ISSN 0178-8930
HZ212333

G 20 141

RDV

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

5/2022

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

SCHWARTMANN/BURKHARDT, Rechts- oder Funktionsträgerprinzip? Unternehmenshaftung nach der Datenschutz-Grundverordnung auf dem rechtlichen Prüfstand

PAAL/GÖTZ, GPS-Daten und Datenschutzrecht – Aktuelle Fragestellungen mit einem Fokus auf den Automobilsektor

BERWARI, Google Analytics auf dem Prüfstand der DS-GVO – Grenzen, Risiken und Möglichkeiten

BENEDIKT, Die DS-GVO als Datenwirtschaftsverfassung

SCHWARTMANN/MÜHLENBECK, Datenschutz durch Ermöglichungstechnik – Anonymität und Pseudonymität nach der DS-GVO im Kontext von Data Act-Entwurf und Data Governance Act

Kurzbeiträge

GOLA, Aus den aktuellen Berichten der Aufsichtsbehörden (62): Feststellungen zu betrieblichen/behördlichen Datenschutzbeauftragten im 50. Tätigkeitsbericht Datenschutz des Hessischen Beauftragten für Datenschutz und Informationssicherheit (HDI) für das Jahr 2021

REIF, Praxisfälle zum Datenschutzrecht XVIII: Videoüberwachung im Pausenraum

Rechtsprechung

Aus dem Inhalt

EUGH bestätigt Unionsrechtswidrigkeit der allgemeinen und anlasslosen Vorratsdatenspeicherung von Verkehrs- und Standortdaten im TKG und benennt Fälle zulässiger Datenspeicherungen (MIT ANM. BURKHARDT)

EUGH, Zum Konflikt zwischen Datenschutz und Korruptionsbekämpfung und der Veröffentlichung sensibler Daten (Ls)

BAG, Zur Höhe eines Anspruchs auf immateriellen Schadenersatz bei Verstoß gegen die DS-GVO

38. Jahrgang
Oktober 2022
Seiten 235–288

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Mitarbeiterinformation Datenschutz

Mitarbeiter einfach und rechtssicher sensibilisieren

Bestseller

millionenfach verkauft

- ideal für alle Mitarbeiter
- leicht verständlich
- anschaulich illustriert
- firmenindividuell gestaltbar
- in 5 Sprachen verfügbar

jetzt bestellen:
datakontext.com/mitarbeiterinformation

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht

38. Jahrgang 2022
Heft 5
Seiten 235–288

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 235

Veranstaltungen 236

Aufsätze

Prof. Dr. Rolf SCHWARTMANN/Lucia BURKHARDT
Rechts- oder Funktionsträgerprinzip? Unternehmenshaftung nach der Datenschutz-Grundverordnung auf dem rechtlichen Prüfstand 237

Prof. Dr. Boris P. PAAL, M.Jur./Matthias GÖTZ, LL.M.
GPS-Daten und Datenschutzrecht
Aktuelle Fragestellungen mit einem Fokus auf den Automobilsektor 247

Dinya BERWARI, LL.M.
Google Analytics auf dem Prüfstand der DS-GVO – Grenzen, Risiken und Möglichkeiten 253

Kristin BENEDIKT
Die DS-GVO als Datenwirtschaftsverfassung 258

Prof. Dr. Rolf SCHWARTMANN/Robin L. MÜHLENBECK
Datenschutz durch Ermöglichungstechnik – Anonymität und Pseudonymität nach der DS-GVO im Kontext von Data Act-Entwurf und Data Governance Act 264

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten der Aufsichtsbehörden (62): Feststellungen zu betrieblichen/behördlichen Datenschutzbeauftragten im 50. Tätigkeitsbericht Datenschutz des Hessischen Beauftragten für Datenschutz und Informationssicherheit (HDI) für das Jahr 2021 268

RAin Yvette REIF LL.M.
Praxisfälle zum Datenschutzrecht XVIII: Videoüberwachung im Pausenraum 269

Rechtsprechung

EuGH bestätigt Unionsrechtswidrigkeit der allgemeinen und anlasslosen Vorratsdatenspeicherung von Verkehrs- und Standortdaten im TKG und benennt Fälle zulässiger Datenspeicherungen (mit Anm. Burkhardt)
(EuGH, Urteil vom 20.09.2022) 272

Zum Konflikt zwischen Datenschutz und Korruptionsbekämpfung und der Veröffentlichung sensibler Daten (Ls)
(EuGH, Urteil vom 01.08.2022) 275

Zur Höhe eines Anspruchs auf immateriellen Schadenersatz bei Verstoß gegen die DS-GVO
(BAG, Urteil vom 05.05.2022) 276

Schlussformulierung eines Arbeitszeugnisses
(BAG Urteil vom 25.01.2022) 278

Streitwert bei Datenschutzauskunftsklage (Ls)
(OLG Köln, Beschluss vom 04.08.2022) 280

Datenschutz steht Nachweis der Zahlung des Mindestlohns nicht entgegen (Ls)
(OLG Brandenburg, Urteil vom 23.02.2022) 280

Teilnahme am betrieblichen Sommerfest einer Klinik nur mit 2G+ und negativem Test (Ls)
(LAG Berlin-Brandenburg, Urteil vom 01.07.2022) 280

Bewerbung über das Internetportal reicht aus, um als Bewerber im Sinne des AGG zu gelten (Ls)
(LAG Schleswig-Holstein, Urteil vom 21.06.2022) 281

Duzen in Stellenzeige als Diskriminierung
(LAG Köln, Urteil vom 10.09.2021) 281

Zwangsweiser Einbau von Funkwasserzähler ist zulässig (Ls)
(Bayerische VerwGH, Beschluss vom 07.03.2022) 283

Zur Verpflichtung, im elektronischen Rechtsverkehr eine dem Stand der Technik entsprechende Verschlüsselung zu verwenden (Ls)
(VerwG Frankfurt/M., Beschluss vom 15.07.2022) 283

Dienstentfernung einer Beamtin infolge der Nichtumsetzung dienstlicher Anordnungen in Bezug auf die Corona-Pandemie (Ls)
(VerwG Trier, Urteil vom 21.06.2022) 283

Berichte, Informationen, Sonstiges

Chatkontrolle-Gesetz: EU will digitalen Schriftverkehr verdachtsunabhängig scannen 284

900.000 Euro Bußgeld wegen unzulässiger Auswertung von Kundendaten eines Kreditinstitutes in Niedersachsen 284

Wegen Datenschutzverstößen bei Forschungsfahrten verhängt die LfDI Niedersachen ein Millionenbußgeld gegen VW 284

Highlights aus dem Data-Agenda Datenschutz Podcast 284

Literaturhinweise

Buchbesprechungen

Schwartmann/Jaspers/Eckhardt (Hrsg.), Heidelberger Kommentar zum TTDSG
(BRINK) 286

Michael Els, Datenschutz für Kindertageseinrichtungen
(FRANCK) 286

Philpp Knitter, Digitale Weisungen – Arbeitgeberentscheidungen auf Grundlage algorithmischer Berechnungen
(SCHRIFTLEITUNG) 287

Nachgefasst 288

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. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 5/2022

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-Sechtem

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
38. Jahrgang 2022 Heft 5
Seiten 235-288

RDV
Recht der Datenverarbeitung

38. Jahrgang · Oktober 2022 · Seiten 235–288

Editorial

Auswege aus dem Cookie-Terror

Mit Hilfe von „Cookie-Bannern" holen Onlinedienste wiederholt Einwilligungen für Datenzugriffe ein. Diese rechtliche Pflicht per „Cookie-Bannern" oder besser „Consent-Bannern" zu erfüllen, hält die Bundesregierung für eine schlechte Lösung. Der Ansatz der Bundesregierung ist richtig und überfällig, denn „Cookie-Banner" sind unbefriedigend. Die meisten denken nicht über das reflexartige Wegklicken nach, das faktisch oft keine reflektierte Zustimmung darstellt. Eine informierte Einwilligung, wie die DS-GVO sie verlangt, sieht anders aus. Seit Dezember 2021 braucht jeder, der auf das Endgerät eines Nutzers zugreifen will, um diesem den Inhalt einer Webseite oder App anzuzeigen, eine Erlaubnis nach TTDSG. Es macht bis auf besondere Ausnahmefälle jeden Zugriff auf ein vernetztes Endgerät von einer Einwilligung abhängig. Erfasst sind vom Computer über das Smartphone bis hin zum vernetzten Toaster alle Geräte, die an das Internet angeschlossen sind und mit denen eine Software über das Internet „kommuniziert", d.h. Daten an das Gerät überträgt oder Daten ausliest.

Um die Erteilung der nach TTDSG und DS-GVO erforderlichen Einwilligungen zu vereinfachen und das ständige Wegklicken von „Cookie-Bannern" zu verhindern, will der Gesetzgeber nun Dienste schaffen, denen gegenüber Nutzer Einwilligungen abgeben können und die die Einwilligungen dann „treuhänderisch" verwalten und an Dritte übermitteln. Diese Dritten können etwa Unternehmen sein, die die Daten der Nutzer zu Werbezwecken benötigen und nur einwilligungsbasiert nutzen dürfen. Überträgt man diesen Ansatz von Webseiten auch auf Apps und Anwendungen im Internet der Dinge, dann wird klar, wie wichtig er ist. Denn schließlich kann man einem vernetzten Auto vor dem Zugriff auf die vernetzte Bremse keine Erlaubnis per Klick auf ein Einwilligungsbanner erteilen, bevor die Technik sie betätigt. Auch ein vernetzter Rasenmäher oder Kühlschrank muss technisch anders adressiert werden, als per Banner. Sind die Einwilligungen einmal hinterlegt, können sie an alle Anbieter übermittelt werden, die dem Nutzer Inhalte zugänglich machen und hierfür auf dessen Endgerät zugreifen wollen. Es ist wichtig, die Einwilligungen im Rahmen eines standardisierten Verfahrens einzuholen und zu übertragen. Eine zentrale Frage wird sein, wie zu verfahren ist, wenn ein Nutzer in den Einstellungen der Verarbeitung etwa gegenüber dem Einwilligungsverwaltungsdienst widerspricht. Gilt dieses Nein für alle Beteiligen, wenn sie keine gesonderte Einwilligung des Nutzers nachweisen können oder soll es Ausnahmen geben?

Aktuell ist das Digitalministerium gefragt. Es arbeitet an einer Verordnung, die den Rechtsrahmen für die Onlinewirtschaft maßgeblich umgestalten und unter anderem Cookie-Banner entbehrlich machen soll. Ein erster Entwurf zu einer Einwilligungs-Verordnung ist die Basis für die weiteren Schritte. Am Ende muss die Lösung des Ministeriums die Interessen der Bürger an einer selbstbestimmten Inanspruchnahme von digitalen Diensten berücksichtigen und faire Bedingungen für die vielschichtig betroffene Digitalwirtschaft schaffen. Wenn es gelingt, dann kann die „Einwilligungsverwaltungs-Verordnung" nicht nur Cookie-Banner entbehrlich machen. Sie kann transparente und datenschutzkonforme Regeln für das Online-Marketing schaffen.

Prof. Dr. Rolf Schwartmann

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

Termine	Thema	Ort	Kontakt
03.11.2022	Einführung in die ISO 27701	Online	GDD e.V. und DATAKONTEXT
08.11.2022	Compliance-Tests und Schwachstellenscannen	Online	GDD e.V. und DATAKONTEXT
08.11.2022	Privacy-Engineering	Online	GDD e.V. und DATAKONTEXT
08.11.2022	Datenschutz in medizinischen Einrichtungen	Berlin	GDD e.V. und DATAKONTEXT
09.11.2022	Grundlagen der Auftragsverarbeitung	Köln	GDD e.V. und DATAKONTEXT
10.11.2022	Datenschutz-Management light	Köln	GDD e.V. und DATAKONTEXT
16.11.2022	41. RDV-Forum	Köln	GDD e.V. und DATAKONTEXT
17.-18.11.2022	46. Datenschutzfachtagung (DAFTA)	Köln	GDD e.V. und DATAKONTEXT
21.11.2022	Konzerndatenschutz	Berlin	GDD e.V. und DATAKONTEXT
21.11.2022	Löschen nach der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
22.11.2022	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
24.11.2022	Die Aufgaben und der Tätigkeitsbericht des betrieblichen DSB praxisnah im Unternehmen	Online	GDD e.V. und DATAKONTEXT
28.11.2022	Datenschutzkonforme Datennutzung in Unternehmen	Köln	GDD e.V. und DATAKONTEXT
29.11.2022	Prüfen des Datenschutz für Revisoren	Online	GDD e.V. und DATAKONTEXT
30.11.2022	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Online	GDD e.V. und DATAKONTEXT
01.12.2022	Datenschutzverletzungen richtig behandeln	Frankfurt/M.	GDD e.V. und DATAKONTEXT
05.12.2022	Planung und Umsetzung der Überwachungsaufgaben der DSB	Köln	GDD e.V. und DATAKONTEXT
05.-09.12.2022	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Online	GDD e.V. und DATAKONTEXT
07.12.2022	Verzeichnis von Verarbeitungstätigkeiten	Online	GDD e.V. und DATAKONTEXT
08.12.2022	Hacker-Tools für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
13.12.2022	Datenschutz in der Kita	Online	GDD e.V. und DATAKONTEXT
14.12.20022	Zertifizierung zum Betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V. und DATAKONTEXT
30.-31.01.2023	GDD-Winter-Workshop	Garmisch-Partenkircchen	GDD e.V. und DATAKONTEXT
01.02.2023	Konzerndatenschutz	Online	GDD e.V. und DATAKONTEXT
02.02.2023	Datenschutz und Betriebsrat unter der DS-GVO	Online	GDD e.V. und DATAKONTEXT
07.02.23	Websites datenschutzkonform gestalten	Online	GDD e.V. und DATAKONTEXT

Datakontext GmbH, www.datakontext.com, Tel. 0 22 34 / 9 89 49 40

Aufsätze

Prof. Dr. Rolf Schwartmann/Lucia Burkhardt

Rechts- oder Funktionsträgerprinzip? Unternehmenshaftung nach der Datenschutz-Grundverordnung auf dem rechtlichen Prüfstand

Art. 83 DS-GVO dient der Datenschutzaufsicht als Grundlage für millionenschwere Bußgelder. Im Fokus der Behörde steht die Sanktionierung von Unternehmen. Dennoch ist das Haftungsmodell, welches den Verbandssanktionen zugrunde liegt, nach wie vor ungeklärt und seit längerem heftig umstritten. Aktuell sorgt eine Stellungnahme des EDSA für Unruhe.[1] Dieser bestimmte im Zuge der Vereinheitlichung der Bußgeldpraxis eher nebenbei das Haftungsmodell des Unionskartellrechts auch für die DS-GVO für anwendbar. Für die Praxis hätte das weitreichende Konsequenzen. Auch sorgfältig und gewissenhaft aufgestellte Chefetagen müssten dann für Datenpannen im Unternehmen haften. Die Positionierung des EDSA ist befremdlich, weil die Frage nach der Unternehmenshaftung nach Art. 83 DS-GVO in einem vom Berliner Kammergericht vorgelegten Fall aktuell beim Europäischen Gerichtshof anhängig ist. Ob er die Auffassung teilt, ist völlig offen. Dennoch bennent der EDSA kaum Argumente für seine Position. Ihm genügt, wie manchen Stimmen in der Literatur, ein pauschaler Verweis auf Rechtsprechung des EuGH zum Unionskartellrecht. Ob diese ungeprüfte Übernahme rechtlich haltbar ist, wird der Beitrag hinterfragen. Fest steht jedoch: Endgültig entschieden ist der Streit durch die Stellungnahme des EDSA noch nicht.

I. Einleitung

Die Frage nach dem anwendbaren Haftungsmodell für Unternehmen beschäftigte in der Vergangenheit nicht nur Aufsichtsbehörden, sondern auch Rechtsprechung, Literatur und Praxis. Während das Bundesinnenministerium im Rahmen der Evaluation des BDSG noch selbstbewusst das hiesige Rechtsträgerprinzip zugrunde legte,[2] sehen sich mittlerweile vermehrt Gerichte mit der Frage konfrontiert. LG Bonn[3] und das LG Berlin[4] beantworteten die Streitfrage Anfang des Jahres mit unterschiedlichen Ergebnissen, aber in Eigenregie. Das Kammergericht Berlin hat nun den EuGH angerufen.[5] Sein Prüfauftrag ist komplex. Schon der Rechtsweg ist nicht eindeutig. Zudem muss nicht nur bestimmt werden, wie Art. 83 DS-GVO auszulegen ist, sondern auch, was das nationale Recht zur Unternehmenshaftung bestimmt und ob Umsetzungsspielraum besteht. Es wird sogar ein Überschreiten der Grenzen der hiesigen Verfassung diskutiert.[6] Orientierungsmöglichkeiten anhand anderer Mitgliedsstaaten gibt es kaum, denn Deutschland ist mit seinem Rechtsträgerprinzip im europäischen Vergleich ein Exot. Die Streitfrage stellt sich daher in kaum einem anderen Land in gleicher Weise.[7]

Mit dem deutschen Rechtsträgerprinzip auf der einen Seite und dem auf supranationaler Ebene vornehmlich zugrunde gelegten Funktionsträgerprinzip auf der anderen Seite, stehen sich zwei grundlegend unterschiedliche Haftungsmodelle gegenüber, die Auswirkungen auf quasi jeden Aspekt der Sanktionierung haben. Sie erstrecken sich von den Zurechnungsvoraussetzungen über die notwendige Bestimmtheit eines Bußgeldbescheides bis hin zum konkreten Haftungsadressaten. Die Frage nach dem anwendbaren Haftungsmodell für Unternehmen hat damit weitreichende praktische Konsequenzen.

Darüber hinaus hat die Frage auch rechtspolitische Bedeutung, denn der Erlass eines Verbandssanktionsgesetzes ist in Deutschland seit langem geplant. Es ist möglich, dass das Haftungsmodell der DS-GVO den diesbezüglichen Diskurs wesentlich prägen und als ein mögliches Vorbild dienen wird. Deshalb bietet es sich an, die materiellrechtlichen und verfahrensrechtlichen Fragen nicht nur im Zusammenhang mit der DS-GVO, sondern übergreifend zu betrachten. Die Linie der DS-GVO könnte als mögliche Änderung, Ergänzung oder gar partielle Ersetzung des OWiG in Betracht kommen. Im Zentrum steht hierbei die Frage, ob neben der handelnden natürlichen Person immer auch ein Arbeitgeber, Rechtsträger oder Unternehmen verantwortlich sein muss. Davon geht der EDSA ungeprüft aus. Das liegt jedoch nur

1 EDSA Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Rn. 117 ff.

2 Bundesministerium des Inneren, für Bau und Heimat Evaluierung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, S. 61 f.

3 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20.

4 LG Berlin, Urt. v. 18.02.2021 – 526 OWi LG, 212 Js-OWi 1/20 (1/20).

5 KG Berlin, Beschl. v. 06.12.2021 – 3 Ws 250/21.

6 LG Berlin, Urt. v. 18.02.2021 – 526 OWi LG, 212 Js-OWi 1/20 (1/20), Rn. 25; Venn/Wybitul, Die bußgeldrechtliche Haftung von Unternehmen nach Art. 83 DS-GVO, NStZ 2021, 204 (208 f.); Dannecker/Dannecker, Europäische und verfassungsrechtliche Vorgaben für das materielle und formelle Unternehmensstrafrecht, NZWiSt 2016, 162 (169 ff.).

7 Lediglich Österreich verfügt über ein mit dem deutschen Modell vergleichbare Unternehmenshaftung. Zur durch den ÖVwGH positiv beschiedenen Frage der Notwendigkeit der Benennung der handelnden Person im Bescheid ÖVwGH, Erk. v. 12.05.2020 – Ro 2019/04/0229.

dann auf der Hand, wenn dieser Kreis gegen Organisations- und Überwachungspflichten verstoßen hat.[8]

Dieser Beitrag soll es leisten, zwei in Betracht kommende, konkurrierenden Haftungsmodelle für Unternehmen gegenüberzustellen. Hierbei sind Fragen, die sich auf unterschiedlichen Ebenen stellen, abzuschichten und zu systematisieren. Die einzelnen Aspekte der Unternehmenshaftung müssen dabei jeweils differenziert betrachtet werden. Die Diskussionen gehen in ihrer Pauschalität zurzeit teilweise fehl. So begründet etwa die Tatsache allein, dass die DS-GVO die Anwendung des „funktionalen Unternehmensbegriff" in ErwG 150 zur Bemessung des Bußgeldes anordnet, nicht zwangsläufig die Unanwendbarkeit des Rechtsträgerprinzips im Gesamten. „Mischmodelle", die die Haftung nach dem Rechtsträgerprinzip an Grundkonzepte und Begrifflichkeiten des Funktionsträgerprinzips angepasst haben, gibt es bereits, etwa im nationalen Kartellsanktionsrecht,[9] und sie sind auch im Datenschutzrecht vorstellbar.

II. Rechtsträger- vs. Funktionsträgerprinzip

Rechtlich stehen sich das Rechtsträger- und das Funktionsträgerprinzip gegenüber.

1. Rechtsträgerprinzip

Die hiesige Verbandshaftung ist im allgemeinen Teil es OWiG normiert. Sie erlaubt es, nach der Begehung einer Ordnungswidrigkeit, durch die Pflichten eines Unternehmens verletzt oder ein Unternehmen bereichert wurde, Geldbußen zu verhängen. Deren Festsetzung ist nicht nur gegenüber dem unmittelbaren Täter möglich, sondern auch gegenüber dem hinter diesem stehenden Verband (§§ 9, 30, 130 OWiG).[10] Dem Haftungsmodell liegt das sog. Rechtsträgerprinzip zugrunde, d.h. Geldbußen können nur gegenüber dem „Rechtsträger" der handelnden Person (sog. Tätergesellschaft) verhängt werden. Auf andere juristische Personen des Konzerns, wie die Muttergesellschaft, erstreckt sich die Haftung nicht. Haftungsadressat sind damit die einzelnen juristischen Personen, aus denen ein Konzern besteht.

Grundnorm ist § 30 OWiG. Die dogmatische Einordnung der Norm und damit auch die der hiesigen Verbandsgeldbuße ist umstritten. Teilweise wird vertreten, es handele sich um eine reine Zurechnungsnorm.[11] Die Haftung knüpfe an eine rechtswidrige und schuldhafte Tat eines Angestellten an, für diese Tat werde das Unternehmen im Wege der Zurechnung sanktioniert. Die Gegenauffassung geht davon aus § 30 würde eine eigene „Verbandstäterschaft" begründen, also eine Verantwortung für ein Organisationsdefizit und damit ein eigenes Fehlverhalten.[12] Unabhängig aber von der dogmatischen Herleitung bestimmt die Norm im Ergebnis eine Haftung des Unternehmens nur für rechtswidrige und schuldhafte Verstöße von Personen in Führungs- oder Aufsichtspositionen, wobei eine Aufsichtspflichtverletzung genügt (§ 130 OWiG).[13] § 30 OWiG normiert ein Modell der Akzessorietät zur volldeliktischen Handlung einer Leitungsperson (Anknüpfungstat). Diese Tat muss im Bußgeldbescheid konkret benannt und bewiesen werden.

2. Funktionsträgerprinzip

Dem steht das Unternehmensbußgeldrecht der europäischen Union gegenüber, welches sich in den letzten Jahrzenten, wesentlich durch den EuGH geprägt, entwickelt hat. Der Kernbereich, in dem das Sanktionsinstrument zum Einsatz kommt, ist das Unionskartellrecht.[14] Auch das Bankenaufsichtsrecht kennt jedoch die Unternehmensstrafe.[15] Vorgesehen sind Unternehmensbußgelder zudem in den Entwürfen zum DMA und DSA.[16] Dem europäischen Haftungsmodell liegt das Funktionsträgerprinzip zugrunde. Es stellt als Haftungsadressat nicht auf juristische Personen oder Rechtsträger ab, sondern auf das Unternehmen als wirtschaftliche Einheit, den sog. Funktionsträger. Als Unternehmen versteht der EuGH „jede wirtschaftliche Tätigkeit ausübende Einheit unabhängig von ihrer Rechtsform sowie der Art ihrer Finanzierung" (sog. kartellrechtlicher Unternehmensbegriff). [17] Alle juristischen Personen, die an einem Rechtsverstoß beteiligt sind, haften für das Unternehmensbußgeld gesamtschuldnerisch.[18] Damit kommt es auf die Ausgestaltung der Rechtssubjekte in den nationalen Rechtsordnungen, ihre Rechtsformen und Haftungsregelungen gerade nicht an.

Wesen des Funktionsträgerprinzips ist es, dass dem Unternehmen selbst die Haftung zugewiesen wird. Dogmatisch wird hierdurch eine unmittelbare Verbandshaftung begründet. Die unionsrechtliche Verbandsverantwortung basiert auf dem Grundgedanken, dass sich jedes Unternehmen so zu organisieren hat, dass es nicht zu Rechtsverstößen kommt. Unternehmen müssen die Handlungen und Arbeitsweisen ihrer Mitarbeitenden kennen und können sich im Konfliktfall nicht auf Unkenntnis berufen.[19] Auch die Tatsache, dass der handelnde Mitarbeiter einen Verhaltenskodex nicht ein-

8 Anderenfalls drohe, so warnt die Praxis, ein erhebliches, teils unkalkulierbares Haftungsrisiko für Unternehmen. Ein Haftungsrisiko besteht jedoch nicht nur mit Blick auf datenschutzrechtliche Sanktionen nach Art. 83 DS-GVO. Vielmehr droht nach Art. 82 DS-GVO, und das kann je nach Entwicklung der Rechtsprechung zu Bagatellschäden deutlich gefährlicher werden, auch eine zivilrechtliche Haftung. Hier werden dem Unternehmen die Taten ihrer Mitarbeitenden zweifelsfrei nach den Grundsätzen der §§ 278, 30, 831 BGB zugerechnet.

9 Hierzu ausführlich Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (90 ff.); Ost/Kallaß/Roesen, Einführung einer Unternehmensverantwortlichkeit im deutschen Kartellsanktionenrecht – Anmerkungen zum Entwurf der 9. GWB Novelle, NZKart 2916, 447; pointiert auch BeckOK Kartellrecht-Heinichen § 81 a GWB Rn. 24 ff.

10 Hierzu pointiert auch Wabnitz/Janovsky/Schmitt, Handbuch Wirtschafts- und Steuerstrafrecht-Dannecker/Müller 19. Kap. Kartellstraf- und -ordnungswidrigkeitenrecht, Rn. 150 ff.

11 BeckOK OWiG, Mayberg § 30 Rn. 17.1 f.; Leitner/Rosenau-Gräfin von Galen/Maas, § 30 OWiG Rn. 2.

12 KK OWiG-Rogall, § 30 Rn. 2 ff.

13 Zur Aufsichtspflichtverletzung KK OWiG, Rogall § 30 Rn. 91, zum erforderlichen Verschulden KK OWiG, Rogall § 130 Rn. 119.

14 Hierzu Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (86 ff.).

15 Hierzu Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (92 ff.).

16 Hierzu Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (95 f.).

17 EuGH, Urt. v. 23.04.1991 – C-41/90, Rn. 21, Urt. v. 17.02.1993 – C-159/91 und C-160/91, Rn. 17, Urt. v. 10.09.2009 – C-97/08 P, Rn. 54.

18 Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (85).

19 Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (94).

gehalten hat, reicht nicht aus, um die Zurechnung zu unterbrechen.[20] Dementsprechend genügt als Anknüpfungstat die Handlung einer jeden Person, die berechtigt ist, für das Unternehmen tätig zu werden, unabhängig davon, ob die Unternehmensleitung hieran beteiligt war. Handlungen sämtlicher Mitarbeitenden werden dem Unternehmen zugerechnet und als eine unmittelbar vom Unternehmen selbst begangene Handlung bzw. Zuwiderhandlung betrachtet.[21] Einzige Ausnahme ist der sog. Exzess.[22]

Die Konsequenzen für die Aufsichtspraxis sind erheblich. Im Bußgeldbescheid muss nach dem Funktionsträgerprinzip nur der Verstoß gegen die DS-GVO benannt und belegt werden.[23] Welcher Mitarbeiter, wann gehandelt hat, ist ohne Bedeutung und muss nicht bewiesen werden. Voraussetzung für die Zurechnung des Verstoßes ist allein die Erkennbarkeit und Vermeidbarkeit des Datenschutzverstoßes. Es genügt, dass „dem Unternehmen der Verstoß bewusst gewesen ist", oder es sich hierüber nicht in Unkenntnis hätte befinden dürfen.[24]

3. Gegenüberstellung

Tabellarisch lassen die Ansätze sich wie folgt gegenüberstellen.

	Funktionsträgerprinzip	Rechtsträgerprinzip nach § 30 OWiG
Haftungsmodell	Unmittelbare Unternehmenshaftung	Akzessorietät zur volldeliktischen Handlung einer Leitungsperson
Anknüpfungstat	Verstoß gegen die DS-GVO, wer den Verstoß begangen hat, ist irrelevant	Tat einer Person in Führungs- oder Aufsichtsposition, wobei neben Datenschutzverstoß durch Leitungspersonen auch Aufsichtspflichtverletzung genügt (§ 130 OWiG)
Schuld/subj. Vorwerfbarkeit	Erkennbarkeit und Vermeidbarkeit des Verstoßes (Vorsatz oder Fahrlässigkeit des Unternehmens)	Erkennbarkeit und Vermeidbarkeit des Verstoßes für handelnden Mitarbeiter (Vorsatz oder Fahrlässigkeit der handelnden Leitungsperson/ebene)
Umgrenzung des Verfahrensgegenstands / Beweispflicht der Behörde	Subjektiv vorwerfbarer Verstoß gegen die DS-GVO muss benannt und bewiesen werden	Verstoß gegen die DS-GVO (Taterfolg), handelnder Mitarbeiter (Täter) und Tathandlung muss ebenso wie Rechtswidrigkeit und Schuld des Täters benannt und bewiesen werden
Exkulpationsmöglichkeiten des Unternehmens	– Einzelabweichung eines Mitarbeiters (Exzess)[25] – vollständige Unvermeidbarkeit des Datenschutzverstoßes, bspw. unvermeidbarer Verbotsirrtum	– keine schuldhafte Aufsichtspflichtverletzung – Unvermeidbarkeit des Datenschutzverstoßes oder keine Handlung „als" Leitungsperson
Haftungsadressat/ Unternehmensbegriff	Das Unternehmen als wirtschaftliche Einheit Einzelne Rechtsträger eines Unternehmens sind nur als formale Adressaten der Sanktionsentscheidung, als Verfahrensbetroffene, relevant, sie haften als Gesamtschuldner	Das Unternehmen als die juristische Person/ Rechtsträger, deren Organ oder Leitungsperson die Ordnungswidrigkeit begangen hat (Tätergesellschaft), auf weitere Rechtsträger/juristische Personen erstreckt sich die Haftung nicht
Haftung des Mutterkonzerns	Mutterkonzern haftet für Verstöße von Tochtergesellschaften, wenn sie wirtschaftliche Einheit bilden, maßgeblich hierfür ist „bestimmender Einfluss", der vermutet wird, wenn die Muttergesellschaft 100% der Anteile der Tochter hält[26]	Verstoß der Tochter wird dem Mutterkonzern nicht zugerechnet, Mutterkonzern haftet nur, wenn sie für die Überwachung der Tochter verantwortlich war (eigener Organisations- oder Überwachungsverstoß)
Gesamtrechtsnachfolge	Geldbuße kann (uneingeschränkt) auch gegen Rechtsnachfolger festgesetzt werden („Vererblichkeit des Bußgeldes"[27])	Rechtsnachfolge möglich aber nach § 30 Abs. 2 a S. 2 OWiG in der Höhe beschränkt, zudem wird „Nahezu-Identität" zur Begründung einer Gesamtrechtsnachfolge gefordert

20 EuGH, Urt. v. 18.07.2013 – C-501/11 P, Rn.114.

21 EuGH, Urt. v. 07.06.1983 – C-100 to 103/80, Rn. 97, Urt. v. 18.09.2003 – C-338/00 P, 93 ff.; hierzu auch Wabnitz/Janovsky/Schmitt, Handbuch Wirtschafts- und Steuerstrafrecht-Dannecker/Müller, 19. Kap., Kartellstraf- und -ordnungswidrigkeitenrecht, Rn. 239 f.

22 Hierzu ausführlich: EDSA-Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Rn. 19.

23 EuGH, Urt. v. 18.09.2003 – C-338/00 P, Rn. 97 f.

24 EuGH, Urt. v. 18.09.2003 – C-338/00 P, Rn. 29 ff. m.w.N.; so auch EuGH, Urt. v. 06.10.1994 – T-83/91, Rn. 238 ff; Urt. v. 08.11.1983 – C-96/82, Rn. 45.; zu den Voraussetzungen der subj. Zurechnung Mansdörfer/Timmerbeil, Das Modell der Verbandshaftung im europäischen Kartellbußgeldrecht, in: EuZW 2011, 214 (216 f); Schwarze/Bechtold, Rechtsstaatliche Defizite im Kartellrecht der Europäischen Gemeinschaft, S. 46 f.

25 Ambrock, Mitarbeiterexzess im Datenschutzrecht, ZD 2020, 492.

26 Nach ständiger Rechtsprechung bilden eine Muttergesellschaft und ihre Tochtergesellschaft eine wirtschaftliche Einheit, wenn die Tochtergesellschaft „trotz eigener Rechtspersönlichkeit ihr Marktverhalten nicht autonom bestimmt, sondern im Wesentlichen Weisungen der Muttergesellschaft befolgt […], und zwar vor allem wegen der wirtschaftlichen, organisatorischen und rechtlichen Bindungen, die die beiden Rechtssubjekte verbinden"; vgl. EuGH, Urt. v. 10.09.2009 – C-97/08, Rn. 58; so auch EDSA-Guidelines 04/2022 on the calculation of administrative findes under the GDPR v. 12.05.2022, Rn. 122, 124 ff.; hierzu ausführlich Dannecker, Europäische und verfassungsrechtliche Vorgaben für das materielle und formelle Unternehmensstrafrecht, NZWiSt 2016, 162 (167); Calliess/Ruffert-Weiß, Art. 101 AEUV Rn. 35 ff.

27 Meixner, WuW 2017, 1281 und 1286, zitiert nach Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (91).

Wirtschaftliche Nachfolge	Bußgeld kann gegen Personen festgesetzt werden, die das Unternehmen in wirtschaftlicher Kontinuität fortführen (Grundsatz der wirtschaftlichen Kontinuität)	Kennt keine wirtschaftliche Nachfolge
Unmittelbare Haftung von Führungs- oder Aufsichtspersonen	Leistungspersonen haften nicht unmittelbar	Leistungspersonen können unmittelbar haften (§§ 9, 130 OWiG)

III. Auslegung von Art. 83 DS-GVO

Eine der zentralen Fragen, wenn es um das nach der DS-GVO anzuwendende Haftungsmodell für Unternehmen geht, ist die nach der Auslegung des Art. 83 DS-GVO. Es geht im Kern um die Frage, ob die DS-GVO das Funktionsträgerprinzip implizit für anwendbar erklärt oder Raum für die Anwendung der hiesigen §§ 30, 130 OWiG und das dort normierte Rechtsträgerprinzip bleibt. Da die DS-GVO gegenüber nationalen Vorschriften Anwendungsvorrang genießt, ist zur Bestimmung des datenschutzrechtlichen Haftungsmodells für Unternehmen primär deren Auslegung entscheidend. Nationale Modelle können nur dort angewendet werden, wo die DS-GVO den Mitgliedsstaaten Umsetzungsspielraum gewährt.

1. Art. 83 DS-GVO als unvollständige Norm

Daran, dass Art. 83 DS-GVO eine unvollständige Norm ist, die durch das nationale Recht ergänzt werden muss, dürfte kein Zweifel bestehen. Immerhin verfügt das europäische Recht bisher weder über einen allgemeinen Teil eines Sanktionsrechts noch über ein hierzu passendes Prozessrecht. Die Mitgliedsstaaten sind daher nicht nur berechtigt, sondern nach der allgemeinen Pflicht zur Durchführung des Unionsrechts (Art. 197 Abs. 3 S. 1, Art. 291 Abs. 1 AEUV) sogar verpflichtet, materielles Bußgeldrecht zu erlassen. Das umfasst nicht nur Bestimmungen etwa zu Versuch und Unterlassen, sondern auch den Bereich der Sanktionierung von Unternehmen. Der Umsetzungsspielraum bzw. die Umsetzungspflicht des hiesigen Gesetzgebers endet erst dort, wo die DS-GVO ausdrücklich oder implizit eigene Regelungen enthält.[28] Der Einwand des LG Bonn, Art. 83 Abs. 8 DS-GVO als explizite Öffnungsklausel beziehe sich nur auf Verfahrensvorschriften und nicht auf materielles Bußgeldrecht, weswegen die materiell-rechtlichen Haftungsbedingungen für Unternehmen gar nicht vom Umsetzungsspielraum der Mitgliedsstaaten umfasst werden könnten, überrascht daher.[29]

2. Das europäische Kartellbußgeldrechts als Vorbild für Art. 83 DS-GVO?

Ein nennenswerter Teil der datenschutzrechtlichen Literatur geht davon aus, der Unionsgesetzgeber habe das System des europäischen Kartellbußgeldrechts in Art. 83 DS-GVO für das Datenschutzrecht übernommen.[30] Dieses sei Vorbild für die Bußgeldregelung des Art. 83 DS-GVO gewesen und werde dort implizit für anwendbar erklärt. Hierfür werden im Wesentlichen drei Argumente herangezogen: erstens Wortlaut und Systematik des Art. 83 DS-GVO, zweitens der Erwägungsgrund 150 der DS-GVO und drittens der sog. effet utile Grundsatz.

Wortlaut und Systematik des Art. 83 DS-GVO belegten eine Anlehnung der DS-GVO an das Sanktionsmodell des Europäischen Kartellrechts, da der Artikel, anders als die hiesigen §§ 30, 130 OWiG, Unternehmen unmittelbar adressiert. Art. 83 DS-GVO Abs. 4 und 5 DS-GVO sprechen von „Unternehmen" als Bußgeldadressat, Art. 83 Abs. 3 DS-GVO von „Verantwortlichen und Auftragsverarbeitern" (Art. 4 Nr. 7 und 8 DS-GVO). Dass Verantwortliche in diesem Sinne nicht zwingend natürliche Personen sind, sondern auch Unternehmen wie Facebook Irland sein können, hat der EuGH bereits entscheiden.[31] Damit stellt Art. 83 DS-GVO als Haftungsadressat nicht, wie es die hiesigen §§ 30, 130 OWiG tun, auf natürliche Personen ab, für deren Taten Unternehmen in die Verantwortung genommen werden. Vielmehr haftet das Unternehmen an sich unmittelbar. Daher sei, so die Stimmen aus der Literatur, die Rechtsprechung des EuGH zur kartellrechtlichen unmittelbaren Unternehmenshaftung zu übertragen.[32] Dies werde von ErwG 150 DS-GVO unterstrichen. ErwG 150 DS-GVO bestimmt: „Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff ‚Unternehmen' im Sinne der Art. 101 und 102 AEUV [kartellrechtlicher, funktionaler Unternehmensbegriff] verstanden werden".[33] Schließlich streite der effet utile Grundsatz für die Übernahme des Haftungsmodells des supranationalen Kartellrechts. Würde die DS-GVO das anzuwendende Haftungsregime nämlich offen lassen, würden in unterschiedlichen Mitgliedsstaaten erheblich unterschiedliche Haftungsrisiken bestehen. Das stünde im Wiederspruch zum effet utile Grundsatz, nach dem Gemeinschaftsvorschriften so umzusetzen und auszulegen sind, dass sie „praktische"[34] bzw. „volle Wirksamkeit"[35] erlangen.[36]

28 Vgl. HK DS-GVO/BDSG-Schwartmann/Burkhardt, § 41 BDSG (im Anh. zu Art. 83 DS-GVO) Rn. 1 f., 6.

29 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20ZD, Rn. 73; zitiert von KG Berlin, Beschl. v. 06.12.2021 – 3 Ws 250/21, Rn. 24 f.; Zelger, Der Begriff des „Unternehmens" im europäischen Datenschutzrecht – Vorbild europäisches Kartellrecht?, EuR 2021, 478.

30 BeckOK Datenschutzrecht-Holländer, Art. 83 DS-GVO Rn. 8, 13 ff.; Ehmann/Selmayr-Nemitz, Art. 83 Rn. 42; Kühling/Buchner-Bergt, Art. 83 DS-GVO Rn. 20; Simitis/Hornung/Spiecker-Boehm, Art. 83 DS-GVO Rn. 43; Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, Born, § 8 Datenschutz und Straf- und Ordnungswidrigkeitenrecht Rn. 23 f.

31 EuGH, Urt. v. 29.07.2019 – C-40/17.

32 EDSA-Guidelines 04/2022 on the calculation of administrative findes under the GDPR v. 12.05.2022, Rn. 123; LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20ZD; BeckOK Datenschutzrecht, Holländer, Art. 83 DS-GVO Rn. 11.

33 EDSA-Guidelines 04/2022 on the calculation of administrative findes under the GDPR v. 12.05.2022, Rn. 118; DSK-Entschließung v. 03.04.2019: Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten; LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20. BeckOK Datenschutzrecht, Holländer, Art. 83 DS-GVO Rn. 13; ausführlich zu diesem Argument Ehmann/Selmayr-Nemitz, Art. 83 Rn. 42.

34 EuGH, Urt. v. 08.04.1976 – Rs. 48/75, Rn. 69/73.

35 Potacs Effet utile als Auslegungsgrundsatz, EuR 2009, 465 (466).

36 Ausführlich hierzu Potacs Effet utile als Auslegungsgrundsatz, EuR 2009, 465.

3. Grenzen der Übertragbarkeit des Unionskartellrechts

In der Tat lässt sich angesichts ErwG 150 DS-GVO nicht leugnen, dass der europäische Gesetzgeber bei Erlass der DS-GVO den kartellrechtlichen Unternehmensbegriff im Blick hatte und in irgendeiner Form berücksichtigen wollte. Auch, dass er davon ausging, dass datenschutzrechtliche Bußgelder nicht nur an natürliche Personen gerichtet werden können, sondern auch eine Sanktionierung von Unternehmen möglich sein muss, ist offenkundig. Warum jedoch die Tatsache allein, dass ein „Unternehmen" Haftungsadressat ist, automatisch bedeuten sollte, die Rechtsprechung des EuGH zur Unternehmenshaftung im Unionskartellrecht sei im Gesamten übertragbar, ist nicht ersichtlich. Das europäische Modell einer „Unternehmenshaftung" ist immerhin keineswegs die einzige Möglichkeit, Verbände zu sanktionieren. Hinzu kommt, dass der EuGH, der Natur der europäischen Rechtsprechung als Case Law entsprechend, Einzelfälle entschieden hat und keine allgemeingültige Theorie zur Sanktionierung von Wirtschaftsunternehmen entwickelt hat.[37] Um eine Übertragbarkeit zu begründen, bedarf es daher einer intensiven Betrachtung beider Rechtsgebiete. Ein pauschaler Verweis auf die im Art. 83 DS-GVO angeordnete „Unternehmenshaftung" kann als Beleg kaum genügen.[38]

a) Die Besonderheiten des kartellakzessorischen Bußgeldrechts

Die pauschale Übertragbarkeit begegnet aus unterschiedlichen Gründen Bedenken. Das Kartellrecht stellt, anders als das Datenschutzrecht, von vornherein auf Unternehmen im Sinne einer „wirtschaftlichen Einheit" ab und nicht auf juristische Personen. Unternehmen werden hier im Sinne einer wirtschaftlichen Einheit verstanden, da innerhalb einer solchen Einheit kartellrechtliche Beschränkungen wegen des fehlenden Wettbewerbs keinen Sinn machen. Art. 101 AEUV (Kartellverbot) ist daher auf die eine wirtschaftliche Einheit bildenden einzelnen Bestandteile eines Unternehmens nicht anwendbar (sog. Konzernprivileg).[39] Aufbauend auf diesem originär kartellrechtlichen Unternehmensbegriff hat der EuGH anhand von Einzelentscheidungen das kartellakzessorische Bußgeldrecht entwickelt und in Bezug auf das Kartellrecht konkretisiert. Im Datenschutzrecht gibt es ein mit dem Kartellrecht vergleichbares Konzernprivileg nicht. Datenschutzrechtliche Vorschriften gelten auch zwischen einzelnen Bestandteilen eines Konzerns bzw. einer Unternehmensgruppe.[40] Datenschutzrechtlich verantwortlich ist das konkrete Rechtssubjekt.[41] Unternehmen im Sinne der DS-GVO[42] ist daher nach Art. 4 Nr. 18 DS-GVO eine natürliche oder juristische Person, nicht „jede wirtschaftliche Tätigkeit ausübende Einheit".[43] Konsequenterweise müsste für das Sanktionsregime des Datenschutzrechts daher wie im Kartellrecht von einem rechtsgebietsspezifischen Unternehmensbegriff auszugehen sein.[44] Er müsste in Bezug auf die Besonderheiten des „nicht-unternehmensbezogenen" Datenschutzrecht[45] entwickelt werden.

Schließlich differieren Datenschutz- und Kartellrecht auch in Zielsetzung, Interessenslagen und Regelungsumfang.[46] Das Kartellrecht hat von vornherein eine rein restriktive Ausrichtung. Kernanliegen ist die Verhinderung der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung (Art. 102 AEUV). Die DS-GVO hingen möchte nicht nur die unsachgemäße Verarbeitung personenbezogener Daten verhindern, sie hat zugleich eine ermöglichende Funktion. ErwG 4 DS-GVO stellt ausdrücklich klar, dass der Datenschutz stets auch in Hinblick auf seine gesellschaftliche Funktion gesehen werden muss. Er soll auch den freien Verkehr personenbezogener Daten erleichtern (Art. 1 Abs. 2, 3 sowie ErwG 123 DS-GVO) und so wirtschaftliche Freiheiten ermöglichen.[47] Die abschreckende Wirkung der Sanktionierung ist im Datenschutzrecht daher zwar ebenso wie im Kartellrecht gewollt, darf aber nicht überspannt werden. Denn, anders als im Kartellrecht, kann eine drakonische Sanktionspraxis hier auch schaden. Müssen Unternehmen aus Angst vor Strafen stets „im Zweifel für den Datenschutz" entscheiden, verhindert das Innovation und wirtschaftliche Freiheiten und schadet damit den dem Datenschutz inhärenten Zielen. Das widerspricht Art. 1 Abs. 3 DS-GVO und deren Erwägungsgrund 4. Zu viel Missbrauchskontrolle nach Art. 102 AEUV kann es hingegen nicht geben.

37 Mansdörfer/Timmerbeil, Das Modell der Verbandshaftung im europäischen Kartellbußgeldrecht, EuZW 2011, 214 (214).

38 Zudem erging die Rechtsprechung des EuGH mit Blick auf Kartellrechtsanktionen, die von europäischen Behörden vollzogen wurden. Betroffen war damit ein „rein europäisches" Sanktionsinstrument. Das Datenschutzrecht hingegen wird von mitgliedstaatlichen Aufsichtsbehörden auf der Grundlage von mitgliedsstaatlichem Recht (vgl. etwa Art. 83 Abs. 9 DS-GVO) exekutiert. Insofern besteht hier schon der Natur der Sache nach nationaler Umsetzungsspielraum (hierzu auch Abschnitt III 1).

39 EuGH, Urt. v. 12.07.1984 – 170/83, Rn. 11; zum „Konzernprivileg" Cornelius Die „datenschutzrechtliche Einheit" als Grundlage des bußgeldrechtlichen Unternehmensbegriff nach der EU-DS-GVO, NZWiSt 2016, 421 (423 m.w.N.).

40 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz-Cornelius Teil XIV, Straf- und Ordnungswidrigkeitenvorschriften im Bereich des betrieblichen Datenschutzes, Rn. 94.

41 Hierzu Faust/Spittka/Wybitul, Milliardenbußgelder nach der DS-GVO? – Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, ZD 2016, 120 (122 f.); Hessel/Potel, Catch Me If You Can – Die Widersprüche der DS-GVO bei Verantwortlichkeit und Bußgeldbemessung im Konzernkontext, K&R 2020, 654 ff.; a.A. Zelger, Der Begriff des „Unternehmens" im europäischen Datenschutzrecht – Vorbild europäisches Kartellrecht?, EuR 2021, 478 (488 ff.).

42 Zum „Unternehmen" in der DS-GVO Forgó/Helfrich/Schneider, Betrieblicher Datenschutz-Cornelius Teil XIV, Straf- und Ordnungswidrigkeitenvorschriften im Bereich des betrieblichen Datenschutzes, Rn. 96 ff.; ausführlich (inkl. Übersicht) auch bei Zelger, Der Begriff des „Unternehmens" im europäischen Datenschutzrecht – Vorbild europäisches Kartellrecht?, EuR 2021, 478, 484 f.; Uebele, Das Unternehmen im europäischen Datenschutzrecht, EuZW 2018, 440; hierzu auch EDSA Guidelines 04/2022 on the calculation of administrative findes under the GDPR v. 12.05.2022, Rn. 119 sowie BeckOK Datenschutzrecht-Holländer Art. 83 DS-GVO Rn. 31.1 ff.

43 Vgl. etwa EuGH, Urt. v. 23.04.1991 – C-41/90, Rn. 21.

44 So Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (97); a.A. BeckOK Datenschutzrecht, Holländer, Art. 83 DS-GVO Rn. 14.1.

45 Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (97); Cornelius, Die „datenschutzrechtliche Einheit" als Grundlage des bußgeldrechtlichen Unternehmensbegriff nach der EU-DS-GVO, NZWiSt 2016, 421; a.A. Zelger, Der Begriff des „Unternehmens" im europäischen Datenschutzrecht – Vorbild europäisches Kartellrecht?, EuR 2021, 478 (488 ff.).

46 Spindler/Schuster-Eckardt, Art. 83 DS-GVO Rn. 77.

47 EuGH, Urt. v. 08.04.2014 – C-288/12, ECLI:EU:C:2014:237, Rn. 51; HK DS-GVO/BDSG-Kugelmann/Buchner, Art. 58 DS-GVO Rn. 22 f.

Die unterschiedlichen Zielsetzungen spiegeln sich auch in der Natur der sanktionsbewehrten Rechtsverstöße wider. Anders als Wettbewerbsverstöße sind Datenpannen nicht ihrer Natur nach konspirativ. Auch das sollte im Haftungsmodell Berücksichtigung finden. So ist nachvollziehbar, wieso ein Unternehmen für jeden Kartellverstoß, der in der Regel vorsätzlich, nicht selten auch gemeinschaftlich begangen wird und wesentlich vom Betriebsklima abhängt, haften soll. Der Grundgedanke, dass Unternehmen die Handlungen und Arbeitsweisen ihrer Mitarbeitenden kennen müssen und sich im Konfliktfall nicht auf Unkenntnis oder eine fehlerhafte interne Organisation berufen können, macht mit Blick auf die Natur von Wettbewerbsverstößen Sinn. Wieso jedoch auch gut organisierte Chefetagen für jede noch so kleine Datenpanne jedes einzelnen Mitarbeitenden in Verantwortung genommen werden sollen, erschließt sich jedenfalls nicht automatisch[48] und ist gerade mit Blick auf die Ermöglichungsfunktion der DS-GVO kritisch zu hinterfragen. Hier droht sich die DS-GVO selbst zu schaden. Die bisher ergangenen Entscheidungen des EuGH zum europäischen kartellakzessorischen Sanktionsrecht, die gerade nicht auf die Schaffung abstrakter Rechtsgrundsätze abzielten, können und sollten daher nicht ohne nähere Prüfung auf das Datenschutzrecht übertragen werden.

b) Das „Mischmodell" des nationalen Kartellrechts

Zudem wird die Rechtsprechung des EuGH zum originär kartellrechtlichen Funktionsträgerprinzip selbst innerhalb des Kartellrechts nicht uneingeschränkt angewendet. Dort, wo kartellrechtliche Sanktionen nicht durch europäische, sondern durch nationale Behörden verhangen werden,[49] gilt konstruktiv nach wie vor das Rechtsträgerprinzip. Ein Verstoß gegen das EU-Recht liegt darin nicht.[50] So liegt dem GWB mittlerweile zwar der europäische Unternehmensbegriff zugrunde. Deshalb können nun bspw. über § 30 OWiG hinaus auch Geldbußen gegen Muttergesellschaften festgesetzt werden.[51] Voraussetzung für eine Unternehmenshaftung ist aber nach wie vor die volldeliktische Tat einer Leitungsperson. So konnte der Gesetzgeber nach eigener Aussage einen „Gleichklang des Bußgeldadressaten mit dem Adressaten der materiellen Gebots- und Verbotsnormen sowie dem gesetzlichen Bußgeldrahmen"[52] herstellen, ohne konstruktiv vom Rechtsträgerprinzip abweichen zu müssen. Die Unternehmenshaftung nach dem § 30 OWiG wurde an das Unionskartellrecht angepasst, ohne das Funktionsträgerprinzip umfassend zu übernehmen.[53]

Einen Verstoß gegen die Richtlinie (EU) 1/2019 (ECN+-RL), die ausdrücklich gewährleisten soll, dass „die nationalen Wettbewerbsbehörden über [...] die Befugnisse im Bereich [...] der Verhängung von Geldbußen verfügen, die sie benötigen, um die Art. 101 und 102 AEUV wirksam anzuwenden", begründet das nicht. Erforderlich war hiernach nur die nationale Auslegung des Begriffs „Unternehmen" i.S.d. Art. 101 und 102 AEUV und die Ermöglichung einer rechtlichen und wirtschaftlichen Nachfolge.[54]

Wenn selbst innerhalb des Kartellrechts die nationale Anwendung des europäischen Funktionsträgerprinzips in toto nicht zwingend ist, dann wird man wohl kaum davon ausgehen können, dass allein das Abstellen auf ein „Unternehmen" genügt, um die Inkorporation des gesamten supranationalen kartellrechtlichen Sanktionsregimes in das nationale Datenschutzrecht zu begründen.[55] Hier dürfte mindestens so viel Umsetzungsspielraum bestehen, wie im nationalen Kartellrecht.

c) Die Notwendigkeit einer differenzierten Betrachtung

Weiterer Grund für vorschnelle, ggf. sogar falsche Ergebnisse ist, dass die Frage, ob Funktions- oder Rechtsträgerprinzip anzuwenden ist, jedenfalls in ihrer Pauschalität fehlgeht. Zu untersuchen ist vielmehr, welche Aspekte des europäischen Modells die DS-GVO für anwendbar bestimmt und wo Umsetzungsspielraum besteht. Zentral und praxisrelevant sind hierbei v.a. drei Fragen:

- Erstens: Ist der funktionale Unternehmensbegriff mit all seinen Konsequenzen anwendbar? Bejaht man dies, wäre im Datenschutzrecht wie im hiesigen Kartellrecht (§ 81 GWB) eine Haftung des Mutterkonzerns sowie eine wirtschaftliche Nachfolge über § 30 OWiG hinaus möglich.
- Zweitens: Kann sich ein Bußgeldbescheid unmittelbar gegen ein Unternehmen richten? Falls ja bedürfte es, anders als im deutschen Kartellrecht, keiner volldeliktischen Ordnungswidrigkeit einer natürlichen Person. In diesem Zusammenhang müsste auch beantwortet werden, ob Tathandlung und Tatzeit im Bescheid benannt werden müssen.

48 Ähnliches gilt, wenn es um die Frage geht, ob die handelnde Person im Bescheid benannt werden muss. Im Unionskartellrecht lehnt der EuGH dies zwar ab (EuGH Urt. v. 19.09.2003 – C-338/00 P), ob das auch für Datenschutzverstöße gilt, ist jedoch, selbst unter Zugrundelegung einer unmittelbaren „Verbandsverantwortlichkeit", höchst fraglich. Der EuGH argumentiert, dass eine Identifizierung nicht erforderlich sei, da die kartellrechtlichen Geldbußen nach Art. 15 Abs. 4 der Verordnung Nr. 17 ausdrücklich keinen strafrechtlichen Charakter hätten, und dass ein solches Erfordernis die Effektivität des Wettbewerbsrechts der EU ernsthaft gefährden würde. Diese Argumentation steht zum einen auf wackeligen Beinen, da es nicht möglich ist, den strafähnlichen Charakter einer Norm gesetzlich abzubedingen. Zum anderen lässt sie sich nicht ohne Weiteres auf das mitgliedstaatlich geprägte Datenschutzrecht übertragen, dessen Verstöße nicht ihrer Natur nach konspirativ sind. So im Ergebnis auch der ÖVwGH, Erk. v. 12.05.2020 – Ro 2019/04/0229, Rn. 23.

49 Kartellrechtsanktionen werden teils (bei grenzüberschreitenden Sachverhalten) von europäischen Behörden, teils von nationalen Aufsichtsbehörden vollzogen. Das Rechtsgebiet teilt sich damit in einen „rein europäischen" Teil (das Unionskartellrecht) und einen mitgliedsstaatlich geprägten Teil.

50 So auch Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (98 ff.); ders. schon ebd. 2016, 162 (166 und 168 ff.).

51 Vgl. die durch die 9. GWB Novelle eingefügten § 81 Abs. 3 a – 3 e) GWB.

52 BT-Drs 18/10207, 86.

53 Zum kartellrechtlichen Modell ausführlich Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (90 ff.); Ost/Kallaß/Roesen, Einführung einer Unternehmensverantwortlichkeit im deutschen Kartellsanktionenrecht – Anmerkungen zum Entwurf der 9. GWB Novelle, NZKart 2916, 447; pointiert auch BeckOK Kartellrecht-Heinichen, § 81 a GWB Rn. 24 ff.

54 Hierzu Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (90).

55 So dennoch Thiel im Interview mit der ZD, ZD 2020, 3 (3); DSK-Entschließung v. 03.04.2019: Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten; LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20.

- Drittens: Haften Unternehmen für Handlungen sämtlicher Mitarbeitenden oder ist die Haftung auf Handlungen von Führungspersonen beschränkt?

Auf dieser differenzierten Linie bewegt sich auch das Kammergericht Berlin mit seiner Vorlagefrage an den EuGH. Es fragt konkret, ob Art. 83 Abs. 4-6 DS-GVO dahingehend auszulegen ist, „dass er [...] das Funktionsträgerprinzip in das innerstaatliche Recht mit der Folge inkorporiert, dass unter Erweiterung des § 30 OWiG zugrundeliegenden Rechtsträgerprinzips ein Bußgeldverfahren unmittelbar gegen Unternehmen geführt werden kann und die Bebußung nicht der Feststellung einer durch eine natürliche und identifizierte Person, gegebenenfalls volldeliktisch, begangenen Ordnungswidrigkeit bedarf".[56]

Eine differenzierte Betrachtung ist wichtig, weil je nach Fallkonstellation unterschiedliche Argumente greifen. Mit Blick auf den anzuwendenden Unternehmensbegriff (Frage 1) wird etwa die Bedeutung des ErwG 150 DS-GVO[57] und eine Unterscheidung in haftungsbegründenden und haftungsausfüllenden Tatbestand diskutiert.[58] Zudem werden Wortlaut und Systematik der DS-GVO und die Begrifflichkeiten der englischen Fassung analysiert, um einen „datenschutzrechtlichen Unternehmensbegriff"[59] zu erarbeiten.[60] Für die Frage nach der unmittelbaren Bebußbarkeit von Verbänden und die hieran anknüpfende Schuldfrage (Frage 2) spielt v.a. das Grundgesetz sowie das Wesen datenschutzrechtlicher Sanktionen eine entscheidende Rolle.

Wichtig ist, sich zu vergegenwärtigen, dass es durchaus möglich ist, die eine Frage im Sinne des europäischen und andere im Sinne des nationalen Modells zu beantworten. So geschieht es im nationalen Kartellrecht. Soll daher bspw. eine unmittelbare Unternehmenshaftung (Frage 2) oder eine Zurechnung der Handlungen sämtlicher Mitarbeitenden begründet werden (Frage 3), genügt weder ein Verweis auf ErwG 150 DS-GVO bzw. den anzuwenden Unternehmensbegriff (Frage 1) noch die pauschale Bezugnahme auf die Rechtsprechung des EuGH zum Unionskartellrecht.[61] Es bedarf vielmehr einer intensiveren Betrachtung der konkret aufgeworfenen Frage. Daran fehlt es[62] bislang sowohl beim EDSA[63] als auch bei den deutschen Gerichten.[64]

4. Das Effektivitätsgebot als entscheidender Faktor

Ein wesentliches Argument für die Anwendung europäischer Haftungsmaximen wird im Ergebnis in allen Bereichen eine wertende Betrachtung im Sinne des sog. effet utile Grundsatz sein. Er hat im Lichte der durch die DS-GVO angestrebten Vollharmoniserung besondere Bedeutung. Hinzu kommt, dass die Verbandssanktionierung in den Mitgliedsstaaten auf völlig unterschiedlichen Rechtstraditionen beruht. Die Unterschiede reichen von den Voraussetzungen, unter denen Verbände und natürliche Personen zur Verantwortung gezogen werden können, bis zu den Rechtsfolgen. Verwaltungssanktionen erfolgen z.B. in Griechenland, Geldbußen und Ordnungswidrigkeiten kennt man in Deutschland und Österreich. Unterschiedliche Ansätze gibt es auch bei der Sanktionsbemessung.[65] Die Verknüpfung der Art. 83 Abs. 4 bis 6 DS-GVO mit nationalen Haftungs- und Zurechnungsvorschriften hätte daher zur Folge, dass die Sanktionierung von Unternehmen in hohem Maße uneinheitlich erfolgen würde.[66] Ob das tatsächlich gewollt ist, ist unklar und wird von den nationalen Gerichten und der Literatur zurzeit unterschiedlich bewertet.[67] Orientierungsmöglichkeiten anhand anderer Mitgliedstaaten gibt es kaum, da diese, wie erwähnt, das deutsche Rechtsträgerprinzip nicht kennen.

IV. Strafverfassungsrechtliche Grenzen der Unternehmenssanktion

1. Das Schuldprinzip

Einige Stimmen in der Literatur bestehen mit Blick auf Schuld- und Gesetzlichkeitsprinzip auf die Anwendung der §§ 30, 130 OWiG und das deutsche Rechtsträgerprinzip.[68] Auch das LG Berlin verweist in seinem Urteil auf die genannten Grundsätze. Ihm zufolge ist ein staatlicher Strafausspruch ohne eine Anknüpfung an eine schuldhafte Handlung nicht möglich.[69] Das gelte nicht nur für das klassische

56 KG Berlin, Beschl. v. 06.12.2021 – 3 Ws 250/21.

57 Ehmann/Selmayr-Nemitz, Art. 83 Rn. 42.

58 LG Berlin, Beschl. v. 18.02.2021 – 526 Owi LG, Rn. 24; Taeger/Gabe-Moos/Schefzig, Art. 83 DS-GVO Rn. 120.

59 Cornelius, Die „datenschutzrechtliche Einheit" als Grundlage des bußgeldrechtlichen Unternehmensbegriff nach der EU-DS-GVO, NZWiSt 2016, 421.

60 Zelger, Der Begriff des „Unternehmens" im europäischen Datenschutzrecht – Vorbild europäisches Kartellrecht?, EuR 2021, 478; Faust/Spittka/Wybitul, Milliardenbußgelder nach der DS-GVO? – Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, ZD 2016, 120 (122 f.); Hessel/Potel, Catch Me If You Can – Die Widersprüche der DS-GVO bei Verantwortlichkeit und Bußgeldbemessung im Konzernkontext, K&R 2020, 654 ff.; Ehmann/Selmayr-Nemitz, Art. 83 Rn. 42.

61 So etwa Thiel im Interview mit der ZD, ZD 2020, 3 (3); DSK-Entschließung v. 03.04.2019: Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten; Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (94f.); BeckOK Datenschutzrecht, Holländer, Art. 83 DS-GVO Rn. 13 ff.; so auch noch Schwartmann/Burkhardt, HK zum Datenschutzrecht in der Kommentierung zum § 41 BDSG (in Anh. zu Art. 83 DS-GVO), Rn. 9; Simitis/Hornung/Spiecker-Boehm, Art. 83 DS-GVO Rn. 40.

62 Kühling/Buchner-Bergt, Art. 83 DS-GVO Rn. 20, 39 ff. differenziert immerhin zwischen dem Haftungsmodell (Rn. 20) und dem Unternehmensbegriff (Rn. 39 ff.).

63 EDSA-Guidelines 04/2022 on the calculation of administrative findes under the GDPR v. 12.05.2022, Rn. 123; dem EDSA genügte als Argument zur Anwendung der gesamten unionskartellrechtlichen Rechtsprechung die Bezugnahme auf ErwG 150 DS-GVO sowie die Tatsache, dass Art. 83 DS-GVO dem Grundsatz der Unternehmenshaftung folgt.

64 Selbst das KG Berlin stellt in der Begründung seiner noch sehr präzise formulierten Vorlagefrage auf ErwG 150 DS-GVO und den funktionalen Unternehmensbegriff ab, ohne darzulegen, wieso hierdurch automatisch eine unmittelbare Unternehmenshaftung begründet werden sollte, vgl. KG Berlin, Beschl. v. 06.12.2021 – 3 Ws 250/21, Rn. 15.

65 Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (86).

66 KG Berlin, Beschl. v. 06.12.2021 – 3 Ws 250/21, Rn. 18.

67 Für einen eingeschränkten Umsetzungsspielraum argumentieren bspw. LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20ZD; KG Berlin, Beschl. v. 06.12.2021 – 3 Ws 250/21, Rn. 18 f.; Qasim, Adressierung eines Bußgeldbescheids nach der DS-GVO, ZD-Aktuell 2021, 05102; Bussche, Anmerkung zu LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20, ZD 2021, 159; Ehmann/Selmayr-Nemitz, Art. 83 Rn. 42 f.; so im Ergebnis auch BeckOK-Holländer, Art. 83 DS-GVO Rn. 14.1.; Kühling/Buchner-Bergt, Art. 83 DS-GVO Rn. 43 a; Simitis/Hornung/Spiecker-Boehm, Art. 83 DS-GVO Rn. 43; a.A. LG Berlin, Urt. v. 18.02.2021 – 526 OWi LG, 212 Js-OWi 1/20 (1/20); ÖVwGH, Erk. v. 12.05.2020 – Ro 2019/04/0229; Taeger/Gabel-Moos/Schefzig, Art. 83 DS-GVO Rn. 121 ff.

68 Venn/Wybitul, Die bußgeldrechtliche Haftung von Unternehmen nach Art. 83 DS-GVO, NStZ 2021, 204 (208 f.); allg. zu den strafverfassungsrechtlichen Grenzen eines europäisch geprägten Verbandssanktionengesetzes Dannecker/Dannecker, Europäische und verfassungsrechtliche Vorgaben für das materielle und formelle Unternehmensstrafrecht, NZWiSt 2016, 162 (169 ff.).

69 LG Berlin, Urt. v. 18.02.2021 – 526 OWi LG, 212 Js-OWi 1/20 (1/20), Rn. 25.

Strafrecht, sondern auch im Ordnungswidrigkeitenrecht. Da einer juristische Person aber kein Schuldvorwurf gemacht werden könne, bedürfe es stets der Anknüpfung an die Handlung einer natürlichen Person. Das mache die Anwendung der §§ 30, 130 OWiG verfassungsrechtlich erforderlich, da diese, anders als das supranationale Funktionsträgerprinzip, die schuldhafte Tat eines Mitarbeiters voraussetzen. Eine unmittelbare Unternehmenshaftung, wie sie das europäische Recht bestimme, sei hierzulande mit Blick auf das Schuldprinzip konstitutionell ausgeschlossen.

Das hätte praktische Konsequenten von enormer Tragweite, weit über das Datenschutzrecht hinaus. Dann wäre das europäische Haftungsmodell für Unternehmen nämlich nicht nur im Datenschutzrecht nicht mit dem integrationsfesten Teil des Grundgesetzes vereinbar. Konflikte würden immer dann entstehen, wenn Sanktionsrechtssysteme auf Unionsebene eingeführt werden. Damit wären nicht nur alle kartellrechtlichen Sanktionen europäischer Behörden verfassungswidrig,[70] sondern bspw. auch die geplanten Sanktionsmöglichkeiten nach dem DGA und DSA. Gleichzeitig herrscht darüber, dass einer juristischen Person konstitutionell kein Schuldvorwurf gemacht werden kann, in der strafrechtlichen Literatur keine Einigkeit. Auch vom Bundesverfassungsgericht wurde diese Wertung bisher nicht bestätigt.[71]

a) Sanktionsfähigkeit des Verbandes

Als Kernargument gegen die Sanktionsfähigkeit juristischer Personen dient in der Regel die Lissabon-Entscheidung des BVerfG, in der sich das BVerfG u.a. mit den Zuständigkeiten der Europäischen Union im Bereich der Strafrechtspflege auseinandersetzt. In diesem Kontakt stellt das Gericht fest, dass die Menschenwürde das Wesen von Strafe und Schuld bestimmt. Es betont, dass der Schuldgrundsatz („Keine Strafe ohne Schuld") in Art. 1 Abs. 1 GG wurzelt und daher die Eigenverantwortung des Menschen, der sein Handeln selbst bestimmt und sich kraft seiner Willensfreiheit zwischen Recht und Unrecht entscheiden kann, voraussetzt.[72] Das trifft mit Blick auf natürliche Personen unstreitig zu. Der Schuldgrundsatz betrifft gegenüber einer natürlichen Person den Aspekt der Menschenwürde.[73] Der Schuldgrundsatz ist jedoch ebenso im Rechtsstaatsprinzip begründet. Laut BVerfG ist die „strafrechtliche oder strafrechtsähnliche Ahndung einer Tat ohne Schuld des Täters [...] rechtsstaatswidrig und verletzt den Betroffenen in seinem Grundrecht aus Art. 2 Abs. 1 GG".[74] Die Feststellung, dass der Schuldvorwurf gegenüber einer natürlichen Person den Aspekt der Menschenwürde betrifft, kann damit nur als Teilaspekt des Schuldprinzips begriffen werden.[75] Mit der Frage, was das für die Sanktionsfähigkeit von Verbänden bedeutet, hat sich das Gericht in der Entscheidung nicht auseinandergesetzt. Die Feststellungen des Gerichts können daher nicht ohne Weiteres als Absage an die Integration der Verbandsstrafe verstanden werden.[76] Das gilt insb., da einem Verband ein verfassungsrechtlich geschütztes Recht nicht allein deshalb abgesprochen werden kann, weil dieses Recht auch unter Hinzuziehung von Art. 1 GG hergeleitet wird. Das hat der BGH bereits mehrfach mit Blick auf das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG abgeleitete allgemeine Persönlichkeitsrecht entschieden. Dieses ist in Teilen auch auf juristische Personen anwendbar.[77]

Insofern ist auch vertretbar, dass der Gesetzgeber mit Blick auf juristischer Personen nicht an die traditionelle, von der Menschenwürde geprägte Vorstellung von Schuld und Strafe gebunden ist.[78] Hierfür spricht, dass die Verfassung nur einen Rahmen setzt und dem demokratisch legitimierten Gesetzgeber die Möglichkeit eröffnet, im Detail zu bestimmen,[79] wann ein schuldhafter Pflichtverstoß (einer natürlichen Person oder eines Unternehmens) begründet ist und wie hierauf zu reagieren ist. So ließe sich auch die Bertelsmann-Lesering-Entscheidung des BVerfG aus dem Jahr 1966 erklären. Hier heißt es: „Die dargelegten Grundsätze [des Schuldprinzips] gelten auch für juristische Personen. Die juristische Person ist rechtsfähig. Sie nimmt gleichwertig mit den natürlichen Personen am Rechtsleben teil. [...] Auch eine juristische Person ist also „wegen einer jeden Zuwiderhandlung" zu einer Geld- oder Haftstrafe zu verurteilen."[80] Die Übertragbarkeit der Lissabon-Entscheidung auf die Schuldfähigkeit von Verbänden ist gerade mit Blick auf die Bertelsmann-Lesering-Entscheidung, die sich hiermit explizit befasst, kritisch zu hinterfragen. Jedenfalls kann die Entscheidung allein als Beleg kaum genügen.

70 Zur Verfassungskonformität der 9. GWB-Novelle mit Blick auf den Schuldgrundsatz Ost/Kallaß/Roesen, Einführung einer Unternehmensverantwortlichkeit im deutschen Kartellsanktionenrecht – Anmerkungen zum Entwurf der 9. GWB Novelle, NZKart 2916, 447 (456 f.).

71 Für die Möglichkeit einer Verbandsschuld argumentieren etwa Ost/Kallaß/Roesen, Einführung einer Unternehmensverantwortlichkeit im deutschen Kartellsanktionenrecht – Anmerkungen zum Entwurf der 9. GWB Novelle, NZKart 2916, 447(456); Dannecker/Dannecker, Europäische und verfassungsrechtliche Vorgaben für das materielle und formelle Unternehmensstrafrecht, NZWiSt 2016, 162 (175); ebenfalls ablehnend MK StGB-Freund, Vorbermerkung zu § 13 Rn. 147 ff. m.w.N.

72 BVerfG, Urt. v. 30.06.2009 – 2 BvE 2/08 u.a., Rn. 364.

73 Osterloh, Strafrechtsdogmatische und strafprozessuale Probleme bei der Einführung und Umsetzung einer Verbandsstrafbarkeit, S. 64.

74 BVerfG, Beschl. v. 25.10.1966 – 2 BvR 506/63.

75 Osterloh, Strafrechtsdogmatische und strafprozessuale Probleme bei der Einführung und Umsetzung einer Verbandsstrafbarkeit, S. 65.

76 Dannecker/Dannecker, Europäische und verfassungsrechtliche Vorgaben für das materielle und formelle Unternehmensstrafrecht, NZWiSt 2016, 162 (175) m.w.N.

77 Osterloh, Strafrechtsdogmatische und strafprozessuale Probleme bei der Einführung und Umsetzung einer Verbandsstrafbarkeit, S. 65.

78 Dannecker/Dannecker, Europäische und verfassungsrechtliche Vorgaben für das materielle und formelle Unternehmensstrafrecht, NZWiSt 2016, 162 (173).

79 Baumann, Grundbegriffe und System des Strafrechts, S. 157; zitiert nach Osterloh, Strafrechtsdogmatische und strafprozessuale Probleme bei der Einführung und Umsetzung einer Verbandsstrafbarkeit, S. 65.

80 BVerfG, Beschl. v. 25.10.1966 – 2 BvR 506/63. Zwar hat das BVerfG ein Jahr später festgestellt, dass „juristische Personen als bloße Zweckgebilde der Rechtsordnung [...] ihren Willen nur durch Organe [bilden] und im [...] Hinblick auf Straftaten oder Ordnungswidrigkeiten nur einer eingeschränkten Verantwortlichkeit [unterliegen]." Weiter stellt es fest: „Begeht ein Organwalter unter Verletzung von Pflichten der juristischen Person eine solche Tat, so ist allein er Täter. Gegen die juristische Person kann lediglich gem. § 30 eine Geldbuße festgesetzt werden, die aber weder einen Schuldvorwurf noch eine ethische Missbilligung enthält, sondern einen Ausgleich für die aus der Tat gezogenen Vorteile schaffen soll" (BVerfG, Urt. v. 26.02.1997 – 1 BvR 2172/96). Um vermeintliche Widersprüche in der Rechtsprechung des BVerfG aufzulösen, ist es hier ebenso wie mit Blick auf die Lissabon-Entscheidung erforderlich, das Urteil im Kontext des zu entscheidenden Falles zu betrachten. Das Gericht wollte keine Aussage zur Bebußbarkeit eines Unternehmens treffen, sondern begründen, warum ein Unternehmen sich nicht auf das Selbstbelastungsprivileg berufen kann. Es bezieht sich hierzu auf die damalige (nach wie vor unveränderte) einfach-rechtliche Ausgestaltung der Rechtsordnung, nicht auf die Verfassung.

Aber auch dann, wenn man davon ausgeht, eine juristische Person könne aus verfassungsrechtlichen Gründen nicht schuldhaft handeln, muss das kein Argument dafür sein, dass ihre Bestrafung das Schuldprinzip verletzt. Es kann auch ein Argument dafür sein, das Schuldprinzip auf juristische Personen gar nicht anzuwenden.[81] Es liegt daher nahe, die Frage nach der Sanktionsfähigkeit von Verbänden als rechtspolitische Entscheidung zu bewerten, der die Verfassung zwar Grenzen setzt (zu denken ist hier insb. an das Übermaßverbot), die aber nicht konstitutionell vorgeprägt ist.

b) Modelle verfassungskonformer Unternehmensverantwortlichkeit

Wenn es um die Frage geht, wie eine strafrechtliche Verbandsschuld/Verantwortlichkeit ausgestaltet werden kann, kommen v.a. zwei verschiedene Modelle in Betracht.[82] Denkbar wäre ein sog. Zurechnungsmodell, wonach stets ein sog. Zurechnungsakt erforderlich wäre. Hierüber würden dem Verband Handlungen und Schuldvorwurf der für das Unternehmen handelnden Mitarbeiter zugerechnet. Eine originäre Verbandsschuld würde es dann nicht geben. Der Zurechnungsakt könnte sowohl zivilrechtsakzessorisch, angepasst an die gesellschaftsrechtlichen Gestaltungsformen, oder aber autonom durch das Sanktionsrecht ausgestaltet werden.[83] Ebenfalls möglich wäre die Normierung eines eigenständigen Schuldvorwurfs, der nicht mit dem des Individualstrafrechts identisch ist. Handlungen im Namen eines Unternehmens würden rechtlich als Handlungen des Verbandes eingestuft, das Unternehmen würde dabei nicht für die Schuld eines Dritten haften, sondern im Wege einer kooperativen Verbandsschuld.[84] Zwar hat das BVerfG festgestellt, dass für die Inanspruchnahme einer juristischen Person für schuldhaftes Verhalten im strafrechtlichen Sinne „nur die Schuld der für sie verantwortlich handelnden Personen maßgebend" sein könne. Hiermit wollte das Gericht aber lediglich klarstellen, dass auch Unternehmen verfassungsrechtlich davor geschützt sind, für „fremdes" Fehlverhalten bestraft zu werden. Eine abstrakte Positionierung in Richtung eines Zurechnungsmodells war ebenso wenig beabsichtigt, wie eine Beschränkung der Zurechnung auf den Rechtsträger der handelnden Person.[85]

2. Gesetzlichkeitsprinzip

Einige Stimmen in Literatur und Rechtsprechung gehen überdies davon aus, die Adaption des europäischen Kartellrechts durch die DS-GVO verstoße gegen das Gesetzlichkeitsprinzip.[86] Über das sowohl in Art. 103 Abs. 2 GG als auch in Art. 49 GRCh verankerte Gesetzlichkeitsprinzip bekommt die Wortsinngrenze im Bereich des Straf- und Ordnungswidrigkeitenrecht eine besondere Bedeutung. Eine gesetzlich nicht vorgesehene strafrechtliche Unternehmensverantwortlichkeit verstößt daher ebenso wie eine Überdehnung des Wortlautes durch teleologische Reduktion oder Analogie gegen das deutsche sowie das europäische Verfassungsrecht. Das gilt selbst dann, wenn sich der eigentliche Wortlaut einer Norm oder eine Haftungslücke als unionsrechtswidrig erweist.[87]

Eine Interpretation der §§ 30, 130 OWiG im Sinne des hier gerade nicht angeordneten Funktionsträgerprinzips (und damit contra legem) verstößt daher, so argumentiert bspw. das LG Berlin, gegen das Gesetzlichkeitsprinzip.[88] Diesem Gedanken ist im Kern zuzustimmen, die §§ 30, 130 OWiG können verfassungskonform nicht so ausgelegt werden, dass sie eine unmittelbare Unternehmenshaftung im Sinne des Unionskartellrechts begründen. Übersehen wird hier jedoch, dass der Sanktionierung von Unternehmen nach dem europäischen Modell keine unionsrechtkonforme Auslegung der §§ 30, 130 OWiG zugrunde läge, sondern Art. 83 DS-GVO selbst. Die §§ 30, 130 OWiG blieben dann wegen eines Widerspruchs zum Unionsrechts unanwendbar.[89]

Entscheidend ist damit die Frage, ob Art. 83 i.V.m. ErwG 150 DS-GVO als unmittelbare Rechtsgrundlage taugt.[90] Bedenken bestehen mit Blick auf das Bestimmtheitsgebot.[91] Würden diese Bedenken durchgreifen, würde das indes nicht bedeuten, dass eine Interpretation der Norm im Sinne des Funktionsträgerprinzips ausgeschlossen wäre. Vielmehr müsste der nationale Gesetzgeber dann tätig werden und durch Erlass unionsrechtskonformen Bußgeldrechts, d.h. insb. unter Berücksichtigung des effet utile Grundsatzes, die Durchführung des Art. 83 DS-GVO gewährleisten. Die allg. Verpflichtung dazu ergibt sich aus Art. 197 Abs. 3 S. 1, Art. 291 Abs. 1 AEUV.[92] Entsprechend hat der Gesetzgeber auch im Kartellrecht reagiert, nachdem der BGH entschieden hat, dass § 30 OWiG mit Blick auf Art. 103 Abs. 2 GG keine generelle Bußgeldverantwortung des Rechtsnachfol-

81 Neumann, Strafrechtliche Verantwortlichkeit von Verbänden – rechtstheoretische Prolegomena, in: Kempf/Lüderssen/Volk (Hrsg.), Unternehmensstrafrecht, 2012, S. 13 (19); Vogel, Umfang und Grenzen der strafrechtlichen. Geschäftsherrenhaftung, StV 427 (429); das gilt insbesondere, da die moderne Strafrechtswissenschaft nicht mehr davon ausgeht, Zweck der Strafe sei der Ausgleich von Schuld (sog. Vergeltungstheorie); vielmehr dient Strafe der Verhinderung zukünftiger Taten (sog. relative Straftheorien); Schuld legitimiert Strafe daher nicht mehr, sondern ist Bedingung für ein faires Strafrecht.

82 Hierzu auch KK-Rogall, § 30 OWiG Rn. 2 ff.

83 Ost/Kallaß/Roesen, Einführung einer Unternehmensverantwortlichkeit im deutschen Kartellsanktionenrecht – Anmerkungen zum Entwurf der 9. GWB Novelle, NZKart 2916, 447 (456).

84 Dannecker/Dannecker, Europäische und verfassungsrechtliche Vorgaben für das materielle und formelle Unternehmensstrafrecht, NZWiSt 2016, 162 (175).

85 Mit Blick auf den letztgenannten Punkt so auch Ost/Kallaß/Roesen, Einführung einer Unternehmensverantwortlichkeit im deutschen Kartellsanktionenrecht – Anmerkungen zum Entwurf der 9. GWB Novelle, NZKart 2916, 447(457).

86 LG Berlin, Urt. v. 18.02.2021 – 526 OWi LG, 212 Js-OWi 1/20 (1/20), Rn. 26 f.; Venn/Wybitul, Die bußgeldrechtliche Haftung von Unternehmen nach Art. 83 DS-GVO, NStZ 2021, 204 (208); a.A. Ebner/Schmidt, Verhängung von Bußgeldern nach Art. 83 DS-GVO gegen deutsche Muttergesellschaften – Eine Praxisbetrachtung, CCZ 2020, 84 (87).

87 So ausdrücklich BGH, Beschl. v. 16.12.2014 – KRB 47/14, Rn. 19 f.

88 LG Berlin, Urt. v. 18.02.2021 – 526 OWi LG, 212 Js-OWi 1/20 (1/20), Rn. 26 f.

89 HK DS-GVO/BDSG-Schwartmann/Burkhardt, § 41 BDSG (im Anh. zu Art. 83 DS-GVO) Rn. 3.

90 Das hat der BGH für den kartellrechtlichen Art. 5 Abs. 1 1 VO (EG) Nr. 1/2003 abgelehnt. Dieser enthält jedoch anders als Art. 83 DS-GVO gar keine eigenständige Rechtsgrundlage nationaler Behörden gegenüber Bürgern, sondern entfalten. Wirkung nur zwischen der Union und den Mitgliedstaaten; vgl. BGH, Beschl. v. 16.12.2014 – KRB 47/14, Rn. 26 ff.

91 KG Berlin, Beschl. vom 06.12.2021 – 3 Ws 250/21, Rn. 27; hierzu auch Schwarze/Bechtold, Rechtsstaatliche Defizite im Kartellrecht der Europäischen Gemeinschaft, 2008, S. 15 ff.

92 HK DS-GVO/BDSG-Schwartmann/Burkhardt, § 41 BDSG (im Anh. zu Art. 83 DS-GVO) Rn. 1 ff.

gern im Sinne des Unionsrechts begründen kann. Er hat § 30 Abs. 2 a OWiG eingeführt,[93] der später durch § 81 Abs. 3 b GWB ergänzt wurde.[94]

V. Fazit

Mit dem deutschen Rechtsträgerprinzip auf der einen Seite und dem auf supranationaler Ebene vornehmlich zugrunde gelegten Funktionsträgerprinzip auf der anderen Seite stehen sich zwei grundlegend unterschiedliche Haftungsmodelle gegenüber. Wahrscheinlich deshalb geht die Diskussion um die Verbandshaftung in ihrer Pauschalität häufig fehl. Die Auslegung und Anwendung des Art. 83 DS-GVO folgt nicht etwa dem Prinzip „ganz oder gar nicht". Die einzelnen Aspekte der Unternehmenshaftung können und müssen vielmehr differenziert betrachtet werden. „Mischmodelle", die die Haftung nach dem Rechtsträgerprinzip an Grundkonzepte und Begrifflichkeiten des Funktionsträgerprinzips angepasst haben, gibt es bereits, etwa im nationalen Kartellsanktionsrecht.[95] Vergleichbares ist auch im Datenschutzrecht vorstellbar. Konstitutionell ausgeschlossen ist in diesem Kontext wahrscheinlich wenig, Grenze ist wie üblich das Übermaßverbot. Die Frage nach der datenschutzrechtlichen Verbandshaftung ist europarechtlich hochpolitisch und eine Entscheidung für das Funktionsträgerprinzip würde eine Abkehr vom Schuldprinzip in seiner bisherigen Form bedeuten. Deutschland wählt mit seinem Rechtsträgerprinzip im europäischen Vergleich einen eigenen Weg. Die Streitfrage stellt sich daher in kaum einem anderen Land in gleicher Weise.

Klar scheint: So einfach, wie es sich der EDSA und einige Stimmen in der Literatur machen, ist es nicht, vertretbar ist Vieles. Vor diesem Hintergrund ist die Positionierung des EDSA, die versucht das Funktionsträgerprinzip im Wege der Verwaltungspraxis vor der Entscheidung des EuGH zu etablieren, rechtlich fragwürdig und datenschutzpolitisch übergriffig. Entscheidend für die Wirtschaft ist es, nun Ruhe zu bewahren. Der nächst Schritt ist die anstehende Auslegung durch den EuGH.

Hält der EuGH den hiesigen Weg für europarechtswidrig, ist es denkbar, dass er Deutschland „nur" ein Umsetzungsdefizit attestiert, ohne zugleich die Anwednung des Funktionsträgerprinzips anzuordnen. Dann würde er zwar nicht davon ausgehen, dass die DS-GVO selbst eine unmittelbare Unternehmenshaftung nach dem Vorbild des europäischen Kartellrechts normiere. Es wäre aber möglich, dass die Umsetzung durch Deutschland wegen der hierdurch bedingten Verfahrenshindernisse als Verstoß gegen den Effektivitätsgrundsatz gewertet würde.

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

Lucia Burkhardt
Wissenschaftliche Mitarbeiterin an der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln.
Foto: TH Köln/Schmülgen

93 Durch das 8. Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen v. 26.06.2013 (BGBl. I S. 1738) eingeführt (8. GWB-Novelle).

94 Eingeführt durch die 9. GWB-Novelle; hierzu Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (91 f.)

95 Hierzu ausführlich Dannecker, Zur bußgeldrechtlichen Verantwortung der Unternehmen in der Europäischen Union, NZWiSt 2022, 85 (90 ff.); Ost/Kallaß/Roesen, Einführung einer Unternehmensverantwortlichkeit im deutschen Kartellsanktionenrecht – Anmerkungen zum Entwurf der 9. GWB Novelle, NZKart 2916, 447; pointiert auch BeckOK Kartellrecht-Heinichen, § 81 a GWB Rn. 24 ff.

Prof. Dr. Boris P. Paal, M.Jur./Matthias Götz, LL.M.

GPS-Daten und Datenschutzrecht Aktuelle Fragestellungen mit einem Fokus auf den Automobilsektor

Der vorliegende Beitrag geht der Frage nach, ob und unter welchen Voraussetzungen GPS-Daten als personenbezogene Daten im Sinne des maßgeblichen Datenschutzrechtsregimes, sprich der Datenschutz-Grundverordnung (DS-GVO – VO 2016/679), zu qualifizieren sind. Vor diesem Hintergrund wird vor allem die Befassung mit der Legaldefinition personenbezogener Daten aus Art. 4 Nr. 1 DS-GVO im Zentrum der Ausführungen stehen. Zudem wird der Fokus auf Fragestellungen aus dem Automobilsektor gerichtet, da es sich hierbei um einen in der Praxis besonders bedeutsamen Anwendungsbereich von GPS-Daten handelt. Zunächst widmet sich der Beitrag jedoch einer näheren Bestimmung des Betrachtungsgegenstands „GPS-Daten" (I.), bevor sodann der Begriff „personenbezogene Daten" einer genaueren Untersuchung unterzogen wird (II.). Die hieraus gewonnenen Erkenntnisse bilden die Grundlage für die anschließende Beschäftigung mit GPS-Daten im Automobilkontext (III.). Zum Abschluss werden die Untersuchungsergebnisse mit praktischen Anwendungsszenarien (IV.) angereichert sowie ein zusammenfassendes Fazit (V.) gezogen.

I. GPS-Daten als Betrachtungsgegenstand

Bei GPS-Daten handelt es sich um Informationen über Zielkoordinaten aus dem Global Positioning System (GPS), welches mithilfe zahlreicher Satelliten in der Erdumlaufbahn die Synchronisierung von Standort, Zeit und Geschwindigkeit bzw. Bewegung eines Empfangsgeräts ermöglicht. Diese Satelliten senden ihre Position und die aktuelle Zeit zum Empfangsgerät des GPS-Signals, durch Auswertung der verschiedenen Signale wird sodann die eigene Position berechnet. Im Automobilkontext stellen vor allem das Navigationsgerät (hier kann differenziert werden zwischen „klassischen" fest verbauten Navigationsgeräten und Apps)[1] oder GPS-Tracker solche Empfangsgeräte dar. Es stellt sich die Frage, wie GPS-Daten in den Gesamtkontext der unterschiedlichen Datenkategorien einzuordnen sind.

1. Datenkategorien

Im Ausgangspunkt ist im vorliegenden Kontext zwischen Identifikations- und Merkmalsdaten zu unterscheiden. Mithilfe von Identifikationsdaten ist grundsätzlich ohne Weiteres eine Identifizierung des Betroffenen möglich (z.B. durch ein Kennzeichen). Demgegenüber ist für Merkmalsdaten zur Beurteilung der Möglichkeiten einer Identifizierung zunächst eine Abgrenzung von Verhaltensdaten und Zustandsdaten vorzunehmen: Verhaltensdaten beziehen sich in erster Linie auf den Fahrer und seine Fahrzeugführung (z.B. Aufenthalts- oder Fortbewegungszeit und -ort). Zustandsdaten hingegen enthalten technische Angaben zum Fahrzeug (z.B. Software, Tankfüllung), wodurch zugleich ein verhaltensbezogener Rückschluss, etwa auf das Fahrverhalten, eröffnet sein kann.[2]

2. GPS-Daten als Geodaten

Bei GPS-Daten wird es sich zunächst vor allem um Geodaten handeln. Geodaten finden ihre Bestimmung in der Lokalisierung des Empfangsgeräts, womit sie als Zustandsdaten zu qualifizieren sind. Zudem können GPS-Daten jedoch auch Verhaltensdaten darstellen. So eröffnen GPS-Daten aus einem Fahrzeug etwa Rückschlüsse auf Lenk- und Ruhezeiten sowie auf die zurückgelegte Wegstrecke bzw. Route. Vielfach werden Geodaten und der Aufenthaltsort des Fahrers – auch und gerade im Automobilkontext – übereinstimmen, sodass es sich sowohl um Zustandsdaten als auch um Verhaltensdaten handeln kann.

II. Personenbezogene Daten nach Maßgabe von Art. 4 Nr. 1 DS-GVO

„Personenbezogene Daten" sind gem. Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Diese Legaldefinition bildet ein zentrales Element des Datenschutzrechts,[3] denn erst die Verarbeitung von personenbezogenen Daten eröffnet überhaupt den Anwendungsbereich der DS-GVO. Aufgrund der hervorgehobenen Bedeutung dieses Begriffes für den nach Art. 1 Abs. 1 DS-GVO angestrebten Schutz von natürlichen Personen wurde die Definition von personenbezogenen Daten in Art. 4 Nr. 1 DS-GVO gesetzgeberisch bewusst weit gefasst.[4]

1. Sachlicher Schutzumfang

Vom sachlichen Schutzumfang sind nur solche Informationen erfasst, die einen Bezug zu einer identifizierten oder identifizierbaren natürlichen Person aufweisen. Nach der Ansicht des EuGH ist der erforderliche Personenbezug einer

1 Siehe hierzu nachfolgend unter IV. 4.

2 Weichert, NZV 2017, 507 (509, 510).

3 Boehme-Neßler, DuD 2016, 419 (419); Hofmannn/Johannes, ZD 2017, 221 (222); Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 Rn. 1; Klar/Kühling, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl., 2020, Art. 4 Nr. 1 Rn. 1; Schwartmann/Mühlenbeck, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 2. Aufl., 2020, Art. 4 Rn. 9; Spindler/Dalby, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl., 2019, Art. 4 Rn. 2.

4 Art. 29-Datenschutzgruppe, WP 136, 2007, S. 4; Boehme-Neßler, DuD 2016, 419 (419); Klabunde, in: Ehmann/Selmayr, DS-GVO, 2. Aufl., 2018, Art. 4 Rn. 7.

Information gegeben, „wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist".[5] Im Fokus der Diskussion steht dabei die Frage, ob und unter welchen Voraussetzungen eine natürliche Person als identifiziert bzw. identifizierbar angesehen werden kann.

a) Identifiziert

Wann eine Person im Sinne von Art. 4 Nr. 1 DS-GVO „identifiziert" ist, wird in der DS-GVO nicht näher festgelegt. Von einer identifizierten Person ist auszugehen, wenn die Individualisierbarkeit der Person unmittelbar aus der Information selbst folgt. Diese Voraussetzung wird gegeben sein, wenn die Information ein Identifikationsmerkmal der Person beinhaltet oder wenn der Inhalt der Information bzw. der Kontext eine eindeutige Identifikation erlaubt, ohne dass auf weitere Informationen zurückgegriffen werden muss.[6] Die Person muss hierzu dergestalt aus einer bestimmten Gruppe hervorgehoben sein, dass sie sich eindeutig von anderen Individuen unterscheidet und somit bestimmt ist.[7] In der Regel wird der Name einer Person ausreichend dafür sein, dass diese identifiziert ist.[8]

b) Identifizierbar

Von hervorgehobener Bedeutung ist die Tatbestandsalternative der „Identifizierbarkeit", wo die Zuordnung eines Merkmals zu einer Person durch weitere Schritte und die Einholung anderer Informationen erreicht wird.[9] So sorgt das Vorhandensein einer dynamischen IP-Adresse gerade nicht bereits dafür, dass eine Person eindeutig identifiziert ist, da sich aus einer solchen dynamischen IP-Adresse nicht unmittelbar die Identität des Nutzers ableitet.[10] Als „identifizierbar" wird gem. Art. 4 Nr. 1 HS. 2 DS-GVO eine natürliche Person angesehen, „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen [sofern die Person nicht durch den Namen bereits identifiziert ist, siehe oben II. 1. a)], zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann." Die Identifizierbarkeit setzt somit voraus, dass die vorhandene Information erst mit weiteren Informationen verknüpft werden muss, um einen Personenbezug herstellen zu können.[11]

Die Frage nach der Auslegung des Begriffs der „Identifizierbarkeit" von natürlichen Personen beschäftigt die Rechtswissenschaft bereits seit der Einführung der der DS-GVO vorangegangenen Datenschutz-Richtlinie (95/46/EG).[12] Der Begriff bildet die äußerste Grenze der Definition des Art. 4 Nr. 1 DS-GVO, daher beeinflussen Auslegung und Verständnis dieses Merkmals im erheblichen Maße die Anwendbarkeit des unionalen Datenschutzrechtes im Einzelfall.

Nach ErwGr. 26 DS-GVO sind bei der Frage, ob eine Person identifizierbar ist, alle Mittel zu berücksichtigen, die von dem datenschutzrechtlich Verantwortlichen (legaldefiniert in Art. 4 Nr. 7 DS-GVO) oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Hieraus leitet sich vor allem die Frage ab, welche Mittel und welches Wissen Dritter sich der Verantwortliche zurechnen lassen muss.

c) Rechtsprechung des EuGH

Ob und inwieweit auch das Wissen und die Mittel anderer Personen als der des Verantwortlichen zu berücksichtigen sind, die diese zur Identifizierung einer Person verwenden können, ist noch nicht abschließend geklärt. Allerdings hat der EuGH in seiner hierzu maßgeblichen Entscheidung hinsichtlich des Personenbezuges von dynamischen IP-Adressen[13] wichtige Anhaltspunkte für die Beantwortung der aufgeworfenen Frage herausgearbeitet.

Im Wesentlichen führt der EuGH an, dass eine Zurechnung der Mittel und des Wissens Dritter (grundsätzlich) nicht zu erfolgen hat, wenn dies gesetzlich verboten oder praktisch nicht durchführbar wäre.[14] An der praktischen Durchführbarkeit fehlt es – im Einklang mit den nach ErwGr. 26 DS-GVO zu berücksichtigenden objektiven Faktoren –, wenn die Identifizierung einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft erfordern würde.[15] Dagegen soll der Rückgriff auf das Wissen und die Mittel eines Dritten nach allgemeinem Ermessen wahrscheinlich sein, wenn der Verantwortliche über rechtliche Mittel verfügt, um an die betreffenden Informationen des Dritten zu gelangen.[16] In diesem Zusammenhang muss beachtet werden, dass der EuGH nicht fordert, dass der Verantwortliche seine rechtlichen Mittel nutzt oder zum jetzigen Zeitpunkt nutzen kann. Daher ist es als ausreichend zu erachten, wenn der Verantwortliche potenziell die rechtlichen Möglichkeiten hat, die erforderlichen Informationen von dem Dritten zu erlangen.[17] Eine besondere Relevanz dieses

5 EuGH, NJW 2018, 767 Rn. 35 – Nowak/Data Protection Commissioner, wobei sich die Entscheidung noch auf die Vorgängervorschrift des Art. 2 Buchst. 1 DSRL bezieht, welcher inhaltlich unverändert in Art. 4 Nr. 1 DS-GVO übersetzt wurde.

6 Klar/Kühling, in: Kühling/Buchner, DS-GVO, Art. 4 Nr. 1 Rn. 18.

7 Arning/Rothkegel, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl., 2022, Art. 4 Rn. 24.

8 Arning/Rothkegel, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl., 2022, Art. 4 Rn. 24; Ziebarth, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl., 2018, Art. 4 Rn. 14.

9 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 Rn. 56.

10 EuGH, Urt. v. 19.10.2016 – C-582/14 NJW C-582/14, NJW 2016, 3759 Rn. 38.

11 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 Rn. 57; Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl., 2020, Art. 4 Nr. 1 Rn. 19; Schwartmann/Hermann, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 2. Aufl., 2020, Art. 4 Nr. 1 Rn. 33; Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 6. Aufl., 2018, Teil 2, Rn. 25.

12 U.a. Arning/Rothkegel, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl., 2022, Art. 4 Rn. 34; Buchholtz/Stenzel, in: Gierschmann/Schlender/Stenzel/Veil, DS-GVO, 2018, Art. 4, Nr. 1, Rn. 9; Specht/Müller-Riemenschneider, ZD 2014, 71 (72).

13 EuGH, Urt. v. 19.10.2016 – C-582/14 – Breyer.

14 EuGH, Urt. v. 19.10.2016 – C-582/14, Rn. 46.

15 EuGH, Urt. v. 19.10.2016 – C-582/14, Rn. 46.

16 EuGH, Urt. v. 19.10.2016 – C-582/14, Rn. 47.

17 EuGH, Urt. v. 19.10.2016 – C-582/14, Rn. 47.

EuGH-Urteils für die vorliegende Fragestellung hinsichtlich des Automobilkontextes ergibt sich daraus, dass unter bestimmten Umständen behördliche Auskünfte über Fahrzeughalter eingeholt und verwendet werden können, um zwischen dem jeweiligen Fahrzeugnutzer und den GPS-Daten eine Verknüpfung herzustellen.[18]

d) GPS-Nutzungsdatenüberwachung durch Datenerhebung bei Telemediendiensten

Ergänzend sei darauf hingewiesen, dass unlängst das OLG Frankfurt a.M. entschieden hat, der in 2021 neu geschaffene § 100k StPO erlaube einen umfassenden Abruf von GPS-Daten bei einem Fahrzeughersteller.[19] In dem zugrundeliegenden Sachverhalt war das Fahrzeug mit einem Dienst verbunden, der seitens des Herstellers zunächst kostenfrei und anschließend, jedenfalls hinsichtlich bestimmter (Teil-) Leistungen, gegen Zahlung überlassen wird. Durch diesen Dienst werden über eine festverbaute SIM-Karte zahlreiche Daten an einen Server übermittelt, wodurch wiederum vielfältige Funktionen eines Multi-Media-Systems ermöglicht werden, so etwa die Übermittlung des Fahrzeugstandorts an den Server und (auch) an ein von dem Nutzer bezeichnetes Mobiltelefon. Auf Antrag der Staatsanwaltschaft hat das LG Gießen den Fahrzeughersteller verpflichtet, Auskunft zu erteilen über sämtliche erhobenen und gespeicherten Verkehrsdaten unter Einschluss der vorhandenen und noch zu erhebenden GPS-Standortdaten für die näher individualisierten Anschlüsse des Fahrzeugs des Nutzers. Die dagegen von dem Fahrzeughersteller eingelegte Beschwerde vor dem OLG Frankfurt a.M. blieb erfolglos. Es wird kontrovers diskutiert, ob die von dem erkennenden Gericht vorgenommene weite Auslegung des Begriffs der „Nutzungsdaten" im Sinne von § 100k StPO in Verbindung mit § 2 Abs. 2 Nr. 3 Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) zutreffend ist.[20]

2. Abstrakte Einordnung von GPS-Daten

Tatbestandlich setzt Art. 4 Nr. 1 DS-GVO zunächst voraus, dass die betreffende Information (abstrakt) in Verbindung zu einer natürlichen Person gebracht werden kann.[21] Diese grundsätzliche Verbindbarkeit einer Information mit einer natürlichen Person kann sich sowohl aus persönlichen als auch aus sachlichen Angaben ergeben. Persönliche Angaben sind unmittelbar personenbezogen, so z.B. Name, Alter, Herkunft oder Gesundheitszustand einer Person.[22] Sachliche Angaben beziehen sich auf die Beziehung der Person zu ihrer Umwelt, sprich zu Sachen oder Dritten, so bspw. Angaben zum Umfeld, der finanziellen Situation (etwa Vermögen, Gehalt oder Kreditwürdigkeit), Vertragsbeziehungen, Freundschaften, Eigentumsverhältnisse, Konsum- oder Kommunikationsverhalten, Arbeitszeiten oder E-Mail-Adressen der betroffenen Person.[23]

Sachliche Angaben sind von den sog. Sachdaten abzugrenzen. Solche Sachdaten liegen vor, wenn sich die Informationen ausschließlich auf Gegenstände beziehen.[24] GPS-Daten liefern nur Informationen bezüglich des konkreten Standortes und der Bewegungen des Empfangsgerätes. Es ist allerdings zu berücksichtigen, dass Informationen, die sich (vordergründig) nur auf eine Sache beziehen, in Abhängigkeit von dem jeweiligen Gesamtkontext durchaus auch einen Bezug zu einer natürlichen Person aufweisen können.[25] Der Umstand, dass es sich bei GPS-Daten zunächst um Sachdaten handelt, schließt somit nicht aus, dass GPS-Daten im Automobilkontext als personenbezogene Daten qualifiziert werden können. Bevor im Folgenden diese Fragestellung vertieft adressiert wird, ist zunächst daran zu erinnern, dass GPS-Daten – auch und gerade im Automobilkontext – Zustands- und / oder Verhaltensdaten darstellen können.[26]

III. GPS-Daten als personenbezogene Daten im Automobilkontext

Auf der Grundlage und am Maßstab der herausgearbeiteten Kriterien ist nachfolgend zu untersuchen, ob und unter welchen Voraussetzungen GPS-Daten im Automobilkontext als personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO einzuordnen sind.

1. GPS-Daten für sich genommen / ohne weitere Informationsverknüpfung

Die aus der GPS-Satellitenortung gewonnenen Daten beziehen sich im Ausgangspunkt gerade nicht unmittelbar auf eine Person, sondern geben für sich genommen als Zustands- und Verhaltensdaten [27] zunächst lediglich Aufschluss über den Standort eines bestimmten Empfängermediums und den Aufenthaltsort einer Person, die dieses Empfängermedium benutzt und dadurch geortet wird (bspw. Ortung eines Smartphones über GPS oder Ortung von gestohlenen Fahrzeugen über eingebaute GPS-Tracker).[28] Die Person selbst wird dabei jedoch nicht identifiziert. Für sich genommenen stellen GPS-Daten somit keine personenbezogenen Daten dar.[29]

18 Hierzu vertieft nachfolgend unter III.2.

19 OLG Frankfurt a.M., Beschl. v. 20.07.2021 – 3 Ws 369/21, MMR 2022, 141.

20 Zu den hiermit verbundenen Fragestellungen Ruppert, StV Spezial 2022, 66.

21 Arning/Rothkegel, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl., 2022, Art. 4 Rn. 10.

22 Ernst, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 4 Rn. 14.

23 Ernst, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 4 Rn. 14.

24 Arning/Rothkegel, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl., 2022, Art. 4 Rn. 10; Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl., 2020, Art. 4 Nr. 1 Rn. 12. So auch Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl., 2019, Teil XIV, Rn. 185; Weisser/Färber, MMR 2015, 506 (508).

25 Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl., 2020, Art. 4 Nr. 1 Rn. 14; Arning/Rothkegel, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl., 2022, Art. 4 Rn. 12.

26 Siehe hierzu vorstehend unter I. 2.

27 Siehe für das Verhältnis von Zustands- zu Verhaltensdaten bei GPS-Daten vorstehend unter I.

28 BGH, NJW 2013, 2530 (2532, Rn. 38 f.); Thüsing, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 12 Rn. 16.

29 So etwa auch zur alten (aber insoweit übertragbaren) Rechtslage BGH, Urt. v. 04.06.2013 – 1 StR 32/13, NJW 2013, 2530 (2532) Rn. 38.

2. Herstellung des Personenbezuges bei GPS-Daten

Wie vorstehend herausgearbeitet wurde, genügt für die Eröffnung des Anwendungsbereichs von Art. 4 Nr. 1 DS-GVO bereits die Identifizierbarkeit einer Person. Ein unmittelbarer Personenbezug der Daten ist somit gerade nicht erforderlich.[30] Grundsätzlich könnten somit zwar sämtliche verfügbaren Informationen zur Identifizierbarkeit einer Person herangezogen werden; es ist dabei aber anerkanntermaßen auch der dafür nötige Aufwand einzubeziehen.[31] Für die Frage, ob GPS-Daten personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO darstellen, kommt es somit maßgeblich darauf an, ob die GPS-Daten des genutzten Empfangsgerätes durch die Verknüpfung mit weiteren Informationen einer identifizierbaren natürlichen Person zugeordnet werden können. Diese Frage ist in Abhängigkeit von dem jeweiligen Empfangsgerät anhand der konkreten Umstände des Einzelfalles zu beantworten.

Ausgangspunkt hierfür ist die Feststellung, dass Automobile über eine individuelle Fahrzeug-Identifikationsnummer (FIN) sowie über ein KFZ-Kennzeichen verfügen müssen.[32] Bei der FIN und dem Kennzeichen handelt es sich jeweils um Identifikationsmerkmale, denn dadurch können die Zulassungsbehörden oder das Kraftfahrt-Bundesamt das jeweilige Fahrzeug einem konkreten Halter zuordnen.[33] Hieraus folgt, dass es durch die Verknüpfung von GPS-Daten des Fahrzeuges mit dem KFZ-Kennzeichen oder der FIN grundsätzlich möglich ist, Bewegungsmuster des Halters zu erfassen. Soweit diese Verknüpfung im Einzelfall erfolgen kann, ist der Halter des Fahrzeugs identifizierbar, weshalb es sich in einem solchen Fall bei den GPS-Daten des Fahrzeugs um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO handelt.

Zur Beantwortung der Frage, ob die GPS-Daten einer identifizierbaren natürlichen Person im Einzelfall zugeordnet werden können, kommt es unter der Beachtung der vorbenannten Maßstäbe darauf an, ob die Verknüpfung der notwendigen Informationen mit einem verhältnismäßigen Aufwand möglich ist. Hierbei ist zu beachten, dass nach § 39 StVG grundsätzlich ein rechtlicher Anspruch gegen die Zulassungsbehörden auf Herausgabe der Halterdaten bestehen kann. Unter Berücksichtigung der dargestellten Vorgaben des EuGH sprechen somit gewichtige Argumente dafür, GPS-Daten in solchen Konstellationen grundsätzlich als personenbezogene Daten des Fahrzeughalters einzuordnen.[34] Allerdings dürfte es in der Praxis kaum vorkommen, dass ein nach § 39 StVG Anspruchsberechtigter auch Zugang zu den relevanten GPS-Daten hat.

Die Besonderheit bei GPS-Daten von Fahrzeugen besteht zudem darin, dass der Fahrzeughalter nicht notwendigerweise der Fahrzeugführer ist. Führt eine andere Person als der Fahrzeughalter das Automobil, so stellt sich die Frage, ob es sich bei diesen GPS-Daten ebenfalls um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO handelt.[35]

3. Personenbezogene Daten des Fahrzeughalters

Auch wenn der Fahrzeughalter nicht selbst das Fahrzeug führt, könnten die erfassten GPS-Daten für diesen personenbezogene Daten darstellen. Zur Begründung lässt sich anführen, dass die Information über den Aufenthaltsort des PKW eine Information ist, die sich auch auf den Fahrzeughalter beziehen lässt.[36] Der Umstand, dass diese Information möglicherweise keinen besonderen Aussagegehalt hat, spielt für die Legaldefinition des Art. 4 Nr. 1 DS-GVO keine Rolle.[37]

Darüber hinaus ist zu beachten, dass die Informationen im Rahmen des Art. 4 Nr. 1 DS-GVO nicht notwendigerweise zutreffend sein müssen.[38] Werden etwa die GPS-Daten unrichtigerweise als Bewegungen des Fahrzeughalters eingeordnet, so bleibt es dabei, dass es sich um Informationen handelt, die sich auf eine identifizierbare natürliche Person beziehen – und somit um personenbezogene Daten des Fahrzeughalters.[39]

4. Identifizierbarkeit des Fahrzeugführers

Komplexer stellt sich die Frage dar, ob die GPS-Daten personenbezogene Daten des Fahrzeugführers sind, wenn es sich bei dem Fahrer nicht zugleich auch um den Halter des Fahrzeugs handelt. Ein fremder Fahrer, d.h. ein Dritter, welchem das Fahrzeug zur Nutzung überlassen wurde, ist über die Fahrzeugzulassungsbehörde nicht ermittelbar. Weder die Zulassungsbehörde noch das Kraftfahrt-Bundesamt werden regelmäßig Kenntnis hinsichtlich der Identität des Fahrzeugführers haben.

Ob es sich vor diesem Hintergrund bei GPS-Daten um personenbezogene Daten des Fahrzeugführers handelt, kann somit nur im Einzelfall anhand der bereits beschriebenen Kriterien erfolgen. Gleichwohl lassen sich einige Leitlinien für die Untersuchung durch die Verantwortlichen aufstellen.

a) Identifizierung durch den Fahrzeughalter

Der Fahrzeughalter verfügt regelmäßig über das notwendige Wissen, um die GPS-Daten einer identifizierbaren natürli-

30 VG Lüneburg, Teilurt. v. 19.03.2019 – 4 A 12/19 – juris Rn. 29; so im Ergebnis zur alten Rechtslage auch LAG Baden-Württemberg, BeckRS 2009, 68144 Rn. 21; LG Lüneburg, NJW 2011, 2225 (2226); BGH NJW 2013, 2530 (2532) Rn. 35.

31 Ziebarth, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl., 2018, Art. 4 Rn. 21, 22.

32 Anbringung der FIN gemäß § 59 Abs. 1 Nr. 4 StVZO; Anbringung des Kennzeichens gemäß § 10 Abs. 5 FZV.

33 Von Bodung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 16 Rn. 12.

34 Vgl. von Bodung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 16 Rn. 13; Weichert, SVR 2014, 201 (206); Weisser/Färber, MMR 2015, 506 (508).

35 Diese Problematik aufgreifend von Bodung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 16 Rn. 13.

36 Von Bodung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 16 Rn. 13.

37 Ernst, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl., 2021, Art. 4 Rn. 3; Klar/Kühling, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl., 2020, Art. 4 Nr. 1 Rn. 9.

38 Eßer, in: Auernhammer, DS-GVO/BDSG, 7. Aufl., 2020, Art. 4 Rn. 11; Art. 29-Datenschutzgruppe, WP 136, 2007, S. 7; Schmitz, in: Moos/Schefzig/Arning, Die neue Datenschutz-Grundverordnung, Kap. 2, Rn. 40; Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl., 2020, Art. 4 Nr. 1 Rn. 8.

39 Von Bodung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 16, Rn. 13.

chen Person, sprich dem Fahrzeugführer, zuzuordnen. Aus der Sicht von Datenverarbeitenden stellt sich die Frage, ob diese sich das Wissen des Fahrzeughalters zurechnen lassen müssen. Dafür müsste der Zugriff auf dieses Wissen in Ansehung von ErwGr. 26 DS-GVO nach dem allgemeinen Ermessen wahrscheinlich sein. Unter Berücksichtigung der dargestellten EuGH-Entscheidung in der Rechtssache Breyer (C –582/14) wäre dies der Fall, wenn jedenfalls ein potenzieller Anspruch des Datenverarbeitenden gegen den Fahrzeughalter auf Auskunft bestehen würde. Ein derartiger Anspruch ist allerdings im deutschen Recht nicht vorgesehen.[40] Folglich muss im Einzelfall untersucht werden, ob der Rückgriff auf das Wissen des Fahrzeughalters nach allgemeinem Ermessen als wahrscheinlich anzusehen ist.

b) Identifizierbarkeit durch die Nutzungsdaten des Fahrzeugs

Bei der Nutzung von modernen Fahrzeugen werden nicht nur GPS-Daten erzeugt und verarbeitet, sondern auch eine Reihe von weiteren Nutzungsdaten des Fahrzeugführers, wie etwa bezüglich des Fahrverhaltens oder der Nutzung des Infotainment-Systems. Eine Identifizierbarkeit im Sinne von Art. 4 Nr. 1 DS-GVO mag sich somit aus dem Rückgriff auf derartige Daten oder deren Gesamtschau ergeben können, so z.B. in Ansehung des individuellen Nutzungsverhaltens betreffend Sitz- und sonstiger Fahrzeugeinstellungen bzw. -konfigurationen, verwendeter Playlists oder Mobilfunkdaten, wenn und soweit diese Daten mit den GPS-Daten zusammengeführt werden. Auch und gerade in dem bereits beschriebenen Szenario des Auseinanderfallens von Halter und Fahrer des Fahrzeugs kann der Rückgriff auf weitere Nutzungs- und Sachdaten zu einer Eingrenzung des Nutzerkreises (maßgeblich) beitragen. So werden Informationen über das Fahr-, Lenk- oder Bremsverhalten zu einer Unterscheidbarkeit der Autofahrer beitragen können, Nutzungsdaten über das Infotainment-System werden zudem Aufschluss über das Alter und die Interessen des Fahrers geben, gespeicherte Sitzeinstellungen erlauben Rückschlüsse auf die Größe und Physiognomie einer Person.

Selbst bei umfangreicher Datenlage dürften jedoch solche Konstellationen den Regelfall bilden, in denen bspw. bei ähnlichem Alter, Größe, Fahrverhalten, Musikgeschmack oder Bewegungsradius des Nutzerkreises eine Zuordnung zu einer bestimmten Person nicht zweifelsfrei vorgenommen werden kann. Die durch die Zusammenführung verschiedener Daten geschaffene (umfassende) Datenlage erlaubt grundsätzlich nur im Ausnahmefall einen belastbaren Rückschluss auf den Fahrer und damit den Nutzer des Empfangsgerätes sowie eine Zuordnung der GPS-Daten zu einer natürlichen Person. Ob GPS-Daten durch eine Verbindung mit weiteren Daten zu personenbezogenen Daten im Sinne des Art. 4 Nr. 1 DS-GVO werden, richtet sich somit maßgeblich nach den Umständen des Einzelfalls, weshalb gerade keine abstrakt-pauschale Aussage dahingehend getroffen werden kann. Insgesamt wird eine Identifizierbarkeit wegen der damit verbundenen tatsächlichen Schwierigkeiten und Fehleranfälligkeit somit allenfalls die Ausnahme darstellen. Dies gilt vor allem dann, wenn der relevante Datensatz die Daten betreffend KFZ-Kennzeichen oder FIN nicht beinhaltet (z.B. wenn diese aus dem Datensatz gelöscht wurden).

c) Besonderheit von Carsharing-Diensten

Carsharing-Dienste zeichnen sich dadurch aus, dass Fahrzeuge fortlaufend durch unterschiedliche Personen geführt werden. Die jeweiligen Nutzer registrieren sich vor jeder Fahrt mit ihrem zuvor angelegten Nutzerkonto. Hierdurch können die Carsharing-Anbieter die GPS-Daten mit dem jeweiligen Nutzer verknüpfen. In diesen Fällen wird es sich somit bei GPS-Daten regelmäßig um personenbezogene Daten des Fahrzeugführers handeln.[41]

IV. Weitere Anwendungsszenarien

Im Folgenden werden zur Veranschaulichung und Vertiefung weitere Anwendungsszenarien für GPS-Daten im Automobilkontext dargestellt und kurz beleuchtet.

1. Rasterfahndung

GPS-Daten können relevant werden im Rahmen von polizeilichen Rasterfahndungen. Hierbei handelt es sich um eine besondere (polizeiliche) Fahndungsmethode unter Nutzung der elektronischen Datenverarbeitung, wobei sich die Polizei von anderen öffentlichen oder privaten Stellen personenbezogene Daten übermitteln lässt, um einen automatisierten Abgleich (Rasterung) mit anderen Daten vorzunehmen. Durch den Abgleich soll eine Schnittmenge von Personen ermittelt werden, auf welche bestimmte, vorab festgelegte Merkmale zutreffen.[42] Für die Frage, ob und inwieweit die in diesem Rahmen verwendeten GPS-Daten als personenbezogen im Sinne von Art. 4 Nr. 1 DS-GVO einzuordnen sind, kann auf die obigen Ausführungen verwiesen werden. Somit muss auch hier auf den Einzelfall abgestellt werden, wobei maßgeblich ist, ob die Umstände eine (ggf. nachträgliche) Feststellung des Fahrers zulassen und damit die GPS-Daten einer bestimmbaren Person zugeordnet werden können.

2. Arbeitnehmerschutz

Im Verhältnis von Arbeitnehmer und Arbeitgeber kann der Einsatz von GPS-Systemen in Automobilen ebenfalls eine wichtige Rolle spielen. Durch die in der Regel in einem Navigationssystem oder GPS-Tracker eines Fahrzeugs als Empfangsgerät „gespeicherten" GPS-Daten besteht für den Arbeitgeber die Möglichkeit, sowohl die Arbeitszeiten und deren Einhaltung als auch die ausschließlich gewerbliche Nutzung des Fahrzeugs[43] durch die Arbeitnehmer zu kont-

40 Gegen die Herleitung eines solchen Anspruches aus § 242 BGB überzeugend Koschinka, SVR 2016, 206 (207 f.).

41 Von Bodung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 16, Rn. 13.

42 BVerfGE 115, 320 (321).

43 Sofern auch eine private Nutzung geduldet ist, besteht die Möglichkeit, die GPS-Geräte für solche (Privat-)Fahrten zu sperren, vgl. hierzu VG Lüneburg, Teilurt. v. 19.03.2019 – 4 A 12/19 – juris Rn. 36.

44 Byers, in: Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil B VII Nr. 2 lit. a Rn. 3.

rollieren.[44] Nach Maßgabe der herausgearbeiteten Grundsätze sind die in diesem Kontext verwendeten GPS-Daten als personenbezogen im Sinne von Art. 4 Nr. 1 DS-GVO zu qualifizieren, falls sich (ggf. nachträglich) ermitteln lässt, welcher Arbeitnehmer zu welchem Zeitpunkt mit welchem Fahrzeug unterwegs war, d.h. die entsprechenden GPS-Daten einem bestimmten Arbeitnehmer zugeordnet werden können und somit eine „Identifizierbarkeit" vorliegt, was wiederum einen entsprechenden Organisationsgrad des Arbeitgebers voraussetzt.[45]

3. Automatisches Notrufsystem eCall

Weiterhin sind sog. „eCalls" in den Blick zu nehmen, bei denen das Betriebssystem des Autos nach einem von Sensoren erfassten und erkannten Zusammenstoß oder Aufprall automatisch einen Notruf inklusive Standortdaten des Autos an die Notrufzentrale absetzt.[46] Hier stellt sich (erneut) die Frage, ob und inwieweit einzelne GPS-Daten als personenbezogen angesehen werden können.[47] Die Beantwortung dieser Frage wird vor allem auch davon abhängen, ob sich der Fahrer feststellen lässt. Jedenfalls aber werden in der beschriebenen Konstellation die GPS-Daten als personenbezogen im Hinblick auf den Halter zu qualifizieren sein.

4. Nutzung eines Smartphones bzw. einer App

Besonderheiten können sich bezüglich der Beurteilung von GPS-Daten ergeben, die im Rahmen der Nutzung eines Smartphones bzw. im Rahmen einer (Navigations-)App wie Google Maps erhoben werden. In derartigen Konstellationen kommt es ebenfalls entscheidend darauf an, ob es dem Hersteller des Smartphones und/oder dem Betreiber der jeweiligen App möglich ist, den Fahrzeuginsassen mit verhältnismäßigem Aufwand anhand der GPS-Daten zu identifizieren. Insbesondere bei einer Anmeldung zur Nutzung einer auf GPS-Daten zugreifenden App mit individualisierenden Informationen wie Name und/oder (E-Mail-)Adresse dürfte regelmäßig eine Identifizierbarkeit ohne Weiteres möglich sein, sodass in solchen Konstellationen personenbezogene Daten vorliegen werden.

V. Zusammenfassung

Zusammenfassend ist festzuhalten, dass GPS-Daten für sich genommen (noch) keine personenbezogenen Daten im Sinne von Art. 4 Nr. 1 DS-GVO darstellen. Zwar kann aus der Verbindung mit anderen Informationen ein Personenbezug im Sinne der DS-GVO erwachsen; ein hieraus abgeleiteter Personenbezug wird aber allenfalls ausnahmsweise in Betracht kommen. Insgesamt muss eine abstrakt-pauschale Beantwortung deshalb regelmäßig ausscheiden, die Beurteilung des Vorliegens eines Personenbezugs unter dem Kriterium der „Identifizierbarkeit" hat einzelfallbezogen stattzufinden. Im Automobilkontext wird es hierbei maßgeblich darauf ankommen, ob die Umstände eine (ggf. nachträgliche) Feststellung des Fahrers ermöglichen oder nicht; ohne einen belastbaren Rückgriff auf Kfz-Kennzeichen oder FIN wird diese Feststellung jedoch zumeist sehr schwierig sein.

Prof. Dr. Boris Paal
Inhaber des Lehrstuhls für Bürgerliches Recht und Informationsrecht, Daten- und Medienrecht sowie Direktor des Instituts für Medien- und Datenrecht sowie Digitalisierung der Universität Leipzig, Of Counsel der Kanzlei Nikol & Goetz

Mattias Götz, LL.M.
Rechtsanwalt und Solicitor (England & Wales). Als solcher berät er nationale und internationale Unternehmen zu sämtlichen Fragen des Datenschutzrechts. Er ist Partner der Rechtsanwaltskanzlei Nikol & Goetz

45 Diese Erwägungen mit einem Beispiel aus der Landwirtschaft veranschaulichend Vogel/Klaus, Zulässigkeit der Verarbeitung von GPS-Daten im Arbeitsverhältnis, in: Stich/Schumann/Beverungen/Gudergan/Jussen (Hrsg.), Digitale Dienstleistungsinnovationen, 2019, 393, 394 ff.

46 Lüdemann, ZD 2015, 247 (248).

47 So kritisch, aber offenlassend Leupold/Wiebe/Glossner/Eul, IT-Recht, Teil 10.2, Rn. 31.

Dinya Berwari, LL.M.

Google Analytics auf dem Prüfstand der DS-GVO – Grenzen, Risiken und Möglichkeiten

Anfang 2022 veröffentlichten sowohl die österreichische als auch die französische Datenschutzaufsicht Bewertungen zum Webanalysetool Google Analytics als Antworten auf die Beschwerden der gemeinnützigen Organisation noyb von Max Schrems und lassen darin kaum Platz für einen DS-GVO-konformen Einsatz von Google Analytics. Da sich die deutsche Datenschutzaufsicht nach den Beschwerden von noyb noch nicht offiziell zum Einsatz von Google Analytics geäußert hat, befasst sich dieser Beitrag mit den Lücken in der Bewertung der Behörden und legt dar, warum diese zu Undurchsichtigkeit für Verantwortliche in der EU führen. Die Einwilligung als Rechtsgrundlage bleibt als einzige Möglichkeit, die Datenverarbeitung in die USA als Drittland zu legitimieren.

I. Google Analytics als breit gefächertes Webanalysetool

Google Analytics ist ein Webanalysetool, welches verschiedene Funktionen für Webseitenbetreiber anbietet. Nicht nur die reine Reichweitenmessung, sondern auch tiefergehende Analysen und Auswertungen zu Webseitenbesuchern und ihrem Verhalten sind möglich.[1] Dies führt nicht nur dazu, dass das Verhalten von Webseitenbesuchern nachverfolgt werden kann. Webseitenbetreiber können auch die Wirksamkeit von Werbeanzeigen analysieren und optimieren.

II. Auswirkungen aus § 25 TTDSG

Google Analytics greift also auf Informationen aus dem Browser oder des Geräts des Webseitenbesuchers zu und verarbeitet diese weiter. An dieser Stelle findet das am 01.12.2021 in Kraft getretene Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) Anwendung. Das neue Stammgesetz regelt die Verarbeitung von Informationen auf Endeinrichtungen, bspw. von Cookies, und setzt damit die Richtlinie 2009/136/EG in nationales deutsches Recht um.[2] Nach § 25 Abs. 1 TTDSG ist ein Zugriff auf Informationen auf der Endeinrichtung des Endnutzers nur dann rechtmäßig, wenn der Endnutzer seine Einwilligung erteilt hat.[3] Für die Verwendung von Google Analytics durch Webseitenbetreiber bedeutet das, dass eine Einwilligung nach § 25 Abs. 1 TTDSG erforderlich ist, da Google Analytics entweder mit Tracking-Cookies arbeitet oder andere Tracking-Methoden wie das Device Fingerprinting verwendet.

III. Personenbezug unabhängig von der „Anonymisierung" der IP-Adresse

Während § 25 TTDSG nicht auf personenbezogene Daten begrenzt ist, ist für die Frage der Relevanz nach der DS-GVO relevant, inwieweit personenbezogene oder -beziehbare Daten durch Google Analytics verarbeitet werden.

Google bietet zwar eine Möglichkeit der IP-Anonymisierung, doch die IP-Adresse der Nutzer kommt erst in Klarform bei Google an, bevor sie dort alsbald anonymisiert wird.[4] Außerdem verarbeitet Google nicht nur die IP-Adresse des Webseitenbesuchers, sondern bspw. auch technische Daten zum Browser, Betriebssystem oder der genauen Zeiten des Besuchs, sodass ein Personenbezug unabhängig von der Aktivierung der IP-Anonymisierungsfunktion anzunehmen ist.

IV. Bisherige Bewertung in Deutschland

Dadurch, dass Google Analytics sehr viele, teilweise tiefgreifende Analysemöglichkeiten bietet, stand das Tool schon seit jeher im Fokus der Datenschutz Aufsichtsbehörden in Deutschland. Schon weitaus vor Inkrafttreten der DS-GVO wurde das Tool durch die Aufsichtsbehörden in Deutschland geprüft und bewertet.[5] In Deutschland wurde seit Inkrafttreten der DS-GVO sowohl durch eine Gerichtsentscheidung als auch durch die Stellungnahme einer Datenschutzaufsichtsbehörde die Ansicht vertreten, dass die Nutzung von Google Analytics auf Webseiten mit einer Einwilligung der Webseitenbesucher legitimierbar ist.

1. Rechtsprechung und Datenschutzbehörden bisher für Einwilligungslösung

Die ausschlaggebende Rechtsprechung nach Inkrafttreten der DS-GVO legte das Landgericht Dresden im Januar 2019.[6] Das Gericht entschied zugunsten des Klägers, dass die Weitergabe der IP-Adresse durch den Webseitenbetreiber an einen Dritten (Google) einen „unzulässige[n] Eingriff in das allgemeine Persönlichkeitsrecht des Klägers"[7] darstellte. Das LG Dresden stellt in seinem Urteil vor allem auf eine mögliche Einwilligung ab, die – nach damaliger Rechtslage – im Rahmen des § 13 Abs. 2 TMG eingeholt werden konnte. § 13 TMG wurde mittlerweile durch den bereits erwähnten § 25 TTDSG ersetzt, womit das LG Dresden im Ergebnis aber dennoch auf die Einwilligung nach dem Telemedienrecht verweist.

1 Weitere Informationen zu den detaillierten Funktionalitäten unter: https://marketingplatform.google.com/about/analytics/, aufgerufen am 08.07.2022.

2 Siehe hierzu: Taeger/Gabel/Ettig, 4. Aufl. 2022, TTDSG, Rn. 1-4.

3 Siehe hierzu: Taeger/Gabel/Ettig, 4. Aufl. 2022, TTDSG § 25.

4 Siehe hierzu: https://support.google.com/analytics/answer/2763052?hl=en, aufgerufen am 08.07.2022.

5 Siehe hierzu u.A. ZD-Aktuell 2011, 19; MMR-Aktuell 2011, 323860; ZD-Aktuell 2014, 03935.

6 LG Dresden, Urt. v. 11.01.2019 – 1a O 1582/18.

7 LG Dresden, Urt. v. 11.01.2019 – 1a O 1582/18, BeckRS 2019, 12930, Rn. 22.

Das Bayrische Landesamt für Datenschutzaufsicht (BayLDA) folgte im Tenor der Entscheidung des LG Dresden und veröffentliche im November 2019 eine Pressemitteilung zur Nutzung von Google Analytics.[8] Das BayLDA geht in dieser Pressemitteilung zwar davon aus, dass jede über die reine Reichweitenmessung hinausgehende Verarbeitung zur Erstellung eines Profils als Tracking verstanden wird und ein solches nur mit einer Einwilligung der Webseitenbesucher möglich ist. Im jüngsten von der Datenschutzkonferenz (DSK) veröffentlichten Papier aus Dezember 2021 wird jedoch darauf hingewiesen, dass selbst die „klassische" Reichweitenmessung nicht ohne Einwilligung funktioniere.[9] Dem Tenor der DSK folgend ist für Webanalysetools wie Google Analytics, die deutlich mehr als nur die reine Reichweitenmessung als Funktion anbieten, eine Einwilligung nach § 25 TTDSG erforderlich. Die DSK weicht nun also von der Richtung des BayLDA ab, nach der die Reichweitenmessung als solche nicht direkt einwilligungsbedürftig war.

V. Schrems II als neuer Maßstab der Bewertung von Transfer in Drittstaaten

Die datenschutzrechtliche Kritikalität von Tools wie Google Analytics, die von Unternehmen angeboten werden deren Mutterkonzern in Drittländern wie den USA sitzen, wurde im Juni 2020 durch den EuGH in der als „Schrems II" bekannten Entscheidung noch einmal in den Fokus gestellt.[10] Der EuGH kam in seiner Entscheidung zu dem Schluss, dass kein angemessenes Datenschutzniveau beim Transfer personenbezogener Daten in die USA gewährleistet werden könne, wenn Verantwortliche sich auf die Verarbeitungsgrundsätze des Privacy Shield beruhten. Insgesamt erklärte der EuGH den Privacy Shield-Beschluss der EU-Kommission für ungültig, da er unvereinbar mit Art. 45 Abs. 1 DS-GVO war.[11] Der EuGH bewertete auch die Standardvertragsklauseln (SVK) in ihrem damaligen Stand und kam zu dem Schluss, dass sie vertragliche Garantien darstellen, die den Vertragsparteien ermöglichen, durch einen vorgeschriebenen Vertrag ein angemessenes Schutzniveau herzustellen, das dann zumindest zwischen den vereinbarenden Parteien herrscht.[12]

VI. Nyob und die auf Schrems II folgenden Beschwerden

Wenige Monate nach der Entscheidung des EuGH zum Privacy Shield wurden durch die von Maximilian Schrems gegründete gemeinnützige Organisation NYOB 101 Beschwerden gegen europäische Unternehmen eingereicht.[13] Google Analytics spielt bei diesen Beschwerden eine zentrale Rolle, da es aus Sicht von NYOB eines der Tools ist, welches von einem der größten US-Unternehmen sehr stark bei europäischen Webseiten eingesetzt wird. Der Europäische Datenschutzausschuss richtete daraufhin zusammen mit dem BfDi in Deutschland eine Task Force ein, um die Beschwerden durch NYOB schnell und möglichst einheitlich zu bearbeiten.[14]

Obwohl die zahlreichen Beschwerden einen Stand widerspiegeln, der sich im Laufe des Jahres 2021 maßgeblich geändert hat – allen voran nämlich durch die Veröffentlichung der neuen Standardvertragsklauseln – sorgte sowohl die österreichische als auch die französische Datenschutzaufsichtsbehörde Anfang des Jahres für großes Aufsehen mit ihren Bewertungen von Google Analytics.

VII. Aktuelle Bewertungen europäischer Datenschutzaufsichtsbehörden

Die Beschwerden durch nyob führen seit Januar 2022 schon zu mehreren Bewertungen von Google Analytics durch die Aufsichtsbehörden. Bedingt durch eben diese zahlreichen Beschwerden ist abzusehen, dass weitere Bewertungen durch nationale Aufsichtsbehörden folgen werden. Zwar haben einige Aufsichtsbehörden wie die spanische oder luxemburgische die Beschwerden fallen gelassen, weil die entsprechenden Webseiten Google Analytics nicht mehr einsetzen.[15] Jedoch müssen die Bewertungen durch die österreichische Datenschutzbehörde sowie der französischen CNIL an dieser Stelle detaillierter betrachtet werden, um die Argumentationslogik und die Lücken darin zu verstehen.

1. Österreichische Datenschutzbehörde

Am 22.12.2021 veröffentlichte die österreichische Datenschutzbehörde einen Bescheid als Antwort auf eine der Beschwerden durch NYOB. Die Behörde kam zu dem Ergebnis, dass der Einsatz von Google Analytics nach dem Schrems II-Urteil des EuGH nur mit den Standardvertragsklauseln als Basis nicht zulässig ist.[16] Die Entscheidung des EuGH zum Privacy Shield und die Zugriffsmöglichkeiten durch US-amerikanische Behörden wurden den Überlegungen zum generellen Einsatz von Google Analytics zugrunde gelegt. Die österreichische Behörde bewertete für ihren Bescheid die Standardvertragsklauseln in ihrem damals gültigen Stand und stellte fest, dass der alleinige Abschluss der SVK nicht ausreichend ist, um ein angemessenes Datenschutzniveau nach Art. 44 DS-GVO herzustellen. Sie betont zwar, dass der EuGH in der Rs. Schrems II die SVK für gültig erklärt hat, aber gleichzeitig auch, dass diese dennoch nur Verträge sind und damit Behörden in Drittländer nicht binden können. Zwar geht die österreichische Behörde davon aus, dass der EuGH zusätzliche Maßnahmen zu den SVK als Option darstellt, ein angemessenes Datenschutzniveau herzustellen. Jedoch werden die zusätzlichen Maßnahmen durch Google als unzureichend bewertet. Selbst die Aussage von Google, dass jede Datenzugriffsanfrage durch US-Behörden geprüft werde, stelle keine effektive Maßnahme dar, da die

8 Vgl. Bayrisches Landesamt für Datenschutzaufsicht, „Google Analytics nur mit Einwilligung", Pressemitteilung vom 15.11.2019.

9 DSK, „OH Telemedien 2021", S. 25.

10 Vgl. EuGH (Große Kammer), Slg. 2020 – C-311/18.

11 Vgl. EuGH (Große Kammer), Slg. 2020 – C-311/18, Rn. 199.

12 Vgl. EuGH (Große Kammer), Slg. 2020 – C-311/18, Rn. 132 ff.

13 Vgl. https://noyb.eu/de/101-beschwerden-zu-eu-us-transfers-eingereicht, aufgerufen am 08.07.2022.

14 Siehe hierzu: BfDI/EDSA: Task Force zu Beschwerden gegen Nutzung von Google- und Facebook-Services, ZD-Aktuell 2020, 07288.

15 Vgl. https://noyb.eu/en/update-noybs-101-complaints-austrian-dpa-rejects-risk-based-approach-data-transfers-third-countries, aufgerufen am 08.07.2022.

16 Vgl. ÖDSB, Teilbescheid v. 22.12.2021 – D155.027, 2021-0.586.257.

Zugriffe auf personenbezogene Daten durch Drittstaaten dennoch gegen Art. 8 GRCh verstoßen.

Eine andere Rechtsgrundlage als die SVK, wie bspw. die Einwilligung nach Art. 49 DS-GVO, wurde durch die österreichische Datenschutzbehörde nicht geprüft, da in dem ihr vorliegenden Fall auch keine Einwilligung auf der Webseite eingeholt wurde.

2. Französische Aufsichtsbehörde CNIL

Die französische Aufsichtsbehörde CNIL folgte am 10.02.2022 mit einer Stellungnahme, die ebenfalls zum Ergebnis hatte, dass der Einsatz von Google Analytics nicht datenschutzkonform sei, und forderte Webseitenbetreiber in Frankreich dazu auf, die Nutzung des Google Analytics-Dienstes unter den gegebenen Umständen einzustellen.[17] Laut der CNIL ist der Datentransfer in die USA nicht ausreichend geregelt und könnte nur dann erfolgen, wenn Google geeignete Maßnahmen ergreift, um ein sicheres Datenschutzniveau herzustellen. Google habe laut der CNIL zwar zusätzliche Maßnahmen zu den SVK getroffen, diese seien aber unzureichend. Sie folgen dem Tenor der österreichischen Datenschutzbehörde und weisen darauf hin, dass der Zugriff US-amerikanischer Geheimdienste auf die übermittelten Daten nicht ausgeschlossen werden kann. Damit sei die Einhaltung der Art. 44 ff. DS-GVO nicht sichergestellt.

3. Europäische Datenschutzbehörde – EDSB

Nicht nur die Datenschutzaufsichtsbehörden der Länder erhielten Beschwerden durch NOYB, auch auf EU-Ebene wurden Beschwerden platziert. Im Fall der EDSB gab es schon im Oktober 2020 Beschwerden von Betroffenen aus dem EU-Parlament an die EDSB, die dann im Januar 2021 von NOYB wiederholt und mit neuen Argumenten hinterlegt wurden.

Das EU-Parlament bot aufgrund der COVID-19 Pandemie eine Webseite an, über der sich Parlamentsmitglieder und Mitarbeiter für PCR-Tests anmelden konnten. Einige Betroffene führten einen Scan durch und stellten fest, dass Cookies von u.a. Google Analytics verwendet wurden, ohne dass hierüber informiert wurde.[18] In seiner Bewertung kam die EDSB zu dem Ergebnis, dass das EU-Parlament in seinem Cookie-Banner auf der Webseite nicht ausreichend über die Datenverarbeitung durch Google Analytics informiert hatte und demnach die Betroffenen nicht gem. der Richtlinie 2009/136/EG zur Verarbeitung ihrer personenbezogenen Daten einwilligen konnten.

VIII. Kritische Auseinandersetzung mit bisherigen Entscheidungen der Datenschutzbehörden in Europa

Die bisherigen Bewertungen der Datenschutzaufsichtsbehörden in der EU schaffen keine Rechtssicherheit in mehreren Aspekten, begonnen bei Google Analytics als spezifisches Tool, bis hin zum Datentransfer in Drittstaaten nach Art. 44 ff. DS-GVO. Betrachtet man die Bewertungen inhaltlich, entstehen einige Kritikpunkte, die näher aufgegriffen werden müssen.

1. Zu eng gefasste Betrachtung der österreichischen Datenschutzbehörde

Die Bewertung der österreichischen Datenschutzbehörde bezieht sich auf einen speziellen Fall und stellt gar nicht auf eine allgemeine Bewertung des Tools ab. Dies könnte man aufgrund der üblichen juristischen Strahlkraft rechtlicher Einschätzungen durch Behörden außer Acht lassen, wenn die gegebenen Umstände des österreichischen Falles nicht ausschlaggebend dafür wären, dass die Bewertung als solche hinterfragt werden muss. Obwohl die österreichische Bewertung viele Kritikfelder öffnet, sollen an dieser Stelle zwei prägnante genannt werden. Die österreichische Datenschutzbehörde legt fest, dass der Einsatz der Anonymisierungsfunktion von Google Analytics keine Rolle spielt, weil der Zugriff von Google auf die Daten des Webseitenbesuchers sowieso anzunehmen ist, da er einen Account bei Google hat. Es ist also darauf hinzuweisen, dass Österreich einen zu hohen Eingriff in die Persönlichkeitsrechte des Betroffenen sieht, wenn auf einer von ihm besuchten Webseite personenbeziehbare Daten zum Gerät, Browser usw. in die USA transferiert werden. Dass der betroffene Webseitenbesucher ein freiwillig erstelltes Google Konto besitzt (über das im Übrigen weitaus mehr und „interessantere" Daten von Google verarbeitet werden) spielt bei der Bewertung des Gesamtrisikos keine Rolle. Fraglich ist daher eher, ob die Datenschutzbehörde in Österreich nicht hätte empfehlen sollen, überhaupt keine Benutzerkonten bei Google zu erstellen.

Zudem bewertete Österreich die Webseite und den Einsatz von Google Analytics zu einem Zeitpunkt, zu dem noch die Google Inc. Vertragspartner des Webseitenbetreibers war. Dies hat sich mittlerweile geändert, denn Google Ireland ist Vertragspartner und damit Datenexporteur an die Muttergesellschaft in den USA. Sollte es keine Rolle spielen, dass der Verantwortliche in der ersten Kette der Verarbeitung mit einem EU-ansässigen Unternehmen arbeitet, weil davon ausgegangen wird, dass ein Transfer von Daten durch diese Entität in der EU in die USA erfolgt, stellt sich die Frage, ob Verantwortliche sowieso immer von einem Drittstaatentransfer ausgehen müssen, wenn Subunternehmer (egal ob Muttergesellschaft oder nicht) des europäischen Vertragspartners in Drittländern sitzen. Hierbei geht Österreich davon aus, dass die US-behördlichen Gesetze es erlauben, unabhängig vom Standort auf personenbezogene Daten zuzugreifen. Jedoch führt eine solche Annahme auch dazu, dass fraglich ist, ob Verantwortliche in der EU überhaupt mit Unternehmen arbeiten können, die eine Muttergesellschaft in den USA haben.

2. Einzelne Tools statt das Große und Ganze im Fokus der Behörden

Doch auch wenn die Bewertungen der nationalen Datenschutzbehörden auf einzelnen Beschwerden durch NYOB be-

17 Vgl. https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply, aufgerufen am 08.07.2022.

18 Vgl. https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf, aufgerufen am 08.07.2022.

ruhen, bleibt die Frage im Raum, weswegen eine Taskforce eingerichtet wurde, wenn diese nicht dazu führt, dass Google Analytics EU-weit, bspw. durch den EDSA, bewertet wird? Während also Unternehmen in Österreich nicht wissen, ob Google Analytics durch eine Einwilligung rechtskonform einsetzbar wäre, bejaht der EDSB dies in seiner Stellungnahme, während die dritte Datenschutzaufsicht in Frankreich eine technische Lösung anbietet.[19] Die nicht in letzter Konsequenz verfolgte Einheitlichkeit in der detaillierten Bewertung der Behörden wird dadurch verstärkt, dass viele Verantwortliche Webseitenbetreiber vor die Entscheidung gestellt werden, ob denn nun nur Google Analytics nicht erlaubt ist, oder nicht doch alle Produkte, die Google und andere große Cloud-Anbieter in Europa anbieten. Die Behörden verbindet bisher eine Ansicht: Google erlaubt den Datentransfer in die USA und (damit auch) Datenzugriff durch US-amerikanische Behörden und kann daher nicht DS-GVO-konform eingesetzt werden. Demnach müssten aber alle Tools der Google Cloud Plattform nicht datenschutzkonform einsetzbar sein, also auch bspw. Google Firebase, Google ReCaptcha oder Google Maps.

3. Ein hohes Risiko durch Zugriff von US-Sicherheitsbehörden?

Eines der einschlägigsten Argumente der bisherigen behördlichen Aussagen zu Google Analytics sind die potenziellen Zugriffe von Behörden und Geheimdiensten in den USA auf personenbezogene Daten von Europäern. Grundlage ist die Schrems II-Entscheidung des EuGH, die genau diesen Zugriff als Verstoß gegen Art. 8 GRCh sieht und das EU-US-Privacy Shield als nicht geeignet eingestuft hat, ein dennoch angemessenes Datenschutzniveau herzustellen. Doch welches Risiko ein möglicher Zugriff einer US-Behörde auf pseudonymisierte Daten zur Webseitennutzung birgt, ist fraglich. Die Bewertung aus Österreich weist auf einen nicht zu vernachlässigenden Fakt hin, nämlich dass viele private Nutzer einen Account bei Google haben und Webseiten besuchen, während sie in mit diesem Konto eingeloggt sind. Es fehlt eine stringente Logik in der Bewertung des Risikos für die informationelle Selbstbestimmung des Einzelnen, wenn man von registrierten Nutzern ausgeht, von denen es mehrere Millionen gibt. Da US-Gesetze wie FISA 702 für eine Mehrheit US-ansässiger Unternehmen gilt, kann angezweifelt werden, ob der Fokus von Behördenanfragen auf Geräteinformationen ist, die entschlüsselt werden müssten, oder der sonstige digitale Fingerabdruck eines Internetnutzers nicht interessanter ist.[20]

4. Abschwächung der neuen Standardvertragsklauseln

Zwar wurden die SVK im Schrems II-Urteil des EuGH nicht für nichtig erklärt, jedoch sah der EuGH zusätzliche, nicht weiter definierte Maßnahmen für notwendig an, um den Datentransfer tatsächlich legitim zu gestalten. Die SVK wurden dann rund ein Jahr später, im Juni 2021, in einer neuen Version von der EU-Kommission verabschiedet. In den neuen Klauseln 14 und 15 der SVK wird nun festgelegt, dass ein sogenanntes Transfer Impact Assessment (TIA), dem Grunde nach eine Bewertung des Risikos des Datentransfers, durchgeführt und dokumentiert werden muss. Bestimmte Aspekte der Bewertung des Schutzniveaus sind zwar in Klausel 14 lit. b genannt, jedoch sind sie in ihrem Detailgrad sehr grob gehalten. Der EDSA veröffentlichte zwar ein Papier zur weiteren Hilfe bei Erstellung des TIA,[21] doch im Ergebnis obliegt es einem gewissenhaften TIA durch den Datenexporteur, um zu entscheiden, dass der Datentransfer kein Risiko birgt. Österreich hatte für seinen Bescheid nur die alte Version der SVK geprüft, aber auch zu einem risikobasierten Ansatz äußerte sich die Behörde kritisch und verwarf diesen.[22] Die CNIL stellte auch in ihrer Bewertung fest, dass die zusätzlich von Google dokumentierten Maßnahmen für einen sicheren Datentransfer nicht ausreichend seien. Wenn aber der durch die neuen SVK versuchte Ansatz, auf Beanstandung des EuGH hin den Drittstaatentransfer mit zusätzlichen Maßnahmen zu legitimieren, offensichtlich nicht ausreicht, stellt sich mitunter die Frage, warum die neuen SVK überhaupt entwickelt wurden.

Datenexporteure müssen die neuen SCCs bis zum 28.12.2022 umgesetzt haben, inklusive der TIA für jeden Datentransfer. Die Frage ist aber, welche Sicherheiten überhaupt gegeben sind, dass die durchgeführten Risikobewertungen einer Prüfung der Behörden standhalten würden. Klausel 15 der SVK gibt zwar zusätzlich vor, dass sich der Datenimporteur an bestimmte Regelungen zu halten hat, wenn Behörden aus dem Drittstaat einen Zugriff anfragen.

Die Behörden halten aber das auch nicht für ausreichend, womit die neuen SVK keine Rechtssicherheit für Datenexporteure darstellen.

5. Politisch geprägter Konflikt

Der Blick auf die bisherigen Bewertungen der Datenschutzbehörden macht erkenntlich, dass die einzige Lösung, wie Google – genauso wie alle anderen Unternehmen in Drittländern, DS-GVO-konform werden kann – ein Verstoß gegen nationale Gesetze in den USA ist. Kann es dann überhaupt Fälle geben, in denen ein Datentransfer in die USA überhaupt DS-GVO-konform möglich ist? Folgerichtig müsste man dies hier verneinen. Denn wenn selbst die Einhaltung der neuen SVK sowie die weiteren von Google getroffenen Maßnahmen nicht ausreichend sind, ist anzuzweifeln, ob überhaupt ein anderes US-amerikanisch-ansässiges Unternehmen Lösungen anbieten könnte, die europäische Datenschutzbehörden als ausreichend bewerten würden.

Microsoft geht sogar so weit, jede behördliche Anfrage anzufechten – soweit juristisch möglich – und Betroffenen

19 Vgl. dazu näher: Votteler, CNIL: Handreichung zur datenschutzkonformen Verwendung von Google Analytics und ähnlichen Analysetools, ZD-Aktuell 2022, 01217.

20 Im Detail zu den Behördenzugriffen mit Fokus auf FISA 702 siehe: Vladeck, Stephen, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, DSK.

21 Siehe https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf, aufgerufen am 08.07.2022.

22 Siehe https://noyb.eu/de/oesterreichische-behoerde-lehnt-risikobasierten-ansatz-fuer-datenuebermittlungen-drittlaender-ab, aufgerufen am 08.07.2022.

finanzielle Entschädigungen anzubieten.[23] Ob dies einer Prüfung durch europäische Datenschutzbehörden als ausreichend angesehen werden würde, ist allerdings nach aktueller Lage fraglich.

Es wird zwar aktuell an einem neuen Abkommen zwischen den USA und der EU gearbeitet.[24] Inwieweit dieses neue Abkommen jedoch die vom EuGH festgestellten Mängel des Schutzniveaus bei Datentransfer in die USA adressiert, ist zum aktuellen Zeitpunkt nicht abzusehen. Ebenso wenig, wie lange ein solches Abkommen Bestand haben wird, bevor der EuGH es wie schon Safe Harbor und Privacy Shield für ungültig erklärt.

IX. Einordnung von Google als Datenimporteur sowie eigene Verantwortliche

Die österreichische Datenschutzbehörde legte in ihrem Bescheid fest, dass Google nicht als Empfänger personenbezogener Daten zu qualifizieren sei, weil keine Daten offengelegt würden, sondern Google die Daten lediglich erhält. Aus Sicht der österreichischen Behörde geht damit einher, dass der Datenexporteur, und nicht etwa auch der Datenimporteur die Vorgaben der Art. 44 ff. DS-GVO einzuhalten hat. Damit folgt Österreich nicht der Ansicht des EDSA, der in einer Guideline Fälle wie den von Google Ireland und Google Inc. als klassischen Fall von Datenexporteur und Datenimporteur sehen würde.[25] Google Inc. ist sehr wohl Datenimporteur, wenn personenbezogene Daten durch Google Ireland als Datenexporteur bereitgestellt werden und damit auch an die Vorgaben aus der DS-GVO gebunden. Der österreichischen Einordnung von Google nicht nur als Auftragsverarbeiter, sondern auch als eigener Verantwortlicher kann leicht gefolgt werden. Zu berücksichtigen ist hierbei, dass Google selbst verschiedene Einstellungen anbietet, die unter anderem auch ermöglichen, dass der Geschäftskunde die Nutzung von Daten zu eigenen Zwecken (wie der Verbesserung der Produkte und Dienste) ausstellt.[26]

X. Deutsche Cloud von Google als Alternative zur Public Cloud

Google und die Tochtergesellschaft der Deutschen Telekom, T-Systems, kündigten an, eine souveräne Cloud für Unternehmen und Behörden aufzubauen.[27] Hierfür sollen die Rechenzentren von Google genutzt werden. Die Server sollen aber dennoch physisch getrennt von den Public Cloud Computing-Servern von Google stehen, und ein Zugriff durch Google Mitarbeiter soll nur dann erfolgen, wenn das Security Operations Center (SOC) von T-Systems diesen freigibt. Das Projekt wird aktuell jedoch erst noch daraufhin geprüft, ob es den Vorgaben des BSI entsprechen kann, sodass erst mit Inbetriebnahme eine nähere Bewertung möglich sein wird.

Betrachtet man dann die Kernproblematik des Zugriffs von US-Behörden auf personenbezogene Daten, bleibt dieses weiterhin bestehen. Mit einem Blick auf die Zugriffsrechte der US-amerikanischen Behörden, bspw. verankert durch den CLOUD Act, wird deutlich, dass die Anbieter von Cloud Computing-Diensten nur begrenzt Möglichkeiten haben, einen solchen Zugriff selbst ohne Transfer der Daten in die USA zu verhindern. Der CLOUD Act erlaubt den US-amerikanischen Behörden einen weiten Zugriff auf in der EU ruhende Daten, soweit die Muttergesellschaft des Unternehmens in den USA sitzt. Theoretisch öffnet der CLOUD Act daher die Möglichkeit, dass selbst auf Rechenzentren in der EU zugegriffen werden kann, und macht damit das Potenzial einer deutschen Google-Cloud, ein sicheres Datenschutzniveau herzustellen, weitgehend obsolet.

XI. Einwilligung als „letzte" mögliche Legitimierung des Datentransfers

Die deutschen Datenschutzaufsichtsbehörden haben nach den Beschwerden durch noyb noch keine offiziellen rechtlichen Meinungen zu Google Analytics veröffentlicht. Es bleibt allerdings nur eine Frage der Zeit, bis diese folgen werden. Auch wenn die Details der Bewertungen nicht im Detail deckungsgleich sind, stellen die bisherigen Beurteilungen durch Frankreich, Österreich und dem EDSB klar, dass ein möglichst einheitlicher Ansatz zur Bewertung EU-weit angestrebt wird. Zumindest die Richtung wird klar. Die Einwilligung der Webseitenbesucher einzuholen, um so den Einsatz von Google Analytics zu legitimieren, bleibt als Möglichkeit, Google Analytics DS-GVO-konform einzusetzen. Wie schon beschrieben, ist beim Einsatz von Google Analytics nach § 25 TTDSG eine Einwilligung notwendig. Diese informierte Einwilligung könnte mit einer Art. 49 Abs. 1 lit. a DS-GVO entsprechenden Einwilligung gekoppelt werden, um dann gleichzeitig auch eine Einwilligung in den möglichen Datenzugriff durch Dritte zu erhalten. Die DSK legt in ihrer Orientierungshilfe für Telemedien zwar Art. 49 DS-GVO streng aus und folgt damit der Ansicht des EDSA.[28] Der EDSA legt Art. 49 Abs. 1 lit. a in Relation zu Abs. 2 so aus, dass eine Einwilligung in den Datentransfer nur bei nichtregelmäßiger Datenverarbeitung rechtmäßig ist. Es braucht keine tiefgehende teleologische Analyse des Artikels, um eine solche Auslegung mindestens als stark bedenklich einzustufen. Vor allem fällt eine solch strenge Auslegung der Einwilligung umso schwerer, wenn man bedenkt, dass nur dann, wenn die Voraussetzungen einer informierten Einwilligung nach Art. 7 DS-GVO gegeben sind, Betroffene eine informierte Entscheidung treffen könnten. Diese Möglichkeit pauschal abzusprechen, ist höchst kritisch zu bewerten,

23 Vgl. Microsoft, Unsere Antwort an Europa: Microsoft ermöglicht Speicherung und Verarbeitung von Daten ausschließlich in der EU, https://news.microsoft.com/de-de/unsere-antwort-an-europa-microsoft-ermoeglicht-speicherung-und-verarbeitung-von-daten-ausschliesslich-in-der-eu/, aufgerufen am 08.07.2022.

24 Vgl. Redaktion beck-aktuell, EU und USA einigen sich im Grundsatz auf neues DatenschutzabkommenVerlag C.H.BECK, 25. März 2022 (dpa).

25 Vgl. dazu Europäischer Datenschutzausschuss (European Data Protection Board), Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

26 Vgl. https://support.google.com/analytics/answer/9019185#zippy=%2Cin-this-article, aufgerufen am 08.07.2022.

27 Vgl. https://www.telekom.com/de/konzern/details/impuls-fuer-souveraene-digitalisierung-643216, aufgerufen am 08.07.2022.

28 Vgl. https://www.datenschutzkonferenz-online.de/media/dsgvo/edpb_guidelines_2_2018_derogations_de.pdf, aufgerufen am 08.07.2022.

wenn dadurch die informationelle Selbstbestimmung des Einzelnen so weit eingeschränkt wird, dass nicht einmal die Entscheidung offen gestellt wird.

XII. Fazit

Die rechtlichen Aussagen der bisherigen Datenschutzbehörden zum Einsatz von Google Analytics bleiben lückenhaft und führen zu geringer Rechtssicherheit für Verantwortliche und Auftragsverarbeiter in der EU, die als Datenexporteur personenbezogene Daten in die USA transferieren oder zumindest die Möglichkeit für US-Sicherheitsbehörden herstellen, auf Daten zuzugreifen. Die Datenschutzbehörden lassen unberücksichtigt, dass es vier neue Sets an SVK gibt, die geeignete Garantien nach Art. 46 Abs. 2 c) DS-GVO darstellen können. Fraglich ist, in welcher Ausgestaltung der SVK, speziell des TIA und der damit einhergehenden Risikobewertung und zusätzlich ergriffenen Maßnahmen durch den Datenimporteur, diese von den Behörden als ausreichend bewertet werden würden. Es bleibt auch abzuwarten, ob die Einwilligung nach Art. 49 Abs. 1 lit. a) DS-GVO als mögliche Rechtsgrundlage Bestand haben wird, die enge Auslegung des Artikels müsste dafür aber in Frage gestellt und überdacht werden.

Dinya Berwari, LL.M.
ist seit 2017 als Datenschutzkoordinatorin bei ALDI Süd beschäftigt. Der Fokus liegt dort auf den Bereichen Kundendatenschutz und Ecommerce, sowie auf Internationalem Datenschutz.

Kristin Benedikt

Die DS-GVO als Datenwirtschaftsverfassung

„So war die DS-GVO nicht gemeint" von Stefan Brink, Jan Oetjen, Rolf Schwartmann und Axel Voß in F.A.Z. 18. Juli 2022 auf dem Prüfstand

Wenn gleich vier Datenschutzexperten behaupten, in der Anwendung der DS-GVO laufe einiges schief, muss etwas dran sein. Die Autoren Stefan Brink, Jan Oetjen, Rolf Schwartmann und Axel Voß kritisieren in ihrem F.A.Z.-Beitrag aus dem Juli 2022 die Anwendung der DS-GVO und fordern in neun Punkten einen Richtungswechsel.1 Auf den Punkt gebracht: Unternehmen sollen nicht im vorauseilenden Gehorsam handeln. Aufsichtsbehörden und Gerichte sollen das Recht auf Schutz personenbezogener Daten nicht als „Supergrundrecht" verstehen, sondern in Einklang mit anderen Schutzgütern bringen. Der Gesetzgeber soll schnell und zukunftsorientiert handeln. Nur so hat Europas Digitalwirtschaft in der Zukunft eine Chance. Klare Worte, doch sind sie berechtigt? Grund genug, um die neun Forderungen auf den Prüfstand zu stellen. Die diskutierten Passagen sind hier grau unterlegt.

„Europas Digitalwirtschaft soll im internationalen Wettbewerb zu einem Ökosystem der fairen digitalen Wertschöpfung werden. Dabei kommt es entscheidend auf die rechtlichen Rahmenbedingungen an. Aktuell entstehen in Ergänzung des Data Governance Act mit dem Data Act und der KI-Verordnung Gesetze, die auf die Weitergabe und Nutzung von Daten zum Wohl von Gesellschaft, Wirtschaft und Staat gerichtet sind. Bei ihnen ist der Datenschutz kein Bremsklotz der wirtschaftlichen Entwicklung, sondern integraler Bestandteil des Rechtsrahmens. Ebenso unbestreitbar ist: „Big Data" und Anwendungen künstlicher Intelligenz setzen die Verkehrsfähigkeit von Daten voraus. Und: Wettberber aus USA und China beherrschen bislang den europäischen Markt. Sie setzen faktisch die Standards und stellen die Plattformen. Wenn Europas Digitalwirtschaft im internationalen Wettbewerb bestehen soll, dann müssen mehrere Faktoren zusammenwirken."

Europas Daten liegen in den Händen von wenigen Tech-Giganten. Das beeinträchtigt nicht nur den Wettbewerb, son-

1 Https://www.faz.net/aktuell/wirtschaft/digitec/so-war-die-DS-GVO-nicht-gemeint-was-bei-ihrer-anwendung-schieflaeuft-18179521.html.

dern hemmt auch Innovationen innerhalb des europäischen Binnenmarktes. Die EU-Kommission hat schon 2020 die Reißleine gezogen und in einem Maßnahmenpapier zur „europäischen Datenstrategie“[2] dargelegt, wie Europa den digitalen Wandel vollziehen kann. Die „europäische Datenstrategie“ sieht vor, dass ein europäischer Binnenmarkt für Daten entsteht. Die EU-Kommission hat eine neue Art der Datenverwaltung vorgeschlagen, bei der Daten EU-weit zum Nutzen von Unternehmen, Forschungseinrichtungen und öffentlichen Stellen weitergegeben werden sollen. Damit dieser ambitionierte Plan aufgeht und zugleich Datenschutz- und Wettbewerbsrecht gewahrt werden, braucht es mehr als bloß eine Absichtserklärung. Daher hat die Kommission eine Vielzahl von Maßnahmen getroffen, um einen digitalen Binnenmarkt für Daten zu schaffen. Das Fundament bildet die DS-GVO, damit Nutzer das nötige Vertrauen aufbringen, um sich auf datengetriebene Innovationen einzulassen.[3] Darauf bauen eine Vielzahl weiterer Rechtsakte auf, darunter das Gesetz über digitale Märkte (DMA), das Gesetz über digitale Dienste (DAS), Datengesetz (DA), Daten-Governance-Gesetz (DGA) und die KI-Verordnung (AIA). Doch es braucht mehr als nur Regelungen zur Datennutzung. Die EU-Kommission schlägt weitere Maßnahmen mit Blick auf Technologien und Infrastrukturen vor. So wird ein einheitlicher elektronischer Identitätsnachweis für alle Onlinedienste vorgeschlagen.[4] Sogar ein europäisches Chip-Gesetz[5] ist geplant, um die Versorgung mit Halbleitertechnologien innerhalb Europas auch in Krisenzeiten zu gewährleisten. Die ambitionierten Pläne der Kommissionspräsidentin Ursula von der Leyen kann man gutheißen oder mit Skepsis betrachten. Doch worin sich alle einig sind, ist dass die Abhängigkeiten von Asien und den USA aufgelöst werden müssen.

I. Die DS-GVO als Wirtschaftsverfassung des Datenbinnenmarktes begreifen

„Die DS-GVO ist mehr als „nur“ eine Datenschutzverordnung, sie ist der Kern der „Wirtschaftsverfassung des Datenbinnenmarktes“. Art. 1 DS-GVO und deren Erwägungsgrund 4 schützen nicht nur natürliche Personen bei der Verarbeitung personenbezogener Daten, sie schützen ausdrücklich auch den „freien Verkehr solcher Daten“. Dieser darf aus Gründen des Datenschutzes in der EU weder eingeschränkt noch verboten werden. Zugleich liefert die DS-GVO die Rechtsgrundlagen für legitime Datenverarbeitungen. Dies sind die Verfolgung interessengerecht abgewogener Zwecke, Verträge über die Datenweitergabe und die freiwillige und informierte Einwilligung. Die im Bürgerlichen Gesetzbuch umgesetzte Richtlinie für Digitale Inhalte hat völlig konsequent Daten zum Wirtschaftsgut erklärt. Das aktuell in der EU entstehende Datenrecht baut diesen Ansatz aus. Es setzt auf eine umfassende Datenweitergabe unter Wahrung der Interessen persönlich Betroffener. Auf dieser Basis kann im Binnenmarkt mit personenbezogenen Daten gearbeitet, geforscht und gewirtschaftet werden. Personenbezogene Daten sind also – anders als uns manche öffentliche Diskurse glauben machen wollen – keine „res extra commercium“, die dem privatnützigen Wirtschaften entzogen wäre. Nur sehr wenige Datenverarbeitungen sind so risikoreich, dass man sie tabuisieren muss und die Weitergabe und Nutzung dieser sensiblen Daten selbst durch Einsatz von Verschlüsselungs- und Pseudonymisierungstechnik nicht rechtfertigen kann.“

Die DS-GVO sollte besser Daten-Grundverordnung heißen, denn sie regelt nicht nur den Datenschutz, sondern auch die Datenverkehrsfreiheit.[6] Das ergibt sich unmittelbar aus dem vollständigen Titel der DS-GVO, denn sie ist eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.[7] Ebenso ausdrücklich regelt das europäische Primärrecht, dass der Unionsgesetzgeber die Kompetenz hat, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und über den freien Datenverkehr zu erlassen, Art. 16 Abs. 2 AEUV. Ist die DS-GVO deshalb eine Wirtschaftsverfassung? Ja, wenn man den Begriff der Verfassung nicht im formellen Sinne, sondern als Rechtsordnung versteht. Wirtschaftsordnung ist die DS-GVO deshalb, weil sie einerseits im europäischen Wirtschaftsraum Pflichten bei der Datenverarbeitung regelt, anderseits regelt sie Rechte der an der Datenverarbeitung Beteiligten. Dazu gehören nicht nur die umfangreichen Betroffenenrechte gem. Art. 12 ff. DS-GVO. Auch Verantwortlichen steht nach den europäischen Grundrechten wie der unternehmerischen Freiheit gem. Art. 16 GRCh und dem Recht auf Eigentum gem. Art. 17 GRCh das Recht auf Datenverarbeitung zu. Darüber hinaus dienen Datenschutz und Datenverkehrsfreiheit nicht nur dem Schutz des Einzelnen. Beide Schutzgüter sollen die in Art. 3 EUV, 179 AEUV verankerten Ziele der Union fördern. Dazu gehört insbesondere die Schaffung eines (digitalen) Binnenmarktes.[8]

II. Mut zur Freiheit bei den Verantwortlichen

„Wir erleben seit 2018 – dem Jahr des Wirksamwerdens der DS-GVO – eine äußerst defensive Debatte über die

2 Europäische Kommission, Eine Europäische Datenstrategie, COM (2020) 66 final.

3 Europäische Kommission, Eine Europäische Datenstrategie, COM (2020) 66 final, S. 1.

4 Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM(2021) 281 final.

5 Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Ein Chip-Gesetz für Europa, COM(2022) 45 final.

6 Vertiefend zur Debatte der Schutzgüter vgl. Botta, DVBl. 2021, 290, 292.

7 Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 25.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

8 Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 final.

Nutzung persönlicher Informationen, gerade so als hätte Europa der zukunftsorientierten und in vielerlei Hinsicht gewinnbringenden Verarbeitung personenbezogener Daten abgeschworen. Umgekehrt schüttet eine frustrierte Datenwirtschaft das Kind mit dem Bade aus, wenn sie dem gewachsenen und vitalen Datenschutz Wirtschaftsfeindlichkeit oder Gestrigkeit unterstellt. Verantwortliche in Staat und Wirtschaft müssen vielmehr den Mut und die Weitsicht aufbringen, die Rolle s.o. des Datenschutzes zu verstehen und zu respektieren, aber eben auch nicht zu überhöhen. Dazu gehört, dass sie ihre Verantwortung bei der Auslegung des Datenschutzrechts erkennen und selbstbewusst wahrnehmen. Dabei darf man auch Widerspruch gegenüber einer zu engen Anwendungspraxis von Aufsichtsbehörden erheben und sollte den Konflikt mit potentiellen Klägern auf Schadensersatz wegen behaupteter Datenschutzverletzungen nicht scheuen. Verantwortliche können europaweit auf die Kontrollmechanismen des Rechtsstaats, insbesondere die fachkundiger werdenden Gerichte vertrauen. Mut statt Frust lautet die Devise."

Es gibt mehrere Gründe, weshalb Unternehmen Konflikte mit den Datenschutzaufsichtsbehörden scheuen. Zwar sind bei vielen Unternehmen bereits kurze Zeit nach Geltung der DS-GVO die Sorgen vor Bußgeldern in Millionenhöhe verschwunden. Auch das Vorabentscheidungsverfahren zur Auslegung des Art. 83 DS-GVO[9] dürfte dafür sorgen, dass die Aufsichtsbehörden in punkto Bußgelder zunächst einmal innehalten. Jedoch dürfte es mehr als nur Mut verlangen, sich gegen die Auffassung der Aufsichtsbehörden zu richten. Unternehmen scheuen einen Konflikt mit den Behörden, denn sie können sich keine negativen Schlagzeilen leisten. Jede behördliche Mitteilung über ein Aufsichts- oder Bußgeldverfahrens kann zu einem Reputationsverlust führen.[10] Zudem muss das Unternehmen damit rechnen, sich vor den Zivilgerichten auf der Beklagtenseite wiederzufinden. Schadensersatz nach Art. 82 DS-GVO ist nicht nur das „neue" Bußgeld, sondern mittlerweile ein florierendes Geschäftsmodell.[11]

Verantwortliche, die dennoch in die Offensive gehen wollen, müssen nicht erst abwarten, bis ein Aufsichts- oder Bußgeldverfahren gegen sie eröffnet wird. Sie können vorbeugenden Rechtsschutz in Anspruch nehmen und vor den Verwaltungsgerichten klären lassen, ob Sanktionsandrohungen der Aufsichtsbehörden, z.B. in Form von Pressemitteilungen, im Einklang mit der DS-GVO stehen.[12] Schließlich braucht es neben Mut vor allem Geduld. Viel Geduld, denn gerichtliche Verfahren im Datenschutz können fast ein Jahrzehnt dauern, wie das Verfahren „Facebook Fanpages" zeigt.[13]

III. Umdenken bei der Datenschutzaufsicht

„Damit die Wirtschaft die von der DS-GVO gewährte Freiheit leben kann, müssen die Datenschutzaufsichtsbehörden ein verlässliches und einheitliches Maß beim Vollzug des Datenschutzes finden. Sie müssen die Wechselwirkung zwischen Datenschutz und der Notwendigkeit nach umfassender Weitergabe von Daten unterstützen. Zugleich müssen sie sich auf ein einheitliches und verlässliches Vorgehen einigen. Genau mit dieser Zielsetzung wurde in der DS-GVO der Europäische Datenschutzausschuss eingesetzt, um für eine harmonische Umsetzung des Rechts in der gesamten EU zu sorgen. Das funktioniert bislang noch nicht überzeugend: Aktuell muss es die Wirtschaft beispielsweise ausbaden, dass Europas Datenschutzaufsichtsbehörden sich nicht auf ein effektives Vorgehen gegen Facebook einigen können, obwohl der Tech-Gigant wesentliche Vorgaben der DS-GVO ignoriert. Irland ist für Facebook zuständig, aber bisher nicht bereit, das Unternehmen in die Schranken zu weisen. Streitpunkt ist u.a. die Intransparenz über die Verantwortung der Datenverarbeitung beim Betrieb von Fanpages. Weil sich unter Europas Datenschutzbehörden keine klare Mehrheit dafür findet, Irland zu einem energischen Vorgehen gegen Facebook zu zwingen, hat man in Deutschland jetzt damit begonnen, gegen die Fanpagebetreiber – zunächst gegen Behörden, dann aber auch gegen Unternehmen – vorzugehen. Sie wollen Facebook „über Bande" dazu zwingen, sich an das Datenschutzrecht anzupassen. Facebook sitzt das bislang aus, während Europas Wirtschaft auf Bußgelder und Schadensersatzklagen wegen Datenschutzverstößen wartet, weil man bei der Kommunikation und in seinen Geschäftsmodellen von Sozialen Netzwerken abhängig ist."

Die Datenschutzaufsichtsbehörden mussten sich schon öfter dem Vorwurf aussetzen, untätig zu sein.[14] Viel gravierender sind hingegen die Meinungsverschiedenheiten unter den Aufsichtsbehörden, die zu Rechtsunsicherheiten bei den Unternehmen führen.[15] Daher wurde schon häufiger eine

9 KG Berlin, Beschl. v. 06.12.2021, 3 Ws 250/21.

10 Schwartmann/Paal/Benedikt, Dataagenda Podcast, Folge 21: Grenzen des Informationshandelns der Datenschutzaufsicht.

11 Wybitul, c't 22/2020, S. 168.

12 Schwartmann/Burkhardt, Rechtsgutachten, Vorbeugender verwaltungsgerichtlicher Rechtsschutz zur Abwehr drohender Bußgeldverfahren im Datenschutzrecht, im Auftrag der Freenet AG.

13 Das OVG Schleswig entschied mit Urteil vom 25.11.2021, 4 LB 20/13, dass die Anordnung des ULD vom 14.12.2012 zur Sperrung des Facebook-Kontos der Wirtschaftsakademie rechtmäßig erging.

14 Vgl. Verfahren wegen Untätigkeit der Datenschutzaufsichtsbehörden: OVG Hamburg, Urt. v. 07.10.2019 – 5 Bf 279/17); VG Wiesbaden, Urt. v. 27.09.2021 – 6 K 549/21.WI, VG Wiesbaden, Urt. v. 24.09.2021 – 6 K 442/21.WI, VG Ansbach, Urt. v. 07.12.2020 – 14 K 18.02503 und v. 16.03.2020 – AN 14 K 19.00464, VG Berlin, Beschl. v. 21.04.2021 – Az.: 1 K 360.19, OVG Koblenz, Urt. v. 26.10.2020 – 10 A 10613/20.OVG, VG Mainz, Urt. v. 16.01.2020 – 1 K 129/19.MZ, SG Frankfurt(Oder), Urt. v. 08.05.2019 – S 49 SF 8/19.

15 Beispielhaft für die unterschiedlichen Auffassungen der deutschen Aufsichtsbehörden zum Einsatz von Microsoft 365: Pressemitteilung vom 02.10.2020, Microsoft Office 365: Bewertung der Datenschutzkonferenz zu undifferenziert – Nachbesserungen gleichwohl geboten, abrufbar unter https://www.lda.bayern.de/media/pm/20201002_office365.pdf [28.08.2022].

Zentralisierung der Datenschutzaufsicht angeregt.[16] Eine Zentralisierung wäre jedenfalls für den nicht-öffentlichen Bereich der Datenschutzaufsicht verfassungsrechtlich möglich.[17] Eine verbindliche und einheitliche Auffassung der deutschen Datenschutzaufsichtsbehörden könnte auch erreicht werden, indem die Datenschutzkonferenz institutionalisiert wird.[18] Anders als beim Europäischen Datenschutzausschuss sind Beschlüsse der Datenschutzkonferenz nicht verbindlich. Zwar sind die Mitglieder der Datenschutzkonferenz bemüht, eine einheitliche Anwendung des Datenschutzrechts zu erreichen.[19] Dem steht jedoch nicht entgegen, dass die Mitglieder der Datenschutzkonferenz in eigenen Publikationen abweichende Positionen vertreten. Zwingend ist eine Neugestaltung der deutschen Datenschutzaufsicht nicht, denn es zeichnet sich bereits ein Umdenken ab. Die Aufsichtsbehörden haben erkannt, dass mehr Prävention geleistet werden muss, indem die Beratung ausgeweitet wird und Digitalisierungsprojekte von Verantwortlichen begleitet werden.[20]

IV. Kurswechsel beim EuGH

„Die Idee des Vorgehens gegen Fanpagebetreiber stammt vom Europäischen Gerichtshof, dem maßgeblichen Treiber für die offensive Umsetzung des europäischen Datenschutzrechts. Das Gericht hat damit einen entscheidenden Anteil am Geschick der DS-GVO. Der EuGH begreift die DS-GVO im Wesentlichen als Verbraucherschutzrecht und verliert dabei deren Ziel, auch das wirtschaftliche Potenzial personenbezogener Daten zu heben, weitgehend aus den Augen. Auf der einen Seite nimmt er weltweit agierende Unternehmen zu Recht in die Pflicht, ihre Angebote dem lokalen Recht anzupassen. Nach dem Marktortprinzip gilt europäisches Recht nun einmal für alle, die hier anbieten. Auf der anderen Seite geht der EuGH zu weit, wenn er etwa die nur abstrakte und hypothetische Möglichkeit des Zugriffs nicht-europäischer Sicherheitsbehörden ohne konkretes und reales Risiko für persönliche Daten von Europäern als Killerkriterium für globalen Datenaustausch begreift. Die „Schrems II"-Entscheidung des EuGH hat enormen Flurschaden angerichtet. Danach ist selbst die technische Einbindung eines Schrifttyps, die per Datenverarbeitung aus den USA erfolgt, eine Datenschutzverletzung mit der Folge des Schadensersatzes für Unternehmen und Behörden. Das Verbot der Nutzung außereuropäischer Anbieter, etwa von Konferenzsystemen, schneidet Europa von der „Digitalen Daseinsvorsorge" und Massenkommunikation zu einem Zeitpunkt ab, da nutzbare europäische Alternativen erst noch im Aufbau sind. Die Verwendung von gebräuchlicher Videokonferenzsoftware etwa kann mit existenzbedrohenden Bußgeldern belegt werden, auch wenn es in der Konferenz nur um Wirtschaftszahlen oder ums Wetter geht. Die Klageindustrie steht mit Unterstützung von Legal Tech in den Startlöchern, um Europas Wirtschaft mit Massenklagen zu überziehen – hier immerhin scheint Europa die Nase vorn zu haben."

Einspruch! Der EuGH ist weder verbraucherfreundlich noch entschied er über ein „Datentransferverbot". Der EuGH wird missverstanden, denn seine Urteile werden fälschlicherweise „ausgelegt" wie Gesetze, und es werden Schlüsse gezogen, die nicht in Rechtskraft erwachsen. Der EuGH entscheidet in Vorabentscheidungsverfahren gem. Art. 267 AEUV über die Anwendung europäischen Rechts. Ist ein nationales Gericht der Auffassung, dass ein Europäischer Rechtsakt ungültig ist oder die Auslegung streitig ist, ruft es den EuGH an. Eine Auslegung des Wortlautes der EuGH-Entscheidungen verbietet sich schon deshalb, weil grundsätzlich nur der EuGH selbst bei Zweifeln über Sinn und Tragweite eines Urteils oder Beschlusses im Wege eines Antragsverfahrens für die Auslegung zuständig ist.[21] Ein solches Auslegungsverfahren ist jedoch ausgerechnet bei Vorabentscheidungsverfahren gem. Art. 267 AEUV ausgeschlossen.[22] Die nationalen Gerichte müssen beurteilen, ob durch ein Vorabentscheidungsverfahren die aufgeworfenen Vorlagefragen hinreichend beantwortet wurden oder ob es erforderlich ist, den Gerichtshof erneut anzurufen.

Es ist nicht von der Hand zu weisen, dass der EuGH tendenziell zu einer extensiven Auslegung neigt, damit der Schutzzweck einer Norm die größtmögliche Wirkung entfalten kann. Verbraucherfreundlich ist er deswegen keinesfalls. Auch sieht der EuGH keinen Vorrang des Rechts auf Schutz personenbezogener Daten gem. Art. 8 GRCh gegenüber anderen Grundrechten, denn „das Recht auf Schutz personenbezogener Daten [ist] kein uneingeschränktes Recht, sondern muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden."[23]

Erforderlich ist daher kein Kurswechsel vom EuGH, sondern vielmehr ein anderes Verständnis seiner Rolle und Funktion innerhalb der Rechtsprechung.

V. Sinnvolle wirtschaftliche Rahmenbedingungen für Datenteilung

„Bei der Anwendung der DS-GVO ist also einiges schiefgelaufen. So war sie nicht gemeint. Rechtsprechung und Aufsichtspraxis müssen sich also ändern, wenn der Wille des Europäischen Gesetzgebers nicht in wesentlichen Teilen ignoriert werden soll. Der setzt in den neuen Datengesetzen zum Datenbinnenmarkt nämlich konsequent

16 Wirtschaftsministerkonferenz, Beschlusssammlung der Wirtschaftsministerkonferenz vom 30. November 2020, 4.12.2020; Datenethikkommission der Bundesregierung, Gutachten der Datenethikkommission der Bundesregierung, 2019, S.103.

17 Martini, DÖV 2021, 609 (612).

18 SPD/Bündnis 90 /Die Grünen/FDP, Koalitionsvertrag 2021-2025, S. 17.

19 Geschäftsordnung der Datenschutzkonferenz, Beschluss der DSK vom 05.09.2018, geändert durch Beschluss der DSK vom 29.09.2021, A. II.

20 Heise Verlag, Auslegungssache: Der Datenschutz-Podcast des c't magazins, Folge 67: „Der Elefant im Datenraum" vom 01.07.2022.

21 Vgl. Art. 158 konsolidierte Fassung der Verfahrensordnung des Gerichtshofs vom 25.09.2012.

22 Vgl. Art. 108 konsolidierte Fassung der Verfahrensordnung des Gerichtshofs vom 25.09.2012.

23 EuGH, Urt. 24.09.2019 – C-507/17, Rn 60.

auf Datenteilung und den Einsatz künstlicher Intelligenz. Er schreibt damit die DS-GVO als „Datenwirtschaftsverfassung" fort. Der Gesetzgeber verfolgt sein Ziel weiter, Anreize für die Datenweitergabe im europäischen Datenökosystem zu schaffen. Das Anwendungsfeld dieses neuen Rechts ist immens. Im Internet der Dinge kommuniziert der Toaster mit Toastbrotlieferanten und die Waschmaschine mit dem Energieversorger. All diese Daten sollen im Binnenmarkt geteilt und verwertet werden. Das ist auch gut so – wirft aber natürlich auch Fragen auf. Etwa beim vernetzten Auto, dem fast alles können den Personal Organizer, der künftig autonom von Budapest nach Dublin fahren wird. Noch ist völlig unklar, wem die Daten gehören, die bei einer Autofahrt durch Europa erhoben werden. Im autonomen Auto sind die Insassen nur noch Fahrgäste des Betreibers und Kunden des Anbieters der Inhalte der Bordelektronik sowie der sie treibenden Werbewirtschaft. Solange es noch einen Fahrer gibt, fragt sich, ob ihm die Daten der Fahrt zustehen, weil er sie produziert hat und sie sich auf ihn beziehen. Oder gehören sie dem Hersteller, der den vernetzten Wagen auf der Straße hält, oder dem Zulieferer für die Bordelektronik, deren Angebote die Insassen nutzen. Oder gehören die Daten dem Navigationsdienst von Google? Da jeder ein gewisses Anrecht auf diese Daten hat, wird der Gesetzgeber die entstehenden Interessenkonflikte weise regeln müssen und eventuell auch zu deren Teilung zwingen können, dabei aber die Unternehmensfreiheiten zu wahren haben."

Fakt ist, dass ein digitaler Wandel auch ein Umdenken in puncto Datenschutz erfordert. Ein europäisches Datenökosystem, in dem Daten gemeinsam genutzt werden, verträgt sich so gar nicht mit dem bisherigen Verständnis vom Grundsatz der Datenminimierung. Die neuen Datenakte regeln einheitlich, dass sie das Unionsrecht zum Datenschutz, insbesondere die DS-GVO, unberührt lassen. Es versteht sich von selbst, dass das Schutzniveau der DS-GVO nicht unterlaufen werden darf, auch nicht zur Erreichung eines digitalen Binnenmarktes. Unklar bleibt jedoch, was der europäische Gesetzgeber konkret mit „unberührt" meint. Handelt es sich um einen klarstellenden Hinweis, dass sich der Geltungsbereich beider Regelungen nicht überschneidet? Sind beide Regelungen nebeneinander anwendbar oder wird ein Vorrang des Datenschutzrechts ausgedrückt?[24] Räumt der europäische Gesetzgeber diese Unklarheiten nicht aus, kann nur noch der EuGH für ein einheitliches Verständnis sorgen.

VI. Künstliche Intelligenz praxisgerecht regulieren

„Wenn der Fahrer während der Fahrt unter Auswertung seines Fahrverhaltens von einem Bordcomputer auf seine Fahrtauglichkeit kontrolliert wird, dann kommt künstliche Intelligenz ins Spiel. Hier gilt es mit Augenmaß für die potentiellen Gefahren für Leib, Leben oder Gesundheit von Insassen und Verkehrsteilnehmern zu agieren. Man darf nicht aus jedem Kaffee, der dem Fahrer wegen künstlich intelligent festgestellter Müdigkeit nahegelegt wird, eine Hochrisikoanwendung machen. Das muss den heftig diskutierten Dilemmasituationen von potentiellen „Tötungsentscheidungen" des Fahrzeugs im Straßenverkehr vorbehalten bleiben. Man muss auf Basis der DS-GVO also zukunftsorientiert ausbuchstabieren, was zulässig ist. In den allermeisten Fällen ist KI ungefährlich und nützlich, und ihr Einsatz dürfte oft, etwa im Gesundheitsbereich oder bei der Verbrechensbekämpfung, sogar ethisch geboten sein, wenn sie ihre Eignung unter Beweis gestellt hat. Wie der Mensch die Kompetenz bekommt, die „intelligente" Maschine zu verstehen, um sich zur Not auch gegen den Vorschlag des Computers entscheiden zu können, der wie ein Schachcomputer in seinem Kontext nicht geschlagen werden kann, muss ebenfalls im Gesetz mitgedacht und vorgegeben werden. Nur wissend kann der Mensch den Druck auf die Stopp-Taste verantworten."

Die DS-GVO enthält bereits Instrumente zur KI-Regulierung. Die Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO soll dazu dienen, mögliche Schäden und deren Eintrittswahrscheinlichkeit bei der Nutzung von KI-Systemen zu ermitteln.[25] Dabei ist insbesondere zu prüfen, welches Diskriminierungspotenzial von einer KI-basierten Datenverarbeitung ausgeht.[26] Das ermittelte Risiko bestimmt, welche technischen und organisatorischen Maßnahmen ergriffen werden müssen, um die Integrität und Vertraulichkeit gem. Art. 5 Abs. 1 lit. f), 32 DS-GVO zu gewährleisten.

Dennoch bietet die DS-GVO weder einen umfassenden Schutz der Betroffenen, noch regelt sie die zulässigen Grenzen, innerhalb derer sich Verantwortlicher bewegen dürfen. Die Regelungen zu Profiling gem. Art. 22 DS-GVO sind lückenhaft, denn sie erfassen nur Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen, nicht hingegen solche, bei denen der Mensch – sei es auch nur in geringem Maße – mitwirkt.[27] Betroffene müssen auch nicht umfassend über Algorithmen informiert werden, denn die Art. 13 Abs. 2 lit. f), 14 Abs. 2 lit. f) DS-GVO fordern nur Angaben zur involvierten Logik, Tragweite und Auswirkungen, soweit eine Verarbeitung im Sinne des Art. 22 Art. 1 DS-GVO vorliegt.

Neben spezifischen Regelungen zur KI braucht es eine gesetzgeberische Klarstellung, in welchen Anwendungsszenarien KI zulässig ist oder nicht. Nicht der Rechtsanwender, sondern der Gesetzgeber muss entscheiden, ob KI im Be-

24 Vgl. zur Auslegung der Wendung „bleiben unberührt" bei nationalen Vorschriften: Bundesministerium der Justiz und für Verbraucherschutz (BMJV), Handbuch der Rechtsförmlichkeiten, 3. Aufl. 2008, S. 42.

25 DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 vom 17.10.2018, Nr. 11.

26 Gutachten der Datenethikkommission, 2019, F 2.6.

27 Gutachten der Datenethikkommission, 2019, F 4.1.1.

schäftigtenverhältnis,[28] zur Kriminalitätsbekämpfung oder für Werbezwecke erlaubt ist.

VII. Datensouveränität stärken

„Wer im Netz unterwegs ist, dem muss der Gesetzgeber Möglichkeiten an die Hand geben, um seine Datensouveränität praktikabel umsetzen zu können. Die Mittel zur Verfügung über Daten sind der Vertrag mit einem Datendienst über die Nutzung der Daten oder die Einwilligung. Beide Erlaubnisgründe konkurrieren miteinander. Das moderne Zivilrecht erkennt das „Zahlen mit Daten" und damit Personendaten als Wirtschaftsgüter durchaus an. Den Willen zur Nutzung von Onlineangeboten, von der Website bis zur Bordelektronik im vernetzten Fahrzeug, kann man per Einwilligung erklären. Das deutsche Recht schlägt den Weg über Einwilligungsdienste vor, mit deren Hilfe Nutzer ihre Einwilligungen selbstbestimmt bündeln und sinnvoll verwalten können. Dieser Weg ist vielversprechend, das Digitalministerium muss nun zügig den Rechtsrahmen hierzu schaffen."

Der deutsche Gesetzgeber hat mit § 26 TTDSG einen Rechtsrahmen für anerkannte Dienste zur Einwilligungsverwaltung geschaffen. Die konkrete Ausgestaltung solcher Dienste soll eine Rechtsverordnung regeln, § 26 Abs. 2 TTDSG.[29] Neben dem Einwilligungsmanagement hat der europäische Gesetzgeber durch die Digitale-Inhalte-Richtlinie[30] im Bereich der Vertragsgestaltung mehr Spielraum zugebilligt. Verbraucher und Unternehmen können vertraglich die Bereitstellung personenbezogener Daten vereinbaren.[31]

Für mehr Datensouveränität braucht es jedoch mehr als nur einen gesetzlichen Rahmen. Souverän kann der Betroffene nur agieren, wenn er Online-Dienste nicht bloß konsumiert, sondern deren Funktionsweise in den Grundzügen umreißt. Solange der Nutzer noch immer nicht erkennt, dass Nachrichten auf Social Media-Plattformen zielgruppenorientiert ausgespielt werden oder Kartendienste durch Routenvorschläge den Verkehr lenken, solange fehlt ihm das Bewusstsein, rechtsgeschäftlich verbindlich zu handeln. Ohne Rechtsbindungswillen kann er weder eine freiwillige Einwilligung abgeben, noch vertraglich die Bereitstellung seiner Daten zusichern.[32]

VIII. Faire Standards für fairen Wettbewerb

„Es kommt bei all dem entscheidend darauf an, dass der Zugang zu Onlineangeboten nach transparenten, neutralen, fairen und offenen Standards ermöglicht wird. Aktuell setzen Apple und Google über ihre Webbrowser und App Stores die Regeln, weil sie den Zugang zum Netz für Milliarden Menschen steuern. Unter dem Deckmantel des Datenschutzes wird das damit legitimiert, dass sich der Wille des Nutzers am besten über den Anbieter des Betriebssystems verwalten ließe. Trifft der souveräne Nutzer jedoch auf monopolartige Anbieterstrukturen, so läuft sein Recht, per Einwilligung die Nutzung seiner Daten zu steuern, faktisch leer. Die Souveränität des Nutzers geht dann im Willen der Anbieter der technischen Infrastruktur auf – und wird aufgehoben. Hier braucht es mehr Wettbewerb, notfalls auch durch staatliche Wettbewerbsregulierung und Zerschlagung von verbraucherfeindlichen Monopolen."

Ein Zuwarten auf die neuen Datenakte DSA und DMA ist gar nicht nötig, um den Wettbewerb datengetriebener Geschäftsmodelle zu regulieren. § 19a GWB erlaubt schon heute die Kontrolle von Digitalkonzernen. Das Bundeskartellamt ist gem. § 19a Abs. 2 GWB befugt, digitalen Plattformen und Netzwerken schädliche Verhaltensweisen im Zusammenhang mit der Datenverarbeitung zu verbieten.[33] Jedenfalls dem Bundeskartellamt kann Untätigkeit nicht vorgeworfen werden. Seit 2021 hat die Behörde mehrere Verfahren gegen Amazon, Google und Facebook eingeleitet und eine überragende marktübergreifende Bedeutung festgestellt.[34]

IX. Medienrecht ist Digitalisierungsrecht: Herausforderungen für Bund und Länder

„Weil alle Bereiche der Wirtschaft im Ergebnis datengetrieben sind, greifen die neu entstehenden EU-Datenakte (zB DA, DGA, KI-VO, DSA, DMA) tief in den Kompetenzbereich von Bund und Ländern in viele Gesetzgebungsfelder über. Insbesondere Medienrecht ist Digitalisierungsrecht und wird zunehmend europarechtlich geprägt. Greifbar ist das bei der Medienregulierung durch den DSA. Bund und vor allem Länder müssen die Entwicklung der europäischen Datenakte in Abgrenzung zur EU beobachten, um die Regulierung in Brüssel frühzeitig politisch begleiten zu können. Der bundes- und länderbezogene Handlungsbedarf und Spielraum muss wegen der Komplexität der Materie auf EU-Ebene und wegen ihres Einflusses auf das innerstaatliche Recht fortlaufend eruiert werden, damit

28 Vgl. Datenschutzkonferenz, Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29.04.2022, Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt"!, abrufbar unter: https://datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf [28.08.2022].

29 Referentenentwurf des Bundesministeriums für Digitales und Verkehr, Verordnung zur Regelung eines nutzerfreundlichen und wettbewerbs-konformen Verfahrens zur Einwilligungsverwaltung, zur Anerkennung von Diensten und zu technischen und organisatorischen Maßnahmen nach § 26 Abs. 2 Telekommunikation-Telemedien-Datenschutzgesetz (Einwilligungsverwaltungs-Verordnung – EinwVO), Bearbeitungsstand: 08.07.2022.

30 Richtlinie (EU) 2019/770 des europäischen Parlaments und des Rates vom 20.05.2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen.

31 Vgl. zur Umsetzung der Digitale-Inhalte Richtlinie §§ 312 Abs. 1 a, § 327 ff. BGB.

32 Kessen/Reif/Burkhardt, RDV 2022, 64 (67).

33 Bechtold/Bosch/Bechtold/Bosch GWB § 19a Rn. 4.

34 Bundeskartellamt, Pressemitteilung vom 06.07.2022: Für Amazon gelten verschärfte Regeln – Bundeskartellamt stellt überragende marktübergreifende Bedeutung fest (§ 19a GWB): Pressemitteilung vom 04.05.2022: Für Meta (vormals Facebook) gelten neue Regeln – Bundeskartellamt stellt „überragende marktübergreifende Bedeutung für den Wettbewerb" fest; Veröffentlichte Entscheidung vom 30.12.2021: Verfahren nach § 19a GWB gegen Alphabet Inc./Google.

Bund und Länder im Rahmen der Umsetzung des EU-Rechts reagieren und agieren können."

Die für die Medienregulierung zuständigen Staatskanzleien der Bundesländer werden auf die per Rechtsverordnungen erfolgende Überformung des nationalen Medienrechts besonderes Augenmerk legen müssen. Hier ist ein schwieriges Spannungsverhältnis zur nationalen Medienordnung entstanden. Sie müssen das erkennen und damit umgehen, dass Medienregulierung Digital- und Datenregulierung wird.[35] Eine besondere Aufgabe kommt hierbei daneben den Verbänden zu, denn sie sollten im Rahmen der Anhörungen im Gesetzgebungsverfahren ihre Expertise einbringen, um Kollateralschäden zu verhindern. Der nationale Gesetzgeber sollte auch mit Bedacht entscheiden, welche Behörden für den Vollzug des Digitalisierungsrechts zuständig sein werden, denn die zuständigen Behörden spielen eine entscheidende Rolle bei der Verwirklichung eines digitalen Binnenmarkes.[36]

Kristin Benedikt
ist Richterin und Datenschutzbeauftragte am Verwaltungsgericht Regensburg sowie Mitglied im Vorstand der GDD e.V.

35 Dazu Fiedler, Das Digitalgesetz der EU vernichtet die Presse im Internet. F.A.Z., abrufbar unter https://www.faz.net/aktuell/feuilleton/medien/digital-services-act-der-eu-vernichtet-pressefreiheit-im-internet-18198207.html.

36 Vgl. Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG, Ergw. 74.

Prof. Dr. Rolf Schwartmann/Robin L. Mühlenbeck

Datenschutz durch Ermöglichungstechnik – Anonymität und Pseudonymität nach der DS-GVO im Kontext von Data Act-Entwurf und Data Governance Act

Die Beurteilung des Personenbezugs eines Datums unter der DS-GVO ist auch fünf Jahre nach ihrem Geltungsbeginn mit erheblicher Rechtsunsicherheit behaftet. In der Rs. Breyer äußerte sich der EuGH erstmals grundlegend zu einer der wichtigsten Fragen des europäischen Datenschutzes, konnte hierbei den Begriff des Personenbezugs allerdings nur bedingt konturieren. Die Anonymität und Pseudonymität von Daten knüpfen an das Verständnis des Personenbezugs an und tragen damit die bestehenden Rechtsunsicherheiten mit Blick auf Fragen des Personenbezugs in sich. Dabei setzen gerade die neuen europäischen Datenakte auf die Instrumente der Pseudonymisierung und Anonymisierung von Daten und fordern einen souveränen Umgang mit Rechtsfragen des Personenbezugs.

I. Personenbezug entscheidet über Anwendbarkeit der DS-GVO

Der Personenbezug eines Datums entscheidet nach Art. 2 Abs. 1, Art. 4 Nr. 1 DS-GVO über die Anwendbarkeit der DS-GVO. Der Personenbezug ist damit die wesentliche Weichenstellung, nach der die Verarbeitung eines Datums entweder den Vorgaben der DS-GVO unterliegt oder im Falle des Fehlens des Personenbezugs von der Anwendbarkeit der DS-GVO befreit ist.[1] Anonyme Daten liegen nach einem Umkehrschluss zu Art. 2 Abs. 1, Art. 4 Nr. 1 DS-GVO und ErwG 26 S. 5 und 6 daher außerhalb des Anwendungsbereichs der DS-GVO.[2] Mit Blick auf Fragen des Personenbezugs befinden sich pseudonyme Daten – wegen des grundsätzlichen Bestands einer Zuordnungsinformation –[3] an der Schnittstelle zwischen personenbezogenem und anonymem Datum.[4] Aufgrund ihres technisch-organisatorisch herbeigeführten

1 Dazu Simitis/Hornung/Spiecker gen. Döhmann-Karg, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 1 und 14 und 19; Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 1 und 31. Ausführlich dazu Mühlenbeck, Anonyme und pseudonyme Daten, Kap. 1 A. III. und IV. 1. (erscheint demnächst).

2 Kühling/Buchner-Klar/Kühling DS-GVO/BDSG Art. 4 Nr. 1 Rn. 31 sowie Simitis/Hornung/Spiecker gen. Döhmann-Karg DS-GVO/BDSG Art. 4 Nr. 1 Rn. 19.

3 Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 2.

4 Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 2 und 11.

Identitätsschutzes[5] (sog. Schutzfunktion[6]) erfahren pseudonyme Daten mit Blick auf die materiellen Rechtsmäßigkeitsanforderungen im Falle ihrer Verarbeitung nach der DS-GVO gemäß Art. 6 Abs. 1 lit. f), Abs. 4 lit. e, Art. 9 Abs. 2, Art. 89 Abs. 1 DS-GVO besondere Erleichterungen (sog. Ermöglichungsfunktion[7]).[8]

II. Personenbezug und „Identifizierbarkeit" nach Art. 4 Nr. 1 DS-GVO und ErwG 26

In datenschutzrechtlicher Hinsicht bildet das Merkmal der „Identifizierbarkeit" nach Art. 4 Nr. 1 DS-GVO und ErwG 26 S. 3 und 4 das maßgebliche Kriterium für eine Kategorisierung der Daten im oben beschriebenen Sinne. Da ErwG 26 S. 3 hinsichtlich des Vorliegens der „Identifizierbarkeit" die Berücksichtigung aller Mittel, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person zu identifizieren, verlangt, setzt sich der schon unter der DS-RL bestehende Streit um ein absolutes oder ein relatives Begriffsverständnis auch unter der DS-GVO fort.[9] Während ein relatives Verständnis im Kern bezüglich einer Identifizierbarkeit die Kenntnisse und Mittel des Verantwortlichen in den Blick nimmt,[10] stellt ein absolutes Begriffsverständnis darauf ab, ob der Verantwortliche oder aber ein Dritter in der Lage ist, die natürliche Person zu identifizieren.[11]

III. Rechtsprechung des EuGH in der Rs. Breyer

In dieser Streitfrage hat der EuGH in der Rs. Breyer[12] erstmals ausführlicher Stellung bezogen. Hierbei hat er im Kern Folgendes festgestellt: Es ist nach Ansicht des EuGH nicht erforderlich, dass sich sämtliche zur Identifizierung erforderlichen Informationen in der Hand eines einzigen Verantwortlichen befinden.[13] Ausreichend ist vielmehr, wenn der Verantwortliche über einen Dritten die betroffene Person bestimmen lässt.[14] Die Grenze der Identifizierbarkeit liegt in der Unmöglichkeit, der Unverhältnismäßigkeit oder im Rechtsverstoß.[15] Damit hat der EuGH sich zwar im Kern einem relativen Begriffsverständnis angeschlossen, allerdings erhebliche Rückausnahmen zugelassen.[16] Die wissenschaftliche und praktische Herausforderung liegt vor allem darin, dass letztlich im Rahmen der Rechtsprechung die mit Blick auf den Personenbezug entscheidende Frage offen bleibt, wann von einer Unmöglichkeit oder Unverhältnismäßigkeit der Re-Identifizierung auszugehen ist.[17] Gerade diese Frage ist aber für die Bestimmung einer Pseudonymität und Anonymität von Daten entscheidend.

IV. Erweitertes relatives Begriffsverständnis des Personenbezugs

Im Grundsatz verdient ein relatives Begriffsverständnis den Vorzug, das allerdings vor dem Hintergrund der Rechtsprechung des EuGH um wesentliche Parameter zu erweitern ist. Die Einbeziehung konkreter Dritter bei der Zurechnung von Kenntnissen und Mitteln im Rahmen einer Datenverarbeitung ist vor dem Hintergrund des Wortlauts von ErwG 26 S. 3 konsequent und folgerichtig.[18] Ein absolutes Begriffsverständnis würde die Tauglichkeit des Merkmals der Identifizierbarkeit zur Abgrenzung letztlich aufheben und kann daher nicht überzeugen.[19] Darüber hinaus würden eine Anonymität und Pseudonymität von Daten letztlich aus dem Werkzeugkasten der DS-GVO verbannt, wenn die Zuordnungsmöglichkeit durch Dritte grundsätzlich die Annahme eines Personenbezugs des Datums begründen könnte.[20] Die Ausklammerung des Einsatzes rechtswidriger Mittel bei der Identifizierung innerhalb der nach ErwG 26 vorgegebenen Risikoanalyse und Bemessung der Identifizierungswahrscheinlichkeit wird diskutiert,[21] der EuGH hat eine Einbeziehung dieser Mittel letztlich außerhalb der Ermessenswahrscheinlichkeit nach ErwG 26 S. 3 und 4 verortet.[22] Dem kann nur eingeschränkt zugestimmt werden. Insbesondere in Fällen, bei denen aufgrund geringer praktischer Hürden oder wirtschaftlicher Interessen[23] eine Identifizierung nach ErwG 26 S. 3 und 4 eine Identifizierung wahrscheinlich erfolgt oder erfolgen könnte, wird man den Einsatz dieser Mittel nicht generell als außerhalb der Identifizierungswahrscheinlichkeit ansiedeln können.[24] In diesem Sinne ist das relative Verständnis des Personenbezugs um die Recht-

5 Simitis/Hornung/Spiecker gen. Döhmann-Hansen, DS-GVO/BDSG Art. 4 Nr. 5 Rn. 4; Schwartmann/Weiß (Hrsg.), Whitepaper zur Pseudonymisierung 2017, S. 10 f.

6 Schwartmann/Weiß (Hrsg.), Whitepaper zur Pseudonymisierung 2017, S. 14; Simitis/Hornung/Spiecker gen. Döhmann-Hansen, DS-GVO/BDSG Art. 4 Nr. 5 Rn. 16.

7 Schwartmann/Weiß (Hrsg.), Whitepaper zur Pseudonymisierung 2017, S. 15; Simitis/Hornung/Spiecker gen. Döhmann-Hansen, DS-GVO/BDSG Art. 4 Nr. 5 Rn. 17.

8 Simitis/Hornung/Spiecker gen. Döhmann-Hansen, DS-GVO/BDSG Art. 4 Nr. 5 Rn. 17. Zur Schutz- und Ermöglichungsfunktion der Pseudonymisierung vgl. ausführlich Mühlenbeck, Anonyme und pseudonyme Daten, Kap. 3 A. I. (erscheint demnächst).

9 Dazu sowie zum Streitstand vgl. Simitis/Hornung/Spiecker gen. Döhmann-Karg, Art. 4 Nr. 1 Rn. 57 ff. sowie HK-DS-GVO/BDSG-Schwartmann/Mühlenbeck, Art. 4 Nr. 1 Rn. 35 f. Dazu auch Mühlenbeck, Anonyme und pseudonyme Daten, Kap. 2 B. II. 2. c. cc. (1) (c) (aa) und (bb) (erscheint demnächst).

10 Simitis/Hornung/Spiecker gen. Döhmann-Karg, Art. 4 Nr. 1 Rn. 59 m.w.N.; HK-DS-GVO/BDSG-Schwartmann/Mühlenbeck, Art. 4 Nr. 1 Rn. 35 f. m.w.N.

11 Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 25 ff.; Simitis/Hornung/Spiecker gen. Döhmann-Karg, Art. 4 Nr. 1 Rn. 58. Zum Meinungsstreit sowie Gemeinsamkeiten und Unterschieden vgl. Mühlenbeck, Anonyme und pseudonyme Daten ab Kap. 2 B. II. 2. c. (erscheint demnächst).

12 EuGH, Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579.

13 EuGH, Urt. v. 19.10.2016 – C-582/14 Rn. 43, NJW 2016, 3579 (3581). Dazu auch Simitis/Hornung/Spiecker gen. Döhmann-Karg Art. 4 Nr. 1 Rn. 61.

14 EuGH, Urt. v. 19.10.2016 – C-582/14 Rn. 48 f., NJW 2016, 3579 (3581).

15 EuGH, Urt. v. 19.10.2016 – C-582/14 Rn. 46, NJW 2016, 3579 (3581).

16 Simitis/Hornung/Spiecker gen. Döhmann-Karg, Art. 4 Nr. 1 Rn. 61; HK-DS-GVO/BDSG-Schwartmann/Mühlenbeck Art. 4 Nr. 1 Rn. 40.

17 Wójtowicz/Cebulla, PinG 2017, 186 (189 f.).

18 Dazu etwa Simitis/Hornung/Spiecker gen. Döhmann-Karg, Art. 4 Nr. 1 Rn. 62.

19 HK-DS-GVO/BDSG-Schwartmann/Mühlenbeck, Art. 4 Nr. 1 Rn. 38 m.w.N.

20 Gierschmann/Schlender/Stentzel/Veil-Buchholtz/Stentzel, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 11; HK-DS-GVO/BDSG-Schwartmann/Mühlenbeck, Art. 4 Nr. 1 Rn. 38.

21 Dazu etwa Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 29; Simitis/Hornung/Spiecker gen. Döhmann-Karg, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 64.

22 EuGH Urt. v. 19.10.2016 – C-582/14 Rn. 46, NJW 2016, 3579 (3581).

23 Simitis/Hornung/Spiecker gen. Döhmann-Karg, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 64.

24 Simitis/Hornung/Spieker gen. Döhmann, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 64.

sprechung des EuGH und nach Maßgabe von ErwG 26 S. 3 und 4 auch um den Einsatz rechtswidriger Mittel zu erweitern.[25] Entscheidend ist aber vor allem die Erkenntnis, dass das aus der DS-GVO abzuleitende Verständnis des Personenbezugs nach ErwG 26 S. 3 und 4 letztlich vor allem auf faktische Maßstäbe bezüglich des (Nicht-)Vorliegens des Personenbezugs rekurriert, indem die tatsächlichen und rechtlichen Mittel des Verantwortlichen oder eines konkreten Dritten, über den der Verantwortliche die betroffene Person bestimmen lassen kann, entscheidend sind.[26]

V. Folgen für die Beurteilung der Pseudonymität und Anonymität von Daten

Dieses Begriffsverständnis des Personenbezugs hat unmittelbare Auswirkungen auf die Voraussetzungen einer Pseudonymität und Anonymität von Daten.[27] Im Rahmen der Pseudonymität stellt sich die praktisch wichtige Frage, ob pseudonyme Daten mitunter für einen Verantwortlichen anonym sein können.[28] Da sich die Frage des Personenbezugs nach Art. 4 Nr. 1 DS-GVO und den oben genannten Maßstäben eines erweiterten relativen Begriffsverständnisses im Sinne von ErwG 26 S. 3 und 4 richtet,[29] so muss letztlich in der Konsequenz dieses Verständnisses auch einer Pseudonymisierung unterzogenen personenbezogenen Daten bzw. pseudonymen Daten anonymisierende Wirkung[30] zukommen können, wenn ein Zugriff auf die Zuordnungsinformation letztlich nach allgemeinem Ermessen unverhältnismäßig oder unmöglich ist.[31] Hierbei hängt die Identifizierungswahrscheinlichkeit insbesondere von der technisch-organisatorischen Ausgestaltung des Pseudonymisierungsverfahrens ab, etwa davon, ob die Pseudonymisierung durch den Verantwortlichen i.S.v. ErwG 29 selbst oder durch Einbindung Dritter oder sonstiger vertrauenswürdiger Stellen durchgeführt wurde.[32] Ferner ist entscheidend, welches Pseudonymisierungsverfahren zum Einsatz kommt[33] und welche technischen Eigenschaften die Pseudonyme[34] aufweisen. Die technisch-organisatorische Ausgestaltung der Pseudonymisierung wirkt sich damit nach ErwG 26 S. 3 und 4 auf die Frage des Personenbezugs aus und muss in diesem Sinne auch zu einer Anonymität des Datums führen können.[35] Dies ist auch vor dem Hintergrund angezeigt, dass der DS-GVO aufgrund von ErwG 26 S. 3 und 4 ein faktischer Anonymitätsbegriff zugrunde liegt.[36] Das faktische Anonymitätsverständnis lässt sich hierbei letztlich auf das (erweiterte) relative Begriffsverständnis des Personenbezugs zurückführen.[37] Dies zeigt, dass sich Fragen des Personenbezugs, insbesondere der Pseudonymität und Anonymität nach der Grundkonzeption der DS-GVO über technisch-organisatorische Maßnahmen maßgeblich steuern lassen. Die DS-GVO hat es sich ausweislich Art. 1 Abs. 1 und 2 DS-GVO zum Ziel gesetzt, personenbezogene Daten zu schützen, aber auch den freien Verkehr von Daten zu ermöglichen. Aus diesem Grund weist ErwG 4 S. 2 darauf hin, dass das Recht auf Schutz personenbezogener Daten kein uneingeschränktes Recht ist, sondern vielmehr unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss. Bedeutsam sind hierbei insbesondere die unternehmerischen Freiheiten nach ErwG 4 S. 3. Der Schutz- und Ermöglichungsfunktion sowohl von einer Pseudonymisierung als auch einer Anonymisierung lässt sich also über ein Verständnis des Personenbezugs im Sinne der Ziele der DS-GVO Rechnung tragen. Kennzeichnend ist hierbei, dass die DS-GVO von einer hohen Faktizität abhängig ist, deren Ursache freilich in ihrer Entwicklungs- und Technologieoffenheit (ErwG 26 S. 4) liegt. Zur Veranschaulichung mögen folgende Beispiele dienen:

Bsp. für mögliche Anonymität

Eine Arbeitgeberin veranstaltet eine Videokonferenz mit ihren Mitarbeitenden. Hierfür nutzt sie einen Videokonferenz-Anbieter. Ein Mitarbeiter kommt zu spät in die Konferenz, allerdings noch vor der Arbeitgeberin. Alle anderen Mitarbeitenden in der Videokonferenz wissen, welcher Mitarbeiter zu spät in die Konferenz kam. Weil die Konferenz durch einen der Mitarbeitenden aufgesetzt wurde, hat die Arbeitgeberin keinen Zugriff auf die Einwahldaten. Ist das Datum („Ein Mitarbeiter kam zu spät") für die Arbeitgeberin personenbezogen?

Im Sinne obiger Ausführungen hängt der Personenbezug nach ErwG 26 S. 3 und 4 maßgeblich davon ab, über welche rechtlichen und tatsächlichen Mittel die Arbeitgeberin verfügt, um den „Zuspätkommer" zu identifizieren. Nimmt man an, dass die Arbeitgeberin im Rahmen ihres Weisungs- und Direktionsrechts die anderen Mitarbeitenden nicht zum „Verpetzen" anweisen und nicht auf die LogIn-Daten des Videokonferenz-Anbieters zugreifen kann, so bedarf die Frage nach dem Personenbezug besonderer Aufmerksamkeit und kann im Sinne der hier vertretenen Auffassung für die Arbeitgeberin zur Anonymität des Datums führen.

Bsp. für mögliche Pseudonymität

Beispiel wie oben. Die Arbeitgeberin kann allerdings auf die durch den Videokonferenz-Anbieter gespeicherten LogIn-Daten der Videokonferenz zugreifen, weil ihr Unternehmen die

25 In diese Richtung ebenfalls Simitis/Hornung/Spiecker gen. Döhmann-Karg, DS-GVO/BDSG Art. 4 Nr. 1 Rn. 64. Dazu auch Mühlenbeck, Anonyme und pseudonyme Daten, Kap. 2 B. II. 2. c. (gg) (β) (erscheint demnächst).

26 Roßnagel, ZD 2017, 243 (244 f.).

27 Dazu ausführlich Roßnagel, ZD 2018, 243 (244 ff.) sowie Wójtowicz/Cebulla, PinG 2017, 186 (186 ff.).

28 Dazu Roßnagel, ZD 2018, 243 (245); Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG Art. 4 Nr. 5 Rn. 12; Sydow-Ziebarth, DS-GVO Art. 4 Nr. 5 Rn. 95 ff.

29 Roßnagel, ZD 2018, 243 (244 f.).

30 Zum Begriff Roßnagel, ZD 2018, 243 (245).

31 Roßnagel, ZD 2018, 243 (245). Dazu auch Mühlenbeck, Anonyme und pseudonyme Daten, ab Kap. 3 B. II. b. bb. (2) (erscheint demnächst).

32 Roßnagel, ZD 2018, 243 (244 und 245). Zur Umsetzung der Pseudonymisierung nach Maßgabe von ErwG 29 vgl. Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG Art. 4 Nr. 5 Rn. 8; Simitis/Hornung/Spiecker gen. Döhmann-Hansen, DS-GVO/BDSG Art. 4 Nr. 5 Rn. 34 f.

33 Dazu Schwartmann/Weiß (Hrsg.), Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen 2018, S. 18 ff.; Simitis/Hornung/Spiecker gen. Döhmann-Hansen, DS-GVO/BDSG Art. 4 Nr. 5 Rn. 38 ff.

34 Schwartmann/Weiß (Hrsg.), Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen 2018, S. 13 f. sowie Simitis/Hornung/Spiecker gen. Döhmann-Hansen, DS-GVO/BDSG Art. 4 Nr. 5 Rn. 26 ff.

35 Dazu Roßnagel ZD 2018, 243 (245); Sydow-Ziebarth, DS-GVO Art. 4 Nr. 5 Rn. 97 m.w.N.

36 Wójtowicz/Cebulla, PinG 2017, 186 (190); BfDI Positionspapier zur Anonymisierung v. 29.06.2020, S. 4; Sydow-Ziebarth, DS-GVO Art. 4 Nr. 1 Rn. 30.

37 So wohl auch BfDI, Positionspapier zur Anonymisierung v. 29.06.2020, S. 4, der u.a. die Rechtsprechung des EuGH in der Rs. Breyer zur Begründung eines faktischen Anonymitätsbegriffs heranzieht. Vgl. dazu auch ausführlich Wójtowicz/Cebulla, PinG 2017, 186 (186 und 189).

Konferenz aufgesetzt hat und deshalb mit diesem einen entsprechenden Dienstleistungsvertrag geschlossen hat. Ist das Datum über den „Zuspätkommer" für sie immer noch anonym?

Wenn sich in diesem Sinne die rechtlichen und tatsächlichen Möglichkeiten der Arbeitgeberin ändern, so beeinflusst dies unmittelbar die nach ErwG 26 S. 3 und 4 anzustellende Risikoprognose und Wahrscheinlichkeit einer Identifizierung. Ist ein Zugriff auf die Zuordnungsinformation durch die Arbeitgeberin (hier: LogIn-Daten) nicht mit hinreichender Sicherheit ausgeschlossen, so rückt dies das Inhaltsdatum in die Nähe einer Pseudonymität und begründet damit den Personenbezug des Datums.

VI. Kollision mit Verständnis der gemeinsamen Verantwortlichkeit nach Art. 4 Nr. 7 und Art. 26 DS-GVO?

Besondere Beachtung verdient die Frage, ob und inwieweit das Verständnis des Personenbezugs und die dort bestehenden Zurechnungsregeln aufgrund der Rechtsprechung des EuGH in den Rs. Fanpage,[38] Jehova[39] und FashionID[40] eine Abweichung erfährt. Der EuGH hat in den Urteilen bekräftigt, dass er ein weites Begriffsverständnis des Verantwortlichen und der gemeinsamen Verantwortlichkeit befürwortet.[41] Aus der sich daraus ergebenden Weite einer gemeinsamen Verantwortlichkeit kann sich daher bei der Beurteilung des Personenbezugs eines Datums eine Ausweitung derjenigen Stellen ergeben, auf deren Mittel und Kenntnisse es für die Identifizierung der betroffenen Person ankommt. ErwG 26 S. 3 und 4 hat die Fähigkeit dafür zu sorgen, den Begriff des Verantwortlichen und der gemeinsamen Verantwortlichkeit in das Verständnis des Personenbezugs miteinzubeziehen, so dass Verantwortliche bei der Ausgestaltung eines Pseudonymisierungs- oder Anonymisierungsverfahrens die Rechtsprechung des EuGH entsprechend zu berücksichtigen haben, etwa indem über entsprechende Rechte- und Rollenkonzepte oder verschiedene Verarbeitungsschritte i.S.d. Rechtsprechung des EuGH eine gemeinsame Verantwortlichkeit und damit eine Zurechnung der Mittel und Kenntnisse der jeweils anderen Stelle gerade nicht erfolgt.

VII. Anforderungen nach den neuen EU-Datenakten und Ausblick

Insbesondere der Entwurf des Data Act (DA-E) sowie der Data Governance Act (DGA) fordern von der DS-GVO einen souveränen und interessengerechten Umgang mit rechtlichen Fragen des Personenbezugs. Nach Art. 1 Abs. 3 DA-E berührt die Verordnung die Anwendbarkeit der DS-GVO nicht, sondern setzt die Rechtmäßigkeit der Verarbeitung nach dieser vielmehr voraus. Nach ErwG 8 des DA-E sollen hierbei alle an einer Datennutzung Beteiligten Maßnahmen zum Schutz von personenbezogenen Daten ergreifen, wozu insbesondere eine Pseudonymisierung von Daten gehört. Art. 1 Abs. 2 DGA, Art. 5 Abs. 3 sowie Art. 7 Abs. 2 DGA setzen ebenfalls auf Maßnahmen zum technisch-organisatorischen Datenschutz, wozu eine Pseudonymisierung und Anonymisierung von Daten als Grundpfeiler zählen. Beide europäischen Rechtsakte eröffnen neue Wege des Datenzugangs, der Datennutzung und -weitergabe. An diesen praktischen Anforderungen der Digitalisierung und des Umgangs mit Daten muss sich nun auch die DS-GVO und mit ihr das Verständnis des Personenbezugs messen lassen.[42]

VIII. Fazit

Die digitale Lebenswirklichkeit erfordert es in Übereinstimmung mit den rechtlichen Vorgaben der DS-GVO, der Pseudonymisierung und Anonymisierung mit Blick auf ihren Identitätsschutz auch eine tatsächliche Ermöglichungsfunktion einzuräumen und Möglichkeiten des Umgangs mit Daten nicht über ein extensives und absolutes Verständnis des Personenbezugs einzuschränken. Andernfalls würde die DS-GVO den ihr nun nachfolgenden Datenakten letztlich ihren Anwendungsbereich nehmen, etwa weil die Rechtmäßigkeitsanforderungen der DS-GVO als „Vorbedingung" für die mit dem DA-E oder DGA einhergehenden Datenverarbeitungen nicht zu erfüllen sind. Dem ist auch über ein Verständnis des Personenbezugs Rechnung zu tragen. Die DS-GVO ist in ihrer Entwicklungsoffenheit für eine Vielzahl von künftigen Verarbeitungssituationen ausgelegt. Pseudonymisierung und Anonymisierung und ein an der DS-GVO orientiertes Begriffsverständnis des Personenbezugs zeigen, dass eine Öffnung für die Nutzbarkeit von Daten nicht mit einer Einbuße des Schutzniveaus einhergehen muss.

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

Robin L. Mühlenbeck
Wissenschaftlicher Mitarbeiter der Kölner Forschungsstelle für Medienrecht an der TH Köln. Er beschäftigt sich im Rahmen seiner wissenschaftlichen Arbeit vorrangig mit medien- und datenschutzrechtlichen Fragestellungen.

Foto: TH Köln/Schmülgen

38 EuGH, Urt. v. 05.06.2018 – C-210/16, EuZW 2018, 534.

39 EuGH, Urt. v. 10.07.2018 – C-25/17, ZD 2018, 469.

40 EuGH, Urt. v. 29.07.2019 – C-40/17, MMR 2019, 579.

41 EuGH, Urt. v. 05.06.2018 – C-210/16 Rn. 28, EuZW 2018, 534 (536); EuGH, Urt. v. 10.07.2018 – C-25/17 Rn. 66, ZD 2018, 469 (472); EuGH, Urt. v. 29.07.2019 – C-40/17 Rn. 65, MMR 2019, 579 (581).

42 Dazu Benedikt, RDV 2022, in diesem Heft; Schwartmann, Pricacy Sells versus Sell Privacy, F.A.Z. v. 27.06.2022 https://www.faz.net/aktuell/wirtschaft/digitec/datenrecht-in-europa-privacy-sells-versus-sell-privacy-18130399.html; Brink/Oetjen/Schwartmann/Voß, „So war die DS-GVO nicht gemeint.". F.A.Z. vom 18.07.2022 https://www.faz.net/aktuell/wirtschaft/digitec/so-war-die-DS-GVO-nicht-gemeint-was-bei-ihrer-anwendung-schieflaeuft-18179521.html#:~:text=So%20war%20sie%20nicht%20gemeint,und%20den%20Einsatz%20K%C3%BCnstlicher%20Intelligenz.

Kurzbeiträge

Aus den aktuellen Berichten der Aufsichtsbehörden (62): Feststellungen zu betrieblichen/behördlichen Datenschutzbeauftragten im 50. Tätigkeitsbericht Datenschutz des Hessischen Beauftragten für Datenschutz und Informationssicherheit (HDI) für das Jahr 2021

Interessenkonflikte bei Datenschutzbeauftragten

Zusammengestellt von Prof. Peter Gola*

Vorbemerkung

Unter Ziffer 1.4 seines Berichts erörtert der HDI auf Grund von Nachfragen die Vereinbarkeit der Tätigkeit als Datenschutzbeauftragter mit anderen Tätigkeiten im Unternehmen oder bei der öffentlichen Stelle. Er weist darauf hin, dass Art. 38 Abs. 6 DS-GVO zu Interessenkonflikten bei Datenschutzbeauftragten lediglich eine kurze Regelung enthält, wodurch die praktische Anwendung der Norm mit einigen Unsicherheiten verbunden sei.

I. Parallel wahrzunehmende Aufgaben nur ohne Interessenkonflikt

Hierzu hält der HDI zunächst fest: „Grundsätzlich können Datenschutzbeauftragte neben den mit der Benennung einhergehenden Aufgaben (vgl. Art. 39 Abs. 1 DS-GVO) auch andere Aufgaben und Pflichten wahrnehmen, sofern diese sonstigen Tätigkeiten nicht zu einem Interessenkonflikt führen. Die Abwesenheit von Interessenkonflikten steht im engen Zusammenhang mit dem Erfordernis einer unabhängigen Tätigkeit (Art. 38 Abs. 3 Satz 1 DS-GVO). Es handelt sich sowohl um eine Benennungsvoraussetzung als auch – nach der Benennung – um eine Organisationspflicht des Verantwortlichen und des Auftragsverarbeiters: Demgemäß dürfen Datenschutzbeauftragte innerhalb des Unternehmens keine Position innehaben, bei der sie über die Zwecke und Mittel der Verarbeitung personenbezogener Daten anderer Organisationseinheiten in anderen Organisationseinheiten entscheiden. Anderes gilt natürlich für eigene, mit ihrem Job verbundene Datenverarbeitungen. Um dies sicherzustellen, ist aufgrund der strukturellen Unterschiede des jeweiligen Unternehmens oder der jeweiligen Branche stets eine Einzelfallbetrachtung vorzunehmen. Gleichwohl lassen sich einige Leitlinien herausarbeiten.“ Anderes gilt natürlich für eigene, mit ihrem Job verbundene Datenweiterverarbeitung.

II. Beispiele von Interessenkonflikten

Interessenkonflikte können sich regelmäßig aus der Stellung im Unternehmen ergeben (Inhaber, Mitglieder der Geschäftsführung oder des Vorstandes). Diese Personen sind originär für die Rechtmäßigkeit der Datenverarbeitung beim Verantwortlichen oder beim Auftragsverarbeiter verantwortlich und können sich nicht wirksam selbst kontrollieren (siehe auch Art. 38 Abs. 3 Satz 3 DS-GVO, nach dem der Datenschutzbeauftragte unmittelbar der höchsten Managementebene berichtet).

Ferner ist in der Regel die Benennung von Leitungspersonen nicht zulässig: Dies gelte insbesondere für die Leitung der Personalabteilung (aufgrund der damit einhergehenden Verantwortung für den Umgang mit Beschäftigtendaten), die Leitung der IT-Abteilung (wegen der mit dieser Funktion einhergehenden Verantwortung für die technisch-organisatorischen Maßnahmen) sowie die Leitung der Marketing- oder Vertriebsabteilung (wegen der Verantwortung für den Umgang mit Kundendaten).

Auch eine Benennung bei hierarchisch nachgeordneten Positionen wie etwa Beschäftigte der IT- (insbesondere mit Administratorenrechten) oder Personal-Abteilung ist regelmäßig unzulässig, sofern diese in der Lage sind, Datenverarbeitungsprozesse zu bestimmen oder wesentlich zu beeinflussen.

Des Weiteren ist die Benennung eines Datenschutzbeauftragten regelmäßig unzulässig, sofern dieser ein besonderes wirtschaftliches Interesse an dem Unternehmenserfolg hat (etwa Gesellschafter sowie Familienangehörige der Geschäftsleitung).

Bei einem IT-Sicherheitsbeauftragten ist häufig ein Interessenkonflikt anzunehmen, da er zwecks Entdeckung von Missbrauch an umfassenden Sammlungen personenbezogener Daten interessiert sein muss. Ein Interessenkonflikt sei noch offensichtlicher, sofern der IT-Sicherheitsbeauftragte Aufgaben der Umsetzung (mit Budgetverantwortung) innehabe.

Auch bei Compliance-Beauftragten sowie bei den Leitern der Rechtsabteilung sieht der HDI ggf. einen Interessenkonflikt, da diese oftmals in die unternehmensinternen Geschäftsprozesse derart eingebunden seien, dass sie aufgrund dieser weitergehenden Aufgabenwahrnehmung nicht mehr über die notwendige Unabhängigkeit in der Bewertung einzelner Datenverarbeitungsprozesse verfügen. Gleichwohl könne dies je nach der Aufgabenwahrnehmung

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

im Einzelfall auch anders zu bewerten sein (siehe dazu Bergt, in: Kühling/Buchner, Art. 38 Rn. 42; sowie abwägend Heberlein, in: Ehmann/Selmayr, Art. 38 Rn. 23).

Interessenkonflikte können auch bei externen Datenschutzbeauftragten auftreten. Es bedarf einer vertraglichen Regelung mit dem externen Dienstleister, die diesbezügliche Tätigkeiten untersagt. Ein unzulässiger Interessenkonflikt läge vor, wenn der externe Datenschutzbeauftragte gleichzeitig IT-Dienstleistungen erbringt oder den „Besteller" in datenschutzrelevanten Rechtsstreitigkeiten vor Gericht vertritt.

Ein Interessenkonflikt bei behördlichen Datenschutzbeauftragten besteht ähnlich wie im nicht öffentlichen Bereich regelmäßig bei der Behördenleitung, bei dem Bürgermeister einer Gemeinde sowie bei herausgehobenen Leitungstätigkeiten (insbesondere bei der Leitung der Personalabteilung und bei der Leitung der IT-Abteilung). Grundsätzlich zulässig ist die Tätigkeit des DSB im Justiziariat ohne Leitungsfunktion sowie die Leitung des Rechnungsprüfungsamtes.

III. Konsequenzen

Der HDI weist sodann darauf hin, dass ihm im Falle eines Interessenkonfliktes verschiedene aufsichtsrechtliche Maßnahmen zur Verfügung stehen. Neben dem Hinweis auf einen Verstoß gegen die DS-GVO kann er ggf. gemäß Art. 58 Abs. 1 lit. d DS-GVO nach § 40 Abs. 6 Satz 2 BDSG die Abberufung des Datenschutzbeauftragten verlangen, wenn ein „schwerwiegender Interessenkonflikt" vorliegt (vgl. Art. 58 Abs. 6 DS-GVO). Allerdings rechtfertigt nicht jeder Interessenkonflikt die Abberufung, vielmehr müsse dieser offenkundig sein (etwa bei dem Leiter der IT-Abteilung, siehe Dix, in: Kühling/Buchner, § 40 Rn. 17 m.w.N. auch zu der Frage der Europarechtskonformität der Regelung).

Des Weiteren sind Verstöße gegen die Vermeidung von Interessenkonflikten nach Art. 83 Abs. 4 lit. a DS-GVO bußgeldbewehrt.

Für hessische öffentliche Stellen übernimmt § 7 Abs. 2 HDSIG die Vorschrift des Art. 38 Abs. 6 DS-GVO. Gleichwohl sind die Sanktionsmöglichkeiten bei behördlichen Datenschutzbeauftragten merklich eingeschränkt. Zwingend, aber vom HDI nicht durchsetzbar, ist im Falle eines nicht behebbaren Interessenkonflikts die Abberufung (vgl. § 6 Abs. 3 Satz 3 HDSIG).

Praxisfälle zum Datenschutzrecht XVIII: Videoüberwachung im Pausenraum

RAin Yvette Reif, LL.M.*

I. Sachverhalt

Das Kaufhaus K verfügt über einen „Sozialraum", in den sich die Verkäufer/-innen in den Pausenzeiten zurückziehen können, um sich auszuruhen und Mahlzeiten zu sich zu nehmen. Der Sozialraum wird videoüberwacht mit der Zweckbestimmung „Schutz des Eigentums der Mitarbeiter/-innen". Als Begründung wird angeführt, dass in der Vergangenheit bereits Wertgegenstände von Mitarbeitern abhandengekommen seien, die diese nach der Pause nicht in ihre Spinde gebracht, sondern im Sozialraum gelassen haben.

Die Datenschutzbeauftragte D wird auf die Maßnahme aufmerksam. Was sollte sie tun? Ergibt sich ein Unterschied, wenn der Betriebsrat der Videoüberwachungsmaßnahme zugestimmt hat und eine diesbezügliche Betriebsvereinbarung geschlossen wurde?

II. Musterfalllösung

1. Allgemeines

Die Aufgaben eines/einer Datenschutzbeauftragten ergeben sich aus Art. 39 DS-GVO. Kernaufgaben sind danach zum einen die Unterrichtung und Beratung des Verantwortlichen oder Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, zum anderen die Überwachung der Einhaltung des Datenschutzrechts beim Verantwortlichen bzw. Auftragsverarbeiter (Art. 39 Abs. 1 lit. a und b DS-GVO). D hat insofern die Aufgabe, die Rechtmäßigkeit der Videoüberwachung zu überprüfen und, sofern diese rechtswidrig sein sollte, gegenüber der Geschäftsleitung die Empfehlung auszusprechen, die Anlage zu deinstallieren. Eigene Weisungsrechte stehen dem/der Datenschutzbeauftragten nicht zu. Als reines Beratungs- und Überwachungsorgan könnte D die Deinstallation der Anlage also nicht selbst anweisen.

2. Rechtmäßigkeit der Videoüberwachung

Entscheidend für das weitere Tätigwerden von D ist die Beantwortung der Frage, ob die Videoüberwachungsanlage im „Sozialraum" des Kaufhauses rechtmäßig ist oder nicht.

Insofern stellt sich zunächst die Frage nach der einschlägigen Rechtsgrundlage für die Beurteilung der Rechtmäßig-

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

keit. Die DS-GVO enthält keine speziellen Vorgaben zur Videoüberwachung, jedoch findet sich eine spezifische Regelung hierzu in § 4 BDSG, die vorliegend einschlägig sein könnte. Allerdings hat § 4 BDSG nur einen eingeschränkten Anwendungsbereich, nämlich „die Beobachtung öffentlich zugänglicher Räume", vgl. Abs. 1 S. 1 der Regelung. Öffentlich zugänglich sind Räume, wenn sie dem öffentlichen Verkehr gewidmet sind oder nach dem erkennbaren Willen des Berechtigten von jedermann genutzt bzw. betreten werden können.[1] Dies gilt etwa für Bahnsteige, Ladenpassagen, Banken, Museen, aber auch allgemein zugängliche Bereiche von Wohnungs- und Bürogebäuden wie Treppenhäuser oder Fahrstühle.[2] Eine vergleichbare Räumlichkeit stellt der „Sozialraum" des Kaufhauses nicht dar. Unternehmensbereiche, die nicht dem öffentlichen Verkehr gewidmet sind oder aufgrund erkennbarer Beschränkungen nicht von jedermann tatsächlich betreten werden, unterfallen nicht § 4 BDSG.[3] Pausen- und Aufenthaltsräume für Kaufhausmitarbeiter/-innen befinden sich typischerweise außerhalb öffentlich zugänglicher Verkaufsflächen. Für den Zugang müssen regelmäßig Bereiche passiert werden, bei denen selbst ohne entsprechende Kennzeichnung oder Absicherung klar ist, dass diese nicht den Kunden gewidmet sind. § 4 BDSG kommt damit vorliegend nicht zur Anwendung. Ohnedies soll nach einer Entscheidung des Bundesverwaltungsgerichts (BVerwG) aus dem Jahr 2019[4] kein Raum für eine Anwendung des hier einzig in Betracht kommenden § 4 Abs. 1 S. 1 BDSG auf Videoüberwachungen privater Verantwortlicher bestehen. Nach Ansicht des Gerichts ist diese Konstellation nicht von den DS-GVO-Öffnungsklauseln erfasst und § 4 Abs. 1 S. 1 BSDG insoweit europarechtswidrig. In dem der Entscheidung des BVerwG zugrundeliegenden Sachverhalt filmte eine Zahnärztin den Eingangsbereich ihrer Praxis.

Als Rechtsgrundlage der Datenverarbeitung im Zusammenhang mit der Videoüberwachungsanlage kommt hier nur die sog. Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO in Betracht. Nach der genannten Regelung ist eine Verarbeitung personenbezogener Daten gestattet, sofern diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Ob die Voraussetzungen von Art. 6 Abs. 1 lit. f DS-GVO vorliegen, ist im Rahmen einer dreistufigen Prüfung zu ermitteln. In einem ersten Schritt ist hierbei das Vorliegen eines berechtigten Interesses des Verantwortlichen bzw. eines Dritten festzustellen. Im zweiten Schritt ist sodann die Erforderlichkeit der Datenverarbeitung zur Wahrung des berechtigten Interesses zu prüfen. Schließlich bedarf es im letzten Schritt der Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Personen im konkreten Einzelfall.

Der Begriff des berechtigten Interesses i.S.v. Art. 6 Abs. 1 lit. f DS-GVO ist grundsätzlich weit zu verstehen, so dass die erste Stufe der Interessenabwägung eine relativ niedrige Hürde darstellt.[5] Nur eine weite Interpretation vermag den Grundrechten und -freiheiten der datenverarbeitenden Stelle angemessen Rechnung zu tragen. Ein solches Verständnis unterminiert auch nicht die Rechte der betroffenen Person, da die eigentliche Rechtmäßigkeitsprüfung erst auf Ebene der Abwägung stattfindet.[6] Als berechtigte Interessen kommen im Ergebnis alle rechtlichen, tatsächlichen, wirtschaftlichen oder ideellen Interessen des Verantwortlichen bzw. eines Dritten in Betracht, die mit der Rechtsordnung vereinbar sind.[7] Nach Angabe des Verantwortlichen hat die vorliegend zu beurteilende Videoüberwachung die Zweckbestimmung „Schutz des Eigentums der Mitarbeiter/-innen". Es ist unzweifelhaft, dass hieran ein grundsätzlich berechtigtes Interesse besteht, insbes. deckt Art. 6 Abs. 1 lit. f DS-GVO, wie angesprochen, auch Datenverarbeitungen im Drittinteresse (hier: im Interesse der Mitarbeiter/-innen des Verantwortlichen).

Fraglich ist allerdings, ob die Videoüberwachung vorliegend zur Erreichung des berechtigten Interesses Eigentumsschutz erforderlich ist oder ob im konkreten Fall nicht weniger eingriffsintensive Mittel zur Verwirklichung dieses Interesses zur Verfügung stehen. Hierfür spricht, dass die Mitarbeiter/-innen laut Sachverhalt die Möglichkeit haben, ihre Wertsachen in einem Spind zu verschließen. Es bestehen aus Sicht des Arbeitgebers also weniger invasive Methoden die Wertsachen vor Diebstahl zu schützen, nämlich, die Mitarbeiter/-innen anzuweisen, die vorhandenen Spinde zu verwenden. Mitarbeiter/-innen, die sich hieran nicht halten, sind nicht schutzwürdig. Eine Rechtfertigung der Datenverarbeitung iR der Videoüberwachung über Art. 6 Abs. 1 lit. f DS-GVO scheitert also bereits auf der zweiten Stufe, nämlich mangels Erforderlichkeit der Verarbeitung zur Wahrung des berechtigten Interesses.

Unabhängig davon gilt, dass bei einer Videoüberwachung am Arbeitsplatz die Intim- oder Persönlichkeitssphäre der Betroffenen nicht verletzt werden darf. Ein Kameraeinsatz in sensiblen Bereichen wie Umkleidekabinen, Sanitär-, Pausen-, Sozial- und Aufenthaltsräumen ist daher unzulässig.[8] Gerade Personen, die im Rahmen ihrer Arbeitstätigkeit typischerweise permanenter Videoüberwachung ausgesetzt sind, wie das Kaufhauspersonal im vorliegenden Fall, brauchen kontrollfreie Rückzugsorte, damit kein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht vorliegt.

1 Gola/Heckmann/Starnecker, BDSG, 13. Aufl. 2019, § 4 Rn. 23.
2 Stöber, NJW 2015, 3681, 3683.
3 Gola/Heckmann/Starnecker, BDSG, 13. Aufl. 2019, § 4 Rn. 26.
4 Urt. v. 27.03.2019, BVerwG 6 C 2.18.
5 Vgl. auch Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 57.
6 Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 57.
7 Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 57.
8 DSK, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, Stand: 17.07.2020, Abschnitt 5.1.1.

Sofern Räumlichkeiten videoüberwacht werden, die gegen Einblick besonders geschützt sind, wie z.B. Mitarbeiterumkleiden oder Toiletten, kann sogar der Straftatbestand des § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen) erfüllt sein, wonach eine Freiheitsstrafe von bis zu zwei Jahren bzw. eine Geldstrafe möglich ist.

Fazit: D sollte der Geschäftsleitung raten, die Anlage zu deinstallieren, da sie rechtswidrig ist.

3. Auswirkungen einer zugrundeliegenden Betriebsvereinbarung

Nach § 26 Abs. 4 S. 1 BDSG kommt als Grundlage einer Verarbeitung von Beschäftigtendaten auch eine Kollektivvereinbarung in Betracht. Dies ist von erheblicher praktischer Relevanz, denn zum einen lassen sich durch Kollektivvertrag die unbestimmten Rechtsbegriffe des Datenschutzrechts konzern-, unternehmens- oder betriebsspezifisch konkretisieren, zum anderen können die Modalitäten eines unternehmens- oder konzernweiten Datenflusses geregelt werden.[9] Eine Betriebsvereinbarung ist eine Kollektivvereinbarung i.S.v. § 26 Abs. 4 S. 1 BDSG.

Die nationale Regelung hat ihre Grundlage in Art. 88 DS-GVO. Art. 88 Abs. 1 DS-GVO gestattet es den Mitgliedstaaten ausdrücklich, den Erlass von Kollektivverträgen zur Verarbeitung von Beschäftigtendaten zuzulassen. Für diese Befugnis hatte sich im Verfahren zum Erlass der DS-GVO insbesondere Deutschland stark gemacht,[10] wo die institutionalisierte Arbeitnehmervertretung in Betrieben, Unternehmen und Konzernen durch Betriebsräte lange Tradition hat. Die DS-GVO räumt den Betriebsparteien allerdings keine unbegrenzte Regelungsmacht im Hinblick auf die Beschäftigtendatenverarbeitung ein. Vielmehr haben die Verhandlungspartner von Kollektivvereinbarungen die materiellen Vorgaben aus Art. 88 Abs. 2 DS-GVO zu beachten, vgl. auch § 26 Abs. 4 S. 2 BDSG. Nach Art. 88 Abs. 2 DS-GVO umfassen Rechtsvorschriften und Kollektivvereinbarungen i.S.v. Abs. 1 der Regelung „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz."

Fraglich ist, ob die Betriebsparteien auf den ihnen eröffneten Regelungsgebieten nicht nur eine Konkretisierung, sondern auch eine Verbesserung bzw. Verschlechterung des von der DS-GVO begründeten Persönlichkeitsschutzes herbeiführen können. Als unzulässig zu betrachten ist nach herrschender Meinung jedenfalls ein Unterschreiten des Schutzniveaus der DS-GVO.[11] Dabei ist aber wohl nicht jedes partielle Abweichen „nach unten" vom Schutzstandard der DS-GVO unzulässig, sondern es ist eine Gesamtbetrachtung der innerbetrieblichen Regelung vorzunehmen und zu prüfen, ob die von Art. 88 Abs. 2 DS-GVO geforderten Maßnahmen zum Schutz der Betroffenen enthalten sind.[12] Es verbleibt also ein Regelungsspielraum, der es den Interessenvertretungen ermöglichen soll, passgenaue spezifischere Vorschriften zu schaffen.[13]

Selbst wenn man der vorbeschriebenen Ansicht folgt, die ein partielles Abweichen „nach unten" vom Schutzstandard der DS-GVO per Betriebsvereinbarung zulassen will, dürfte eine Betriebsvereinbarung im vorliegenden Fall keine wirksame Rechtsgrundlage der Datenverarbeitung per Videoüberwachung darstellen. Denn eine nicht erforderliche Videoüberwachung, noch dazu in sensiblen Bereichen des Unternehmens, welche den Beschäftigten als Rückzugsort dienen sollen, an dem sie unbeobachtet sind, stellt keine partielle, im Rahmen der Gesamtbetrachtung ggf. noch legitimierbare Abweichung vom Schutzstandard der DS-GVO dar. Vielmehr wird mit dem Grundsatz der Erforderlichkeit eine der tragenden Säulen der DS-GVO verletzt, was auch mittels Abschluss einer Betriebsvereinbarung nicht geheilt werden kann. Bei dem Grundsatz der Erforderlichkeit handelt es sich um ein „übergreifendes Prinzip" der DS-GVO, welches darin zum Ausdruck kommt, dass die gesetzlichen Erlaubnistatbestände der DS-GVO jeweils unter dem ausdrücklichen Vorbehalt stehen, dass die Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn dies im Rahmen des jeweiligen Erlaubnistatbestands erforderlich ist.[14]

Das Vorliegen einer die Datenverarbeitung im Zusammenhang mit der Videoüberwachung rechtfertigenden Betriebsvereinbarung kann folglich an dem unter 1. gefundenen Ergebnis nichts ändern.

9 Kühling/Buchner/Maschmann, DS-GVO BDSG, 3. Aufl. 2020, BDSG § 26 Rn. 65 unter Hinweis auf die Gesetzesbegründung zu § 26 BDSG.

10 Kühling/Buchner/Maschmann, DS-GVO BDSG, 3. Aufl. 2020, BDSG § 26 Rn. 66.

11 Gola, Handbuch Beschäftigtendatenschutz, 8. Aufl., Rn. 1958 ff., 1966 ff.

12 Heidelberger Kommentar DS-GVO/BDSG/Thüsing/Schmidt, § 26 BDSG Rn. 50 m.w.N.

13 Heidelberger Kommentar DS-GVO/BDSG/Thüsing/Schmidt, § 26 BDSG Rn. 50.

14 Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 6 Rn. 15.

Rechtsprechung

EuGH bestätigt Unionsrechtswidrigkeit der allgemeinen und anlasslosen Vorratsdatenspeicherung von Verkehrs- und Standortdaten im TKG und benennt Fälle zulässiger Datenspeicherungen

(**Europäischer Gerichtshof**, Urteil vom 20. September 2022 – C-793/19 und C-794/19 – SpaceNet AG und Telekom Deutschland GmbH –)

Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union [ist] dahin auszulegen, dass er nationalen Rechtsvorschriften entgegensteht, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen; er nationalen Rechtsvorschriften nicht entgegensteht, die

– es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht;

– zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;

– zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen

– zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;

– es zur Bekämpfung schwerer Kriminalität und, a fortiori, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.

Zur Vorlagefrage

Mit seiner Vorlagefrage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 6 bis 8 und 11 sowie des Art. 52 Abs. 1 der Charta und des Art. 4 Abs. 2 EUV dahin auszulegen ist, dass er einer nationalen Rechtsvorschrift entgegensteht, die – von bestimmten Ausnahmen abgesehen – die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste für die in Art. 15 Abs. 1 der genannten Richtlinie aufgeführten Zwecke, insbesondere zur Verfolgung schwerer Straftaten oder zur Abwehr einer konkreten Gefahr für die nationale Sicherheit, zu einer allgemeinen und unterschiedslosen Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten der Endnutzer dieser Dienste verpflichtet und eine Speicherungsfrist von mehreren Wochen sowie Regeln vorsieht, die einen wirksamen Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang gewährleisten sollen. […]

Zu einer Maßnahme, die für eine Dauer von mehreren Wochen eine allgemeine und unterschiedslose Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vorsieht

Was erstens den Umfang der auf Vorrat gespeicherten Daten anbelangt, geht aus der Vorlageentscheidung hervor,

dass im Rahmen der Erbringung von Telefondiensten die durch diese Regelung auferlegte Pflicht zur Vorratsspeicherung insbesondere die Daten betrifft, die erforderlich sind, um die Quelle und den Adressaten einer Nachricht, Datum und Uhrzeit von Beginn und Ende der Verbindung oder – im Fall der Übermittlung von Kurz-, Multimedia- oder ähnlichen Nachrichten – die Zeitpunkte der Versendung und des Empfangs der Nachricht sowie, im Fall der mobilen Nutzung, die Bezeichnung der Funkzellen, die vom Anrufer und vom Angerufenen bei Beginn der Verbindung genutzt wurden, zu identifizieren.

[…]

Zwar nimmt die in den Ausgangsverfahren in Rede stehende nationale Regelung den Inhalt der Kommunikation sowie die Daten über aufgerufene Internetseiten von der Speicherpflicht aus und schreibt die Speicherung der Funkzellenkennung lediglich zu Beginn der Kommunikation vor, jedoch ist darauf hinzuweisen, dass dies im Wesentlichen auch für die nationalen Regelungen zur Umsetzung der Richtlinie 2006/24 galt, um die es in den Rechtssachen ging, in denen das Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), ergangen ist. Trotz dieser Beschränkungen hat der Gerichtshof in diesem Urteil aber entschieden, dass die Kategorien der nach der genannten Richtlinie und diesen nationalen Regelungen auf Vorrat gespeicherten Daten sehr genaue Schlüsse auf das Privatleben der betroffenen Personen – etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren – und insbesondere die Erstellung eines Profils dieser Personen ermöglichen konnten. […]

[Außerdem] werden u. a. Daten von Nutzern gespeichert, die dem Berufsgeheimnis unterliegen, wie beispielsweise Rechtsanwälte, Ärzte und Journalisten.

[…] Aus der Vorlageentscheidung geht somit hervor, dass die in dieser nationalen Regelung vorgesehene Vorratsspeicherung von Verkehrs- und Standortdaten nahezu alle die Bevölkerung bildenden Personen betrifft, ohne dass diese sich auch nur mittelbar in einer Lage befänden, die Anlass zur Strafverfolgung geben könnte. Ebenso schreibt sie die anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vor, deren Umfang im Wesentlichen dem der Daten entspricht, die in den Rechtssachen gespeichert wurden, die zu der […] angeführten Rechtsprechung geführt haben.

[…] In Bezug auf die in der in den Ausgangsverfahren in Rede stehenden nationalen Regelung vorgesehenen Garantien, die die gespeicherten Daten gegen Missbrauchsrisiken und vor jedem unberechtigten Zugang schützen sollen, [ist] festzustellen, dass die Vorratsspeicherung dieser Daten und der Zugang zu ihnen […] unterschiedliche Eingriffe in die in den Art. 7 und 11 der Charta garantierten Grundrechte darstellen, die eine gesonderte Rechtfertigung nach Art. 52 Abs. 1 der Charta erfordern. Daraus folgt, dass nationale Rechtsvorschriften, die die vollständige Einhaltung der Voraussetzungen gewährleisten, die sich im Bereich des Zugangs zu auf Vorrat gespeicherten Daten aus der Rechtsprechung zur Auslegung der Richtlinie 2002/58 ergeben, naturgemäß den schwerwiegenden Eingriff weder beschränken noch beseitigen können. […]

Zu den Maßnahmen, die eine gezielte Vorratsspeicherung, eine umgehende Sicherung oder eine Speicherung der IP-Adressen vorsehen

[…] Eine Rechtsvorschrift, die eine allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung vorsieht [verstößt], grundsätzlich nicht gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta, sofern diese Möglichkeit von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig gemacht wird, die die Nutzung dieser Daten regeln müssen (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 155).

Angesichts der Schwere des mit dieser Vorratsdatenspeicherung verbundenen Eingriffs in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, sind neben dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet, diesen Eingriff zu rechtfertigen. Außerdem darf die Dauer der Speicherung das im Hinblick auf das verfolgte Ziel absolut Notwendige nicht überschreiten. Schließlich muss eine derartige Maßnahme strenge Voraussetzungen und Garantien hinsichtlich der Auswertung dieser Daten, insbesondere in Form einer Nachverfolgung, in Bezug auf die Online-Kommunikationen und -Aktivitäten der Betroffenen vorsehen (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 156).

[…] Was […] die gezielte Vorratsspeicherung anbelangt, so hat der Gerichtshof entschieden, dass Art. 15 Abs. 1 der Richtlinie 2002/58 auf objektiven Kriterien beruhenden nationalen Rechtsvorschriften nicht entgegensteht, mit denen zum einen Personen erfasst werden können, deren Verkehrs- und Standortdaten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten zu offenbaren, zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit oder eine Gefahr für die nationale Sicherheit zu verhüten (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 76 und die dort angeführte Rechtsprechung).

Der Gerichtshof hat insoweit klargestellt, dass diese objektiven Kriterien zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterschiedlich sein können, zu den erfassten Personen aber insbesondere diejenigen gehören können, die zuvor im Rahmen der einschlägigen nationalen Verfahren und auf der Grundlage objektiver und nicht diskriminierender Kriterien als Bedrohung der öffentlichen Sicherheit oder der nationalen Sicherheit des betreffenden Mitgliedstaats eingestuft wurden (Urteil vom 5. April 2022,

Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 77).

Die Mitgliedstaaten haben somit u. a. die Möglichkeit, Maßnahmen zur Speicherung zu ergreifen, die Personen betreffen, die aufgrund einer solchen Einstufung Gegenstand aktueller Ermittlungen oder anderer Überwachungsmaßnahmen sind oder zu denen im nationalen Strafregister eine frühere Verurteilung wegen schwerer Straftaten vermerkt ist, die ein hohes Rückfallrisiko bedeuten können. […]

Zum anderen kann eine Maßnahme gezielter Vorratsspeicherung von Verkehrs- und Standortdaten […] auch auf ein geografisches Kriterium gestützt werden […]. Dabei kann es sich insbesondere um Orte handeln, die durch eine erhöhte Zahl schwerer Straftaten gekennzeichnet sind, um Orte, an denen die Gefahr, dass schwere Straftaten begangen werden, besonders hoch ist, wie Orte oder Infrastrukturen, die regelmäßig von einer sehr hohen Zahl von Personen aufgesucht werden, oder um strategische Orte wie Flughäfen, Seehäfen, Bahnhöfe oder Mautstellen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 79 und die dort angeführte Rechtsprechung).

Was die Möglichkeit betrifft, andere Unterscheidungskriterien […] für die Durchführung einer gezielten Vorratsspeicherung von Verkehrs- und Standortdaten vorzusehen, so kann nicht ausgeschlossen werden, dass andere objektive und nicht diskriminierende Kriterien in Betracht kommen, um sicherzustellen, dass der Umfang einer gezielten Vorratsspeicherung auf das absolut Notwendige beschränkt wird, und um eine zumindest indirekte Verbindung zwischen den schweren Straftaten und den Personen, deren Daten auf Vorrat gespeichert werden, herzustellen. Da sich Art. 15 Abs. 1 der Richtlinie 2002/58 auf Rechtsvorschriften der Mitgliedstaaten bezieht, obliegt es allerdings diesen und nicht dem Gerichtshof, solche Kriterien zu bestimmen, wobei es nicht darum gehen kann, auf diesem Weg wieder eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrs- und Standortdaten einzuführen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 83).

[…] Was […] die umgehende Sicherung der von den Betreibern elektronischer Kommunikationsdienste auf der Grundlage der Art. 5, 6 und 9 der Richtlinie 2002/58 oder auf der Grundlage von Rechtsvorschriften, die gemäß Art. 15 Abs. 1 dieser Richtlinie erlassen wurden, verarbeiteten und gespeicherten Verkehrs- und Standortdaten anbelangt, ist darauf hinzuweisen, dass solche Daten grundsätzlich nach Ablauf der gesetzlichen Fristen, innerhalb deren sie gemäß den nationalen Bestimmungen zur Umsetzung der Richtlinie verarbeitet und gespeichert werden müssen, je nach Fall, entweder gelöscht oder anonymisiert werden müssen. Allerdings hat der Gerichtshof entschieden, dass während dieser Verarbeitung und Speicherung Situationen auftreten können, die es erforderlich machen, die betreffenden Daten zur Aufklärung schwerer Straftaten oder von Beeinträchtigungen der nationalen Sicherheit über diese Fristen hinaus zu speichern, und zwar sowohl dann, wenn die Taten oder Beeinträchtigungen bereits festgestellt werden konnten, als auch dann, wenn nach einer objektiven Prüfung aller relevanten Umstände der begründete Verdacht besteht, dass sie vorliegen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 85).

In einer solchen Situation steht es den Mitgliedstaaten angesichts dessen, dass nach den Ausführungen in den Rn. 65 bis 68 des vorliegenden Urteils die widerstreitenden Rechte und berechtigten Interessen miteinander in Einklang gebracht werden müssen, frei, in Rechtsvorschriften, die sie gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassen, vorzusehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben wird, für einen festgelegten Zeitraum die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern (Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 163, sowie vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 86).

Da die Zielsetzung einer solchen umgehenden Sicherung nicht mehr den Zielsetzungen entspricht, aufgrund deren die Daten ursprünglich gesammelt und gespeichert wurden, und da nach Art. 8 Abs. 2 der Charta jede Datenverarbeitung für festgelegte Zwecke zu erfolgen hat, müssen die Mitgliedstaaten in ihren Rechtsvorschriften angeben, mit welcher Zielsetzung die umgehende Sicherung der Daten vorgenommen werden kann. Angesichts der Schwere des Eingriffs in die in den Art. 7 und 8 der Charta verankerten Grundrechte, der mit einer solchen Speicherung verbunden sein kann, sind nur die Bekämpfung schwerer Kriminalität und, a fortiori, der Schutz der nationalen Sicherheit geeignet, diesen Eingriff zu rechtfertigen, sofern diese Maßnahme sowie der Zugang zu den auf Vorrat gespeicherten Daten die Grenzen des absolut Notwendigen, wie sie in den Rn. 164 bis 167 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), dargelegt sind, einhalten (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 87).

Anmerkung zu EuGH, Urt. v. 20.09.2022 – C-793/19 und C-794/19 – SpaceNet AG und Telekom Deutschland GmbH

Der EuGH hat entschieden, die Vorratsdatenspeicherung, wie sie im TKG normiert ist (§§ 113 a ff. TKG), ist unionsrechtswidrig. Das überrasch nicht. Mit dem Urteil bestätigt der Gerichtshof seine bisherige Rechtsprechung. Wegen vermuteter Unionsrechtswidrigkeit werden die Regelungen ohnehin seit 2017 nicht mehr angewandt. Revolutionär ist das Urteil daher kaum, für die Praxis aber dennoch bedeutsam. Denn mit einer Neuregelung der Vorratsdatenspeicherung wollte die Politik warten, bis der EuGH entschieden hat. Diese Entscheidung liegt nun vor. Neben Verboten bekräftigt der EuGH in seinem Urteil auch eine Reihe an Ausnahmen bzw. Kategorien zulässiger Datenspeicherungen. Hierbei unterscheidet das Gericht im Wesentlichen anhand drei

Kriterien: Erstens dem Ziel der Datenspeicherung (Schutz der nationalen Sicherheit und Schutz vor schwerer Kriminalität), zweitens der betroffenen Datenkategorie (Verkehrs- und Standortdaten, Identitätsdaten und IP-Adressen) und drittens der Vorgehensweise der Behörden (allgemeine und unterschiedslose Vorratsdatenspeicherung, gezielte Vorratsdatenspeicherung und umgehende Sicherung).

Die Kernthesen des Gerichts lassen sich wie folgt zusammenfassen:

I. Die allgemeine und unterschiedslose Vorratsdatenspeicherung von Verkehrs- und Standortdaten ist grundsätzlich unabhängig vom Umfang der erfassten Daten und der Speicherlänge unionsrechtswidrig, und zwar auch dann, wenn sie zur Bekämpfung schwerer Kriminalität erfolgt. Eine Ausnahme gilt nur dann, wenn eine aktuelle und ernste Bedrohung für die nationale Sicherheit vorliegt. Dafür müssen laut EuGH tragende Strukturen eines Landes im Bereich Verfassung, Politik, Wirtschaft oder im sozialen Bereich real und aktuell, zumindest aber vorhersehbar bedroht sein. Hiervon dürften Bedrohungen durch Terror oder Krieg erfasst sein, wenn sie über eine latente Gefahr hinausgehen.

II. Bestimmte Formen der Vorratsdatenspeicherung sind weiterhin unionsrechtskonform möglich, auch wenn sie „nur" zum Schutz vor schwerer Kriminalität erfolgen:

1. Gezielte Vorratsspeicherung von Verkehrs- und Standortdaten, wenn sie auf der Grundlage von objektiven und nicht diskriminierenden Kriterien erfolgt. Der EuGH nennt hier ausdrücklich Kategorien betroffener Personen (bspw. Gefährder oder rückfallgefährdete Vorbestrafte) oder geografische Kriterien (bspw. Schwerpunkte der Verbrechensbegehung oder besonders gefährdete Orte wie Flughäfen und Bahnhöfe).

2. Allgemeine und unterschiedslose Vorratsdatenspeicherung von der die Identität der Nutzer elektronischer Kommunikationsmittel betreffende Daten. Ausweislich des Urteils ist es daher bspw. zulässig, den Erwerb von vorausbezahlten SIM-Karten von einer Überprüfung amtlicher Dokumente abhängig zu machen und den Verkäufer zu verpflichten, die sich daraus ergebenen Informationen, zu erfassen.

3. Allgemeine und unterschiedslose Vorratsspeicherung von IP-Adressen. Insb. zulässig ist ausweislich des EuGH die Sicherung von IP-Adressen zur Bekämpfung von Kinderpornografie. Tatverdächtige sind hier nur anhand der IP-Adressen zu ihren Anschlüssen und Endgeräten zu erkennen.

III. Die Pflicht zur umgehende Sicherung von den Betreibern elektronischer Kommunikationsmitteln zur Verfügung stehenden Verkehrs- und Standortdaten ist zum Schutz vor schwerer Kriminalität zulässig. Bei dieser unter dem Schlagwort „Quick-Freeze" diskutierten Vorgehensweise handelt es sich jedoch weder nach dem allgemeinen Begriffsverständnis noch rechtsdogmatisch um einen Fall der Vorratsdatenspeicherung. Vielmehr geht es um eine Regelung zur erleichterten Verhinderung von Datenlöschung. Das Problem begrenzter Datenverfügbarkeit wird hierdurch nicht gelöst.

Der EuGH hat damit erneut betont, was unionsrechtlich im Bereich der Vorratsdatenspeicherung möglich ist und was nicht. Wie die vom EuGH eingeräumten Spielräume genutzt werden, ist – und das ist seit Jahren klar – eine rechtspolitische Frage. Geht es nach dem Willen des Justizministeriums wird Deutschland „nur" einen sog. Quick-Freeze implementieren und damit von einer Vorratsdatenspeicherung im eigentlichen Sinne Abstand nehmen. Nancy Faeser und das Innenministerium fordern hingegen beharrlich eine zeitlich eingeschränkte IP-Adressen Speicherung. Wie der Streit ausgeht, ist auch nach dem Urteil unklar. Es dürfte die Diskussion jedoch erneut befeuert haben. Das lässt hoffen, dass der politischer Wille nun ausreicht, um endlich eine Lösung für das langsam überfällige Problem der Vorratsdatenspeicherung zu finden.

(Lucia Burkhardt, Wissenschaftliche Mitarbeiterin an der Kölner Forschungsstelle für Medienrecht)

Zum Konflikt zwischen Datenschutz und Korruptionsbekämpfung und der Veröffentlichung sensibler Daten (Ls)

(**Europäischer Gerichtshof**, Urteil vom 1. August 2022 – C-184/20 –)

Art. 7 Buchst. c der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie Art. 6 Abs. 1 Unterabs. 1 Buchst. c und Abs. 3 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) sind im Licht der Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass sie nationalen Rechtsvorschriften, nach denen die Erklärung über private Interessen, die jeder Leiter einer öffentliche Mittel erhaltenden Einrichtung abgeben muss, im Internet zu veröffentlichen ist, insbesondere insoweit entgegenstehen, als diese Veröffentlichung namensbezogene Daten über den Ehegatten, Lebensgefährten oder Partner der erklärungspflichtigen Person oder über ihr nahestehende oder bekannte Personen, die einen Interessenkonflikt begründen können, oder Daten über jede in den letzten zwölf Kalendermonaten abgeschlossene Transaktion mit einem Wert von über 3 000 Euro betrifft.

2. Art. 8 Abs. 1 der Richtlinie 95/46 und Art. 9 Abs. 1 der Verordnung 2016/679 sind dahin auszulegen, dass die Veröffentlichung personenbezogener Daten, die geeignet sind, die sexuelle Orientierung einer natürlichen Person indirekt zu offenbaren, auf der Website der Behörde, die für die Entgegennahme und die inhaltliche Kontrolle von Erklärungen über private Interessen zuständig ist, eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne dieser Bestimmungen darstellt.

Zur Höhe eines Anspruchs auf immateriellen Schadenersatz bei Verstoß gegen die DS-GVO

(**Bundesarbeitsgericht** Urteil vom 5. Mai 2022 – 2 AZR 363/21 –)

1. **Mangels einschlägiger unionsrechtlicher Vorschriften zur Bemessung des Schadenersatzes nach Art. 82 Abs. 1 DS-GVO findet, entscheidet hierüber das Gericht gemäß § 287 Abs. 1 Satz 1 ZPO unter Würdigung aller Umstände nach freier Überzeugung.**
2. **Der Betrag muss fühlbar (hier 1.000,00 Euro) und nicht nur symbolischen Charakter haben.**
3. **Ebenfalls eine Präventionsfunktion wegen einer Verletzung des allgemeinen Persönlichkeitsrechts kann mit einem Betrag in Höhe von 1.000,00 Euro ausreichend bewirkt sein.**
4. **Der immaterielle Schaden nach Art. 82 Abs. 1 DS-GVO hat – anders als eine Entschädigung nach § 15 Abs. 2 AGG (dazu BAG 28. Mai 2020 – 8 AZR 170/19 – Rn. 17 ff., BAGE 170, 340) – keinen erkennbaren Bezug zur Höhe eines dem Gläubiger zustehenden Arbeitsentgelts.**

(Nicht amtliche Leitsätze)

Tatbestand:

Die Parteien streiten noch über die Höhe eines Schadenersatzanspruchs nach Art. 82 Abs. 1 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung; im Folgenden DS-GVO).

Die Klägerin war bei der Beklagten bis zum 29. Februar 2020 als Hauswirtschafterin mit einer regelmäßigen Arbeitszeit von 45 Stunden pro Monat zu einem Bruttostundenentgelt von 10,00 Euro beschäftigt. Der Arbeitsvertrag der Parteien sah eine zweistufige Verfallklausel für alle beiderseitigen Ansprüche aus dem Arbeitsverhältnis vor, von der ua. Ansprüche aus vorsätzlichen oder grob fahrlässigen Pflichtverletzungen des Arbeitgebers sowie Ansprüche auf den gesetzlichen Mindestlohn ausgenommen waren.

Mit außergerichtlichem Schreiben ihres Prozessbevollmächtigten vom 30. Januar 2020 machte die Klägerin gegenüber der Beklagten unter Fristsetzung bis zum 13. Februar 2020 einen „Auskunftsanspruch nach der Datenschutzgrundverordnung im Hinblick auf sämtliche bei Ihnen gespeicherten Daten, insbesondere die Daten der Arbeitszeiterfassung geltend".

Die Klägerin hatte zuvor von der Beklagten mit Schriftsatz vom 19. Februar 2020 im Wege einer Stufenklage Auskunft über ihre im Zeitraum vom 1. März 2019 bis zum 30. Januar 2020 geleistete Arbeitszeit, eine eidesstattliche Versicherung über die Richtigkeit der Auskunft und eine sich aus der Auskunft ergebende Nachzahlung von Vergütung begehrt. Mit Schreiben vom 13. August 2020 übersandte ihr die Beklagte die Stundenzettel und -nachweise für den fraglichen Zeitraum.

Mit Schriftsatz vom 14. August 2020 hat die Klägerin die Zahlung eines in das Ermessen des Gerichts gestellten immateriellen Schadenersatzes „auf der Grundlage von Art. 15 DS-GVO" verlangt.

Das Arbeitsgericht hat die Klage abgewiesen. Das Landesarbeitsgericht hat ihr unter Zurückweisung der weitergehenden Berufung in Höhe von 1.000,00 Euro nebst Zinsen stattgegeben. Mit ihrer Revision verfolgt die Klägerin ihr Begehren auf Zahlung eines höheren Schadenersatzes weiter.

Aus den Gründen:

Die Revision ist unbegründet. Das Landesarbeitsgericht hat der Klägerin zu Recht keinen über 1.000,00 Euro hinausgehenden Schadenersatz zugesprochen.

I. Die Würdigung des Landesarbeitsgerichts, die gem. § 287 Abs. 1 Satz 1 ZPO festzusetzende Höhe des der Klägerin nach Art. 82 Abs. 1 DS-GVO gegen die Beklagte zustehenden Schadenersatzanspruchs betrage unter Berücksichtigung und Abwägung aller Umstände des Einzelfalls nicht mehr als 1.000,00 Euro, hält einer revisionsrechtlichen Überprüfung stand.

a) Da sich die Beklagte gegen ihre Verurteilung nicht mit einem eigenen Rechtsmittel gewandt hat, ist die Entscheidung des Landesarbeitsgerichts insoweit mit dem Ablauf der Frist für eine mögliche Anschlussrevision rechtskräftig geworden (vgl. BGH 19. November 2020 – VII ZR 193/19 – Rn. 18 f.).

b) Es bedarf daher keiner Entscheidung, ob allein eine nicht vollständige Erfüllung des Auskunftsanspruchs gem. Art. 15 Abs. 1 DS-GVO einen immateriellen Schaden i.S.v.. Art. 82 Abs. 1 DS-GVO begründen kann (zur Frage, ob der Nachweis eines konkreten Schadens erforderlich ist, vgl. die Vorabentscheidungsersuchen BAG 26. August 2021 – 8 AZR 253/20 (A) – Rn. 33, vor dem EuGH anhängig unter – C-667/21 – [Krankenversicherung Nordrhein], und OGH Österreich 15. April 2021 – 6Ob35/21x –, vor dem EuGH anhängig unter – C-300/21 – [Österreichische Post]; vgl. auch OLG Frankfurt am Main 2. März 2022 – 13 U 206/20 – juris – Rn. 70 ff.).

Zweifel daran könnten sich ergeben, weil der Erwägungsgrund 146 Satz 1 DS-GVO nur von solchen Schäden spricht, „die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht". Verarbeitung im Sinne der DS-GVO ist nach ihrem Art. 4 Nr. 2 „jede(r) mit oder ohne Hilfe automatisierter Verfahren ausgeführte(r) Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, de(r) Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung". Die Nichterfüllung oder nicht vollständige Erfüllung des Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO muss danach für sich genommen nicht gleichbedeutend sein mit einer verordnungswidrigen „Verarbeitung". Ebenso kann zugunsten der Klägerin unterstellt werden, dass ein Schadenersatzanspruch nach Art. 82 Abs. 1 DS-GVO keinen in bestimmter Weise qualifizierten Verstoß gegen die DS-GVO, also kein Überschreiten einer gewissen Erheblichkeitsschwelle, voraussetzt (vgl. dazu auch BVerfG 14. Januar 2021 – 1 BvR 2853/19 – Rn. 21). Beide Fragen sind für das vorliegende Revisionsverfahren nicht entscheidungserheblich, da sich die Entscheidung, soweit sie von der Klägerin angefochten ist, als rechtsfehlerfrei erweist.

2. Das Landesarbeitsgericht hat zu Recht angenommen, dass es bei der Bestimmung der von der Klägerin in sein Ermessen gestellten Höhe des Schadenersatzes gem. § 287 Abs. 1 Satz 1 ZPO alle Umstände des Einzelfalls würdigen musste. Davon kann der Senat für die Beurteilung der Revision der Klägerin ohne ein darauf bezogenes Vorabentscheidungsersuchen an den Gerichtshof der Europäischen Union nach Art. 267 Abs. 3 AEUV ausgehen.

a) Nach der ständigen Rechtsprechung des Gerichtshofs der Europäischen Union ist es mangels einschlägiger unionsrechtlicher Vorschriften nach dem Grundsatz der Verfahrensautonomie Sache der innerstaatlichen Rechtsordnung jedes Mitgliedstaats, die Verfahrensmodalitäten für Klagen, die den Schutz der dem Einzelnen aus dem Unionsrecht erwachsenden Rechte gewährleisten sollen, zu regeln, wobei die betreffenden Anforderungen jedoch nicht ungünstiger sein dürfen als diejenigen, die gleichartige, dem innerstaatlichen Recht unterliegende Sachverhalte regeln (Äquivalenzgrundsatz), und die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren dürfen (Effektivitätsgrundsatz) (EuGH 7. April 2022 – C-385/20 – [Caixabank] Rn. 47; 6. Oktober 2020 – C-511/18 ua. – [La Quadrature du Net ua.] Rn. 223; 19. Dezember 2019 – C-752/18 – [Deutsche Umwelthilfe] Rn. 33; 24. Oktober 2018 – C-234/17 – [XC ua.] Rn. 21 f. m.w.N.; 6. Oktober 2015 – C-69/14 – [Târ ia] Rn. 26 f.).

b) Dies führt im Streitfall mangels einschlägiger unionsrechtlicher Vorschriften zur Anwendbarkeit von § 287 Abs. 1 Satz 1 ZPO. Art. 82 DS-GVO regelt selbst keine Verfahrensmodalitäten zur Durchsetzung des Schadenersatzanspruchs. Art. 79 Abs. 1 DS-GVO sieht lediglich vor, dass jede betroffene Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf hat, wenn sie der Ansicht ist, dass die ihr aufgrund der DS-GVO zustehenden Rechte infolge einer nicht mit ihr im Einklang stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden. Dem Äquivalenz- oder Effektivitätsgrundsatz ist durch die Anwendung von § 287 Abs. 1 Satz 1 ZPO Rechnung getragen. Die Bestimmung findet im nationalen Recht ebenso bei der Durchsetzung anderer Ansprüche auf immateriellen Schadenersatz Anwendung (zur Bemessung einer Entschädigung nach § 15 Abs. 2 AGG vgl. auch BAG 28. Mai 2020 – 8 AZR 170/19 – Rn. 27, BAGE 170, 340; generell zu Ansprüchen auf Ersatz immaterieller Schäden i.S.d. § 253 BGB vgl. Musielak/Voit/Foerste ZPO 19. Aufl. § 287 Rn. 2). Sie ermöglicht überdies in besonderer Weise eine effektive Durchsetzung von Schadensersatzansprüchen, weil sie nach Wahl des Klägers das Beweismaß mindert (vgl. nur Musielak/Voit/Foerste a.a.O. Rn. 6 m.w.N.).

3. Das Landesarbeitsgericht hat die Höhe des immateriellen Schadenersatzes mit 1.000,00 Euro nicht ermessensfehlerhaft zu niedrig festgesetzt.

a) Bei der Bemessung der Höhe eines Schadenersatzanspruchs nach § 287 Abs. 1 ZPO steht den Tatsachengerichten ein weiter Ermessensspielraum zu, innerhalb dessen sie die Besonderheiten jedes einzelnen Falls zu berücksichtigen haben. Die Festsetzung unterliegt nur einer eingeschränkten Überprüfung durch das Revisionsgericht. Sie kann von diesem nur darauf überprüft werden, ob die Rechtsnorm zutreffend ausgelegt, ein Ermessen ausgeübt, die Ermessensgrenze nicht überschritten wurde und ob das Berufungsgericht von seinem Ermessen einen fehlerfreien Gebrauch gemacht hat, indem es sich mit allen für die Bemessung der Entschädigung maßgeblichen Umständen ausreichend auseinandergesetzt und nicht von sachfremden Erwägungen hat leiten lassen (vgl. BAG 28. Mai 2020 – 8 AZR 170/19 – Rn. 28, BAGE 170, 340; BGH 23. April 2012 – II ZR 163/10 – Rn. 68, BGHZ 193, 110).

b) Danach ist die Bemessung der Höhe des Schadenersatzes durch das Landesarbeitsgericht revisionsrechtlich nicht zu beanstanden. Ob die vom Berufungsgericht als „naheliegend" erachtete Orientierung am Kriterienkatalog in Art. 83 Abs. 2 Satz 2 DS-GVO möglich oder sogar geboten ist, kann dahinstehen.

Selbst wenn dies nicht der Fall sein sollte, hätte sich das Landesarbeitsgericht nicht von sachfremden Erwägungen zulasten der Klägerin leiten lassen.

aa) Es hat zunächst zugunsten der Klägerin in Rechnung gestellt, dass die Beklagte eine vollständige Auskunft nach Art. 15 Abs. 1 DS-GVO bis zuletzt nicht erteilt und ihre Verpflichtung jedenfalls grob fahrlässig verkannt habe. Selbst wenn das Berufungsgericht einen dieser Gesichtspunkte zu Unrecht in seine Erwägungen eingestellt hätte, wäre die Klägerin dadurch nicht beschwert.

bb) Das Landesarbeitsgericht hat ferner ohne Rechtsfehler in seine Würdigung einbezogen, dass die persönliche Betroffenheit der Klägerin durch die nicht vollständige Erfüllung ihres Auskunftsanspruchs in Anbetracht des maßgeblichen Anliegens ihres Auskunftsbegehrens „überschaubar" gewesen sei.

(1) Es hat das Auskunftsbegehren dahin ausgelegt, dass es der Klägerin maßgeblich um die Arbeitszeitaufzeichnungen gegangen sei. Diese habe ihr die Beklagte mit Schreiben vom 13. August 2020 aber übersandt. Damit hat das Landesarbeitsgericht eine Gewichtung des konkreten Ausmaßes der Beeinträchtigung der Klägerin durch die nicht vollständige Erfüllung ihres Auskunftsanspruchs vorgenommen und dieser eine relativ geringere Bedeutung beigemessen, als wenn es der Klägerin ebenso maßgeblich um Auskunft über ihre übrigen bei der Beklagten gespeicherten personenbezogenen Daten gegangen wäre.

(2) Das lässt keinen Ermessensfehlgebrauch erkennen. Wenn die Erlangung von Kontrolle über ihre übrigen personenbezogenen Daten nicht das primäre Ziel der Klägerin war, wiegt auch die Beeinträchtigung durch das Vorenthalten dieses Teils der begehrten Auskunft weniger schwer. Einen Rechtsfehler zeigt insoweit auch die Revision nicht auf. Sie beanstandet zwar, das Landesarbeitsgericht habe nicht berücksichtigen dürfen, dass die Klägerin den Auskunftsanspruch gerichtlich nicht weiterverfolgt habe. Das Berufungsgericht hat dies aber nicht für sich genommen als einen die Beklagte entlastenden Umstand bewertet, wie die Klägerin meint, sondern lediglich als – weiteren – Beleg für sein Verständnis des primären Ziels des Auskunftsverlangens. Dass dieses Verständnis unzutreffend sei, macht auch die Klägerin nicht geltend.

cc) Andere Aspekte hat das Landesarbeitsgericht nicht zu Lasten der Klägerin gewürdigt.

dd) Soweit das Berufungsgericht bei der Anspruchsbemessung nicht ausdrücklich problematisiert hat, ob der Schadenersatzanspruch nach Art. 82 Abs. 1 DS-GVO auch einen präventiven Charakter hat und damit auch eine Abschreckungsfunktion erfüllen muss (vgl. auch zu dieser Fragestellung das Vorabentscheidungsersuchen BAG 26. August 2021 – 8 AZR 253/20 (A) –, vor dem EuGH anhängig unter – C-667/21 – [Krankenversicherung Nordrhein]), ist dies im Ergebnis ebenfalls ohne Rechtsfehler. Zugunsten der Klägerin kann unterstellt werden, dass dem Anspruch ein solcher Präventionscharakter zukommt. Seine vom Berufungsgericht festgesetzte Höhe hat hinreichend abschreckende Wirkung.

(1) Der Betrag von 1.000,00 Euro ist fühlbar und hat nicht nur symbolischen Charakter (vgl. zur nicht ausreichenden Umsetzung der Richtlinien 2000/43/EG und 2000/78/EG bei einer nur symbolischen Sanktion EuGH 15. April 2021 – C-30/19 –

[Braathens Regional Aviation] Rn. 39; 25. April 2013 – C-81/12 – [Asociaţia Accept] Rn. 64). Bloß symbolisch wäre es etwa, die Entschädigung einer Person, die Opfer einer Diskriminierung beim Zugang zur Beschäftigung wurde, auf die Erstattung ihrer Bewerbungskosten zu beschränken (EuGH 10. April 1984 – C-14/83 – [von Colson] Rn. 24). Darüber geht der hier zugesprochene Schadensersatz deutlich hinaus.

(2) Ebenfalls eine Präventionsfunktion hat eine wegen einer Verletzung des allgemeinen Persönlichkeitsrechts geschuldete Entschädigung; auch diese kann mit einem Betrag in Höhe von 1.000,00 Euro ausreichend bemessen sein, wie etwa im Falle einer datenschutzwidrigen Observation mit heimlichen Videoaufnahmen durch einen Detektiv (BAG 19. Februar 2015 – 8 AZR 1007/13 – Rn. 14 und 33).

(3) Der immaterielle Schaden nach Art. 82 Abs. 1 DS-GVO hat – anders als eine Entschädigung nach § 15 Abs. 2 AGG (dazu BAG 28. Mai 2020 – 8 AZR 170/19 – Rn. 17 ff., BAGE 170, 340) – keinen erkennbaren Bezug zur Höhe eines dem Gläubiger zustehenden Arbeitsentgelts, so dass keine Anhaltspunkte dafür bestehen, dass es sich dabei um ein relevantes Bemessungskriterium für die Höhe des Schadensersatzes handeln könnte. Selbst wenn dies anders zu sehen sein sollte, entspräche der hier festgesetzte Betrag mehr als dem zweifachen der zwischen den Parteien vereinbarten monatlichen Vergütung. Für eine Entschädigung nach § 15 Abs. 2 AGG, die ebenfalls eine Abschreckungsfunktion erfüllen muss, ist bereits ein Betrag in Höhe des 1,5-fachen des auf einer Stelle erzielbaren Entgelts als ausreichend anzusehen, um die notwendige abschreckende Wirkung zu erzielen (BAG 28. Mai 2020 – 8 AZR 170/19 – Rn. 39, a.a.O.).

(4) Entgegen der Auffassung der Klägerin musste das Landesarbeitsgericht dem Umstand, dass die Beklagte anwaltlich vertreten war, auch unter dem Gesichtspunkt der Prävention keine den Schadenersatzanspruch erhöhende Bedeutung beimessen. Die Abschreckungsfunktion kann sich nur auf die Vermeidung künftiger Verstöße gegen die DS-GVO beziehen, nicht aber darauf, ob sich eine Partei bei der Erfüllung ihrer Verpflichtungen nach der DS-GVO anwaltlich hat vertreten lassen. Die Hinzuziehung eines Rechtsanwalts ist weder allgemein noch nach der DS-GVO verpönt.

ee) Sonstige Umstände, die im Interesse der Klägerin zu einem höheren Schadenersatz führen müssten, aber vom Landesarbeitsgericht nicht berücksichtigt worden wären, führt weder die Revision an, noch sind sie objektiv ersichtlich.

Schlussformulierung eines Arbeitszeugnisses

(**Bundesarbeitsgericht,** Urteil vom 25. Januar 2022 – 9 AZR 146/21 –)

Beschäftigte haben keinen Anspruch, dass ihnen in der Schlussformulierung eines Arbeitszeugnisses Dank oder gute Wünsche für die Zukunft ausgesprochen werden.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Parteien streiten über die Berichtigung eines Arbeitszeugnisses.

Der Kläger war vom 1. März 2017 bis zum 31. März 2020 als Personaldisponent bei der Beklagten, einer Personaldienstleisterin, tätig. In einem zur Erledigung eines Kündigungsschutzverfahrens geschlossenen gerichtlichen Vergleich verpflichtete sich die Beklagte ua., dem Kläger ein qualifiziertes wohlwollendes Arbeitszeugnis zu erteilen, das sie unter dem Datum des 31. März 2020 mit folgendem Wortlaut endete:

……..

„Zusammenfassend bestätigen wir Herrn J, dass er die ihm übertragenen Aufgaben zu unserer vollen Zufriedenheit erledigte.

Herr J scheidet mit dem heutigen Tage aus unserem Unternehmen aus."

Der Kläger hat die Ansicht vertreten, die Beklagte sei verpflichtet, das Zeugnis mit einer Schlussformel zu versehen, in der sie ihm für die geleistete Arbeit dankt und ihm für die Zukunft alles Gute und viel Erfolg wünscht.

Aus den Gründen:

Die Revision der Beklagten ist begründet. Das Landesarbeitsgericht hat das Urteil des Arbeitsgerichts auf die Berufung des Klägers zu Unrecht teilweise abgeändert und die Beklagte zur Aufnahme einer Dankes- und Wunschformel in den Zeugnistext verurteilt.

II. Die Revision hat in der Sache Erfolg. Die Klage ist unbegründet.

Die Annahme des Landesarbeitsgerichts, die Beklagte sei gemäß § 109 Abs. 1 Satz 3, Abs. 2 GewO i.V.m.. § 241 Abs. 2 BGB verpflichtet, das Zeugnis mit einer Schlussformel zu versehen, in der sie dem Kläger für die geleistete Arbeit dankt und ihm für die Zukunft alles Gute und viel Erfolg wünscht, hält einer revisionsrechtlichen Prüfung nicht stand.

1. Das Landesarbeitsgericht hat zunächst zutreffend erkannt, dass ein Arbeitnehmer unmittelbar aus § 109 Abs. 1 Satz 3 GewO keinen Anspruch auf eine Dankes- und Wunschformel ableiten kann. An dieser Rechtsprechung (BAG 11. Dezember 2012 – 9 AZR 227/11 – Rn. 9 ff., sowie vom 20. Februar 2001 – 9 AZR 44/00 – zu B I der Gründe, BAGE 97, 57, jeweils mit ausführlicher Begründung) hält der Senat uneingeschränkt fest. Auch eine verfassungskonforme Auslegung der Vorschrift führt zu keinem anderen Ergebnis.

a) Die Zivilgerichte haben bei der Auslegung und Anwendung des einfachen Rechts die durch die Grundrechte gezogenen Grenzen zu beachten. Sie müssen die im Gesetz zum Ausdruck kommende Interessenabwägung in einer Weise nachvollziehen, die die konkurrierenden Grundrechte der verschiedenen Grund-rechtsträger beachtet und unverhältnismäßige Grundrechtsbeschränkungen vermeidet. Sind bei der gerichtlichen Auslegung und Anwendung einfachrechtlicher Normen mehrere Deutungen möglich, verdient diejenige den Vorzug, die den Wertentscheidungen der Verfassung entspricht und die Grundrechte der Beteiligten möglichst weitgehend in praktischer Konkordanz zur Geltung bringt.

Der Einfluss der Grundrechte auf die Auslegung und Anwendung der zivilrechtlichen Normen ist nicht auf Generalklauseln beschränkt, sondern erstreckt sich auf alle auslegungsfähigen und -bedürftigen Tatbestandsmerkmale der zivilrechtlichen Vorschriften (vgl. BVerfG 30. März 2021 – 1 BvR 160/19 – Rn. 18; 18. Februar 2019 – 1 BvR 2556/17 – Rn. 9; BAG 21. September 2011 – 7 AZR 375/10 – Rn. 29, BAGE 139, 213).

b) Bei der Beurteilung, ob der Anspruch auf Erteilung eines qualifizierten Arbeitszeugnisses aus § 109 GewO auch die Formulierung einer gegebenenfalls auf die Gesamtnote abgestimmten Schlussformel umfasst, sind auf Seiten des Arbeitsgebers die Meinungsfreiheit des Art. 5 Abs. 1 GG und seine durch Art. 12 Abs. 1 GG geschützte Unternehmerfreiheit und auf Seiten des Arbeitnehmers aufgrund der durch eine Schlussformel erhöhten Bewerbungschancen (vgl. BAG 11. Dezember 2012 – 9 AZR 227/11 – Rn. 12, BAGE 144, 103) dessen Berufsausübungsfreit (Art. 12 Abs. 1 GG) und – gegebenenfalls – das aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG abgeleitete allgemeine Persönlichkeitsrecht betroffen. Das Interesse des Arbeitgebers, seine innere Einstellung zu dem Arbeitnehmer sowie seine Gedanken- und Gefühlswelt nicht offenbaren zu müssen, ist dabei höher zu bewerten als das Interesse des Arbeitnehmers an einer Schlussformel.

aa) Der Arbeitnehmer ist durch die Erteilung eines Arbeitszeugnisses ohne Schlussformel nur in geringem Maße in seinen grundrechtlich geschützten Positionen betroffen. Der Grad seiner Betroffenheit ist in erster Linie unter Berücksichtigung des Zeugniszwecks zu bewerten. Je stärker die Realisierung des Zeugniszwecks durch das Fehlen der Schlussformel gefährdet ist, desto näher liegt eine wesentliche Beeinträchtigung grundrechtlicher Positionen des Arbeitnehmers. Spiegelbildlich betrachtet ist der Arbeitgeber nicht aus verfassungsrechtlichen Gründen gehalten, das Zeugnis mit einem den Zeugniszweck überschießenden Inhalt zu versehen.

(1) Ein qualifiziertes Zeugnis enthält gemäß § 109 Abs. 1 Satz 3 GewO Angaben über Leistung und Verhalten des Arbeitnehmers. Es dient dem Arbeitnehmer regelmäßig als Bewerbungsunterlage und dadurch Dritten, insbesondere möglichen künftigen Arbeitgebern, als Grundlage für die Personalauswahl. Dem Arbeitnehmer gibt es zugleich Aufschluss darüber, wie der Arbeitgeber sein Verhalten und seine Leistung beurteilt. Daraus ergeben sich als inhaltliche Anforderungen das Gebot der Zeugniswahrheit und das in § 109 Abs. 2 GewO auch ausdrücklich normierte Gebot der Zeugnisklarheit (st. Rspr., vgl. BAG 27. April 2021 – 9 AZR 262/20 – Rn. 11). Als individuelle Beurteilung der beruflichen Verwendbarkeit des Arbeitnehmers muss das Arbeitszeugnis seinem Leser Auskunft über Leistung und Ver-halten des Arbeitnehmers im Arbeitsverhältnis geben (BAG 27. April 2021 – 9 AZR 262/20 – Rn. 17).

(2) Positive Schlusssätze können zwar geeignet sein, die Bewerbungschancen des Arbeitnehmers zu erhöhen. Ein Zeugnis wird durch einen Schlusssatz aufgewertet, in dem der Arbeitgeber seinen Dank für die guten Leistungen zum Ausdruck bringt und dem Arbeitnehmer für die berufliche Zukunft weiterhin alles Gute wünscht (BAG 11. Dezember 2012 – 9 AZR 227/11 – Rn. 12, BAGE 144, 103; 20. Februar 2001 – 9 AZR 44/00 – zu B I 2 b bb (3) der Gründe, BAGE 97, 57).

(3) Der materielle Aussagegehalt von auf die Gesamtnote abgestimmten Schlusssätzen beschränkt sich allerdings im Wesentlichen darauf, dass der Arbeitgeber die bereits abgegebene Leistungs- und Verhaltensbeurteilung mit anderen Worten nochmals formelhaft wiederholt (vgl. BAG 11. Dezember 2012 – 9 AZR 227/11 – Rn. 13, BAGE 144, 103, 20. Februar 2001 – 9 AZR 44/00 – BAGE 97, 57). Damit trägt eine Schlussformel nicht zur Realisierung des Zeugniszwecks bei. Aus ihr ergeben sich für den Zeugnisleser bei objektiver Betrachtung keine über die eigentliche Leistungs- und Verhaltensbeurteilung hinausgehenden Informationen zur Beurteilung, inwieweit der Arbeitnehmer für eine zu besetzende Stelle geeignet ist. Durch eine Dankes- und Wunschformel bringt der Arbeitgeber vielmehr nur Gedanken und Gefühle zum Ausdruck, die weder Rückschlüsse auf die Art und Weise, in der der Arbeitnehmer die ihm übertragenen Aufgaben erledigt hat, noch auf dessen für das Arbeitsverhältnis wesentlichen Charaktereigenschaften und Persönlichkeitszüge zulassen.

bb) Wäre eine Dankes- und Wunschformel integraler Bestandteil eines qualifizierten Zeugnisses, wäre der Arbeitgeber verpflichtet, innere Gedanken über und Gefühle für den aus dem Arbeitsverhältnis ausscheidenden Arbeitnehmer zu äußern. Hierdurch würde seine durch Art. 5 Abs. 1 Satz 1 GG geschützte negative Meinungsfreiheit beeinträchtigt, die Freiheit also, eine Meinung nicht zu haben, nicht zu äußern und insoweit zu schweigen und nicht gezwungen zu werden, eine fremde Meinung als eigene zu verbreiten (vgl. BVerfG 2. Mai 2018 – 1 BvR 666/17 – Rn. 17; 22. Januar 1997 – 2 BvR 1915/91 – zu C II 1 a der Gründe, BVerfGE 95, 173; BAG 24. Oktober 2018 – 10 AZR 69/18 – Rn. 26; BGH 19. Juli 2018 – IX ZB 10/18 – Rn. 18 m.w.N.). Entgegen der Ansicht des Landesarbeitsgerichts handelt es sich bei einer Dankes- und Wunschformel nicht um eine bloße Höflichkeitsformel ohne Beziehung zur Wirklichkeit. Selbst wenn Arbeitgeber die Schlussformel teilweise nur floskelhaft aus Gründen der Höflichkeit verwenden, ohne die mitgeteilten Gefühle zu empfinden, enthält sie überprüfbare innere Tatsachen (BAG 20. Februar 2001 – 9 AZR 44/00 – zu B I 2 b bb (4) der Gründe, BAGE 97, 57). Der Arbeitgeber kann Dank empfinden und dem Arbeitnehmer für die Zukunft alles Gute und viel Erfolg wünschen oder auch nicht. Ist die Tatsachenbehauptung wahr, unterfällt ihre Äußerung wie ihre Nichtäußerung dem Schutzbereich der Meinungsfreiheit (BVerfG 27. August 2019 – 1 BvR 811/17 – Rn. 16; 22. Juni 2018 – 1 BvR 673/18 – Rn. 20). Der Eingriff in den Schutzbereich wird nicht dadurch gerechtfertigt, dass eine Vielzahl von Arbeitgebern dazu übergegangen ist, Schlussformeln in ihre Arbeitszeugnisse aufzunehmen, und deshalb entsprechendes von anderen Zeugnisverfassern erwartet. Erst recht kann ein Arbeitgeber, der seinem ausscheidenden Arbeitnehmer gegenüber weder Dank empfindet noch ihm eine positive Zukunft wünscht, nicht gezwungen werden, aus Höflichkeit oder aufgrund einer Erwartungshaltung Dritter eine unwahre Erklärung über seine innere Haltung abzugeben. Dies stände weder im Einklang mit dem einfachgesetzlichen Verbot der Zeugniswahrheit noch mit der negativen Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 GG.

cc) Aufgrund der erheblichen Beeinträchtigung der negativen Meinungsfreiheit des Arbeitgebers und der geringen Relevanz bei der Realisierung des Zeugniszwecks besteht weder ein Anspruch des Arbeitnehmers auf ein Arbeitszeugnis mit entsprechender Schlussformel noch eine Verpflichtung des Arbeitgebers, ein solches zu erteilen. Ob dies auch dann gilt, wenn der Arbeitgeber in den von ihm erteilten Arbeitszeugnissen standardmäßig entsprechende Schlussformeln verwendet, bedarf keiner Entscheidung. Darauf hindeutende Umstände sind weder vorgetragen noch ersichtlich.

2. Entgegen der Ansicht des Landesarbeitsgerichts ist ein Anspruch auch bei einer leicht überdurchschnittlichen Bewertung nicht aus dem Rücksichtnahmegebot des § 241 Abs. 2 BGB i.V.m. § 109 Abs. 1 Satz 3, Abs. 2 GewO abzuleiten.

a) Nach 241 Abs. 2 BGB ist jede Partei des Arbeitsvertrags zur Rücksichtnahme auf die Rechte, Rechtsgüter und Interessen ihres Vertragspartners verpflichtet. Dies dient dem Schutz und der Förderung des Vertragszwecks. Im Arbeitsverhältnis können die Vertragsparteien deshalb zur Verwirklichung des Leistungsinteresses zu leistungssichernden Maßnahmen verpflichtet sein. Dazu gehört auch die Pflicht, im Zusammenwirken mit dem an-

deren Teil die Voraussetzungen für die Durchführung des Vertrags zu schaffen, Erfüllungshindernisse nicht entstehen zu lassen oder zu beseitigen und dem anderen Teil den angestrebten Leistungserfolg zukommen zu lassen (BAG 21. Februar 2017 – 1 AZR 367/15 – Rn. 16, BAGE 158, 148; 2. November 2016 – 10 AZR 596/15 – Rn. 32, BAGE 157, 153).

b) Aus dem Rücksichtnahmegebot lassen sich auch nachwirkende Schutzpflichten ableiten (vgl. MüKoBGB/Bachmann 8. Aufl. BGB § 241 Rn. 118; BeckOK BGB/Sutschet BGB § 241 Rn. 99). Dazu gehört die Pflicht des Arbeitgebers, auf Wunsch und im Interesse des Arbeitnehmers Dritten gegenüber Auskünften über den Arbeitnehmer zu erteilen (vgl. bereits vor der Normierung in § 241 Abs. 2 BGB BAG 18. August 1981 – 3 AZR 792/78 – zu I 1 der Gründe; 5. August 1976 – 3 AZR 491/75 – zu II der Gründe).

c) Das Rücksichtnahmegebot kann aber nicht herangezogen werden, um abschließende gesetzliche Regelungen zu erweitern. Die Regelung zum Inhalt eines qualifizierten Arbeitszeugnisses in § 109 Abs. 1 Satz 2 und Satz 3 GewO ist abschließend. Der Gesetzgeber hat dort ausdrücklich aufgelistet, auf welche Inhalte ein Arbeitnehmer einen Anspruch hat. Der Gesetzgeber kannte bei der Neufassung des § 109 GewO am 24. August 2002 die kurz zuvor ergangene Entscheidung des Senats, dass der Arbeitnehmer keinen Anspruch auf eine Schlussformel hat (vgl. BAG 20. Februar 2001 – 9 AZR 44/00 – zu B I der Gründe, BAGE 97, 57). Im Hinblick auf die gesetzgeberische Entscheidung, § 109 Abs. 1 Satz 3 GewO nicht um weitere Inhalte zu ergänzen, würde die Ableitung eines Anspruchs aus § 241 Abs. 2 BGB die Grenzen zulässiger Auslegung und richterlicher Rechtsfortbildung (vgl. dazu BVerfG 6. Juni 2018 – 1 BvL 7/14 – Rn. 72 ff., BVerfGE 149, 126) überschreiten. Der Senat konnte die betroffenen Grundrechtspositionen bereits im Rahmen der verfassungskonformen Auslegung berücksichtigen.

Streitwert bei Datenschutzauskunftsklage (Ls)

(**Oberlandesgericht Köln**, Beschluss vom 4. August 2022 – 7 U 137/21 –)

1. **Bei der Klage auf Herausgabe einer Urkunde ist der Streitwert gem. § 3 ZPO nach freiem Ermessen festzusetzen, wenn mit deren Besitz z.B. eine Beweisführung angestrebt wird.**
2. **Die Geltendmachung einer Datenauskunft gem. Art. 15 DS-GVO zur Verfolgung wirtschaftlicher Ziele ist zulässig.**
3. **Wenn die Datenauskunftsklage nach dem Vortrag des Klägers jedoch nicht vorrangig einem in der Datenschutz-Grundverordnung geregelten Ziel dient (z.B. der Verfolgung der weiteren Rechte aus Art. 16-18 oder Art. 82 DS-GVO), sondern der Verfolgung zivilrechtlicher Ansprüche, ist der Wert der Datenauskunftsklage wie nach deutschem Recht mit einem Teilwert dieses wirtschaftlichen Interesses (i.d.R. 1/10 bis 1/4) zu bemessen.**

(Eingesandt und Leitsätze von RA Martin Riemer, Brühl)

Datenschutz steht Nachweis der Zahlung des Mindestlohns nicht entgegen (Ls)

(**Oberlandesgericht Brandenburg**, Urteil vom 23. Februar 2022 – 4 U 111/21 –)

1. **Pauschale Erklärungen eines Steuerberaters genügen einer vertraglichen Vereinbarung, wonach der Nachunternehmer geeignete Nachweise darüber vorzulegen hat, dass die Mitarbeiter-Entlohnung nicht unter den geltenden Lohntarifen/Mindestlöhnen erfolgt, nicht.**
2. **Der Nachunternehmer ist durch die Vorschriften der Datenschutzgrundverordnung (DS-GVO) nicht gehindert, gegenüber seinem Auftraggeber Nachweise über die Zahlung des Mindestlohns an die Mitarbeiter, die er zur Erfüllung der Aufträge eingesetzt hat, zu erbringen.**
3. **Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.**

(Nicht amtliche Leutsäze)

Teilnahme am betrieblichen Sommerfest einer Klinik nur mit 2G+ und negativem Test (Ls)

(**Landesarbeitsgericht Berlin-Brandenburg**, Urteil vom 1. Juli 2022 – 6 Ta 673/22 –)

1. **Die von einer Klinik für ein Sommerfest festgelegte Zugangsregelung, wonach für die Teilnahme am Fest eine gültige vollständige Impfung und/oder Genesung sowie eine Auffrischungsimpfung und ein tagesaktueller negativer Antigen-Schnelltest erforderlich ist, ist rechtmäßig.**
2. **Eine besondere Rechtsgrundlage für die Zugangsbeschränkungen ist nicht erforderlich, da die Klinik nicht hoheitlich handelt. Vielmehr ist für den begehrten Zutritt eine Anspruchsgrundlage erforderlich.**
3. **Die vorgenommene Gruppenbildung bei der Gewährung von Leistungen – hier dem Zutritt zum Betriebsfest – ist hier schon angesichts der gesetzlichen Wertung in § 20a IfSG gegeben.**

(Nicht amtliche Leitsätze)

Bewerbung über das Internetportal reicht aus, um als Bewerber im Sinne des AGG zu gelten (Ls)

(**Landesarbeitsgericht Schleswig-Holstein**, Urteil vom 21. Juni 2022 – 2 Sa 21/22 –)

Wer sich auf eine Stellenanzeige im Internetportal „Ebay-Kleinanzeigen" über die dortige Chat-Funktion bewirbt, genießt den Status eines Bewerbers. Denn wer eine Stellenanzeige in Ebay Kleinanzeigen veröffentlicht, muss damit rechnen, dass sich die Bewerber über die Ebay-Kleinanzeigen-Chatfunktion bewerben und nicht auf klassische Weise schriftlich unter Beifügung von Bewerbungsunterlagen. Ein inhaltliches Mindestmaß an Angaben zur Person des Bewerbers wird gesetzlich nicht gefordert, sodass das Einreichen weiterer Unterlagen nicht erforderlich ist.

(Nicht amtliche Leitsätze)

Duzen in Stellenzeige als Diskriminierung

(**Landesarbeitsgericht Köln**, Urteil vom 10. September 2021 – 10 Sa 1264/20 –)

1. **Das Benachteiligungsverbot des § 7 Abs. 1 AGG erfasst nicht jede Ungleichbehandlung, sondern nur eine Ungleichbehandlung wegen eines in § 1 AGG genannten Grundes. Dabei müsse zwischen der benachteiligenden Behandlung und einem in § 1 AGG genannten Grund ein Kausalzusammenhang bestehen.**
2. **Die gewählte Duz-Form in der Stellenausschreibung hin sichtlich der Ansprache an die potentiellen Stellenbewerber ist nicht als hinrei chendes Indiz für eine Altersdiskriminierung anzusehen, son dern lässt sich plausibel auf die von der Beklagtenseite gewählte Unternehmenssprache zurückführen.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien streiten darüber, ob die Beklagte verpflichtet ist, an den Kläger eine Entschädigung wegen eines Verstoßes gegen das Benachteiligungsverbot des AGG zu zahlen.

Der 49-jährige Kläger, Jurist, bewarb sich mit Schreiben vom 01.12.2019 auf eine Stellenanzeige der Beklagten aus Dezember 2019 auf der Online-Jobplattform „Step Stone" auf die ausgeschriebene Stelle als Legal Consultant.

In der Stellenanzeige lautet es auszugsweise wie folgt:

Für den Standort in K suchen wir ab sofort ein/eine Legal Consultant, Jurist (m/w/div.). Das werden deine Aufgaben sein: In einem Team aus Wirtschaftsjuristen, Anwälten und Internationalen Juristen verstärkst du uns mit deinem Expertenwissen. Du schreibst rechtliche Einschätzungen und arbeitest an unseren Legal Tech Produkten mit (z.B. Rechtstexten-Generatoren).

Das solltest du mitbringen: Du hast ein juristisches Studium erfolgreich abgeschlossen. Eine Anwaltszulassung ist prima, aber kein Muss. Du besitzt gute Kenntnisse in den relevanten Rechtsgebieten (Datenschutzrecht, E-Commerce-Recht, Verbraucherschutzrecht, Wettbewerbsrecht und AGB-Recht).

Wenn du dein Studium der Rechtswissenschaften oder des Wirtschaftsrechts abgeschlossen und jetzt Lust darauf hast, unser Team als Legal Consultant mit einem Fokus auf E-Commerce- und Datenschutz-Recht zu verstärken, dann bist du bei uns genau richtig!

Das bieten wir dir: Intensive Einarbeitung in deiner Abteilung und in der T Organisation Buddy-Programm – ein erfahrener TS-Mitarbeiter, der die ersten Schritte mit dir macht.

Die Beklagte lehnte die Bewerbung des Klägers mit E-Mail vom 30.12.2019 ab.

Daraufhin machte der Kläger mit Schreiben vom 05.01.2020, welches am 07.01.2020 bei der Beklagten zugegangen ist, geltend, einen Entschädigungsanspruch wegen Altersdiskriminierung i.H.v. 4900 € anzuerkennen. Dies lehnte die Beklagte durch ihre Mitteilung vom 10.01.2020 gegenüber dem Kläger ab.

Sein Entschädigungsverlangen verfolgt der Kläger in Höhe von 7.900 € mit seiner Klage vom 10.03.2020, die am 12.03.2020 beim Arbeitsgericht in Köln eingegangen ist, weiter.

Der Kläger hat erstinstanzlich geltend gemacht, aus der Stellenanzeige der Beklagten ließen sich hinreichende Indizien für eine Altersdiskriminierung gegenüber ihm herleiten. Dies ergebe sich hinreichend durch die Wahl der Duz-Form gegenüber den potentiellen Bewerbern in der Ausschreibung. Weiterhin sei zu berücksichtigen, dass in der Ausschreibung das Merkmal der „ersten Erfahrung in der Rechtsberatung" aufgeführt sei. Zudem fordere die Beklagte in der Stellenanzeige die Bewerber auf, sich nach Absolvierung des Studiums „jetzt" zu bewerben. Indiziell sei auch zu berücksichtigen, dass die Beklagte keine Zeugnisse im Rahmen der Ausschreibung verlangt habe. Die Bewerbung des Klägers weise keine erheblichen Lücken im Lebenslauf auf. Der berufliche Bezug des Klägers zum Bereich des E-Commerce ergebe sich hinreichend aus seinen einschlägigen Qualifikationen.

Der Kläger hat erstinstanzlich beantragt, die Beklagte zu verurteilen, an ihn eine Entschädigung zu zahlen, deren Höhe in das Ermessen des Gerichts gestellt wird, die jedoch 7800 € nicht unterschreiten sollte, nebst 5 % Zinsen über dem Basiszinssatz seit dem 07.01.2020.

Das Arbeitsgericht Köln hat durch Urteil vom 13.11.2020 – 1 Ca 1564/20 – die Klage als unbegründet abgewiesen und zur Begründung darauf abgestellt, dass ein Verstoß gegen das Benachteiligungsverbot nach § 7 Abs. 1 AGG nicht hinreichend zu erkennen sei, da der Kläger hierfür keine hinreichenden Indizien vorgetragen habe.

Gegen das ihm am 05.12.2020 zugestellte Urteil des Arbeitsgerichts hat der Kläger am 30.12.2020 Berufung eingelegt und diese zugleich begründet.

Aus den Gründen:

Die Berufung des Klägers ist zulässig, weil sie statthaft und fristgerecht eingelegt wie auch begründet worden ist (§§ 64, 66 ArbGG, 519, 520 ZPO).

II. Die Berufung ist jedoch unbegründet, da das Arbeitsgericht zu Recht und mit überzeugender Begründung das Entschädigungsbegehren des Klägers wegen Verstoß gegen das Benachteiligungsverbot nach § 7 Abs. 1 AGG abgelehnt hat.

Es ist kein Verstoß gegen das Benachteiligungsverbot nach § 7 Abs. 1 AGBG wegen Altersdiskriminierung des Klägers festzustellen.

a. § 7 Abs. 1 AGG verbietet sowohl unmittelbare als auch mittelbare Benachteiligungen. Nach § 3 Abs. 1 Satz 1 AGG liegt eine unmittelbare Benachteiligung vor, wenn eine Person wegen eines in § 1 AGG genannten Grundes, u.a. wegen des Alters, eine weniger günstige Behandlung erfährt als eine an-

dere Person in einer vergleichbaren Situation erfährt, erfahren hat oder erfahren würde. Nach § 3 Abs. 2 AGG liegt eine mittelbare Benachteiligung vor, wenn dem Anschein nach neutralen Vorschriften, Kriterien oder Verfahren Personen wegen eines in § 1 AGG genannten Grundes gegenüber anderen Personen in besonderer Weise benachteiligen können, es sei denn, die betreffenden Vorschriften, Kriterien oder Verfahren sind durch ein rechtmäßiges Ziel sachlich gerechtfertigt und die Mittel sind zur Erreichung dieses Ziels angemessen und erforderlich.

b. Das Benachteiligungsverbot des § 7 Abs. 1 AGG erfasst allerdings nicht jede Ungleichbehandlung, sondern nur eine Ungleichbehandlung wegen eines in § 1 AGG genannten Grundes. Zwischen der benachteiligenden Behandlung und einem in § 1 AGG genannten Grund muss demnach ein Kausalzusammenhang bestehen. Dafür ist es nicht erforderlich, dass der betreffende Grund i.S.v. § 1 AGG das ausschließliche oder auch nur ein wesentliches Motiv für das Handeln des Benachteiligenden ist; es muss nicht – gewissermaßen als vorherrschender Beweggrund, Hauptmotiv oder „Triebfeder" des Verhaltens – handlungsleitend oder bewusstseinsdominant gewesen sein; vielmehr ist der Kausalzusammenhang bereits dann gegeben, wenn die Benachteiligung an einen Grund i.S.v. § 1 AGG anknüpft oder durch diesen motiviert ist, wobei die bloße Mitursächlichkeit genügt (vgl. etwa BAG 26. Juni 2014 – 8 AZR 547/13 – Rn. 34 m.w.N.).

c. § 22 AGG sieht für den Rechtsschutz bei Diskriminierungen im Hinblick auf den Kausalzusammenhang eine Erleichterung der Darlegungslast, eine Absenkung des Beweismaßes und eine Umkehr der Beweislast vor. Wenn im Streitfall die eine Partei Indizien beweist, die eine Benachteiligung wegen eines in § 1 AGG genannten Grundes vermuten lassen, trägt nach § 22 AGG die andere Partei die Beweislast dafür, dass kein Verstoß gegen die Bestimmungen zum Schutz vor Benachteiligung vorgelegen hat. Danach genügt eine Person, die sich durch eine Verletzung des Gleichbehandlungsgrundsatzes für beschwert hält, ihrer Darlegungslast bereits dann, wenn sie Indizien vorträgt, die mit überwiegender Wahrscheinlichkeit darauf schließen lassen, dass eine Benachteiligung wegen eines in § 1 AGG genannten Grundes erfolgt ist (vgl. BAG 21. Juni 2012 – 8 AZR364/11 – Rn. 33, BAGE 142, 158; 15. März 2012 – 8 AZR 37/11 – Rn. 65, BAGE 141, 48). Besteht die Vermutung einer Benachteiligung, trägt die andere Partei die Darlegungs- und Beweislast dafür, dass der Gleichbehandlungsgrundsatz nicht verletzt worden ist (vgl. EuGH 25. April 2013 – C-81/12 – [Asociatia ACCEPT] Rn. 55 m.w.N.; 10. Juli 2008 – C-54/07 – [Feryn] Rn. 32, Slg. 2008, I-5187; BAG 26. September 2013 – 8 AZR 650/12 – Rn. 27). Hierfür gilt jedoch das Beweismaß des sog. Vollbeweises (vgl. etwa BAG 18. September 2014 – 8 AZR 753/13 – Rn. 33). Der Arbeitgeber muss demnach Tatsachen vortragen und ggf. beweisen, aus denen sich ergibt, dass ausschließlich andere als die in § 1 AGG genannten Gründe zu einer ungünstigeren Behandlung geführt haben (vgl. etwa BAG 16. Februar 2012 – 8 AZR 697/10 – Rn. 58; 17. August 2010 – 9 AZR 839/08 – Rn. 45).

d. Nach § 11 AGG darf ein Arbeitsplatz nicht unter Verstoß gegen § 7 Abs. 1 AGG ausgeschrieben werden.

Das AGG knüpft an einen Verstoß gegen § 11 AGG keine unmittelbaren Rechtsfolgen. Der Arbeitgeber schuldet einem/einer abgelehnten Bewerber/in eine Entschädigung oder Schadensersatz auch nicht allein deshalb, weil die Stellenausschreibung Formulierungen, insb. Anforderungen enthält, die „auf den ersten Blick" den Anschein erwecken, der Arbeitgeber habe den Arbeitsplatz unter Verstoß gegen § 11 AGG ausgeschrieben.

Schreibt der Arbeitgeber eine Stelle unter Verstoß gegen § 11 AGG aus, so kann dies allerdings die Vermutung i.S.v. § 22 AGG begründen, dass der/die erfolglose Bewerber/in im Auswahl-/Stellenbesetzungsverfahren wegen eines Grundes i.S.v. § 1 AGG benachteiligt wurde. Zwar verweist § 11 AGG nach seinem Wortlaut nur auf § 7 Abs. 1 AGG; dennoch muss die Bestimmung so ausgelegt werden, dass ein Verstoß gegen das Benachteiligungsverbot des § 7 Abs. 1 AGG nicht vorliegt, wenn die mögliche mittelbare Benachteiligung nach § 3 Abs. 2 AGG oder die unmittelbare Benachteiligung nach §§ 8, 9 oder § 10 AGG gerechtfertigt ist. Es ist kein Grund ersichtlich, warum Stellenausschreibungen strengeren Anforderungen unterliegen sollten, als dies bei allen anderen benachteiligenden Handlungen i.S.d. AGG der Fall ist. Dies hat zur Folge, dass bei Formulierungen, insb. Anforderungen in Stellenausschreibungen, die eine unmittelbare Benachteiligung wegen eines in § 1 AGG genannten Grundes bewirken, ein Verstoß gegen § 11 AGG nicht vorliegt, wenn die Diskriminierung nach §§ 8, 9 oder § 10 AGG zulässig ist, und dass bei Formulierungen, insb. Anforderungen in Stellenausschreibungen, die eine mittelbare Benachteiligung wegen eines in § 1 AGG genannten Grundes bewirken können, nach § 3 Abs. 2 AGG ein Verstoß gegen § 11 AGG dann ausscheidet, wenn die Anforderung durch ein rechtmäßiges Ziel sachlich gerechtfertigt und zur Erreichung dieses Ziels angemessen und erforderlich ist. Enthält eine Stellenausschreibung Formulierungen, insb. Anforderungen, die „auf den ersten Blick" den Anschein erwecken, der Arbeitgeber habe den Arbeitsplatz unter Verstoß gegen § 11 AGG ausgeschrieben, kann dies nach alledem die Vermutung nach § 22 AGG begründen, der/die erfolglose Bewerber/in sei im Auswahl-/Stellenbesetzungsverfahren wegen eines in § 1 AGG genannten Grundes benachteiligt worden.

e. Zu prüfen verbleibt, ob aus der Stellenausschreibung der Beklagten in der Jobplattform Step Stone hinreichende Indizien für eine Altersdiskriminierung des Klägers als Bewerber auf die ausgeschriebene Stelle gemäß § 22 AGG herzuleiten sind.

aa. Die Auslegung des Textes veröffentlichter Stellenanzeigen richtet sich nach folgenden Maßstäben: Unter einer Ausschreibung im Sinne von § 11 AGBG ist die an eine unbekannte Vielzahl von Personen gerichtete Aufforderung eines Arbeitgebers zu verstehen, sich auf die ausgeschriebene Stelle zu bewerben. Danach ist die Stellenausschreibung nach ihrem objektiven Inhalt und typischen Sinn einheitlich so auszulegen, wie sie von verständigen und redlichen potentiellen Bewerbern unter Abwägung der Interessen der normalerweise beteiligten Verkehrskreise verstanden werden, wobei die Verständnismöglichkeiten des durchschnittlichen Bewerbers zugrunde zu legen sind (BAG, Urteil vom 16.12.2015 – 5 AZR 567/14, Rn. 12).

bb. Hieraus ergibt sich für die einzelnen Passagen des Ausschreibungstextes der Beklagten folgendes Auslegungsergeb-nis:

(1.) Die Textpassage hinsichtlich der Anforderung eines erfolgreichen Abschlusses eines juristischen Studiums enthält keine unmittelbare Altersangabe.

Eine Einschränkung dahingehend, dass das Studium erst kürzlich abgeschlossen sein sollte oder müsste, ist dem nicht zu entnehmen (vergleiche BAG, Urteil vom 23.11.2017 – 8 AZR 372/16, Rn. 32). Bestärkt wird dieses Auslegungsergebnis durch die weitere Formulierung in der Stellenausschreibung der Beklagten, wonach gute Kenntnisse in relevanten Rechtsgebieten gewünscht werden, die in speziellen Rechtsgebieten angesiedelt und typischerweise nicht von Berufsanfängern bzw. Hochschulabsolventen beherrscht werden. So bezieht sich die Beklagte in der Stellenausschreibung auf gute Kenntnisse in den Rechtsgebieten Datenschutzrecht, E-Commerce-Recht, Verbraucherschutzrecht, Wettbewerbsrecht und AGB-Recht.

(2.) Die Passage in der Stellenausschreibung, mit der die Beklagte auf den Vorteil hinweist, dass bereits erste Erfahrungen

in der Rechtsberatung mitgebracht werden, stellt typischerweise einen Altersbezug her (vergleiche BAG, Urteil vom 19.05.2016 – 8 AZR 583/14, Rz. 70). Allerdings ist dieser Gesichtspunkt im Rahmen der gebotenen Auslegung unter Berücksichtigung des gesamten Kontextes der Ausschreibung zu würdigen. Hierbei ist festzuhalten, dass erste Erfahrungen in der Rechtsberatung speziell in der Ausschreibung angesprochen werden. Entgegen der Auffassung des Klägers ist aber nicht als typisch anzusehen, dass Rechtsberatung in einem bestimmten Alter begonnen bzw. ausgeübt wird (vergleiche BAG, Urteil vom 26.01.2017 – 8 AZR 73/16, Rz. 32). Dabei ist der Gesamtkontext der Ausschreibung mit einzubeziehen. Hier gilt es die Formulierung zu berücksichtigen, dass in der Ausschreibung gewünscht wird, dass dank rascher Auffassungsgabe und Knowhow in der juristischen Recherche eine Einarbeitung in neue Rechtsgebiete als möglich angesehen wird. Dabei wird in der Stellenausschreibung von einem vorhandenen Know-how ausgegangen, dass für Berufsanfänger ohne weiteres nicht typisch ist.

cc. Auch die Formulierung in der Stellenausschreibung, dass für den Fall des Abschlusses des Studiums der Rechtswissenschaften oder des Wirtschaftsrechts „jetzt Lust darauf bestehe", sich zu bewerben, eine sinnvolle Verstärkung des Teams gewünscht sei, lässt keinen hinreichenden Schluss im Sinne eines tragfähigen Indizes gemäß § 22 AGG für eine Altersdiskriminierung des Klägers zu. Die zeitliche Festlegung ist aufgrund des zuvor dargestellten Gesamtzusammenhangs der Stellenausschreibung nicht als nahe zeitliche Abfolge von Studienabschluss und Bewerbung zu verstehen. Wiederum fällt ins Gewicht, dass im sonstigen Kontext der Stellenausschreibung ein vorhandenes – für Berufsanfänger bzw. jüngere Mitarbeiter – ohne weiteres nicht kennzeichnendes Know-how angesprochen ist.

dd. Die gewählte Duz-Form in der Stellenausschreibung hinsichtlich der Ansprache an die potentiellen Stellenbewerber ist gemäß den Ausführungen des Arbeitsgerichts nicht als hinreichendes Indiz für eine Altersdiskriminierung anzusehen, sondern lässt sich plausibel auf die von der Beklagtenseite gewählte Unternehmenssprache zurückführen.

Nach alldem liegen hinreichende diskriminierungsbegründende Indizien im Sinne von § 7 Abs. 1 AGG i.V.m. § 22 AGG nicht vor, so dass dem Entschädigungsbegehren des Klägers vom Arbeitsgericht zu Recht nicht entsprochen worden ist. Die Berufung des Klägers hiergegen ist unbegründet.

III. Die Kosten des Berufungsverfahrens trägt nach § 97 ZPO der unterlegene Kläger.

Gründe für die Zulassung der Revision nach § 72 ArbGG sind nicht gegeben, da die Entscheidung unter Berücksichtigung der höchstrichterlichen Rechtsprechung auf den Umständen des Einzelfalles beruht.

Zwangsweiser Einbau von Funkwasserzähler ist zulässig (Ls)

(**Bayerische Verwaltungsgerichtshof**, Beschluss vom 7. März 2022 – 4 CS 21.2254 –)

1. **Die Pflicht zum Einbau von Funkwasserzählern stellt keinen unzulässigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.**
2. **Die Versorgung mit Trinkwasser und die Messung des Verbrauchs mittels Wasserzählern sind zur Daseinsvorsorge gehörende gemeindliche Pflichtaufgaben und dienen dem öffentlichen Interesse.**
3. **Der Betrieb eines Funkwasserzählers stellt keinen unzulässigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Selbst wenn der Betrieb Rückschlüsse auf den Wasserverbrauch einzelner Personen ermögliche, ist die Verarbeitung der personenbezogenen Daten gerechtfertigt.**
4. **Der Einsatz von Funkwasserzählern ist im Hinblick auf das Grundrecht der Unverletzlichkeit der Wohnung sogar als eine besonders schonende Art der Datenerfassung anzusehen, weil er das Betreten von privaten Räumen entbehrlich mache.**

(Nicht amtliche Leitsätze)

Zur Verpflichtung, im elektronischen Rechtsverkehr eine dem Stand der Technik entsprechende Verschlüsselung zu verwenden (Ls)

(**Verwaltungsgericht Frankfurt/M.**, Beschluss vom 15. Juli 2022 – 5 L 1281/22 –)

Bei der elektronischen Kommunikation im Zusammenhang mit der Meldung von Kriegswaffenbeständen an das Bundesamt für Wirtschaft und Ausfuhrkontrolle wäre wegen ihrer Sensibilität eine unverschlüsselte elektronische Kommunikation nicht zulässig: Jedoch ist gegenwärtig eine Transportverschlüsselung ausreichend.

Dienstentfernung einer Beamtin infolge der Nichtumsetzung dienstlicher Anordnungen in Bezug auf die Corona-Pandemie (Ls)

(**Verwaltungsgericht Trier**, Urteil vom 21. Juni 2022 – 3 K 802/22 –)

Die Dienstentfernung einer Justizvollzugsbeamtin aufgrund beharrlicher Verweigerungshaltung sowie wiederholter innerdienstlicher Äußerungen in Bezug auf die staatlichen Maßnahmen zur Pandemiebekämpfung sowie zur Impfung ist rechtmäßig. Das Verhalten der Beamtin stellt ein einheitliches schweres Dienstvergehen dar, mit dem die Beamtin das Vertrauen des Dienstherrn und der Allgemeinheit endgültig verloren hat.

(Nicht amtliche Leitsätze)

Berichte, Informationen, Sonstiges

Chatkontrolle-Gesetz: EU will digitalen Schriftverkehr verdachtsunabhängig scannen

Die EU-Kommission hat offiziell ihre Pläne für das Chatkontrolle-Gesetz vorgestellt: Im Kampf gegen die Verbreitung von Kinderpornografie und zum Schutz von Kindern vor „Grooming" soll künftig die digitale Kommunikation, ob Mails, Chats oder über Messenger wie WhatsApp und Signal auf entsprechende Inhalte hin geprüft werden. Die Frage ist, inwieweit die verdachtsunabhängige, anlasslose Massenüberwachung mit dem „digitalen Briefgeheimnis" vereinbar ist.

Im Zuge der Pandemie hat die Verbreitung von Darstellungen sexuellen Missbrauchs von Kindern im Netz stark zugenommen. Allein rund 40.000 solcher Missbrauchsdarstellungen wurden 2021 in der EU erfasst. Die Dunkelziffer dürfte weit darüber hinausgehen. Die EU-Kommission möchte den Schutz von Kindern deshalb stärken.

Unternehmen sollen nunmehr dazu verpflichtet werden, mithilfe von KI-Software selbst private Chats und andere digitale Kommunikation vollautomatisch auslesen zu lassen – wofür im Übrigen oftmals auch eine Herabsetzung der derzeitigen Verschlüsselungsstandards erforderlich wäre. Erkennt das Programm hierbei bestimmte Inhalte, die auf die Verbreitung von Kinderpornografie – oder „Grooming" – hindeuten, soll dies an Strafverfolgungsbehörden weitergeleitet werden. Diese sichten dann die betroffenen Inhalte und prüfen, ob sich der technisch erfasste Anfangsverdacht bestätigt.

Nach einer PM der Kommission vom 11.05.2022 sollen Unternehmen, die eine Anordnung zur Aufdeckung von Inhalten erhalten haben, hierfür ausschließlich Indikatoren für sexuellen Kindesmissbrauch nutzen, die vom EU-Zentrum überprüft und bereitgestellt wurden. Die Erkennungstechnologien dürfen nur für die Aufdeckung von sexuellem Kindesmissbrauch eingesetzt werden. Die Anbieter müssen Technologien einsetzen, die nach dem Stand der Technik in der Branche am wenigsten in die Privatsphäre eingreifen und dafür sorgen, dass die Fehlerquote falsch positiver Ergebnisse so gering wie möglich ist.

900.000 Euro Bußgeld wegen unzulässiger Auswertung von Kundendaten eines Kreditinstitutes in Niedersachsen

Die LfDI Niedersachsen verhängte gegen die Hannoversche Volksbank ein Bußgeld 900 000 Euro, weil sie ohne Rechtsgrundlage die Daten aktueller und früherer Kunden bzgl. deren Online-Nutzerverhaltens auswertete. Zur Durchführung der Auswertung hatte die Bank einen Dienstleister beauftragt, die erhaltenen Ergebnisse mit Informationen einer Wirtschaftsauskunftei verglichen und entsprechend ergänzt. Die Betroffenen waren zwar über die Analyse informiert worden; Die nach Art. 6 Abs. 1 lit. a) DS-GVO notwendige Einwilligung war jedoch nicht eingeholt worden. Ein Stützen auf ein berichtigtes Interesse nach Art. 6 Abs. 1 lit. f) DS-GVO wurde verneint, da die entgegenstehenden Interessen der Betroffenen überwiegen. Dass die Bank die Analyseergebnisse nicht verwendet und mit der Aufsichtsbehörde kooperiert hatte, wirkte sich mildernd auf die Höhe des Bußgelds aus.

Wegen Datenschutzverstößen bei Forschungsfahrten verhängt die LfDI Niedersachen ein Millionenbußgeld gegen VW

Unter anderem weil ein VW-Testfahrzeug die anderen Verkehrsteilnehmer ohne deren Kenntnis filmte, muss VW nun ein Bußgeld zahlen. Einen Betrag von 1,1 Millionen Euro setzte die Landesdatenschutzbeauftragte Niedersachsens fest, den VW akzeptiert hat.

Im Jahr 2019 hat die österreichische Polizei ein Erprobungsfahrzeug von VW bei einer Verkehrskontrolle angehalten. Dabei stellte sich heraus, dass am Fahrzeug Kameras angebaut waren. Diese sollten zur Fehleranalyse das Verkehrsgeschehen rund um das Fahrzeug herum aufzeichnen. Aufgrund eines Versehens fehlten an dem Fahrzeug jedoch Magnetschilder mit einem Kamerasymbol und weiteren vorgeschriebenen Informationen für die datenschutzrechtlich Betroffenen, also in diesem Fall die anderen Verkehrsteilnehmenden. Gemäß Art. 13 der Datenschutzgrundverordnung (DS-GVO) müssten diese aber eigentlich über die Datenverarbeitung aufgeklärt werden. Das sei auch nicht der einzige Verstoß, unter anderem sei ebenfalls kein Auftragsverarbeitungsvertrag mit dem Unternehmen geschlossen worden, das die Fahrten durchführte.

Highlights aus dem Data-Agenda Datenschutz Podcast

„Der Bundesgerichtshof muss die vorrangige Zuständigkeit des EuGH beachten."

Data Agenda Datenschutz Podcast 6 mit Dr. Peter Allgayer, Richter am Bundesgerichtshof.

Datenschutzrecht beschäftigt zunehmend nationale Zivilgerichte bis hin zum Bundesgerichtshof. Dort geht es vor allem auch um die Reichweite der DS-GVO in Abgrenzung zum nationalen Recht. Dr. Peter Allgayer, Richter am zuständigen VI. Zivilsenat des BGH hat in RDV 5/2021[1] über aktuelle Entwicklungen zum Datenschutzrecht am BGH berichtet. Ab 2023 wird der Bundesrichter regelmäßig in Heft 1 der RDV über die Rechtsprechung des Bundesgerichtshofs zum Datenschutzrecht schreiben.

Begleitend dazu hat Peter Allgayer im Data Agenda Datenschutzpodcast 6 mit RDV-Herausgeber Rolf Schwartmann ein Gespräch über das Datenschutzrecht in der Rechtsprechung des BGH geführt. Ab 2023 ist ein Data Agenda Podcast ist jeweils in der zweiten Jahreshälfte ein Podcast mit Dr. Allgayer geplant. In diesem Experten-Talk diskutiert Professor Schwartmann regelmäßig mit Gästen aus Wirtschaft, Politik, Justiz oder Verwaltung.

Im Podcast 6[2] warf Allgayer einen Blick auf die Geschäftsverteilung des BGH, in dessen Zuständigkeit auch zivilrechtliche Ansprüche aus der DS-GVO fallen. Umfasst sind etwa Auskünfte eines Versicherungsnehmers gegen seine Versicherung[3] oder solche gegenüber einem Suchmaschinenbetreiber[4] oder die mittlerweile beim dem EuGH vorgelegten Schadensersatzansprüche nach Art. 82 DS-GVO.[5] Jenseits dieser originär datenschutzrechtlichen Ansprüche befasse den BGH aber auch die Frage, ob Vorschriften der DS-GVO zivilrechtliche Ansprüche ausschließen oder modifizieren. Das sei in der Grundlagenentscheidung zum digitalen Erbe thematisiert worden, die anlässlich eines geltend gemachten Anspruchs von Erben auf Zugang zu dem Benutzerkonto eines sozialen Netzwerks und der darin vorgehaltenen Kommunikationsinhalte erging.[6] DS-GVO-Fragen dürften künftig auch in kartellrechtlichen Verfahren eine Rolle spielen.[7] Hier sieht er mögliche Aufgaben auf den Kartellsenat mit Blick auf § 19 a GWB zukommen.

Die BGH-Richter beschäftigt aber auch das Alltagsgeschäft der Datenschutzpraxis, vor allem mit Blick auf Schadenersatzansprüche nach Art. 82 DS-GVO. Die Breite der diskutieren Themen ist hier denkbar groß. Von der Frage des Rechtsmissbrauchs, über die Geringfügigkeitsgrenze bis hin zu der Frage nach Bemessungskriterien kommt mit sehr unterschiedlichen Ansätzen gegenwärtig vieles auf den Prüfstand. Allgayer sortiert das am Beispiel des Kammerbeschlusses des BVerfG zur Entscheidung des AG Goslar ein, bei der es um die Frage ging, ob eine fehlgeleitete Werbemail mit Zweifeln an deren Einwilligung einen Anspruch auf Schadensersatz bis zu 500 € auslösen kann.[8] Die Aufhebung und Zurückweisung an das Amtsgericht ist für ihn nicht überraschend und rechtlich richtig. Die Entscheidung will er aber dennoch nicht überbewertet wissen. Künftig werde es häufig um Fragen gehen, die von den nationalen Gerichten nicht ohne vorherige Vorlage an den EuGH entschieden werden können. Jedes oberste deutsche Fachgericht als „Sandwichgericht" zwischen EuGH, EGMR und BVerfG müsse seine europarechtlich determinierte Zuständigkeit als gesetzlicher Richter achten.

(Lucia Burkhardt, Wissenschaftliche Mitarbeiterin an der Kölner Forschungsstelle für Medienrecht)

1 Allgayer Die Datenschutzgrundverordnung in der Rechtsprechung des Bundesgerichtshofs, RDV 2021, 243 ff.

2 Abrufbar unter: https://dataagenda.de/folge-6-von-der-risikoorientierung-bis-zu-einem-rechtsrahmen-fuer-kuenstliche-intelligenz-datenschutz-in-europa-zukunftsoffen-gestalten/.

3 BGH, Urteil vom 15.06.2021 – ZR VI 576/19.

4 BGH, Urteil v. 03.05.2022 – VI ZR 832/20.

5 BGH, Urteil v. 22.02.2022 – VI ZR 1175/20.

6 BGH, Urteil vom 12.07.2018 – III ZR 183/17.

7 Dazu Data Agenda Podcast 4 mit Jürgen Kühling, Drei Jahre DS-GVO – Licht und Schatten, abrufbar unter: https://dataagenda.de/drei-jahre-ds-gvo-licht-und-schatten/.

8 BVerfG, Beschl. v. 14.01.2021 – 1 BvR 2853/19.

JETZT ANMELDEN!

41. RDV-Forum

16. November 2022

46. DAFTA

„Datenschutz – Gestaltungsauftrag im Zeitalter der Digitalisierung"

17. – 18. November 2022

im Maternushaus Köln und auch online

Literaturhinweise

Schwartmann/Jaspers/Eckhardt (Hrsg.), **Heidelberger Kommentar zum TTDSG**, C.F. Müller Heidelberg, 2022, 477 S., 119,00 €

Mit dem Telekommunikation-Telemedien-Datenschutz-Gesetz wurde im Dezember 2021 die deutsche Gesetzeslage an europäisches Recht, insbesondere die ePrivacy-Richtlinie (von 2002 (!)) und die DS-GVO (von 2016) angepasst. Zugleich wurden die Datenschutzbestimmungen von TKG und TMG im TTDSG zusammengefasst – also hinreichende Anlässe für eine vertiefte Befassung mit der neuen und neugefassten Rechtsmaterie in Gestalt einer Kommentierung.

Diese wird verantwortet von Professor Dr. Rolf Schwartmann (TH Köln), Andres Jaspers (Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit GDD) und Dr. Jens Eckhardt (Fachanwalt für IT-Recht), also drei ausgewiesenen Kennern der Datenschutzmaterie und allesamt der Datenschutzgemeinde als didaktisch versierte Vermittler eines praxisorientierten Rechtsverständnisses bekannt. Unterstützt werden sie von einer Riege 20 weiterer Kommentierender aus den Bereichen Ministerialverwaltung, Rechtsanwaltschaft, Datenschutz-Aufsichtsbehörden und Hochschulen.

Mit dieser Truppe liefern die Herausgeber auf absolut angemessenen 350 Druckseiten eine Erst-Kommentierung „state of the art“, mit hilfreichem Fußnotenapparat, nützlichem Stichwortverzeichnis und sinnvollen Anhängen von verwandten Gesetzesmaterien.

Die Einzelkommentierungen gewichten zwar jeweils nach Bedeutsamkeit der untersuchten Norm, folgen jedoch einem einheitlichem Bearbeitungsschema, das zunächst eine Einordnung der Vorschrift und die Erläuterung ihres systematischen und historischen Hintergrunds vorsieht und nach der fachlichen Kommentierung auch Praxishinweise und Vollzugs-/Sanktionsfragen anspricht. Auf hohem Niveau und immer unter Einbeziehung von einschlägiger Rechtsprechung und praktischer Erfahrung werden die Einzelvorschriften des TTDSG erörtert, natürlich unter intensiver Diskussion der relevanten Rechtspositionen, etwa zur Bindung des die Privatnutzung gestattenden Arbeitsgebers ans Fernmeldegeheimnis (§ 3), zur Verwendung von Verkehrs- und Steuerdaten gegen Angreifer (§ 12, vgl. § 100 TKG a.F.) oder zum Schutz der Privatsphäre bei Endeinrichtungen (§ 25, der Art. 5 Abs. 3 ePrivacy-RL umsetzt). Immer finden sich Verweise auf die aktuellen Positionierungen der deutschen und europäischen Datenschutz-Aufsichtsbehörden, die mit der gebotenen kritischen Sichtweise einbezogen werden. Hinweise auf die umfangreiche Literatur finden sich den Kommentierungen vorangestellt und werden in Fußnoten konkret zugeordnet, ohne den Lesefluss zu stören.

Wenige Monate nach In-Kraft-Treten eines Gesetzes, dessen Anwendungsbereich mit „hoch komplex“ noch zurückhaltend bezeichnet ist (vgl. die konzise Kommentierung zu § 1) und das trotz seiner Verspätung massive Regelungsdefizite aufweist (so hat der Gesetzgeber von notwendigen Übergangsvorschriften ganz abgesehen), eine so fundierte und hilfreiche Kommentierung vorzulegen, belegt die Klasse aller Bearbeiter/-innen. Damit liegt viel mehr als nur ein „erster Einstieg“ ins Telekommunikations- und Telemedien-Datenschutzrecht vor, sondern eine ebenso hilfreiche wie belastbare Auseinandersetzung mit einer zukunftsträchtigen Rechtsmaterie. Dem Werk ist daher eine weite Verbreitung zu wünschen, denn Datenschutz lebt nur in seinem Ausgangspunkt vom Enthusiasmus, danach hilft nur noch fundierte Fachlichkeit.

(Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg)

Michael Els, **Datenschutz für Kindertageseinrichtungen**, Wolters Kluwer, Hürth 2022, ISBN 978-3-556-09092-3, 35,00 €

Die Bedeutung eines funktionierenden Datenschutzes in der Kita ist evident. Jüngst wurden 42 Kita-Apps durch IT-Sicherheitsexperten untersucht, wobei z.T. gravierende Mängel zutage getreten sind (https://t1p.de/cu25y). Mehrere Aufsichtsbehörden haben sich in der Vergangenheit mit den spezifischen Verarbeitungssituationen in Kindertageseinrichtungen auseinandergesetzt (vgl. etwa Niedersachsen, https://t1p.de/4hlp1; Rheinland-Pfalz, https://t1p.de/47v68; Baden-Württemberg, https://t1p.de/hds7). Die dort zur Verfügung gestellten knappen Informationen bleiben jedoch zwangsläufig an der Oberfläche.

Diese spürbare Lücke wurde nun von Michael Els geschlossen. Der Verfasser macht es sich zur Aufgabe, „eine möglichst praxisnahe Instruktion an die Hand zu geben“ (S. 11), weshalb das Werk nach einer grundlegenden Einführung entlang der Arbeitsprozesse innerhalb einer Kita gegliedert sei.

In der Praxis stellt sich zunächst die Frage, welches Datenschutzrecht für die verschieden kommunalen, freien und kirchlichen Träger jeweils Anwendung findet. Für kommunale Kitas sind dies unzweifelhaft die bereichsspezifischen Vorschriften des SGB VIII und SGB X (S. 16). Schwieriger ist die Ausstrahlungswirkung des § 68 Abs. 3 SGB VIII einzuschätzen, wonach bei der Inanspruchnahme freier Träger sicherzustellen ist, dass der Schutz der personenbezogenen Daten bei der Verarbeitung in entsprechender Weise wie im Sozialdatenschutz gewährleistet ist. Els geht insoweit nicht davon aus, dass es sich um eine partielle Rechtsfolgenverweisung ähnlich § 78 Abs. 1 Satz 3 SGB X (hierzu Franck, ZD 2015, 155 ff.) handelt. Er kommt gleichwohl über öffentlich-rechtliche Sicherstellungsvereinbarungen sowie die zivilvertragliche Rücksichtnahmepflicht – bzw.

im Falle katholischer Einrichtungen über eine Anordnung der deutschen Bischöfe – zu einer entsprechenden Anwendung der SGB-Vorschriften für freie (S. 19) und kirchliche (S. 21) Träger. Zweifelhaft ist freilich, ob allein hierdurch der nötige Konnex zwischen Art. 6 Abs. 1 lit. e DS-GVO und den §§ 62 ff. SGB VIII geschaffen werden kann (vgl. ErwGr 41 DS-GVO).

Das Werk folgt dem „Lebenszyklus" (S. 34) des personenbezogenen Datums von seiner Erhebung – im Sozialdatenschutz ist weiterhin der Vorrang der Direkterhebung angeordnet – über die Verarbeitung bis zur Übermittlung. Der Verfasser beschäftigt sich intensiv mit der Einwilligung als Erlaubnistatbetand und vertritt die pragmatische Auffassung, dass in Routinefällen entgegen § 1627 BGB nicht stets beide sorgeberechtigten Elternteile einwilligen müssen. Diese Auffassung ist für sich genommen nicht neu, sie wird aber ganz praxisbezogen unterlegt mit einer anschaulichen Tabelle eher erheblicher bzw. eher unerheblicher Angelegenheiten.

Gleich vier Kapitel widmen sich der allgegenwärtigen Verarbeitung von Bildmaterial, sei es im Kita-Alltag, bei Veranstaltungen, durch Dritte (z.B. Großeltern) sowie schließlich bei der Veröffentlichung von Beschäftigtenphotos. Außerdem sind knappe Darstellungen des Beschäftigtendatenschutzes (insb. Fragerechte; erweitertes Führungszeugnis!), des Datensicherheitsrechts, des Outsourcings sowie der Betroffenenrechte enthalten.

Überraschend knapp fallen die Ausführungen zum DSB aus (S. 33), obschon jede Kita unabhängig von ihrer jeweiligen Trägerschaft zwingend einen solchen benennen muss (vgl. Eßer/Franck, Datenschutzrecht, 2022, Rn. 79 ff.; ULD Schleswig-Holstein, 37. TB 2017/2018, S. 92 f.). Etwaige Haftungsrisiken werden nicht behandelt, möglicherweise geht der Verfasser davon aus, dass es im Bereich des Kita-Datenschutzes keiner extrinsischen Motivation zur Compliance bedarf.

Els gibt insgesamt einen dichten Überblick über das anwendbare Recht beim Betrieb einer Kindertageseinrichtung. Zahlreiche Beispiele und Muster runden die Kapitel ab und machen die Materie handhabbar. Hervorgehoben sei hier nur die umfangreiche Übersicht über Aufbewahrungsfristen im Zusammenhang mit dem Löschanspruch (S. 229 ff.).

Das Werk ist vor allem für Kita-Leitungen sowie deren Datenschutzbeauftragte von immensem Wert. Die Leitungen bekommen eindrucksvoll das gesamte Ausmaß ihrer datenschutzrechtlichen Pflichten aufgezeigt, Datenschutzbeauftragte finden schnell Antworten auf ihre drängendsten Fragen.

(Prof. Dr. Lorenz Franck, Brühl)

Philpp Knitter, **Digitale Weisungen – Arbeitgeberentscheidungen auf Grundlage algorithmischer Berechnungen**, Duncker&Humblot, Schriften zum Sozial- und Arbeitsrecht (SAR), Band 372, 2022, 284 S., Buch 89,90 €

Seit Jahrzehnten wird prognostiziert, wann welche Berufe von Maschinen übernommen werden. Dass auch klassische Arbeitgeberfunktionen, wie die Ausübung des Weisungsrechts, an technische Systeme delegiert werden, wird bislang kaum beachtet. Die Arbeit definiert digitale Weisungen, als Arbeitgeberweisungen, denen entweder unmittelbar oder mittelbar Entscheidungen eines algorithmischen Systems zugrunde liegen. Digitale Weisungen ergehen vor allem in der Schicht- und Einsatzplanung. Ihre Implementierung in Betrieben löst nicht nur Beteiligungsrechte des Betriebsrats aus. Das geltende Recht fordert, dass automatisierte Weisungsentscheidungen transparent und billig (§ 106 GewO) getroffen werden. Arbeitnehmer und Betriebsräte müssen die Möglichkeit haben, mit dem Weisungsgeber in einen argumentativen Austausch zu treten. Dort, wo technische Systeme diesem Erfordernis von »Responsivität« (noch) nicht genügen, stehen Weisungen unter dem Vorbehalt einer menschlichen Letztentscheidung.

Im Einzelenen werden u.a. angesprochen: Digitale Weisungen in Praxis und Rechtskontext. Die. Implementierung digitaler Weisungen im Betrieb: und die Beteiligung des Betriebsrats bei ihrer Implementierung. Das ggf. erforderliche Verbot automatisierter Entscheidungen im Einzelfall, Art. 22 DSGVO. Ihre Erlaubnis auf Grundlage von Kollektivvereinbarungen. Die Transparenz der Entscheidung und der Anspruch des Arbeitnehmers auf Auskunft über Billigkeitsaspekte. Abschluss bildet ein Literatur- und Stichwortverzeichnis Ausgezeichnet wurde dir Arbeit mit dem Wissenschaftspreis der Stiftung Theorie und Praxis des Arbeitsrechts (Wolfgang-Hromadka-Stiftung) 2022.

(Schriftleitung)

Paketboten als „TikTok-Tanzbären" – Datenschutz schützt vor Entwürdigung

In den U.S.A. ist es ein Trend, Amazon-Boten nur dann gut zu bewerten, wenn sie bei der Ablieferung eines Paketes vor der Hauskamera tanzen. Da Paketboten von ihren Arbeitgebern an den positiven Bewertungen im Netz gemessen werden, geraten sie in eine Drucksituation. Das mutet man aus guten Gründen keinem Tanzbären im Zirkus zu. Dennoch wurde das mit dem Song „Teach Me How to Dougie" unterlegte Video eines tanzenden Paketfahrers über sechs Millionen Mal auf TikTok angeschaut. Lassen wir den in der nicht autorisierten Nutzung des Liedes möglicherweise liegenden Urheberrechtsverstoß beiseite. Datenschutzrechtlich wäre das Video in Europa ein Problem. Stefan Brink, der oberste Datenschützer aus Baden-Württemberg, findet klare Worte. „Wer Kundenbewertungen bei Personalentscheidungen eine maßgebliche Bedeutung zumisst, macht seine Mitarbeitenden nicht nur erpressbar, er verstößt auch gegen Prinzipien des Beschäftigtendatenschutzes: Solche personenbezogenen Bewertungen darf ein Arbeitgeber nur erheben, wenn er die Daten auch verwerten dürfte (Grundsatz der Erforderlichkeit). Dies scheitert aber schon daran, dass Kundenbewertungen nicht nach objektiven Maßstäben erfolgen und daher unbrauchbar sind. Auch auf Basis der bloßen Menge an positiven oder negativen Bewertungen ein Urteil zu bilden, wäre willkürlich. Ein klarer Verstoß gegen den Datenschutz."

Der Wissensvorsprung für Ihre Arbeit

Die Datenschutz Newsbox versorgt Sie monatlich mit aktuellen Themen rund um den Datenschutz.

PDF-Download auch ohne Abo verfügbar

www.dataagenda.de/datenschutz-newsbox

DA

DATAKONTEXT

Jetzt hybrid: Online & in Köln

46. DAFTA

17.–18. November 2022

41. RDV-Forum

16. November 2022

DATENSCHUTZ – GESTALTUNGSAUFTRAG IM ZEITALTER DER DIGITALISIERUNG

Jetzt anmelden: **datakontext.com/dafta-2022**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT