, ohne dass insoweit im Wege der teleologischen Reduktion ein reines Abwehrrecht statuiert werden kann, kam es auf die vor allem in der Literatur diskutierte Frage (vgl. Richnow/Hördt, ArbRAktuell 2021, 148f m.w.Nachw.), ob europarechtliche Vorgaben nach der Entscheidung des EuGH vom 14.05.2019, C 55/18 ein Initiativrecht des Betriebsrates bei der Einführung einer elektronischen Zeiterfassung begründen können, nicht an.

b) Auch die Richtlinie 2002/14/EG vom 11.03.2002 zur Festlegung eines allgemeinen Rahmens für die Unterrichtung und Anhörung der Arbeitnehmer in der Europäischen Gemein-

schaft ist für die Annahme oder Ablehnung eines Initiativrechtes des Betriebsrates bei der Einführung einer elektronischen Zeiterfassung nicht einschlägig, beschreibt sie doch in Art. 1 „Gegenstand und Grundsätze“ ausdrücklich lediglich die Festlegung eines allgemeinen Rahmens mit Mindestvorschriften für das Recht auf Unterrichtung und Anhörung der Arbeitnehmer und überlässt in Art. 1 Abs. 2 die Modalitäten der Unterrichtung und Anhörung den einzelstaatlichen Rechtsvorschriften.

4. Ebenso wenig spielt es für die Entscheidung der Beschwerdekammer danach eine Rolle, dass seitens der Arbeitgeberinnen die für die elektronische Zeiterfassung benötigte „Hardware“ angeschafft wurde und letztlich nach Aufnahme der Verhandlungen über eine Betriebsvereinbarung zur Zeiterfassung diese wieder abgebrochen wurden. Soweit die Arbeitgeberinnen in diesem Zusammenhang auf Kosten der Inbetriebnahme und der Wartung u.a. durch Beauftragung eines externen Dienstleisters hingewiesen haben, sind das Punkte, die die Einigungsstelle gemäß § 76 Abs. 5 BetrVG bei ihrer Beschlussfassung angemessen zu berücksichtigen haben wird.

III. Wegen der Abweichung der Beschwerdekammer vom Beschluss des Bundesarbeitsgerichts vom 28.11.1989, 1 ABR 97/88, war die Rechtsbeschwerde gemäß §§ 92 Abs. 1 Satz 1, 72 Abs. 2 Ziffer 2 zuzulassen.

Äußerungen im WhatsApp-Chat als Kündigungsgrund (Ls)

(Landesarbeitsgericht Berlin-Brandenburg, Urteil vom 19. Juli 2021 – 21 Sa 1291/20 –)

Herabwürdigende und verächtliche Äußerungen durch einen technischen Leiter eines gemeinnützigen Vereins über Geflüchtete und in der Flüchtlingshilfe tätige Menschen in einem Chat stellen keine eine Kündigung rechtfertigende Pflichtverletzung dar, weil eine vertrauliche Kommunikation unter den Schutz des allgemeine Persönlichkeitsrechts fällt. Eine Auflösung des Arbeitsverhältnisses gem. § 9 KSchG ist jedoch möglich.

(Nicht amtlicher Leitsatz)

Kein Anspruch auf Bedauern des Ausscheidens oder (gute) Wünsche für die Zukunft im Arbeitszeugnis (Ls)

(Landesarbeitsgericht München, Urteil vom 15. Juli 2021 – 3 Sa 188/21 –)

1. Eine Arbeitnehmerin, deren Leistung und Verhalten im Endzeugnis – nur – mit „gut“ bewertet worden ist, hat keinen Anspruch auf Bescheinigung des Bedauerns über ihr Ausscheiden, schon gar nicht auf die Steigerung „wir bedauern sehr“.

2. Es besteht kein üblicher Anspruch darauf, dass (gute) Wünsche für die private Zukunft in die Schlussformel eines Endzeugnisses aufgenommen werden (vgl. LAG Düsseldorf, Urt. v. 12.01.2021 – 3 Sa 800/20 – Rn. 39).

3. Das gilt unabhängig von der Auffassung des BAG, (vgl. Urteil vom 11.12.2012 – 9 AZR 227/11 – Rn. 11), nach der ein Arbeitnehmer schon grundsätzlich keinen Anspruch auf Aufnahme einer persönlichen Schlussformel in ein Arbeitszeugnis hat.

(Nicht amtliche Leitsätze)

Keine Ansprüche aus der DS-GVO bei Sicherheitsakten (Ls)

(Oberverwaltungsgericht Münster, Beschluss vom 28.07.2021 – 16 B 1733/19 –)

Auf Maßnahmen nach dem Sicherheitsüberprüfungsgesetz finden weder die EU-Grundrechte-Charta noch die Datenschutz-Grundverordnung Anwendung. Daher ist ein Anspruch auf Kopie der in einer Sicherheitsakte enthaltenen personenbezogenen Daten weder nach den Art. 7 und 8 GrCh noch gemäß Art. 15 Abs. 3 DS-GVO gegeben.

(Nicht amtlicher Leitsatz)

Zur Abtretung des Anspruchs aus Art. 82 DS-GVO wegen USB-Stick-Verlust (n. rk.)

(Landgericht Essen, Urteil vom 23. September 2021)

1. Der Anspruch auf immateriellen Schadenersatz nach Art. 82 Abs. 1 DSGVO ist abtretbar.

2. Der postalische Rückversand eines USB-Sticks mit sensiblen Daten aus einer Immobilienfinanzierungsanfrage in einem einfachen Briefumschlag an den Betroffenen verstößt nicht gegen Art. 32 DSGVO, selbst wenn der Verantwortliche alternativ einen mit Multifaktor-Authentifizierung geschützten File Transfer für die Kundenkommunikation bereit hält.

(Leitsätze der Einsenderin)

Tatbestand:

Der Kläger macht gegen die Beklagte immaterielle Schadensersatzansprüche im Zusammenhang mit dem vermeintlichen Verlust eines USB-Sticks, auf dem sich personenbezogene Daten des Klägers und seiner Ehefrau befanden, geltend.

Der Kläger und seine Ehefrau fragten bei der Beklagten eine Immobilienfinanzierung an. Hierfür stellten sie der Beklagten auf verschiedenen Wegen, u.a. per E-Mail und über einen File-Transfer-Link per Dropbox, Unterlagen zu Verfügung. Am 21.01.2021 warfen

der Kläger und seine Ehefrau zudem einen unverschlüsselten USB-Stick in den Briefkasten der Beklagten.

Der USB-Stick enthielt Kopien von Ausweisdokumenten, Steuerunterlagen, Daten zu Bestandsimmobilien, der avisierten Immobilie sowie weitere Unterlagen, die die finanzielle Leistungsfähigkeit des Klägers und seiner Ehefrau nachweisen sollten.

Zu einem Vertragsschluss kam es letztlich nicht.

Am 22.01.2021 sendete die Beklagte den USB-Stick per einfacher Post an den Kläger und seine Ehefrau zurück. In der Folgezeit wandte sich die Ehefrau des Klägers wegen eines vermeintlichen Verlustes des USB-Sticks telefonisch an die Beklagte. Mit Schreiben vom 27.01.2021 teilte die Beklagte mit, dass ein „Lost and Found-Auftrag“ bei der Deutschen Post in die Wege geleitet worden sei. Mit Schreiben vom 22.02.2021 teilte die Beklagte mit, dass dieser Auftrag erfolglos geblieben sei. In diesem Schreiben heißt es außerdem: „Auch die Handhabung moderner, digitaler Informationstechnik ist für unsere Mitarbeitenden in Dienstvereinbarungen und Arbeitsanweisungen umfassend geregelt. Es tut uns sehr leid, dass in Ihrem Fall vom vorgesehenen Verfahren abgewichen wurde.“

Mit anwaltlichem Schreiben vom 26.03.2021 forderten der Kläger und seine Ehefrau die Beklagte zur Zahlung eines Schadensersatzes in Höhe von insgesamt 25.000,00 € auf Grundlage von Art. 82 DSGVO auf. Die Beklagte lehnte eine Zahlung mit Schreiben vom 16.04.2021 ab.

Unter dem 06.06.2021 trat die Ehefrau des Klägers diesem ihre vermeintlichen Ansprüche im Zusammenhang mit dem Abhandenkommen des USB-Sticks ab; er nahm die Abtretung an.

Der Kläger behauptet, den USB-Stick auf ausdrücklichen Vorschlag der Sachbearbeiterin der Beklagten übersandt zu haben. Einen anderen – verschlüsselten – Kommunikationsweg habe die Sachbearbeiterin weder erwähnt noch vorgeschlagen, obwohl es verschlüsselte Kommunikationswege (Zwei-Faktor-Authentifizierung) gegeben habe, wie sich im späteren Verlauf gezeigt habe. Der Kläger behauptet weiter, dass der USB-Stick auf dem Rückversand abhandengekommen sei. Seine – des Klägers – Ehefrau habe lediglich einen leeren Briefumschlag empfangen, der seitlich einen Riss aufgewiesen habe. Er ist der Auffassung, dass die Beklagte gegen Vorschriften der DSGVO verstoßen habe, wodurch es zu einem Datenverlust und einem immateriellen Schaden i.S.d. Art. 82 DSGVO für ihn und seine Ehefrau gekommen sei.

Der Versand des USB-Sticks mit sensiblen personenbezogenen Kundendaten per einfachem Brief ohne jegliche weitere Sicherheitsmaßnahme verstoße gegen die in Art. 24, 25 Abs. 1, 32 DSGVO geregelten Anforderungen an die Sicherheit, Ausgestaltung und Vertraulichkeit der Datenverarbeitung.....

Zudem – so ist der Kläger weiter der Ansicht – seien er und seine Ehefrau, nachdem der Verlust des USB-Sticks festgestellt worden sei, nicht ordnungsgemäß i.S.d. Art. 34 Abs. 2, 33 Abs. 3 lit. b – d DSGVO informiert worden. Insbesondere seien – unstreitig – die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten nicht beschrieben worden. Keinem der Schreiben der Beklagte könne ferner – ebenfalls unstreitig – entnommen werden, ob eine Meldung des Vorfalles an die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen erfolgt sei, was binnen 72 Stunden hätte erfolgen müssen.

Die Beklagte behauptet, dass sie zu keinem Zeitpunkt darum gebeten habe, dass die für die Finanzierungsanfrage benötigten Informationen auf einem USB-Stick zur Verfügung gestellt würden. Dem Kläger und seiner Ehefrau hätten vielmehr auch andere Übertragungswege zur Verfügung gestanden, die sie zuvor bereits genutzt hätten. Die Ehefrau des Klägers habe jedoch auf die Übermittlung per USB-Stick bestanden. Zudem hätte der Kläger den USB-Stick selbst verschlüsseln müssen, wenn er – dies für erforderlich gehalten hätte. Da er dies nicht getan habe, habe er – so meint die Beklagte – bereits zum Ausdruck gebracht, dass den dar-

auf befindlichen Informationen seiner Ansicht nach entweder keine hohe Bedeutung zukomme oder er zumindest billigend in Kauf genommen habe, dass etwaige unbefugte Dritte auf die Daten zugreifen könnten. Sie – die Beklagte – selbst sei zur Verschlüsselung des USB-Sticks vor dessen Rücksendung mit Blick auf § 303a StGB jedenfalls nicht berechtigt gewesen. Insofern treffe den Kläger ein Mitverschulden in Höhe von 100 %.

Die Beklagte bestreitet ferner, dass dem Kläger durch den Verlust des USB-Sticks negative Auswirkungen entstanden seien.

Die Beklagte vertritt die Auffassung, dass der Kläger hinsichtlich vermeintlicher Ansprüche seiner Ehefrau nicht aktivlegitimiert sei. Der Abtretungsvertrag sei nicht wirksam, da die fragliche Forderung nicht hinreichend bestimmt bezeichnet sei. Zudem handele es sich bei dem geltend gemachten Anspruch auf immateriellen Schadensersatz um einen höchstpersönlichen Anspruch, der nicht abgetreten werden könne.

Aus den Gründen:

Die Klage ist zulässig aber unbegründet.

1.

Dem Kläger steht gegen die Beklagte der geltend gemachte immaterielle Schadensersatzanspruch aus keinem rechtlichen Gesichtspunkt zu.

a)

Ein Anspruch des Klägers ergibt sich zunächst nicht aus Art. 82 Abs. 1 DSGVO.

Danach hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen i.S.d. DSGVO. Zwar ist der Kläger auch hinsichtlich der Ansprüche seiner Ehefrau aktivlegitimiert. Es liegt auch – zumindest hinsichtlich der fehlenden Mitteilung an die Landesbeauftragte für Datenschutz und Informationsfreiheit in NRW – ein Verstoß gegen die DSGVO vor. Der Kläger hat jedoch nicht hinreichend substantiiert dargetan, dass ihm ein erheblicher Schaden entstanden ist.

Im Einzelnen:

aa)

Der Kläger ist zunächst aktivlegitimiert. Für seinen eigenen Anspruch ist dies unproblematisch der Fall. Die Aktivlegitimation besteht darüber hinaus – entgegen der Ansicht der Beklagten – auch hinsichtlich des Anspruchs seiner Ehefrau.

Aufgrund des Abtretungsvertrags vom 06.06.2021 (Anlage K 5, BI. 20 d. A.) ist der Kläger Forderungsinhaber geworden, § 398 BGB.

Grundsätzlich ist jede Forderung abtretbar (vgl. Grüneberg in: Palandt, 80. Aufl. 2021, § 398 BGB Rn. 8); insbesondere auch Schmerzensgeldansprüche (vgl. Grüneberg in: Palandt, 80. Aufl. 2021, § 253 BGB Rn. 22). Ein Abtretungsverbot nach §§ 399, 400 BGB besteht nicht. Die vermeintliche Forderung der Ehefrau des Klägers gegen die Beklagte unterliegt weder der Pfändung (§ 400 BGB) noch wurde die Abtretung durch Vereinbarung ausgeschlossen oder erfordert die Abtretung eine Inhaltsänderung der Leistung (§ 399 BGB).

Die Abtretung ist zudem wirksam.....

bb)

Der Beklagten ist ein Verstoß gegen Art. 33 DSGVO vorzuwerfen – unterstellt, der USB-Stick ist tatsächlich verloren gegangen. Gemäß Art. 33 Abs. 1 DSGVO meldet der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Auf-

sichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die erforderlichen zu meldenden Informationen ergeben sich aus Art. 33 Abs. 3 DSGVO. Eine solche Meldung ist indes — unstrittig — nicht erfolgt. Unerheblich ist dabei, dass der Kläger und seine Ehefrau als Betroffene bereits Kenntnis von dem vermeintlichen Datenverlust hatten, da sie ihn selbst gemeldet haben. Denn die Meldepflicht dient zum einen der Minimierung der negativen Auswirkungen von Datenschutzverletzungen durch Publizität gegenüber der Aufsichtsbehörde (und dem Betroffenen). Gleichzeitig gewährt die Vorschrift so vorbeugenden Schutz der informationellen Selbstbestimmung des Betroffenen, indem sie Anreize zur Vermeidung zukünftiger Verletzungen beim Verantwortlichen setzt. Die Vorschrift dient also nicht nur dem Schutz des Betroffenen. Die Meldung gegenüber der Aufsichtsbehörde ermöglicht es dieser, über Maßnahmen zur Eindämmung und Ahndung der Rechtsverletzung zu entscheiden (vgl. BeckOK DatenschutzR/Brink, 37. Ed. 1.11.2019 Rn. 10, DS-GVO Art. 33 Rn. 10). Insofern genügt bereits ein solch formeller Verstoß gegen die DSGVO zur Begründung eines Schadensersatzanspruches dem Grunde nach (BeckOK DatenschutzR/Quaas, 37. Ed. 1.8.2021, DS-GVO Art. 82 Rn. 14).

Zudem liegt ein Verstoß gegen Art. 34 Abs. 2 DSGVO vor. Zwar ist der Beklagten insofern zuzustimmen, als sie selbst erst durch den Kläger bzw. seine Ehefrau von dem vermeintlichen Datenverlust informiert wurde. Die Informationspflichten des Art. 34 DSGVO sehen über die reine Information über den Datenverlust selbst hinaus jedoch vor, dass die in Art. 33 Abs. 3 lit. b-d DSGVO genannten Informationen und Maßnahmen auch dem Betroffenen – hier dem Kläger und seiner Ehefrau – mitgeteilt werden. Dies ist jedoch – unstrittig – nicht erfolgt.

cc)

Dagegen liegt kein Verstoß gegen Art. 24, 25 Abs. 1, 32 DSGVO vor.

Danach hat der Verantwortliche i.S.d. DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen und umzusetzen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt und die Rechte der betroffenen Personen geschützt werden. In Art. 25 Abs. 1 und Art. 32 Abs. 1 DSGVO werden dafür exemplarisch die Pseudonymisierung und Verschlüsselung personenbezogener Daten genannt.

Ein Verstoß der Beklagten liegt indes nicht vor. Die Kammer konnte kein Fehlverhalten im Haus der Beklagten feststellen. Dabei ist zunächst zu berücksichtigen, dass der vermeintliche Verlust der Daten jedenfalls nicht im Haus der Beklagten erfolgt ist. Dies wird auch von Klägerseite nicht behauptet. Vielmehr soll der USB-Stick auf dem Postversand verloren gegangen sein.

Die Kammer sieht zudem keinen Grund, weshalb die Beklagte den USB-Stick nicht per einfachem Brief an den Kläger und seine Ehefrau hätte versenden dürfen. Zwar waren auf dem USB-Stick Dokumente mit sensiblen persönlichen und wirtschaftlichen Informationen enthalten. Dies ist jedoch kein Grund, nicht den Service der Deutschen Post nutzen zu dürfen. Von verschiedensten Stellen werden ausgedruckte Dokumente mit sensiblen Informationen, z.B. Steuerbescheide, Schreiben von Anwälten und Steuerberatern o.Ä., mit einfacher Post versandt.

Hiergegen ist ebenfalls nichts einzuwenden; eine irgendwie geartete Pflichtverletzung der handelnden Stellen ist nicht ersichtlich. Weshalb zwischen ausgedruckten Dokumenten, die naturgemäß unverschlüsselt übersandt werden, und digitalen Dokumenten auf einem unverschlüsselten USB-Stick im Zuge der postalischen Übermittlung unterschieden werden soll, erschließt sich der Kammer nicht.

Die Beklagte war zudem nicht gehalten, den USB-Stick in einem gepolsterten Umschlag zu versenden. Bei dem USB-Stick handelt es sich weder um einen leicht zu beschädigenden Gegenstand, der vor äußeren Einwirkungen geschützt werden müsste, noch musste die Beklagte davon ausgehen, dass ein USB-Stick als relativ leichter Gegenstand ohne scharfe Kanten den Briefumschlag von innen heraus zerstören könnte.

Ferner bestand keine Verpflichtung der Beklagten, den USB-Stick dem Kläger oder seiner Verlobten persönlich zu übergeben. Unstrittig wurde dies nicht durch den Kläger oder seine Ehefrau gefordert. Zudem bestand für die Beklagte – wie bereits ausgeführt – keine Veranlassung, an dem zuverlässigen Versand durch die Deutsche Post zu zweifeln.

dd)

Der Kläger hat jedoch ohnehin nicht hinreichend substantiiert dargetan, dass ihm und seiner Ehefrau ein konkreter immaterieller Schaden entstanden ist.

Für den – hier geltend gemachten – immateriellen Schadensersatz gelten dabei die im Rahmen von § 253 BGB entwickelten Grundsätze; die Ermittlung obliegt dem Gericht nach § 287 ZPO (BeckOK DatenschutzR/Quaas, 32. Ed. 1.2.2020, DS-GVO Art. 82 Rn. 31). Es können für die Bemessung die Kriterien des Art. 83 Abs. 2 DSGVO herangezogen werden, bspw. die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie die betroffenen Kategorien personenbezogener Daten. Zu berücksichtigen ist auch, dass die beabsichtigte abschreckende Wirkung nur durch für den Anspruchsverpflichtenden empfindliche Schmerzensgelder erreicht wird, insbesondere wenn eine Kommerzialisierung fehlt. Ein genereller Ausschluss von Bagatellfällen ist damit nicht zu vereinbaren (BeckOK DatenschutzR/Quaas, 32. Ed. 01.02.2020, DS-GVO Art. 82 Rn. 31) (vgl. LG Köln, Urteil vom 07.10.2020 – 28 O 71/20). Die Pflicht zur Erstattung immaterieller Schäden ist daher nicht nur auf schwere Schäden beschränkt (vgl. LG Landshut, Urteil vom 06.11.2020 – 51 O 513/20).

Allein die – etwaige – Verletzung des Datenschutzrechts als solche begründet allerdings nicht bereits für sich gesehen einen Schadensersatzanspruch für betroffene Personen. Die Verletzungshandlung muss in jedem Fall auch zu einer konkreten, nicht nur unbedeutenden oder empfundenen Verletzung von Persönlichkeitsrechten der betroffenen Personen geführt haben (vgl. LG Hamburg, Urteil vom 04.09.2020 – 324 S 9/19). Es ist zwar eine schwere Verletzung des Persönlichkeitsrechts nicht (mehr) erforderlich. Andererseits ist auch weiterhin nicht für einen Bagatellverstoß ohne ernsthafte Beeinträchtigung bzw. für jede bloß individuelle empfundene Unannehmlichkeit ein Schmerzensgeld zu gewähren; vielmehr muss dem Betroffenen ein spürbarer Nachteil entstanden sein, und es muss um eine objektiv nachvollziehbare, mit gewissem Gewicht erfolgte Beeinträchtigung von persönlichkeitsbezogenen Belangen gehen (vgl. LG Landshut, Urteil vom 06.11.2020 – 51 O 513/20).

Gemessen an diesen Grundsätzen kann die Kammer anhand des klägerischen Vortrags spürbare Beeinträchtigung von per-

sönlichen Belangen des Klägers und seiner Ehefrau in keiner Weise feststellen.

Der Kläger hat lediglich vorgetragen, dass er und seine Ehefrau infolge des vermeintlichen Verlustes des USB-Sticks einen Kontrollverlust erlitten hätten. Weiter wird dies indes nicht ausgeführt. Die Kammer hat dabei berücksichtigt, dass der Verlust eines USB-Sticks, auf dem sich ungesicherte persönliche und wirtschaftliche Informationen befinden, durchaus zu einem „ungenuten Gefühl“ führen kann. Der Kläger hat jedoch in keiner Weise vorgetragen, inwiefern sich für ihn bzw. seine Ehefrau eine ernsthafte Beeinträchtigung ergeben hat. Negative Auswirkungen des Verlustes haben sich nicht gezeigt – zumindest wurden sie weder vorgetragen noch ergeben sie sich aus den sonstigen Umständen des Falles. Es ist zudem völlig unklar, was mit dem USB-Stick passiert ist – unterstellt, er ist tatsächlich abhandengekommen. Negative Auswirkungen des behaupteten Verlustes – etwa in Form eines Identitätsdiebstahls oder ähnliches – müssten der Kläger und seine Ehefrau allenfalls befürchten, wenn der USB-Stick in die Hände eines Dritten gelangt ist. Ob das der Fall ist, ist völlig unklar. Genauso gut ist es möglich, dass der USB-Stick bei der Verarbeitung der Briefe im Bereich der Deutschen Post zerstört oder beschädigt wurde. Im klägerischen Schriftsatz vom 15.09.2021 ist die Rede von einer walzen- und rollenbetriebenen Sortieranlage der Deutschen Post. Inso-

fern ist es durchaus wahrscheinlich, dass ein USB-Stick in dieser Sortieranlage beschädigt werden kann. In diesem Fall wäre es somit ausgeschlossen, dass ein unbefugter Dritter überhaupt an die Daten des Klägers und seiner Ehefrau gelangen könnte.

Dieses Ergebnis steht nicht im Widerspruch zu der Entscheidung des Bundesverfassungsgerichts vom 14.01.2021 (1 BvR 2853/19), in der es um die Ablehnung eines immateriellen Schadensersatzanspruchs wegen fehlender Erheblichkeit ging, was „weder unmittelbar in der DSGVO angelegt [sei], noch von der Literatur befürwortet oder vom Gerichtshof der Europäischen Union verwendet [werde]“. Denn im vorliegenden Fall wurde nicht einmal eine spürbare Beeinträchtigung des Klägers und seiner Ehefrau vorgetragen. Über die Frage der Erheblichkeit musste die Kammer daher nicht entscheiden.

Im Übrigen hält die Kammer das Vorgehen des Klägers, außergerichtlich zunächst einen niedrigeren Schmerzensgeldbetrag zu fordern, unter Androhung, den Betrag zu erhöhen, falls ein gerichtliches Verfahren erforderlich werde, für äußerst befremdlich. Generell ist der vom Kläger geforderte Betrag deutlich übersetzt, wie insbesondere ein Vergleich mit Schmerzensgeldansprüchen wegen Körperverletzungen verdeutlicht, was insgesamt ein überbordendes Gewinnstreben des Klägers aufzeigt, hingegen nicht, dass er sich durch die behaupteten Vorgänge in irgendeiner Art und Weise persönlich beeinträchtigt sieht.

(Eingereicht von RAin Viktoria Lehner)

So entwickeln Sie ein rechtskonformes Löschkonzept

Leitfaden inklusive:

- ✓ Checklisten
- ✓ Musterentwurf
- ✓ Vorlagen
- ✓ Ausfüllhinweise



Bestellen Sie direkt unter: www.datakontext.com/loeschkonzepte

Berichte, Informationen, Sonstiges

BSI-Lagebericht der IT-Sicherheit in Deutschland 2021 – Bitkom-Stellungnahme

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Oktober seinen Bericht zur Lage der IT-Sicherheit in Deutschland 2021 veröffentlicht. Dazu erklärt Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung:

„Cyberangriffe sind zu einer enormen Bedrohung für die deutsche Wirtschaft geworden. Jedes zehnte Unternehmen sieht deshalb laut unseren Erkenntnissen seine Existenz bedroht. Der diesjährige Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik untermauert eindrucksvoll, wie ernst die Lage für die deutsche Wirtschaft, aber auch für Privatpersonen, Behörden und andere Institutionen ist.“

Cyberangriffe haben laut Bitkom-Studien bei 86 Prozent der Unternehmen in Deutschland zuletzt einen Schaden verursacht. Die Wucht, mit der insbesondere Ransomware-Angriffe unsere Wirtschaft erschüttern, ist besorgniserregend und trifft Betriebe aller Branchen und Größen. Die Schäden durch Erpressung, verbunden mit dem Ausfall von Systemen oder der Störung von Betriebsabläufen, sind seit 2019 um 358 Prozent gestiegen.

Auch Schutzgeld wird mittlerweile im Internet erpresst. Die Angreifer drohen damit, bestimmte Ressourcen gezielt zu überlasten und zum Beispiel Server mit massenhaften Anfragen in

die Knie zu zwingen. Zuletzt waren 27 Prozent der Unternehmen im Land von solchen DDoS-Attacken betroffen.

Darauf müssen wir reagieren. Wir brauchen die Möglichkeit, dass sich jeder Mensch und jedes Unternehmen in Echtzeit über die Cyber-Bedrohungslage informieren kann. Dazu müssen wir Echtzeit-Informationen nutzen und EU-weit in einem zentralen Dashboard sammeln – ähnlich dem Corona-Dashboard des Robert-Koch-Instituts. Nur wenn Hinweise auf Gefahren sekundengenau gesammelt werden, können wir auch umgehend darauf reagieren und uns sowie unsere Wirtschaft besser schützen.

Wesentlich für mehr Cybersicherheit ist auch die zukunftsfähige Bildung aller Menschen. Medienkompetenz und IT-Wissen müssen spätestens ab der Grundschule in die Bildungspläne integriert werden. Wir brauchen deshalb unbedingt Informatik als Pflichtfach ab Sekundarstufe I.“

Notwendigkeit voller Cloud-Kontrolle

Sind Cloud-Infrastrukturen unzureichend gesichert, sind sie anfällig für physische Gefahren, Datenverletzungen und Cyber-Attacken. Cloud Security umfasst eine Vielzahl von Maßnahmen, die vor diesen Risiken schützen und die Einhaltung gesetzlicher Datenschutzvorgaben gewährleisten.

8 von 10 Unternehmen greifen heute auf Rechenleistung aus der Cloud zurück. Das zeigt der von Bitkom Research und KPMG veröffentlichte

Cloud-Monitor 2021. Durch Cloud Security wird das Risiko von Ausfällen, Datenverlusten und Zugriff durch Unbefugte minimiert. Hierfür müssen Regeln, Prozesse und technische Vorgaben festgelegt werden. Kenntnisse und Fähigkeiten für die Absicherung von Cloud-Services nach ISO/IEC 27001 und ISO/IEC 27018 sind daher für Verantwortliche sinnvoll.“

Als Nachweis der Sicherheit von Cloud-Dienstleistungen dient die ISO/IEC 27017. Die Norm stellt sicher, dass das Sicherheitsniveau genutzter Cloud-Systeme allen Anforderungen des Unternehmens sowie geltenden Gesetzen und Vorschriften entspricht. Sie unterliegt einer Methodik, mit der Sicherheitsvorgaben schneller identifiziert und in das Sicherheitsmanagementsystem eines Unternehmens integriert werden können. Die Norm betrifft nicht nur die Anbieter von Cloud-Services, sondern bezieht sich auf die Sicherheit der Cloud insgesamt.

Als Datenschutz-Standard für Cloud-Dienste befasst sich die ISO/IEC 27018 speziell mit der Regulierung der Verarbeitung von personenbezogenen Daten in einer Cloud. Für Anbieter von Cloud-Computing besteht damit die Möglichkeit, ihre Dienste zertifizieren zu lassen und das Vertrauen potenzieller Kunden in die angebotenen Dienste zu stärken.

Damit Verantwortliche für Cloud Security die erforderlichen Kompetenzen erwerben und normgerecht umsetzen können, bietet CARMAO als einziges Unternehmen in Deutschland die Ausbildung zum „Lead Cloud Security Manager“ an.

(Pressemitteilung v. 29.10.21)

Literaturhinweise

Kosmider, Thomas, Die Verantwortlichkeit im Datenschutz – Die Zuordnung zum Verantwortlichen und deren Bedeutung für Rechtfertigung, Geldbußen und Schadensersatz, Verlag Boorberg, Stuttgart 2021, 309 S., 48,- €

Das nunmehr im Boorberg-Verlag erschienene, handliche und bereits optisch ansprechende Buch geht auf die im Wintersemester 2020/2021 von der juristischen Fakultät der Universität Bayreuth angenommene Dissertation von Thomas Kosmider zurück. Bekanntlicherweise stellt eine Dissertation den Hauptbestandteil einer Promotion dar, bei der es inhaltlich grds. um die Auseinandersetzung mit wichtigen Themen, optimalerweise a.E. mit neuen Erkenntnissen für die behandelte Problematik, geht. In der Praxis stellt die von Kosmider behandelte Verantwortlichkeit im Datenschutz nach wie vor und auch in Zukunft bekanntlich einen wesentlichen/wenn nicht „den Dreh- und Angelpunkt“ im Datenschutzrecht dar – was der Rezensent als insbesondere in der Schnittmenge aus Datenschutz und Insolvenzverwaltung, Nachlasspflegschaft sowie Testamentsvollstreckung tätiger Praktiker ebenfalls bestätigen kann. Der Frage der Verantwortlichkeit dieser „Amtsträger“ im Umgang mit personenbezogenen Daten begegnet man selbst in diesem spezialisierten Teilbereich fast täglich. Die Einheit von entsprechender (zivilrechtlicher) Rechtsordnung mit dem Datenschutzrecht ist nach wie vor nicht hergestellt. Selbst hier hilft aber im Grundsätzlichen das Werk von Kosmider weiter: Es beleuchtet die Frage, wann jemanden eine Verantwortlichkeit trifft – und zwar zunächst in sachlicher Hinsicht und im Anschluss, wie von einer Dissertation zu erwarten, in der persönlichen Hinsicht/Auffassung des Promovenden. Dem schließen sich gut nachvollziehbare Folgerungen zu Datenverarbeitungen innerhalb der festgestellten Ver-

antwortlichkeit an. Letztlich erfolgen Ausführungen zur Zurechnung bei Bußgeldern und Schadensersatzansprüchen. Als Fazit empfiehlt sich das Werk von Kosmider daher, „gerade weil“ Dissertation, auch für Praktiker wie Datenschutzbeauftragte, Justiziere bzw. Rechtsanwälte mit datenschutzrechtlichen Bezügen, nicht zuletzt im Übrigen, weil neben umfassendem Literaturverzeichnis im Wesentlichen auch Beiträge aus einschlägigen Praktiker-magazinen wie CR/RDV/ZD als Quellen herangezogen wurden. Der Literatur- und Rechtsprechungsstand ist mit Februar 2021 nach wie vor und auch für die Praxis hinreichend aktuell.

(RA/FA InsR/Testamentsvollstrecker (AGT) Christian Weiß, Wellensiek Rechtsanwälte Köln)

Steinbach, Kathrin, Regulierung algorithmenbasierter Entscheidungen – Grundrechtliche Argumentation im Kontext von Artikel 22 DSGVO, Duncker & Humblot, Berlin, Internetrecht und Digitale Gesellschaft (IDG), Band 28, 2021, 288 S., 89,90 €

Algorithmenbasierte Entscheidungen sind Teil unseres Alltags: Staatliche Institutionen und private Akteure nutzen Algorithmen in vielen Lebensbereichen, um personenbezogene Entscheidungsprozesse rationaler und effizienter zu gestalten, beispielsweise in der Sozial- und Steuerverwaltung, bei Kreditvergaben oder im Personalmanagement. Angesichts neuer technologischer Möglichkeiten scheinen das Verhalten und die Lebensumstände von Menschen zunehmend kalkulierbar. Die Prämissen eines automatisierten Entscheidungsprozesses werfen Fragen auf im Hinblick auf menschliche Würde, Selbstbestimmung, Verantwortung und Gleichheitsrechte. Die zentrale Frage der Untersuchung lautet: Wie wird die Regulierung algorithmenbasierter Entscheidungen im öffentlichen und privaten Sektor grundrechtlich verankert?

Dabei dient Artikel 22 Datenschutz-Grundverordnung – eine atypische Norm im Datenschutzrecht – als Ausgangspunkt. Die Genese im französischen Recht und die heutige wissenschaftliche Rezeption der Norm stellen einen legislativen »Steinbruch« für grundrechtliche Argumente dar. Eine Diskursstrukturierung anhand dieser Norm kann damit einen Beitrag zur breiteren Debatte um die Regulierung künstlicher Intelligenz leisten:

(Redaktion)

Walker, Matthias, Die Kosten kostenloser Dienste – Personenbezogene Daten als neues Zahlungsmittel, Duncker & Humblot, Berlin 2021, (Internetrecht und Digitale Gesellschaft (IDG), Band 27, 250 S., 79,90 €

Im Zuge der Digitalisierung aller Lebensbereiche „bezahlen“ Verbraucher für die Inanspruchnahme digitaler Dienste zunehmend mit ihren personenbezogenen Daten. Verbraucher und Unternehmer partizipieren jedoch nicht gleichermaßen an der Wertschöpfung mit personenbezogenen Daten. Während die Schaffung eines absoluten Rechts an Daten zur Beseitigung dieser zuungunsten der Verbraucher bestehenden Diskrepanz derzeit nicht erfolgsversprechend erscheint, rückt durch Erlass der Digitale-Inhalte-Richtlinie der Europäischen Union die vertragsrechtliche Erfassung der Bereitstellung von Inhalten und Diensten gegen personenbezogene Daten in den Fokus. Zwar wurde derartigen Datentransaktionen durch die Richtlinie erstmalig ein rechtlicher Rahmen verliehen, es stellen sich dennoch datenschutz-, verbraucherschutz-, und vertragsrechtliche Folgefragen. Fest steht: Für eine künftig faire und nachhaltige Wertschöpfung mit personenbezogenen Daten, die Verbraucher nicht benachteiligt, wird es weiterer Regeln bedürfen.

(Redaktion)

Neuerscheinungen

Aufsätze

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

Benkert, Daniel, **Die Modernisierung der Betriebsverfassung**, NJW-Spezial 2021, S. 434

Der Verfasser stellt in diesem Beitrag das am 18.06.2021 in Kraft getretene Gesetz zur Förderung der Betriebsratswahlen und der Betriebsarbeit in einer digitalen Arbeitswelt vor und gibt einen kurzen Überblick über die wesentlichen Änderungen.

Böhm, Wolf-Tassilo/Brahms, Isabelle, **Aktuelle Entscheidungen der Arbeitsgerichte zum Beschäftigtendatenschutz**, NZA-RR 2021, S. 521

Es handelt sich um eine ausgewählte Übersicht der Rechtsprechung.

Gola, Peter/Klug, Christoph, **Die Entwicklung des Datenschutzrechts**, NJW 2021, S. 680

Der Text gibt in der seit 35 Jahren bestehenden Folge die Übersicht über das 2. Halbjahr 2020 wieder.

Imping, Andres, **Digitalisierung im Personalbereich: Rechtliche Rahmenbedingungen und Gestaltungsoptionen bei Betriebsvereinbarungen – Künstliche Intelligenz, Big Data & Co.: Der (un-)verstellte Blick in die HR-Kristallkugel**, DB 2021, S. 1808

Die fortschreitende Digitalisierung führt auch zu Änderungen im Bereich des Personalmanagements. Hierzu gehört die Anwendung von Software im Bereich der künstlichen Intelligenz. Erklärt werden die technischen Möglichkeiten und die dazugehörigen rechtlichen Rahmenbedingungen.

Koreng, Ansgar, **Reichweite des datenschutzrechtlichen Auskunftsanspruchs**, NJW 2021, S. 2692

Der Beitrag kommentiert die unterschiedliche Rechtsprechung zur genannten Problematik.

Körner, Marita, **Drei Jahre Beschäftigtendatenschutz unter der Datenschutzgrundverordnung**, NZA 2021, S. 1137

Im Hinblick auf § 26 BDSG sei unklar, ob Art. 88 DS-GVO als Öffnungs- oder Konkretisierungsklausel zu verstehen sei und inwiefern die deutsche Rechtsprechung zukünftig auf abweichende EuGH-Entscheidungen reagieren müsse.

Lembke, Mark/Tegel, Johannes, **Die formularmäßige Frage nach Vorbeschäftigungen**, NZA 2021, S. 984

Eine sachgrundlose Befristung eines Arbeitsvertrags kann unwirksam sein, wenn ein Arbeitnehmer schon einmal im Betrieb angestellt war. Streng gesehen, müsste der Arbeitgeber ohne Befragung des Arbeitnehmers an die benötigten Informationen kommen. Gleichwohl empfehlen die Autoren einen separaten Fragebogen.

Schürmann, Kathrin, **Besonderheiten im Datenschutz bei digitalen 360-Grad-Feedback**, PinG 2021, S. 204

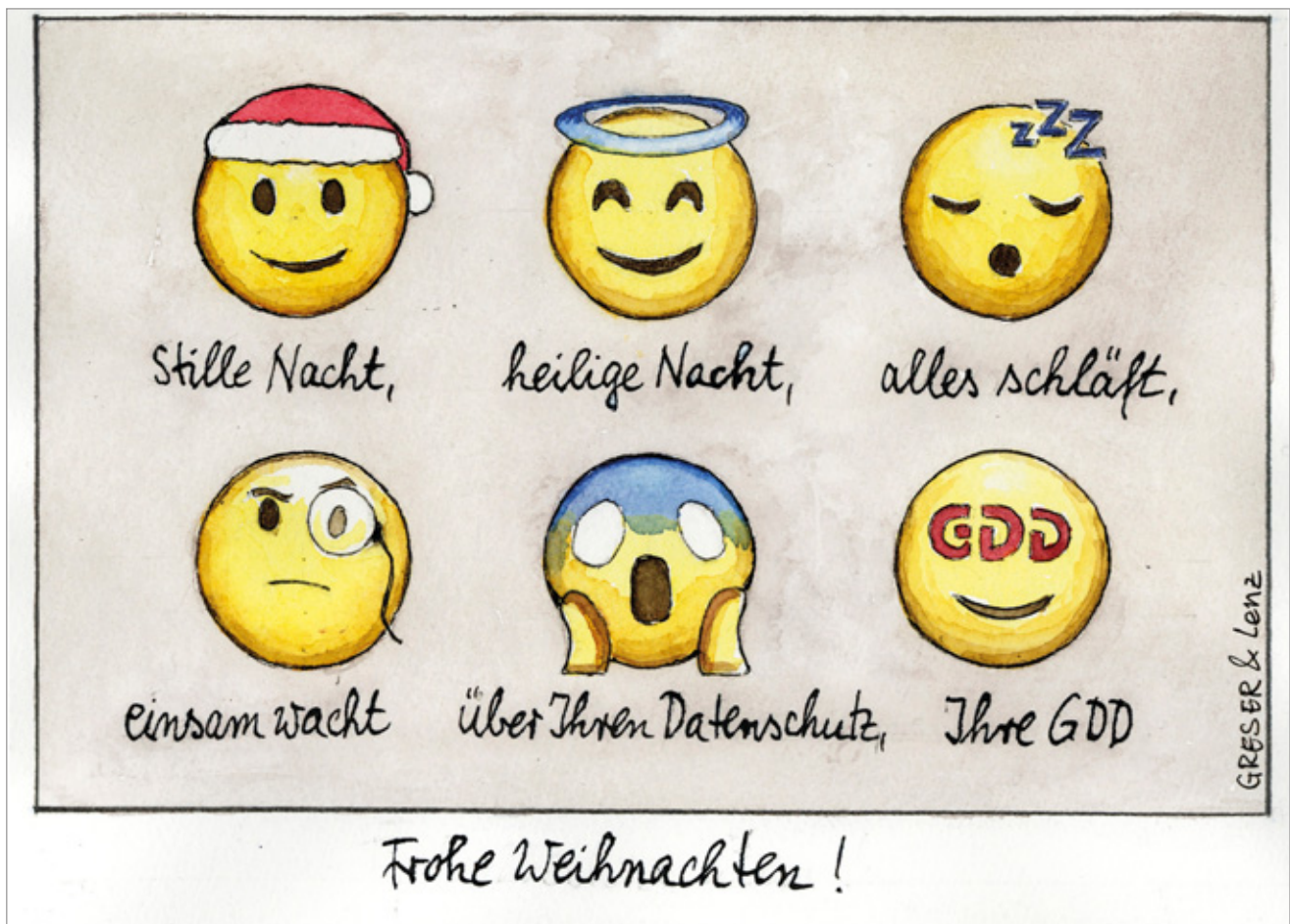
Durch die Digitalisierung ergeben sich neue Möglichkeiten per 360-Grad-Feedback, zeitgemäße und faire Beurteilungen zu erstellen. Transparenz und Objektivität können an die Stelle von Überwachung und Denunziation treten.

Thüsing, Gregor, **Lehren aus der Pandemie: Zwang, Anreiz und Apell als Instrumente des (Arbeits-)Rechts**, NJW 2021, S. 2789

Der Verfasser gibt in seinem Beitrag einen Ausblick darüber, welche Folgen die Corona-Pandemie für die Arbeitswelt allgemein und für das Arbeitsrecht mit sich ziehen könnte.

Thüsing, Gregor/Rombey, Sebastian, **Anonymisierung an sich ist keine rechtfertigungsbedürftige Datenverarbeitung**, ZD 2021, S. 548

Der Beitrag setzt sich mit der dem Aufsatztitel gegenteiligen Ansicht des BfDI und einer möglichen Bewertung der Frage durch den EuGH auseinander.



Familienrecht für Influencer – Können Kinder ihre Eltern wegen der Löschung eines Tiktok-Accounts verklagen?

Eine Brasilianerin löschte die Accounts ihrer 14-jährigen Tochter bei Instagram und Tiktok. Nun sind 1,7 Millionen Follower der Tochter futsch. Wer haftet für den Schaden der Tochter und wer muss für die Erfüllung der Werbeverträge gerade stehen? Betrachten wir das nach deutschem Recht. Ob das Kind seine Mutter verklagen könnte, hinge davon ab, ob die Mutter ihre Pflichten aus der Personen- oder Vermögenssorge für ihre Tochter verletzt hätte. Ab 14 Jahren ist das Kind verfahrensfähig. Es könnte behaupten, dass die Mutter sein Vermögen gefährdet und die Anordnung richterlicher Maßnahmen beantragen, die diese Ge-

fahr abwenden. Wenn das nicht mehr helfen würde, könnte es die Mutter auf Schadensersatz verklagen. Aber die Mutter hat das Wohl des Kindes nicht gefährdet. Zu viel Internet ist schädlich. Dass es in der Entwicklungsphase zu Ängsten, Burnout und Depressionen führen kann und dass zu viel Ruhm für Kinder charakterschädigend sein kann, liegt auf der Hand. Das Kindeswohl ist Trumpf, das dürfte die Mutter durch die Löschung gefördert haben. Wenn Kinder Werbeverträge schließen wollen, geht das nicht ohne die gesetzlichen Vertreter. Es dürfte für deren Pflicht zur Erfüllung darauf ankommen, ob die Mutter die Tochter mit

Genehmigung des Familiengerichts zum selbstständigen Betrieb ihres Erwerbsgeschäft für Dienstleistungen im Werbegeschäft ermächtigt hat. Wenn eine Ermächtigung vorlag, wäre eine Genehmigung des Familiengerichts für deren Rücknahme erforderlich. Werbeverträge die genehmigt worden sind, müssten wohl erfüllt werden.





**Live
Online-
Schulung**

© Ingo Bartussek - stock.adobe.com

Das neue Betriebsrätemodernisierungs- und Bundespersonalvertretungsgesetz

18. Januar 2022 | online
Referent/in: Yvette Reif, Andreas Jaspers

Schwerpunkte:

- ✓ Anlass für die Neuregelungen im BetrVG und BPersVG
- ✓ Arbeitgeber als Verantwortlicher für die Datenverarbeitung beim Betriebsrat
- ✓ Kontrolle des Betriebsrats durch den Datenschutzbeauftragten (DSB)
- ✓ Neue Verschwiegenheitspflicht des DSB
- ✓ Neue Beteiligungsrechte der Mitarbeitervertretung

Jetzt anmelden: www.datakontext.com



**24.-25.01.2022
online**

Praxisthemen:

- ✓ Vorlageverfahren EuGH
- ✓ Aktuelle Entwicklungen in der nationalen und europäischen Bußgeldpraxis
- ✓ Arbeitsaufwand im Datenschutz quantifizieren – am Beispiel Gesundheitswesen
- ✓ „Garantien“ im Datenschutz – aktueller Stand zu Verhaltensregeln nach Art. 40 DS-GVO
- ✓ Datenschutz bei Microsoft
- ✓ TTDSG – Anforderungen und Herausforderungen für die Praxis
- ✓ Tracking auf Webseiten
- ✓ Nutzung von Videokonferenzlösungen außereuropäischer Anbieter

Jetzt anmelden: www.datakontext.com