ISSN 0178-8930
HZ212337

G 20 141

RDV

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

1/2022

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

FRANCK, Gesetzgebungskompetenz(en) des Bundes für das IT-Sicherheitsrecht Kritischer Infrastrukturen – Teil I

GOLA, Sanktionsminderung infolge Compliance – ein Überblick

PILTZ/ZWERSCHKE, Missbräuchliche Ausübung von DS-GVO-Betroffenenrechten – zulässiger Verteidigungseinwand für Verantwortliche?

Kurzbeiträge

REIF, Praxisfälle zum Datenschutzrecht XIV: Datenschutz bei Unternehmensverkauf und Due Diligence

GOLA, Aus den aktuellen Berichten der Aufsichtsbehörden (58): TLfDI; 3. TB (2020) nach der DS-GVO: Vier Fälle einwilligungsbedürftiger Verarbeitungen

Rechtsprechung

Aus dem Inhalt

BGH, Zu den Grenzen der Internet-Werbung für ärztliche Fernbehandlungen (Ls)

BGH, Zu den Voraussetzungen und der Annahme einer Kennzeichnungspflicht bei Instagram Posts von Influencern (Influencer I) (Ls)

BAG, Erschütterung des Beweiswerts einer Arbeitsunfähigkeitsbescheinigung

BAG, Vorlagebeschluss: Verarbeitung von Gesundheitsdaten im Arbeitsverhältnis (Ls)

BSOZG, Weg vom Bett ins Homeoffice ist gesetzlich unfallversichert (Ls)

LAG NIEDERSACHSEN, Auskunftsrecht nach Art. 15 DS-GVO und Immaterieller Schadensersatz nach Art. 82

38. Jahrgang
Februar 2022
Seiten 1–56

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Datenschutzorganisationen prüfen und bewerten nach der Systematik der Aufsichtsbehörden

Datenschutzorganisationen prüfen und beurteilen mit begrenztem Zeitaufwand

Ihr ständiger Begleiter im Datenschutz-Management

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

Kirchliche Stellen mit begrenztem Zeitaufwand zum Datenschutz auditieren

Wie DS-GVO-konform arbeitet Ihr Unternehmen?

Machen Sie den Test mit unseren Excel-Tools!

Bestellen Sie direkt unter: **datakontext.com**

DATAKONTEXT

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht

38. Jahrgang 2022
Heft 1
Seiten 1–56

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 1

Veranstaltungen 2

Aufsätze

Prof. Dr. Lorenz FRANCK
Gesetzgebungskompetenz(en) des Bundes für das IT-Sicherheitsrecht Kritischer Infrastrukturen – Teil I 3

Prof. Peter GOLA
Sanktionsminderung infolge Compliance – ein Überblick 7

Carlo PILTZ/Johannes ZWERSCHKE
Missbräuchliche Ausübung von DS-GVO-Betroffenenrechten – zulässiger Verteidigungseinwand für Verantwortliche? 11

Kurzbeiträge

RAin Yvette REIF, LL.M.
Praxisfälle zum Datenschutzrecht XIV: Datenschutz bei Unternehmensverkauf und Due Diligence 18

Prof. Peter GOLA
Aus den aktuellen Berichten der Aufsichtsbehörden (58): TLfDI; 3. TB (2020) nach der DS-GVO: Vier Fälle einwilligungsbedürftiger Verarbeitungen 21

Rechtsprechung

Zu den Grenzen der Internet-Werbung für ärztliche Fernbehandlungen (Ls)
(BGH, Urteil vom 09.12.2021) 23

Zu den Voraussetzungen und der Annahme einer Kennzeichnungspflicht bei Instagram Posts von Influencern (Influencer I) (Ls)
(BGH, Urteil vom 09.09.2021) 23

Erschütterung des Beweiswerts einer Arbeitsunfähigkeitsbescheinigung
(BAG, Urteil vom 08.09.2021) 24

Vorlagebeschluss: Verarbeitung von Gesundheitsdaten im Arbeitsverhältnis (Ls)
(BAG, Beschluss vom 26.08.2021) 26

Weg vom Bett ins Homeoffice ist gesetzlich unfallversichert (Ls)
(BSozG, Urteil vom 08.12.2021) 27

Auskunftsrecht nach Art. 15 DS-GVO und Immaterieller Schadensersatz nach Art. 82
(LAG Niedersachsen, Urteil vom 22.10.2021) 27

Offenlegung von Gesundheitdaten im Betrieblichen Eingliederungs-Management
(LAG Baden-Württemberg, Urteil vom 20.10.2021) 28

Schadensersatz bei verzögerter Datenauskunft
(LAG Hamm, Urteil vom 11.05.2021) 33

Keine Zuständigkeit der Aufsichtsbeörde bei abgeschalteten überwachungskameras (Ls)
(OVG Koblenz, Urteil vom 25.06.2021) 35

Keine Diskriminierung bei Nichtaufnahme von Mädchen im Knabenchor (Ls)
(OVG Berlin-Brandenburg, Urteil vom 21.05.2021) 35

Kein Anspruch auf Aufhebung des Entzugs der DSB-Funktion wegen eventueller Inkompatibilität im vorläufigen Rechtsschutzverfahren
(VerwGH Baden-Württemberg, Beschluss vom 26.07.2021) 36

Zur Rechtsgrundlage des Auskunftsrechts gegenüber einem in kirchlichen Besitz befindlichen Krankenhaus
(LG Siegen, Beschluss vom 26.11.2021) 37

Ein immaterieller Schadensersatz nach Art. 82 DS-GVO muss konkretisiert sein (Ls)
(LG Bremen, Beschluss vom 16.07.2021) 40

Schadensersatzanspruch aus Art. 82 DS-GVO wegen der unberechtigten Nutzung einer anwaltlichen E-Mail-Adresse zwecks Werbung
(AG Pfaffenhoven, Urteil vom 09.09.2021) 40

Schmerzensgeld auf Grund der Verwendung eines diskriminierenden Fotos einer Beschäftigen zwecks Firmenwerbung (Ls)
(AG Münster, Urteil vom 25.03.2021) 43

Polizei darf Bahnreisenden nicht allein wegen Hautfarbe kontrollieren
(VerwG Dresden, Urteil vom 18.01.2022) 43

Zur Speicherung des Geburtsdatums und der Anrede eines Apotheken-Online-Kunden
(VerwG Hannover, Urteil vom 09.11.2021) 43

Anwaltliches Berufsgeheimnis contra Informationszugangsanspruch (Ls)
(VerwG Baden-Württemberg, Urteil vom 22.06.2021) 49

Berichte, Informationen, Sonstiges

BlnLfDI: TTDSG trat in Kraft: Klare Regeln für Cookies und ähnliche Technologien 51

Zu guter Letzt:
BVerwG: Entfernung aus dem Beamtenverhältnis bei Leugnung der Existenz der Bundesrepublik Deutschland 51

Literaturhinweise

Buchbesprechungen

Diermann, Patrick, Datenschutzaufsicht über die Tätigkeit der Finanzverwaltung
(REDAKTION) 52

Harte-Bavendamm, Henning/Henning-Bodewig, Frauke/Goldmann, Michael/Tollmitt, Jan (Hrsg.), Gesetz gegen den unlauteren Wettbewerb – Mit Preisangabenverordnung und Geschäftsgeheimnisgesetz
(SCHRIFTLEITUNG) 52

Krimphove, Dieter, Werberecht
(SCHRIFTLEITUNG) 52

Anton Barrein, Das Recht auf Home-Office-Handlungs-spielräume und Grenzen des Arbeits- undSozialversicherungs-gesetzes für die digitalisierte Arbeitswelt 4.0
(REDAKTION) 52

Nachgefasst 54

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 1/2022

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 1
Seiten 1-56

RDV
Recht der Datenverarbeitung

38. Jahrgang · Februar 2022 · Seiten 1–56

Editorial

Beschäftigtendatenschutz – Quo vadis?

„Mehr Fortschritt wagen" – so der Titel des neuen Koalitionsvertrags. Aber was ist Fortschritt, was Rückschritt, und was nur ein Tippeln zur Seite? Auch im Datenschutzrecht stellt sich immer wieder diese Frage neu. Konkret heißt es da:

> „Wir schaffen Regelungen zum Beschäftigtendatenschutz, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen".

Aber was heißt das? Wer ist schon gegen Rechtsklarheit, und wer wollte nicht den effektiven Schutz von Persönlichkeitsrechten? Wer das so abstrakt formuliert, der wird keinen Widerspruch erwarten müssen. Wer konkreter wird, muss sagen, was er tatsächlich will. Und da beginnt die Diskussion. Hilfreich wäre in der Tat größere Rechtssicherheit. Die kann insbesondere durch Betriebsvereinbarungen gewährleistet werden.

Eigentlich ist das ein Wiedergänger. Schon der Koalitionsvertrag von CDU/CSU u. SPD (19. Legislatur, Zeilen 6086-6088) formulierte einen Prüfauftrag, der sich ebenso in den Materialien zum 1. DSAnpUG-EU wiederfindet, dort aber noch konkreter gefasst ist, indem exemplarisch verschiedene Regelungsziele aufgezählt werden: „das Fragerecht bei der Begründung eines Beschäftigungsverhältnisses, den expliziten Ausschluss von heimlichen Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten sowie den Ausschluss von umfassenden Bewegungsprofilen, den Ausschluss von Dauerüberwachungen und die Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken." (BT-Drucks. 18/11325, S. 97). Aber was könnte jetzt gemeint sein?

In der Suche nach einem besseren Beschäftigtendatenschutz sind alle möglichen Handlungsoptionen in den Blick zu nehmen. Gesetzliche Neuformulierungen oder Ergänzungen sind jedoch nur dort möglich, wo es sich um abstrakte Regelungen handelt, die hinreichende Verallgemeinerungsfähigkeit besitzen. Eine Vielzahl von Einzelfragen zu regeln, birgt die Gefahr, dass die Systematik verloren geht und dass die Regelung dann eben – weil zu kategorisch – den Einzelfall nicht richtig erfasst. Deshalb ist ergänzend nach weiteren Instrumenten der Konkretisierung und der Rechtsklarheit zu suchen. Hierfür kann es hilfreich sein, gesetzgeberische Hinweise zur Gewichtung der Verhältnismäßigkeitskriterien und Abwägungsmaßstäbe bei einzelnen Datenverarbeitungen im Beschäftigungskontext zu geben: Nicht die Lösung im Einzelfall wird vorgegeben, sondern die Kriterien benannt, nach denen die Abwägung im Einzelfall zu erfolgen hat. Dies kann im Gesetz selbst geschehen oder aber in einer Stärkung der Selbstregulierung durch Sozial- und Betriebspartner. Wiederum ergänzend dazu können Stellungnahmen der Aufsichtsbehörden treten, die zahlreicher als bisher die Einzelfälle des Beschäftigtendatenschutzes adressieren. Durch eine ausführliche auch rechtliche Begründung ermöglichen sie der Praxis, sich hiermit auseinanderzusetzen und diese Empfehlungen sinnvoll auch im eigenen Betrieb umzusetzen.

Vieles ist also möglich. Prüfet alles und behaltet das Gute, mahnt der hl. Paulus die Gemeinde von Thessaloniki. Das gilt auch hier und heute. Das Ziel ist klar. Jeder Schritt auf dem Weg ist verdienstvoll.

Prof. Dr. Gregor Thüsing

Prof. Dr. Gregor Thüsing
Direktor des Instituts für Arbeitsrecht und Recht der sozialen Sicherheit der Universität Bonn und Vorstandsmitglied der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn.

Termine	Thema	Ort	Kontakt
28.03.2022	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
30.03.2022	IT-Sicherheitsmanagement aus Sicht der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
31.03.2022	Teleworking unter Beachtung von Datenschutz und Sicherheit	Frankfurt/M.	GDD e.V. und DATAKONTEXT
05.04.2022	Einführung in die ISO 27701	Berlin	GDD e.V. und DATAKONTEXT
06.-07.04.2022	Datenschutz-Management nach der DS-GVO – Teil 3	Köln	GDD e.V. und DATAKONTEXT
11.04.2022	Hacker-Tools für Datenschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
12.04.2022	Datenschutz International	Frankfurt/M.	GDD e.V. und DATAKONTEXT
12.04.2022	Mobile Endgeräte im Zeitalter von DS-GVO und ePrivacy-Verordnung	München	GDD e.V. und DATAKONTEXT
25.04.2022	ISO 27001 und Datenschutz	Online	GDD e.V. und DATAKONTEXT
26.04.2022	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Köln	GDD e.V. und DATAKONTEXT
27.-28.04.2022	Datenschutz kompakt	Berlin	GDD e.V. und DATAKONTEXT
02.-06.05.2022	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
03.05.2022	Datenschutzverletzungen richtig behandeln	Köln	GDD e.V. und DATAKONTEXT
04.05.2022	Websites datenschutzkonform gestalten	Online	GDD e.V. und DATAKONTEXT
10.05.2022	Datenschlöschung und andere SAP-Funktionen für den Datenschutz	Berlin	GDD e.V. und DATAKONTEXT
11.05.2022	Löschen nach DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
12.05.2022	Strategischer Umgang mit Bußgeldbescheiden und Verbandssanktionengesetz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
17.05.2022	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
17.05.2022	Konzerndatenschutz	Köln	GDD e.V. und DATAKONTEXT
19.05.2022	Verzeichnis von Verarbeitungstätigkeiten	Online	GDD e.V. und DATAKONTEXT
24.05.2022	DS-GVO-konforme Verarbeitung personenbezogener Daten mit SAP-Systemen	Frankfurt/M.	GDD e.V. und DATAKONTEXT
08.06.2022	Strafverfolgung, Whistleblowing, International Investigations – Datenschutz und Strafrecht	Frankfurt/M.	GDD e.V. und DATAKONTEXT
21.06.2022	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Köln	GDD e.V. und DATAKONTEXT
22.06.2022	Datenschutz in medizinischen Einrichtungen	Online	GDD e.V. und DATAKONTEXT
23.06.2022	Zertifizierung zum Betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V. und DATAKONTEXT
23.06.2022	Datenschutz und Betriebsrat unter der DS-GVO	Online	GDD e.V. und DATAKONTEXT

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

Aufsätze

Prof. Dr. Lorenz Franck

Gesetzgebungskompetenz(en) des Bundes für das IT-Sicherheitsrecht Kritischer Infrastrukturen – Teil I

Dem Grundgesetz ist eine spezifisch auf das IT-Sicherheitsrecht zugeschnittene Gesetzgebungskompetenz unbekannt. Der Bund sieht sich insofern einem Mosaik einzelner Befugnisse für unterschiedliche Branchen und Dienstleistungen gegenüber. Die Gesetzgebungsbefugnis des Bundes ist in der Praxis unterdessen nicht unwidersprochen geblieben. Es überwiegen jedoch gute Gründe für ein einheitliches Regelungskonzept der IT-Sicherheit sowie deren Durchsetzung auf Bundesebene.

I. Überblick

Die IT-Sicherheitsgesetzgebung des Bundes – namentlich das ITSiG von 2015, das NIS-Umsetzungsgesetz von 2017 sowie das jüngst vom Bundestag verabschiedete[1] ITSiG 2.0 – begründet wesentliche Pflichten für Betreiber sog. Kritischer Infrastrukturen[2] sowie korrespondierende Aufgaben und Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die Gesetzgebungskompetenz des Bundes wird dabei ausweislich der Gesetzgebungsmaterialien zum Teil aus speziellen Kompetenztiteln hergeleitet.[3] Soweit in der Verfassung keine eigenständige branchenbezogene Gesetzgebungskompetenz niedergelegt ist, wird auf die allgemeinere Befugnis des Art. 74 Abs. 1 Nr. 11 GG (Recht der Wirtschaft),[4] auf eine ungeschriebene Kompetenz kraft Natur der Sache[5] bzw. auf eine Annexkompetenz abgestellt.[6]

Den Gesetzgebungsmaterialien ist zu entnehmen, dass „[e]ine bundesgesetzliche Regelung dieser Materie [...] zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich" sei.[7] Auch in der Literatur findet sich die Bestätigung, dass „das Bedürfnis einer einheitlichen bundesweiten Regelung [...] auf der Hand" liege.[8] Jedenfalls wird die Bundeskompetenz, soweit sie in der Literatur überhaupt thematisiert wird, hingenommen.[9]

Wie jedoch eine erste gerichtliche Auseinandersetzung zeigt, ist die Frage der Gesetzgebungskompetenz durchaus diskussionswürdig. Die Berliner Verkehrsbetriebe (BVG) wendeten sich jüngst gegen eine Maßnahme des BSI und gingen dabei unter anderem von einer teilweisen Unzuständigkeit des Bundesgesetzgebers für IT-Sicherheitsbelange des öffentlichen Nahverkehrs aus.[10] Aus diesem Grunde lohnt es sich, die für die IT-Sicherheitsgesetzgebung einschlägigen Gesetzgebungskompetenzen im Einzelnen zu beleuchten.

II. Gesetzgebungskompetenzen von Bund und Ländern

Aufgabe der Verfassung ist unter anderem, die Gesetzgebungskompetenzen im föderalen System festzulegen.[11] Die Artt. 70 ff. GG statuieren zu diesem Zweck ein mehrschichtiges Regelungsgefüge. Dabei sind gem. Art. 70 Abs. 1 GG grundsätzlich die Länder zuständig, soweit sich nicht aus der Verfassung etwas anderes ergibt.

Der Bund kann aufgrund ausschließlicher oder konkurrierender Gesetzgebungszuständigkeit handeln. Soweit ein ausschließlicher Kompetenztitel in den Katalogtatbeständen des Art. 73 GG (oder an anderer Stelle in Einzelnormen der Verfassung) enthalten ist, ergeben sich keine Schwierigkeiten. Agiert der Bund hingegen im Rahmen der konkurrierenden Gesetzgebung gem. Art. 74 GG, ist zu beachten: Auf sog. Bedarfskompetenzen im Sinne von Art. 72 Abs. 2 GG, darf sich der Bundesgesetzgeber nur berufen, wenn dies zur Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet oder zur Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse erforderlich ist.

1 BGBl. I 2021, S. 1122 ff. Zum ITSiG 2.0 insbesondere Kipker/Scholz, DuD 2021, 40 ff.; Müllmann/Ebert/Reissner, CR 2020, 584, 587 ff.; Atug, ICLR 2021, 7 ff.; Schallbruch, CR 2021, 516; Niemann/Karniyevich, K&R 2021, 441.

2 Von den Kritischen Infrastrukturen sind die Anbieter digitaler Dienste (§ 2 Abs. 12 BSIG) und die Unternehmen von besonderem öffentlichen Interesse (§ 2 Abs. 14 BSIG) begrifflich zu unterscheiden.

3 Vgl. im Einzelnen für das ITSiG BT-Drs. 18/4096 S. 19; für das NIS-Umsetzungsgesetz BT-Drs. 18/11242, S. 25 f.; für das ITSiG 2.0 BT-Drs. 19/26106, S. 31 f.

4 BT-Drs. 18/4096 S. 19; BT-Drs. 18/11242, S. 25; BT-Drs. 19/26106, S. 31.

5 BT-Drs. 19/26106, S. 32.

6 BT-Drs. 19/26106, S. 31 f.

7 BT-Drs. 18/4096, S. 19.

8 Roth, ZD 2015, 17, 18.

9 Roos, MMR 2014, 723, 724; Roßnagel, DVBl. 2015, 1206, 1207; Hornung, NJW 2015, 3334, 3335; Schallbruch, CR 2017, 648, 653; Buchberger, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BSIG Rn. 12; Remy/Stettner, DuD 2021, 254, 255; Fischer, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2021, § 13 Rn. 40 f. Vgl. Rehbohm/Kalmbach, MMR-Aktuell 2021, 438461, welche die Länderzuständigkeit annehmen, wenn es um Einrichtungen geht, die nicht kritisch, aber dennoch dem Gemeinwohl dienlich sind (wohl als Folge von Art. 72 Abs. 1 GG).

10 Siehe Stiebel, Behörden Spiegel vom 09.02.2021, online unter https://www.behoerden-spiegel.de/2021/02/09/bsi-nicht-zustaendig/. Die Klage wurde zwischenzeitlich zurückgenommen, s. Krempl, Heise Online vom 04.04.2021, online unter https://heise.de/-6005170.

11 Überblick bei Jarass, NVwZ 2000, 1089 ff.; Hebeler, JA 2010, 688 ff.; Voßkuhle/Wischmeyer, JuS 2020, 315 ff.

Macht der Bundesgesetzgeber von einer konkurrierenden Kompetenz Gebrauch, erlischt gem. Art. 72 Abs. 1 GG zugleich die Länderkompetenz (sog. Sperrwirkung). Für einige abschließend aufgeführte Bereiche der konkurrierenden Gesetzgebung wird den Ländern gem. Art. 72 Abs. 3 Satz 1 GG unterdessen eine Abweichungskompetenz zugestanden.

Ebenfalls von Bedeutung sind die ungeschriebenen Gesetzgebungskompetenzen des Bundes. Gemeint sind die Gesetzgebungskompetenz kraft Sachzusammenhangs bzw. Annexkompetenz, welche äußerlich weitestgehend identische Wirkungen entfalten und daher hier nicht unterschieden werden müssen.[12] Diese ungeschriebene Kompetenz zugunsten des Bundes greift, wenn eine ausdrücklich zugewiesene Materie „verständigerweise nicht geregelt werden kann, ohne dass zugleich eine nicht ausdrücklich zugewiesene andere Materie mitgeregelt wird".[13] Ordnungsbehördliche Befugnisse zur Durchsetzung und Gefahrenabwehr in der jeweiligen Rechtsmaterie sind typische Anwendungsfälle für eine derartige Kompetenzerweiterung.

Für Fragen im Zusammenhang mit der IT-Sicherheit[14] existiert mithin keine gesondert niedergelegte Gesetzgebungskompetenz in der Verfassung.[15] Stattdessen müssen je nach Regelungszusammenhang und einschlägiger Branche die im Grundgesetz angelegten Befugnisse auf ihre Stichhaltigkeit geprüft werden. Dabei ist davon auszugehen, dass sich konkrete Regelungen zur IT-Sicherheit stets unmittelbar aus der einschlägigen Gesetzgebungskompetenz für die Branche oder den Sektor ergeben.[16] Es handelt sich insoweit nicht etwa um eine thematisch verbundene Annexkompetenz zum eigentlichen Regelungskomplex. Vielmehr ist die IT-Sicherheit kraft ihrer betriebssichernden Funktion unauflöslich mit der Erbringung der in Rede stehenden Dienstleistung verknüpft.

III. Regelungsgegenstand IT-Sicherheit

1. Regelungsinhalte

a) Ausgangspunkt

Ein allgemeines IT-Sicherheitsrecht sollte die abzusichernden Systeme und Dienste spezifizieren und eingrenzen, Schutzziele verbindlich definieren, eine Handhabe für die Ermittlung und Bewertung von Risiken liefern und eine Bestimmung des sogenannten „Stands der Technik" ermöglichen.[17] Freilich fehlt es derzeit an einem solchen Allgemeinen Teil des IT-Sicherheitsrechts.

Immerhin definiert § 2 Abs. 2 Satz 4 BSIG die „Sicherheit in der Informationstechnik" als die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit („Integrität") oder Vertraulichkeit von Informationen betreffen. An mehreren Stellen im Gesetz tritt zudem das Schutzziel der Authentizität hinzu (vgl. etwa § 8a Abs. 1 Satz 1 bzw. § 8b Abs. 4 Satz 1 Nr. 1 BSIG). Art. 4 Nr. 2 NIS-RL beschreibt parallel hierzu die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, welche die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit beeinträchtigen.

- Verfügbarkeit = Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen, IT-Netzen oder Informationen ist gegeben, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.[18] Dazu gehören die Auffindbarkeit, Zugriffsmöglichkeit und Anwendbarkeit der vorgesehen Methoden.
- Integrität = Sicherstellung der Korrektheit von Daten und der korrekten Funktionsweise von Systemen. Hierzu gehört, dass Daten vollständig und unverändert sind.[19]
- Vertraulichkeit = Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.[20]
- Authentizität = Es ist sichergestellt, dass die Informationen von der angegebenen Quelle erstellt wurden.[21]

Diese allgemein anerkannten Schutzziele der Informationssicherheit können insofern als maßgebliche Stellschrauben des IT-Sicherheitsrechts angesehen werden.[22]

Aufgabe der aktuellen IT-Sicherheitsgesetzgebung ist es u.a., die Sicherheit Kritischer Infrastrukturen besonders zu schützen.[23] Gemäß § 2 Abs. 10 Satz 1 Nrn. 1 und 2 BSIG sind hierunter Einrichtungen und Anlagen zu verstehen, die den im Gesetz genannten Sektoren angehören und zugleich von hoher Bedeutung für das Funktionieren des Gemeinwesens sind.

Die Bedeutung einer Infrastruktur misst sich stets daran, ob durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Sektorenzugehörigkeit und Gemeinwichtigkeit müssen zwingend zusammentreffen.[24] Durch Rechtsverordnung (BSI-KritisV) wird bestimmt, welche genauen Anforderungen an die jeweiligen Einrichtungen zu stellen sind, um tatsächlich als Kritische Infrastrukturen angesehen zu werden.

Bei der Betrachtung Kritischer Infrastrukturen steht immer die verlässliche Erbringung oder Nichterbringung der jeweiligen Dienstleistung im Fokus. Die Schutzziele Verfügbarkeit, Integrität und Authentizität hängen hiermit leicht fasslich zusammen. Beim Schutzziel der Vertraulichkeit ist dies hingegen nicht ganz so offensichtlich. Solange etwa

12 So auch Jarass, NVwZ 2000, 1089, 1090.

13 BVerfGE 3, 407, 421; BVerfGE 98, 265, 299.

14 Kritisch hingegen Schallbruch, CR 2021, 516, 522, der für den Bereich der Gefahrenabwehr in der IT-Sicherheit eine Grundgesetzänderung erwägt.

15 Eine solche Kompetenz befürwortend Poscher/Lassahn, in: Hornung/Schallbruch (Fn. 9), § 7 Rn. 52. Zum Regierungsvorschlag einer Gesetzgebungskompetenz hinsichtlich der Informationstechnik öffentlicher Stellen des Bundes und der Länder anlässlich der Föderalismuskommission II siehe Komm.-Drs 098, S. 7. Zur Gesetzgebungskompetenz für alle Fragen der Digitalisierung nach Vorbild von Art. 73 Abs. 1 Nr. 7 GG, worunter auch Belange der IT-Sicherheit fielen NeXT, Diskussionspapier Digitalministerium im Bund, 2021, S. 2 (online unter https://next-netz.de/aktuelles/unser-diskussionsbeitrag-zum-digitalministerium-im-bund).

16 So auch Kipker, in: Kipker, Cybersecurity, 2020, § 1 Rn. 31; Poscher/Lassahn, in: Hornung/Schallbruch (Fn. 9), § 7 Rn. 52.

17 Raabe/Schallbruch/Steinbrück, CR 2018, 706, 714 f.

18 BSI, IT-Grundschutz-Kompendium, Ed. 2021, Glossar S. 8.

19 BSI, IT-Grundschutz-Kompendium, Ed. 2021, Glossar S. 4.

20 BSI, IT-Grundschutz-Kompendium, Ed. 2021, Glossar S. 9.

21 BSI, IT-Grundschutz-Kompendium, Ed. 2021, Glossar S. 1.

22 Schmidl, NJW 2010, 476, 477; Raabe/Schallbruch/Steinbrück, CR 2018, 706, 707.

23 Einzelheiten bei Hornung, NJW 2015, 3334 ff.; Roßnagel, DVBl. 2015, 1206 ff.; Schallbruch, CR 2017, 648 ff.

24 Zu Qualität und Quantität der Dienstleistung BT-Drs. 18/4096, S. 30 f.; näher Buchberger, GSZ 2019, 183, 185; Fischer in Hornung/Schallbruch (Fn. 9), § 13 Rn. 32 ff.

die Versorgung der Allgemeinheit mit Energie oder Wasser gewährleistet ist, mag der Schutz vor Preisgabe von Informationen nachranging erscheinen. Eine solche Sichtweise greift jedoch zu kurz.

Erstens können Mängel in der Vertraulichkeit überhaupt erst den Weg ebnen für Angriffe Dritter. Dies ist der Fall, wenn anlagenbezogene Informationen nach außen dringen, die es Angreifern ermöglichen, vorhandene Schwachstellen auszunutzen oder diese leichter ausfindig zu machen. Spezifisches Sonderwissen kann zudem für Methoden des Social Engineering[25] eingesetzt werden, um einen Rapport zwischen Angreifer und Zielperson zu erzeugen.

Zweitens gehört die Vertraulichkeit in zahlreichen Branchen denknotwendigerweise zur Geschäftsgrundlage, etwa im Gesundheits-, Finanz-, Telekommunikations- oder IT-Bereich. Ohne Vertraulichkeit besteht kein Vertrauen in die ordnungsgemäße Erbringung der jeweiligen Dienstleistung, wodurch sich Teile der Bevölkerung gehindert sehen könnten, die Dienstleistung weiterhin in Anspruch zu nehmen.

Drittens sind die verfolgten Schutzziele der IT-Sicherheit nicht eineindeutig bestimmten technisch-organisatorischen Sicherheitsmaßnahmen zuzuordnen.[26] Insofern vermag dieselbe Maßnahme verschiedene Schutzziele zu fördern. Eine Sicherheitslücke, die bei der einen Kritischen Infrastruktur zu einem Bruch der Vertraulichkeit geführt hat, kann bei der nächsten zu einer schwerwiegenden Störung im Betriebsablauf führen. Eine Aufspaltung der Gesetzgebungskompetenzen nach Schutzzielen erscheint daher nicht nur nicht sinnvoll, sondern ist nach hiesiger Auffassung gar nicht möglich.

b) Betreiberpflichten im Überblick

Betreiber Kritischer Infrastrukturen sind gem. § 8a Abs. 1 Satz 1 BSIG verpflichtet, angemessene organisatorische und technische Vorkehrungen zu treffen, die geeignet sind, Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu vermeiden. Dabei soll gem. § 8a Abs. 1 Satz 2 BSIG der Stand der Technik eingehalten (und nicht nur berücksichtigt) werden. Die zu treffenden Vorkehrungen sind gem. § 8a Abs. 1 Satz 3 BSIG angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.[27]

Mindestens alle zwei Jahre ist ein Nachweis notwendig, was z.B. durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen kann. Die Ergebnisse einschließlich der dabei aufgedeckten Sicherheitsmängel sind dem BSI zu übermitteln (§ 8a Abs. 3 BSIG).

Gem. § 8b Abs. 3 BSIG ist eine Kontaktstelle einzurichten. Störungen sind gem. § 8b Abs. 4 unverzüglich über diese Kontaktstelle an das BSI zu melden.[28] Sofern sich ein Ausfall oder eine erhebliche Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur ereignet hat, ist diese Störung unter Angabe des Betreibers zu melden. Erhebliche Störungen, die potentiell zu einem Ausfall oder zu einer erheblichen Beeinträchtigung führen können, sind ohne Nennung des Betreibers zu melden.

Eine Störung liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann bzw. versucht wurde, entsprechend auf sie einzuwirken.[29]

Mit Inkrafttreten des ITSiG 2.0 ist gem. § 8a Abs. 1a BSIG die Pflicht zur Implementierung eines Systems zur Angriffserkennung zwecks Störungsvermeidung statuiert worden.

Gemäß § 8d Abs. 2 Nr. 1 sowie Abs. 3 Nr. 1 BSIG gelten die oben genannten Vorgaben nicht für Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen. Insoweit trifft das TKG eigenständige Regelungen (vgl. § 109 TKG).[30]

Betreiber Kritischer Energieversorgungsnetze oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes sind gem. § 8d Abs. 2 Nr. 2 sowie Abs. 3 Nr. 2 BSIG ebenfalls vom Anwendungsbereich obiger Vorschriften ausgenommen. Entsprechende Regelungen sind stattdessen im EnWG enthalten (vgl. § 11 EnWG).[31]

Inhaber atomrechtlicher Genehmigungen unterliegen abermals nicht den genannten Vorschriften des BSIG (§ 8d Abs. 2 Nr. 4 sowie Abs. 3 Nr. 4 BSIG). Stattdessen haben diese gem. § 44b Satz 1 AtG Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit führen können, unverzüglich dem BSI zu melden.[32]

c) Befugnisse des BSI gegenüber Betreibern Kritischer Infrastrukturen

Das BSI ist die Cyber-Sicherheitsbehörde des Bundes.[33] Es sammelt gem. § 8b Abs. 2 BSIG insbesondere Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen und zeichnet hieraus ein Lagebild. Es unterrichtet auf dessen Grundlage Betreiber Kritischer Infrastrukturen sowie andere Behörden.

Gem. § 8a Abs. 5 BSIG kann das BSI das Verfahren von Sicherheitsaudits, Prüfungen und Zertifizierungen für Kritische Infrastrukturen näher ausgestalten. Das BSI kann sodann gem. § 8a Abs. 4 BSIG die organisatorischen und tech-

25 Grundlegend Mitnick, The Art of Deception, 2002; ferner Sohr/Kemmerich, in: Kipker (Fn. 15), § 12 Rn. 68 ff.; Fischer, in: Hornung/Schallbruch (Fn. 9), § 2 Rn. 178 ff.

26 Zu Mehrfachverknüpfungen von Schutzzielen und Maßnahmen am Beispiel des technischen Datenschutzes, Franck, in: Schwartmann/Pabst, DSG NRW, 2021, § 58 Rn. 27 ff.

27 Überblick bei Buchberger, GSZ 2019, 183, 186; eingehend Beucher/Fromageau, in: Kipker (Fn. 15), § 12 Rn. 68 ff.; Fischer, in: Hornung/Schallbruch (Fn. 9), § 13 Rn. 65 ff.

28 Überblick über die Meldepflichten bei Roos, MMR 2015, 636, 639 f.; Wimmer/Mechler, in: Gabel/Heinrich/Kiefner, Rechtshandbuch Cyber-Security, 2019, S. 149 ff.; Buchberger, GSZ 2019, 183, 186; Fischer, in: Hornung/Schallbruch (Fn. 9), § 13 Rn. 88. Eingehend zu den Meldepflichten Beucher/Fromageau, in: Kipker (Fn. 15), § 12 Rn. 84 ff. Synopse der unterschiedlichen Meldepflichten nach BSIG und DS-GVO bei Winter, CR 2020, 576 ff.

29 BT-Drs. 18/4096, S. 27 f.

30 Näher Wimmer/Mechler, in: Gabel/Heinrich/Kiefner (Fn. 27), S. 139 ff.

31 Näher Wimmer/Mechler, in: Gabel/Heinrich/Kiefner (Fn. 27), S. 137 ff.

32 Näher Wimmer/Mechler, in: Gabel/Heinrich/Kiefner (Fn. 27), S. 139.

33 Zu den Aufgaben des BSI insgesamt Buchberger, GSZ 2019, 183 ff.; Schallbruch, DuD 2021, 229, 230; Gitter, in: Hornung/Schallbruch (Fn. 9), § 15 Rn. 39 ff.

nischen Vorkehrungen beim Betreiber der Kritischen Infrastruktur kontrollieren. Dies ermöglicht Vor-Ort-Prüfungen in den Geschäfts- und Betriebsräumen ebenso wie das Verlangen von Aufzeichnungen, Schriftstücken und sonstigen Unterlagen (siehe auch § 8a Abs. 3 Satz 4 BSIG). Gem. § 8a Abs 3 Satz 5 BSIG kann das BSI im Einvernehmen mit der zuständigen Aufsichtsbehörde schließlich die Beseitigung von Sicherheitsmängeln anordnen. Soweit erforderlich, kann das BSI gem. § 8b Abs. 6 Satz 1 BSIG vom Hersteller betroffener informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer gemeldeten Störung beanspruchen. Gem. § 5b Abs. 1 Satz 1 BSIG kann das BSI u.U. Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Es kann auch hier gem. § 5b Abs. 6 BSIG vom Hersteller des informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken.

Portscans von Systemen Kritischer Infrastrukturen sind künftig gem. § 7b Abs. 1 Satz 1 BSIG ausdrücklich geregelt.

Sofern in den oben skizzierten Konstellationen die Voraussetzungen vorliegen, besteht die Möglichkeit von Verwaltungszwangsmaßnahmen nach den allgemeinen Regeln der Verwaltungsvollstreckung (vgl. §§ 6 ff. VwVG).

Das BSI ist zudem Bußgeldstelle für Verstöße nach § 14 Abs. 1 BSIG,[34] § 95 Abs. 1 Nr. 2b EnWG sowie § 395 Abs. 2a SGB V. Für die Verhängung sonstiger bereichsspezifischer Bußgelder[35] ist das BSI dagegen nicht als zuständige Verwaltungsbehörde festgelegt.

2. Kompetenzübersicht

Die Übersicht zeigt, welche Sektoren mit ausschließlichen bzw. konkurrierenden Gesetzgebungskompetenzen korrespondieren und inwieweit es sich jeweils um Bedarfskompetenzen iSv Art. 72 Abs. 2 GG handelt.

Sektor	Kompetenztitel	Bund	Bedarfsk.
Energie	Kernenergie: Art. 73 Abs. 1 Nr. 14 GG	ausschl.	
	Bergbau: Art. 74 Abs. 1 Nr. 11 GG	konkurr.	ja
	Energiewirtschaft: Art. 74 Abs. 1 Nr. 11 GG	konkurr.	ja
Wasser	Wasserhaushalt: Art. 74 Abs. 1 Nr. 32 GG	konkurr.	
	Sicherung der Ernährung: Art. 74 Abs. 1 Nr. 17 Var. 2 GG	konkurr.	
	Wirtschaft: Art. 74 Abs. 1 Nr. 11 GG	konkurr.	ja
Ernährung	Sicherung der Ernährung: Art. 74 Abs. 1 Nr. 17 Var. 2 GG	konkurr.	
	Recht der Lebens- bzw. Futtermittel, Verkehr mit Saat- und Pflanzgut: Art. 74 Abs. 1 Nr. 20 GG	konkurr.	ja
	Handel: Art. 74 Abs. 1 Nr. 11 GG	konkurr.	ja
Informationstechnik und Telekommunikation	Telekommunikation: Art. 73 Abs. 1 Nr. 7 Alt. 2 GG	ausschl.	
	Gewerbe: Art. 74 Abs. 1 Nr. 11 GG	konkurr.	ja
Gesundheit	Apotheken, Arzneien, Medizinprodukte, Heilmittel: Art. 74 Abs. 1 Nr. 19 GG	konkurr.	
	Bundeswehrkrankenhäuser: Art. 73 Abs. 1 Nr. 1 GG	ausschl.	
	Gewerbe: Art. 74 Abs. 1 Nr. 11 GG (Krankenhäuser/Labore)	konkurr.	ja
Finanz- und Versicherungswesen	Geld- und Münzwesen: Art. 73 Abs. 1 Nr. 4 GG	ausschl.	
	Bank- und Börsenwesen, privatrechtliches Versicherungswesen: Art. 74 Abs. 1 Nr. 11 GG	konkurr.	ja
	Bundesbank: Art. 88 Abs. 1 GG	ausschl.	
	Sozialversicherung: Art. 74 Abs. 1 Nr. 12 GG	konkurr.	
Transport und Verkehr	Luftverkehr: Art. 73 Abs. 1 Nr. 6 GG	ausschl.	
	Eisenbahnen des Bundes: Art. 73 Abs. 1 Nr. 6a GG	ausschl.	
	Schienenbahnen: Art. 74 Abs. 1 Nr. 23 GG	konkurr.	
	Hochsee-, Küsten- und Binnenschiffahrt: Art. 74 Abs. 1 Nr. 17 GG	konkurr.	
	Straßenverkehr: Art. 74 Abs. 1 Nr. 22 GG	konkurr.	ja
	Gewerbe: Art. 74 Abs. 1 Nr. 11 GG (ÖPNV; Logistik)	konkurr.	ja
	Postwesen: Art. 73 Abs. 1 Nr. 7 Var. 1 GG	ausschl.	
Siedlungsabfallentsorgung	Abfallwirtschaft: Art. 74 Abs. 1 Nr. 24 Var. 1 GG	konkurr.	ja
BSI-Befugnisse	Durchsetzung, Gefahrenabwehr: Sachzusammenhang/Annex	ausschl.	
	Strafrecht: Art. 74 Abs. 1 Nr. 1 Var. 2 GG (Ordnungswidrigkeiten)	konkurr.	

Ausblick

Der Beitrag wird fortgesetzt. Teil II widmet sich detaillierter den einzelnen Sektoren sowie den BSI-Befugnissen und erörtert Inhalt und Reichweite der einschlägigen Gesetzgebungskompetenzen. Im Hinblick auf die Bedarfskompetenzen werden in einem weiteren Schritt die in Art. 72 Abs. 2 GG niedergelegten Voraussetzungen („gleichwertige Lebensverhältnisse"; „Rechtseinheit"; „Wirtschaftseinheit") untersucht.

Prof. Dr. Lorenz Franck
Professor für IT-Recht mit öffentlich-rechtlichem Schwerpunkt an der Hochschule des Bundes für öffentliche Verwaltung, Brühl.

34 Hierzu Beucher/Ehlen, in: Kipker (Fn 15), § 12 Rn. 153 ff. Die Bußgeldvorschrift wurde durch das ITSiG 2.0 verschärft, vgl. BT Drs. 19/26106, S. 24 f.

35 Überblick bei Beucher/Ehlen, in: Kipker (Fn. 15), § 12 Rn. 165 ff.

Prof. Peter Gola

Sanktionsminderung infolge Compliance – ein Überblick

Drohen einem Unternehmen wegen Datenschutz-Rechtsverstößen staatliche finanzielle Sanktionen, so kann dabei eine effektive Compliance-Organisation honoriert werden. Auch wenn diesbezügliche Regelungen im VerbSanG[1] in der vergangenen Legislaturperiode infolge Nichtbefassung im Bundestag gescheitert sind, geben jedenfalls die Rechtsprechung, die Aufsichtsbehörden und auch gesetzliche Regelungen die Vorgaben, nach denen es bei der Bemessung einer Geldbuße auch von Bedeutung ist, ob ein effizientes, auf die Vermeidung von Rechtsverstößen ausgelegtes Compliance-System existiert.[2] Konkretisiert wird die von der „Compliance-Organisation" abhängige Sanktionsminimierung zudem in aktueller Gesetzgebung. So gebietet eine Neuregelung im Gesetz gegen Wettbewerbsbeschränkungen (GWB)[3] dem Bundeskartellamt, effektive Compliance-Maßnahmen bei einem gegen ein Unternehmen verhängtem Kartellbußgeld zu berücksichtigen.[4]

I. Compliance als allgemeine Sorgfaltspflicht

1. Begriffsdefinition

Auch wenn „unabhängig von Sondertatbeständen oder besonderen Anhaltspunkten für eine Rechtsverletzung oder speziellen Gefahrenlagen" nach wohl h.M. eine umfassende Verpflichtung von Unternehmen zur Etablierung eines allgemeinen Überwachungssystems im Rahmen von unternehmerischen Sorgfaltspflichten nicht bestehen soll,[5] ist gleichwohl angemessene Compliance-Überwachung nicht nur eine Option, sondern eine im Eigeninteresse liegende Pflicht der Leitung eines Unternehmens (§ 130 OWiG). Das gilt allgemein und auch für spezielle Rechtspflichten wie die der Einhaltung des Datenschutzes.[6]

Compliance spiegelt sich in den deutschen Begriffen der Rechtstreue bzw. Regelkonformität.[7] Sie bedeutet im engeren Sinn[8] die Einhaltung von Gesetz und Recht, d.h. aller gesetzlichen Bestimmungen sowie interner Richtlinien durch das Unternehmen und seine Mitarbeiter, wobei durch das interne Compliance Management bzw. Compliance-System diese Rechtskonformität zu gewährleisten ist. Dies erfordert strukturierte interne Regeln und Richtlinien, deren Einhaltung den Mitarbeitern vorgegeben und von dem Unternehmen überwacht wird. Für deutsche börsennotierte Gesellschaften enthält der deutsche Corporate Governance Kodex (DCGK)[9] die wesentlichen gesetzlichen Vorschriften zur Überwachung und Leitung und gibt zudem – ohne rechtliche Verbindlichkeit – Empfehlungen und Anregungen für die Unternehmensführung.

I.d.R. wird somit Compliance als Gesamtheit aller betrieblichen Maßnahmen verstanden, welche das regelkonforme Verhalten aller Unternehmensangehöriger sicherstellen und gleichwohl stattfindende Verstöße aufdecken oder frühzeitig verhindern sollen. Über das gesetzeskonforme Verhalten hinaus umfasst der Begriff Compliance im Sinne von „Best Practice" (und nicht nur „Good Practice") auch das (ethisch) korrekte Verhalten des Unternehmens und seiner Mitarbeiter. Dieses Ziel verfolgen Unternehmen durch die Einführung von Verhaltensregeln (Codes of Conducts).[10] Beinhalten diese Meldepflichten, dann liegt es nahe, als ggf. einen der Ansprechpartner den Compliancebeauftragten vorzusehen.

Insoweit ist auf Art. 5 DS-GVO hinzuweisen, der den Verantwortlichen verpflichtet, die Einhaltung der Verarbeitungsgrundsätze des Abs. 1 nachzuweisen (Rechenschaftspflicht), wofür eine Einbeziehung der hierzu unternehmensspezifisch erstellten Grundsätze und die Kontrolle ihrer Einhaltung in einer Compliance-Organisation sachgerecht ist.

2. Sanktionsmindernde Honorierung einer Compliance-Organisation

Drohen einem Unternehmen wegen Rechtsverstößen staatliche finanzielle Sanktionen, so kann dabei eine effektive Compliance-Organisation ggf. honoriert werden. Jede Unternehmenssanktion steht in dem Konflikt, dass sie gegenüber dem Unternehmen erfolgt, die Zuwiderhandlungen aber durch Individuen, d.h. Beschäftigte begangen werden. In diesem Spannungsverhältnis erlangen Compliance-Maßnahmen als Beitrag des Unternehmens zur Prävention von Zuwiderhandlungen seiner Repräsentanten und Mitarbeiter herausgehobene Bedeutung. Effektive, d.h. angemessene Compliance-Maßnahmen haben – je nach Konstellation – tatbestandsausschließende oder bußgeldmindernde Bedeutung.

1 Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft; Art. 1 Gesetz zur Sanktionierung von verbandsbezogenen Straftaten (Verbandssanktionengesetz – VerSanG). BT-Drucksache 19/23568 vom 21.10.2020.

2 BGH, Urteil v. 09.05.2017 – 1 StR 265/16, Entscheidungsgründe Rz. 118.

3 Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und andere Bestimmungen (GWB-Digitalisierungsgesetz) vom 18.01.2021, BGBl. 2021, 2.

4 Trüg/Ruppert, Die Bedeutung von Compliance-Management-Systemen für die Kartell- und sonstige Verbandsgeldbußen – zugleich ein Plädoyer für rationale Unternehmenssanktionen, Zeitschrift für Wettbewerbsrecht, 1/2020, 69.

5 Im Einzelnen vgl. Thüsing, Beschäftigtendatenschutz und Compliance, § 2 Rn. 2 und 16.

6 Jung, Datenschutz-(Compliance)Management-Systeme – Nachweis und Rechenschaftspflichten nach der DS GVO, ZD 2018, 208.

7 Zur Definition nach wikipedia: Compliance ist die betriebswirtschaftliche und rechtswissenschaftliche Umschreibung für die Regeltreue (auch Regelkonformität) von Unternehmen, also die Einhaltung von Gesetzen, Richtlinien und freiwilligen Kodizes.

8 Vgl. z.B. Hein, Compliance – Haftungsrisiken für die Unternehmensleitung, EWerk 2/2015, 25.

9 Https://www.dcgk.de.

10 Vgl. die Beispiele bei Gola, Handbuch Beschäftigtendatenschutz, Rn. 795 ff.

Geltendes und neues Recht erlauben eine Reduzierung der finanziellen Sanktionen eines Unternehmens, wenn das Unternehmen durch ein angemessenes Compliancesystem das Mögliche zur Vermeidung der zur Ahndung anstehenden Rechtsverstöße unternommen hatte. Dies belegt zunächst ergangene Rechtsprechung des BGH[11], nach der bei der Bemessung einer Geldbuße neben den §§ 30 Abs. 3 und 17 Abs. 4 S. 1 OWiG auch von Bedeutung ist, „inwieweit die Nebenbeteiligte ihrer Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein effizientes Compliance-Management installiert hat, das auf die Vermeidung von Rechtsverstößen ausgelegt ist."[12]

Bei Verhängung dieser Sanktionen[13], d.h. als Kriterium für die Bemessung eines Datenschutz-Bußgelds (Art. 83 Abs. 2 DS-GVO) berücksichtigen die Aufsichtsbehörden die Praktizierung eines Compliancesystems, indem die Sanktionsminimierung auch deshalb erfolgen kann, weil sich ein Unternehmen nach erfolgtem Rechtsverstoß einsichtig zeigt und sich kooperativ zur Erstellung eines neuen Datenschutzkonzepts (mit u.a. einem neu berufenen Datenschutzkoordinator, monatlichen Datenschutz-Statusupdates, verstärktem kommunizierten Whistleblower-Schutz) bereitfindet. Im konkreten Fall ausdrücklich positiv wurde auch das Bemühen der Konzernleitung bewertet, die Betroffenen zu entschädigen und das Vertrauen in das Unternehmen als Arbeitgeber wiederherzustellen.[14]

II. Gesetzliche Regelungen

1. Das gescheiterte Verbandssanktionengesetz (VerbSanG)

Eine besondere Regelung bzw. zumindest eine Konkretisierung sollten compliancebedingte Sanktionsminderungen im Zusammenhang mit dem Bundestag in der vergangenen Legislaturperiode vorliegenden, aber nicht behandelten Verbandssanktionengesetz[15] erhalten.[16] Dieses Gesetz sollte die seit geraumer Zeit geführte Diskussion um ein Unternehmensstrafrecht[17] zu einem positiven Ergebnis führen[18] und zugleich eine gesetzliche Grundlage schaffen, um explizit Compliance-Maßnahmen zu stärken und Anreize für die Aufklärung von Straftaten durch interne Untersuchungen zu schaffen,[19] indem sowohl vor- als auch nachgeschaltete Compliance-Bemühungen beispielsweise bei der Bußgeldbemessung Beachtung finden sollten.[20]

Auch wenn es das Verbandssanktionengesetz in der vergangenen Legislaturperiode infolge des Prinzips der (sachlichen) Diskontinuität[21], nach dem alle Gesetzentwürfe, die bis zum Ende einer Legislaturperiode nicht abgearbeitet sind, verfallen, nicht geschafft hat,[22] so ist das bei einer anderen gesetzlich eingeführten sanktionsmindernden Complianceregelungen anders.

2. Sanktionsmilderung bei Kartellverstößen

a) Kurswechsel im Kartellrecht

In Deutschland fehlte es bis zum Inkrafttreten des GWB-Digitalisierungsgesetzes an einer gesetzlich geregelten Compliance-Defence. Mit der 10. GWB-Novelle[23] wurde das deutsche Kartellrecht bzw. Wettbewerbsrecht grundlegend verändert. Neben einer „Digitalisierung des Kartellrechts" im Bereich der Missbrauchsaufsicht und neuen Regeln für große Digitalunternehmen bringt die Novelle auch grundlegende Änderungen und Ausweitungen des Eingriffs-, Ermittlungs- und Verfahrensrechts, des Kartellschadensersatzrechts und Bußgeldrechts.[24] Hierzu gehören die Berücksichtigung effektiver Compliance-Programme und des Nachtatverhaltens von Unternehmen bei der Zumessung von Geldbußen oder die Absenkung der Voraussetzungen für den Erlass einstweiliger Maßnahmen.

Ausgangspunkt für die Berechnung des konkreten Bußgeldes (3 ff GWB) gegen Unternehmen und Unternehmensvereinigungen sind die Schwere und Dauer der Tat. Hinzu kommen weitere Kriterien. Dazu zählt vor allem der tatbefangene Umsatz, aber etwa auch, ob das Unternehmen ein Wiederholungstäter ist, Compliance-Maßnahmen ergriffen hat und bestrebt ist, den entstandenen Schaden wiedergutzumachen. Im Rahmen einer Bußgeldsanktion können sich somit Unternehmen mit einem wirksamen und angemessenen Compliance-Management-System auf eine nunmehr gesetzliche Regelung berufen, um bei der Bußgeldbemessung durch das Bundeskartellamt eine Reduzierung zu erreichen.[25] Die kartellrechtliche „Compliance Defence" hat damit Eingang in das GWB gefunden:[26]

11 Kaiser, https://www.cmshs-bloggt.de/gesellschaftsrecht/bgh-bussgeldmindernde-wirkung-eines-compliance-management-systems; Görtz: https://www.awb-international.de/august-2017/bgh-spricht-compliance-management-systemen-eine-bussgeldmindernde-wirkung-zu.

12 Vgl. BGH, Urt. v. 09.05.2017 – 1 StR 265/16, Entscheidungsgründe Rz. 118; 5.

13 Zur aktuell ungeklärten Rechtslage der Sanktionierung von Unternehmen nach der DS-GVO vgl. Kubiciel, Ungeklaerte Rechtsfragen der Sanktionierung von Unternehmen nach der DS-GVO, PinG, 2021, 81; Wybitul/Venn, Verteidigung von Unternehmen gegen Geldbußen nach Art. 83 DS-GVO, ZD 2021, 343; Nietsch/Osmonovic, Zurechnung von DS-GVO-Verstößen im Unternehmensbereich, BB 2021, 858.

14 HambLfDI: 35,3 Millionen Euro Bußgeld wegen Datenschutzverstößen https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren; vgl. insgesamt Wenzel/Wybitul, Vermeidung hoher DS-GVO-Bußgelder und Kooperation mit Datenschutzbehörden Strategische Möglichkeiten zur Vermeidung von Sanktionen, ZD 2019, 290.

15 BT-Drs.19/23568 v. 21.10.2020.

16 Vgl. Gola, Das Verbandssanktionengesetz-E und betriebliche Datenschutzbeauftragte, DuD 2021, 472; Stück, Entwurf eines Verbandssanktionengesetzes – Datenschutz- und arbeitsrechtliche Bedeutung für unternehmensinterne Untersuchungen, ZD 2021, 307.

17 Zöller, Zur Frage der Einführung eines Unternehmensstrafrechts https://www.familienunternehmen.de/media/public/pdf/publikationen-studien/studien.

18 Roxi, Compliance-Maßnahmen und Unternehmenssanktionierung de lege lata, ZIS 2018, 342.

19 Schulz, Wirksames Compliancemanagement; Anreize und Orientierungshilfe zur Vermeidung von Verbandssanktionen, CCZ 2020, 40.

20 Vgl. Gola, Das Verbandssanktionengesetz-E und betriebliche Datenschutzbeauftragte, DuD 2021, 472 (474).

21 Vgl. § 125 S. 1 Geschäftsordnung des Deutschen Bundestages (GOBT): „Am Ende der Wahlperiode des Bundestages gelten alle Vorlagen als erledigt.".

22 Der Koalitionsvertrag zur Bildung der neuen Bundesregierung erwähnt die Thematik nicht.

23 BGBl. I, 2021 Teil I; 2021 Nr. 1 v. 18.01.2021.

24 Bien/Käseberg/Klumpe/Körber/Ost Die 10. GWB-Novelle Das neue Kartellrecht, 2021, München.

25 DISCO-Stellungname: Zur Auslegung der Compliance Defense im GWB-Digitalisierungsgesetz (§ 81d Abs. 1 S. 2, Ziff. 4 und 5 GWB) https://www.dico-ev.de/wp-content/uploads/2021/06.

26 Marck, Kartellrechtliche Compliance – Neue Chancen im GWB https://www.marck.eu/aktuelles/kartellrechtliche-compliance-neue-chancen-im-gwb.

Soll gegen ein Unternehmen oder eine Unternehmensvereinigungen wegen u.a. nach § 1 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) unzulässiger wettbewerbsbeschränkender Vereinbarungen, Beschlüssen oder abgestimmter Verhaltensweisen nach § 81d Abs. 1 Satz 2 GWB eine Geldbuße verhängt werden, ist dabei Compliance-Maßnahmen, die zur Vermeidung und Aufdeckung von Kartellverstößen geführt haben, unabhängig davon, ob sie vor oder nach der Zuwiderhandlung getroffen wurden, Rechnung zu tragen. Zu berücksichtigen ist das Bemühen des Unternehmens, die Zuwiderhandlung aufzudecken und den Schaden wiedergutzumachen sowie nach der Zuwiderhandlung in Vorkehrungen zur Vermeidung und Aufdeckung von Zuwiderhandlungen zu investieren.

b) Angemessenheit und Wirksamkeit

aa) Allgemeines

Voraussetzung ist, dass die Vorkehrungen angemessen und wirksam sind. Das Gesetz fordert das für Maßnahmen vor der Tat (§ 81d Abs. 1 Nr. 4 GWB).[27] Für die Nachtat-Compliance fehlt es zwar ein einer entsprechenden Qualifizierung (vgl. § 81d Abs. 1 S. 2 Nr. 5). Allerdings spricht eine Auslegung nach Sinn und Zweck dafür, dass auch hier eine Verbesserung des Compliance-Programms auf ein „angemessenes und wirksames" Niveau erforderlich ist. Wenngleich diese Kriterien nicht ausschließen, dass einzelne Zumessungsfaktoren von Kartellbehörde und Gericht unterschiedlich gewertet werden und sich in der Folge auch die Ergebnisse unterscheiden, ist hiermit der Maßstab gesetzt.[28]

bb) Wirksamkeit

Bei dem Erfordernis der Wirksamkeit kann logischerweise keine absolute Wirksamkeit gemeint sein, weil sonst jeder trotzdem eingetretene Verstoß die Unwirksamkeit belegen würde. Entscheidend kann daher nur sein, dass die konkret geschaffenen Vorkehrungen dazu geeignet waren, den jeweiligen Vorfall zu vermeiden, auch wenn es im Einzelfall zu einem Verstoß gekommen ist oder kommen könnte. Wirksamkeit wird somit unterstellt, wenn „der Inhaber eines Unternehmens alle objektiv erforderlichen Vorkehrungen ergriffen hat, um Zuwiderhandlungen gegen wettbewerbsrechtliche Bestimmungen durch Mitarbeiter zu verhindern.[29] Damit ist Sanktionsreduzierung als „Belohnung" dafür eingeführt, dass ein Unternehmen systematisch vorgibt und kontrolliert, dass nach den „Regeln gespielt wird."

Die Wirksamkeit der Compliancevorgaben hängt von den erkennbaren Willen zu ihrer Durchsetzung ab. Ist ein Verstoß eingetreten, so ist ein Indiz für die Wirksamkeit auch die aktive Kooperation des Unternehmens zur Aufklärung des eingetretenen Verstoßes.

cc) Angemessenheit

Mit der Forderung der Angemessenheit wird dem Umstand Rechnung getragen, „dass die Art und der Umfang von Compliance-Maßnahmen typischerweise von der Unternehmensgröße abhängig sind. Welche Maßnahmen und Vorkehrungen erforderlich sind, hängt „vom jeweiligen Einzelfall ab und dabei insbesondere von Art, Größe und Organisation eines Unternehmens, Gefährlichkeit des Unternehmensgegenstandes, Anzahl der Mitarbeiter, den zu beachtenden Vorschriften sowie dem Risiko ihrer Verletzung. Bei kleinen und mittleren Unternehmen mit geringem Risiko von Rechtsverletzungen können auch wenige einfache Maßnahmen ausreichend sein; der „Zukauf" eines Compliance-Programms oder von Zertifizierungen ist regelmäßig nicht erforderlich.[30]

dd) Ausmaß der Anrechnung

Hat das bestehende Compliancesystem zur Aufdeckung eines Datenschutzvertoßes geführt, wird die Angemessen- und Wirksamkeit der Kontrolle unterstellt. Jedoch ist dem Unternehmen ggf. auch nur das grundsätzliche Bemühen positiv anzurechnen. Ausgeschlossen ist die Bußgeldreduzierung allerdings dann, wenn die Geschäftsleitung selbst an der Zuwiderhandlung beteiligt war und damit zu erkennen gibt, nicht hinter den Compliance-Anstrengungen zu stehen.

ee) Verhalten nach der Tat

§ 81d Abs. 1 S. 2 Nr. 5 GWB ermöglicht bei der Bußgeldbemessung neben der Berücksichtigung von Compliance-Maßnahmen, die ergriffen wurden, um durch die Tat aufgezeigte Defizite der Compliance zu beheben, auch die Berücksichtigung des sog. Nachtatverhaltens, das in der Gesamtschau zu würdigen ist. Die Vorschrift ermöglicht nicht nur eine Berücksichtigung von Compliance-Maßnahmen, die nach der Tat ergriffen wurden, insbesondere um durch die Tat aufgezeigte Defizite der Compliance zu beheben. Zugleich erlaubt die Norm die Berücksichtigung von Schadenswiedergutmachung und von Maßnahmen des Unternehmens zur Aufklärung der Zuwiderhandlung. Die aktive Kooperation eines Unternehmens kann ein Indiz für die Ernsthaftigkeit solcher Bemühungen sein.[31] Schließen Unternehmen etwa mit den durch das Kartell geschädigten Abnehmern einen Vergleich und zahlen Schadenersatz, könnte das Bundeskartellamt im Gegenzug einen Teil des behördlichen Bußgeldes erlassen. Das setzt aber verfahrensmäßig voraus, dass Vergleichsgespräche schon während des Bußgeldverfahrens geführt werden.

Unternehmen können und sollten somit mit Blick auf die Bußgeldzumessung ihre vor und/oder nach dem Vorfall getroffenen kartellrechtlichen Compliancebemühungen einerseits und mit den Geschädigten getroffene Entschädigungsregelungen andererseits umfassend und um billigende Unterstützung nachfragend vortragen, damit diese in der Bußgeldbemessung von der Behörde pflichtgemäß berücksichtigt werden.

27 Stammwitz, 10. GWB-Novelle: Compliance-Maßnahmen können Kartellbußgelder reduzieren; https://www.pinsentmasons.com/de-de/outlaw/analyse/10gwb-novelle-compliance-massnahmen-kartellbussgelder.

28 Gesetzesbegründung, BT-Drs. 19/23492, S. 127.

29 Gesetzesbegründung, BT-Drs. 19/23492, S. 127.

30 Vgl. hierzu Gesetzesbegründung, BT-Drs. 19/23492, S. 128.

31 Vgl. hierzu Gesetzesbegründung, BT-Drs. 19/23492, S. 128.

III. Die Compliance-Beauftragten

1. Bestellung von Compliance-Beauftragten

Die Einhaltung einer Compliance-Organisation bedarf jemanden, der sich um sie kümmert und die routinemäßigen und insbesondere auch die „fallbezogen" notwendigen Abläufe koordiniert. In größeren Unternehmen werden hierzu Compliance-Beauftragte[32] bzw. Compliance-Officer eingesetzt; wobei ihre Bestellung freiwillig oder auch der Vollzug einer allgemeinen Organisationspflicht sein kann. So verpflichtet § 91 Abs. 2 Aktiengesetz (AktG) den Vorstand einer Aktiengesellschaft, geeignete Maßnahmen und insbesondere ein Überwachungssystem zu etablieren, um Entwicklungen, die den Fortbestand der Gesellschaft gefährden könnten, früh zu erkennen, wobei jedoch die konkrete Gestaltung des Überwachungssystems offenbleibt. Eine entsprechende branchenspezifische Spezialregelung gilt für Kredit- und Wertpapierinstitute. § 25 a Kreditwesengesetz (KWG) begründet explizit die Pflicht, für ein angemessenes Risikomanagement zu sorgen, welches die Errichtung eines internen Kontrollsystems enthalten muss. Nach § 25h Abs. 1 KWG besteht die Pflicht, ein angemessenes Risikomanagement zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen, die zu einer Gefährdung des Vermögens des Instituts führen, zu schaffen und hierzu Datenverarbeitungssysteme zu betreiben.

Nach § 80 und § 83 Wertpapierhandelsgesetz (WpHG) sind ebenfalls Wertpapierhandelsunternehmen zur Errichtung einer dauerhaften und wirksamen Compliance-Organisation verpflichtet. Dazu zählt dann die konkrete Pflicht, zur Bestellung von – hier jedoch nicht weisungsfreien – Compliance-Beauftragten. Auch für Versicherungsunternehmen gilt nach § 29 Versicherungsaufsichtsgesetz (VAG) eine entsprechende Verpflichtung.

Je nach den Unternehmensspezifika kann daneben eine freiwillige Bestellung eines Compliance-Beauftragten sinnvoll sein. Aufgabe des Compliance-Beauftragten ist es somit, das gesetzmäßige Verhalten, d.h. die Compliance des Unternehmens, mit zu gewährleisten, wobei seine Kompetenzen unterschiedlich sein können.

2. Compliance- und Datenschutzbeauftragte

Eine Personalunion zwischen Datenschutz- und Compliance-Beauftragten scheidet aus, wenn der Compliancebeauftragte auch – wie das bei den genannten gesetzlich vorgegebenen Compliancebeauftragten zutrifft – Regelungskompentenzen hat,[33] deren Ausübung vom Datenschutzbeauftragten kontrolliert werden muss. Personen dürfen nicht zum Datenschutzbeauftragten berufen werden, wenn sie aufgrund noch anderweitiger Funktionen in Interessenkonflikte geraten würden, die über das unvermeidliche Maß hinausgehen.

Sofern in der Aufgabenbeschreibung keine Beschränkungen oder Vorgaben vorgesehen sind, obliegt dem Compliance-Beauftragten die Überwachung der Einhaltung sämtlicher von dem Unternehmen zu beachtenden Rechtsvorschriften. Sofern noch erforderlich, hat er das Compliance Management System zu implementieren und zu überwachen, präventive Maßnahmen umzusetzen und Mitarbeiter zu schulen sowie Compliance Vorfälle zu untersuchen und zu melden. Er hat eine Berichts- und ggf. Beratungsfunktion aber keine Weisungsbefugnis oder ein Vetorecht.[34]

Somit hat der Compliance-Beauftragte generell und der Datenschutzbeauftragte speziell auf den Datenschutz bezogen die Aufgabe, Gesetzesverletzungen vorzubeugen, d.h. zu dem pauschalen Aufgabenbereich das Compliance-Beauftragten gehört auch die Überwachung des Datenschutzes,[35] und die Beratungs- und Kontrollaufgaben des Datenschutzbeauftragten dienen gleichzeitig der Compliance.[36] Beide sind Bestandteil des unternehmerischen Risikomanagements.[37] Gleichwohl ist fraglich, ob die Funktion des Datenschutzbeauftragten und des Compliance-Beauftragten ohne inhärente Interessenkonflikte in Personalunion ausgeübt werden können.[38] Die Meinungen hierzu differieren.[39]

Trotz der gleichen Zielrichtung ihrer Aufgaben besteht ein Spannungsfeld zwischen Datenschutzbeauftragten und Compliance-Beauftragten, das sich daraus ergibt, dass der Compliance-Beauftragte in erster Linie Haftungsfälle des Unternehmens und seines Vorstands vermeiden und somit Unternehmensinteressen verfolgen soll und dass deshalb der Compliance dienende Kontrollmaßnahmen in ihrer Zulässigkeit durch den Compliance-Beauftragten ggf. anders beurteilt werden[40] als durch den Datenschutzbeauftragten und diese zudem eben auch selbst wiederum der datenschutzrechtlichen Kontrolle bedürfen.[41]

Eine andere Frage ist, ob wegen der sich teilweise überlappenden Aufgabenstellung von Datenschutzbeauftragten und Compliance-Beauftragten eine Eingliederung des Datenschutzbeauftragten in die Compliance-Abteilung allein schon zur Erzielung von Synergieeffekten sinnvoll ist.[42] Dabei kann jedoch – entgegen anderer Ansicht[43] – nur eine

32 Klopp, Der Compliance-Beauftragte, S. 317 ff.

33 Kamp/Körffer, Auswirkungen des § 32 BDSG auf die Aufgabenerfüllung und die strafrechtliche Verantwortung des Compliance Officers, RDV 2010, 72 (73), sofern in der vertraglichen Aufgabenbeschreibung des Compliancebeauftragten keine Beschränkungen oder Vorgaben vorgesehen sind, wird ihm die Überwachung der Einhaltung sämtlicher Rechtsvorschriften obliegen.

34 Forgo/Helfrich/Schneider/Schröder, Betrieblicher Datenschutz, 3. Aufl., S. 648 ff.

35 Plath/v. d. Busche, 1. Aufl., BDSG a.F. § 4f Rn. 34c.

36 Baumgarten/Hansch, Der betriebliche Datenschutzbeauftragte, ZD 2019, 99 (100).

37 Jaksch/von Daacke, Datenschutzbeauftragter und Datenschutzorganisation unter des DS-GVO, DuD 2018, 758; Renz/Frankenberger, Compliance und Datenschutz. Ein Vergleich der Funktionen unter Berücksichtigung eines risikobasierten Ansatzes, ZD 2015, 158.

38 Zustimmend Ehmann/Selmayr/Heberlein, DS-GVO, Art. 38 Rn. 23, sofern dem Compliancebeauftragten nicht selbst die Verarbeitung personenbezogener und ggf. sensibler Personaldaten obliegt. Vgl. auch Forgo/Helfrich/Schneider/Haag, Betrieblicher Datenschutz, Teil II.1. Rn. 67.

39 Ablehnend Kühling/Buchner/Bergt, DS-GVO Art. 38 Rn. 42 mwN; Simitis/Hornung/Spiecker/Drewes, DS-GVO Art. 38 Rn. 57; Baumgartner/Hansch, Der betriebliche Datenschutzbeauftragte, ZD 2019, 99 (100); Forgo/Helfrich/Schneider/Schröder, Betrieblicher Datenschutz, S. 648 ff; Gierschmann/Saeugling/Schmitz/Thoma, BDSG 1. Aufl. § 4f Rn. 32; ebenso im Ergebnis v. Plath/v. d. Busche, 1. Aufl., BDSG § 4f Rn. 34h.

40 Forgo/Helfrich/Schreiber/Schröder, Betrieblicher Datenschutz, Teil V, Kap. 3 Rn. 72, 84.

41 Vgl. hierzu Gola, Das Geschäftsgeheimnisgesetz und die Datenschutz-Grundverordnung, DuD 2019, 569.

42 Forgo/Helfrich/Schreiber/Schröder, Betrieblicher Datenschutz, Teil V, Kap. 3 Rn. 72.

43 Vgl. hierzu bei Plath/v. d. Busche, 2. Aufl. BDSG § 4f Rn. 34.

Pflicht zur beratenden Kooperation und allein eine disziplinarische Aufsicht bestehen. Das gilt umso mehr, wenn das Unternehmen eine der Weisung des Compliancebeauftragten unterliegende Datenschutzabteilung hat.[44]

IV. Fazit

Zur Compliance eines Unternehmens gehört auch seine Datenschutzkonformität. Der Compliance dienende Kontrollmaßnahmen müssen ebenso wie solche der IT-Sicherheit datenschutzkonform verlaufen. Die Einhaltung der Datenschutzgesetze liegt sowohl im Interesse des Compliance-Officer als auch des Datenschutzbeauftragten – hier lohnt sich also jedwede Kooperation. Gleichwohl sollte wegen der teilweise unterschiedlichen Schutzobjekte – der DSB ist auch Anwalt der Betroffenen[45] – und der beim Compliance-Beauftragten nicht bestehenden Unabhängigkeit zwar eine Personalunion nicht die Regel sein. Geboten ist aber regelungsbasierte Kooperation.

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

44 Zu diesbezüglichen Organisationsfragen ausführlich Simitis/Hornung/Spiecker/Drewes, Datenschutzrecht, DS-GVO Art. 39 Rn. 58 ff.

45 Vgl. Gola, Handbuch zum Beschäftigtendatenschutz, Rn. 311 ff.

Carlo Piltz/Johannes Zwerschke

Missbräuchliche Ausübung von DS-GVO-Betroffenenrechten – zulässiger Verteidigungseinwand für Verantwortliche?

Im Rahmen der Geltendmachung von Auskunftsansprüchen nach Art. 15 DS-GVO wird immer wieder die Frage diskutiert, ob der Einwand des Rechtsmissbrauchs bzw. der missbräuchlichen Ausübung des Betroffenenrechts durch den Verantwortlichen erhoben werden kann. Nachfolgend wird untersucht, inwieweit sich Verantwortliche auf eine missbräuchliche Ausübung insbesondere von Art. 15 DS-GVO berufen können.

I. Kennt die DS-GVO den Einwand des Missbrauchs?

In Bezug auf die Betroffenenrechte findet sich der Einwand des Missbrauchs in der DS-GVO nicht wortwörtlich. Gleichwohl hat der europäische Normgeber in den Art. 12 ff. DS-GVO Regelungen zu verschiedenen Missbrauchskonstellationen vorgesehen.

Hier ist zunächst Art. 12 Abs. 5 S. 2 lit. b) DS-GVO zu erwähnen. Nach der Norm kann sich der Verantwortliche bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person weigern, aufgrund des Antrags tätig zu werden. Die Regelung wird in der Literatur u.a. auch als Missbrauchsabwehr bezeichnet.[1]

Eine weitere Regelung zum Missbrauch in Bezug auf Betroffenenrechte findet sich in Art. 15 Abs. 4 DS-GVO. Nach der Norm darf das Recht auf Erhalt einer Kopie gemäß Art. 15 Abs. 3 DS-GVO die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Eine Beauskunftung darf demnach also nicht dazu dienen, um beim Verantwortlichen Informationen über andere Personen oder zu Geschäftsgeheimnissen zu erlangen.

II. Ansichten deutscher Gerichte und Behörden zum Missbrauch des Auskunftsrechts nach Art. 15 DS-GVO

Über die vorstehend genannten Regelungen hinaus, finden sich in Bezug auf die Betroffenenrechte in den Art. 12 ff. DS-GVO ersichtlich keine den Missbrauch betreffenden Tatbestände. Umso bemerkenswerter sind die Entwicklungen zu dieser Frage in der Rechtsprechung und bei den Aufsichtsbehörden.

1. Rechtsprechung

a) LG Detmold

Nach einer Entscheidung des LG Detmold kann sich im Rahmen des Auskunftsanspruchs nach Art. 15 DS-GVO der Einwand des Rechtsmissbrauchs aus § 242 BGB ergeben.[2] Gemäß § 242 BGB ist der Schuldner verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern. Es handele sich dabei um

1 Bäcker, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 12 vor Rn. 35.

2 LG Detmold, Urt. v. 26.10.2021 – 02 O 108/21, BeckRS 2021, 34230.

einen Grundsatz, der als nationale Ausformung auch im Rahmen des Art. 15 DS-GVO Geltung beansprucht.[3] Das Gericht beruft sich dabei auf die in Bezug auf § 242 BGB herausgebildete Fallgruppe, nach der die Ausübung eines Rechts u.a. nicht erlaubt ist, wenn der Anspruchsinhaber eine formale Rechtsstellung ausnutzt oder etwas geltend macht, an dem er kein schützenswertes Eigeninteresse hat.[4]

Das LG Detmold begründet den Ausschluss des Auskunftsanspruchs damit, dass die Geltendmachung des Auskunftsanspruchs hier ausschließlich der Verfolgung von Leistungsansprüchen diene, wobei es sich um einen der DS-GVO vollkommen fremden Zweck handele.[5] Zur Begründung verweist das Gericht auf ErwG 63 S. 1 DS-GVO, nach dem Art. 15 DS-GVO vielmehr dazu diene, dass sich der Betroffene der Verarbeitung seiner personenbezogenen Daten bewusst werden und deren Rechtmäßigkeit überprüfen könne.[6] Weiterhin diene die Auskunft dazu, der betroffenen Person die Wahrnehmung der weiteren Betroffenenrechte nach den Art. 16 ff. DS-GVO zu ermöglichen.[7] Schließlich weist das LG darauf hin, dass sich das Auskunftsbegehren in dem vorliegenden Fall nach dem klar geäußerten Willen des Klägers und Auskunftstellers allein darin erschöpfen soll, etwaige geldwerte Ansprüche gegen die Beklagte zu prüfen.[8] Ein Begehren, das sich derart weit vom Regelungsinhalt einer Rechtsgrundlage entfernt habe, sei nach Ansicht des Gerichts nicht schützenswert.[9]

Der Verweis auf ErwG 63 DS-GVO ist nach Ansicht der Verfasser unter dem Aspekt der Missbrauchsabwehr richtig und begrüßenswert. Denn im hiesigen Verfahren hat der Kläger und Auskunftsteller hinreichend zum Ausdruck gebracht, dass es ihm in keinster Weise um seine Rechte als datenschutzrechtlich Betroffener geht. Gleichwohl ist das Argument des LG Detmold, dass es sich „nur" um geldwerte Ansprüche und damit nicht um datenschutzbezogene Betroffenenrechte handele, mit Vorsicht zu betrachten. Denn auch die DS-GVO kennt geldwerte Ansprüche. So hat nach Art. 82 Abs. 1 DS-GVO jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Möchte der Betroffene im Rahmen eines Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO gegenüber dem Verantwortlichen die Rechtmäßigkeit der Datenverarbeitung prüfen, um diesen anschließend nach Art. 82 Abs. 1 DS-GVO in Anspruch zu nehmen, wäre das Argument des LG Detmold nach hier vertretener Ansicht mithin eher abzulehnen.

b) LAG Niedersachsen

Dagegen lehnte das LAG Niedersachsen in einem zu beurteilenden Fall ein Verweigerungsrecht nach Art. 12 Abs. 5 S. 2 lit. b) DS-GVO hinsichtlich der von der Beklagten zu erteilenden Auskunft ab.[10] Demnach können Anträge rechtsmissbräuchlich sein, „die ua vornehmlich auf die Schikanierung des Verantwortlichen abzielen".[11] Das Gericht deutet in diesem Zusammenhang an, dass ein Antrag nach Art. 15 DS-GVO rechtsmissbräuchlich sein kann, wenn er darauf gerichtet ist, den Verantwortlichen auszuforschen.[12] Denkbar wäre es demnach, die Ausforschung als eine Fallgruppe des Rechtsmissbrauchs im Zusammenhang mit den Art. 15 ff. DS-GVO einzuordnen. Gleichwohl wird man nach Ansicht der Verfasser hohe Anforderungen an die Erbringung des Nachweises einer Ausforschung stellen müssen. Andernfalls scheint es wahrscheinlich, dass sich zur Auskunfterteilung verpflichtete Verantwortliche regelmäßig auf den Rechtsmissbrauch in Form der Ausforschung berufen. Hierfür könnten z.B. die im deutschen Zivilprozess für den Ausforschungsbeweis aufgestellten Grundsätze herangezogen werden.[13]

Nicht nachvollziehbar ist, weshalb das Gericht dabei problematisierte, ob Art. 12 Abs. 5 DS-GVO überhaupt hinsichtlich Art. 15 DS-GVO anwendbar sei.[14] Denn sowohl Art. 12 DS-GVO als auch Art. 15 DS-GVO befinden sich im Kapitel III („Rechte der betroffenen Person") und die Vorgaben des Art. 12 DS-GVO sind bei der Beantwortung von Betroffenenanfragen zu beachten. Unabhängig davon ist es aus Sicht der Verfasser zu begrüßen, dass sich das LAG Niedersachsen für die Beantwortung der Frage des Vorliegens eines Rechtsmissbrauchs an Art. 12 Abs. 5 S. 2 DS-GVO und nicht an § 242 BGB orientiert hat. Ob § 242 BGB nämlich dogmatisch tatsächlich als gesetzliche Grundlage für einen Rechtsmissbrauch im Rahmen von den Art. 15 ff. DS-GVO in Betracht kommt, ist derzeit zumindest unklar. Da Art. 15 DS-GVO unmittelbar anwendbares Unionsrecht darstellt, erscheint es dogmatisch schlüssiger und damit auch sicherer, diese Frage anhand einer Norm aus der DS-GVO oder dem übrigen Unionsrecht zu beantworten.

c) LG Krefeld

Auch das LG Krefeld hat in einer Entscheidung einen Auskunftsanspruch nach Art. 15 DS-GVO wegen Rechtsmissbräuchlichkeit abgelehnt.[15] Ebenso wie das LG Detmold[16] stützte sich das LG Krefeld auf ErwG 63 DS-GVO und verwies darauf, dass der Kläger und Auskunftsteller im Rahmen seines Begehrens gänzlich DS-GVO-fremde Erwägungen verfolge.[17] Jedoch verfolgte der Kläger auch hier nach Überprüfung der Rechtmäßigkeit einen etwaig bestehenden Bereicherungsanspruch gegen die Beklagte, was wiederum die Frage aufwirft, ob die Verfolgung geldwerter Ansprüche im Rahmen von Art. 15 DS-GVO per se rechtsmissbräuchlich ist.[18]

3 LG Detmold, Urt. v. 26.10.2021 – 02 O 108/21, BeckRS 2021, 34230 Rn. 44.

4 Siehe ebenda.

5 LG Detmold, Urt. v. 26.10.2021 – 02 O 108/21, BeckRS 2021, 34230 Rn. 46.

6 Siehe ebenda.

7 Siehe ebenda.

8 LG Detmold, Urt. v. 26.10.2021 – 02 O 108/21, BeckRS 2021, 34230 Rn. 48.

9 Siehe ebenda.

10 LAG Niedersachsen, Urt. v. 22.10.2021 – 16 Sa 761/20, BeckRS 2021, 32008 Rn. 177.

11 Siehe ebenda.

12 Siehe ebenda.

13 Instruktiv: z.B. Stöhr, Der Ausforschungsbeweis im Zivilprozess, JA 2020, 688.

14 Siehe ebenda.

15 LG Krefeld, Urt. v. 06.10.2021 – 2 O 448/20, BeckRS 2021, 34436.

16 Siehe II.a.i.

17 LG Krefeld, Urt. v. 06.10.2021 – 2 O 448/20, BeckRS 2021, 34436 Rn. 22.

18 Siehe II.a.i.

d) LG Wuppertal

Ebenso wie das LG Detmold[19] lehnte auch das LG Wuppertal in einem Rechtstreit den Auskunftsanspruch des Klägers wegen Rechtsmissbrauchs auf Grundlage des § 242 BGB ab.[20] Das LG Wuppertal begründete sein Vorgehen ähnlich wie das LG Detmold damit, dass es sich bei § 242 BGB um einen das gesamte Rechtsleben durchziehenden Grundsatz handele, der als nationale Ausformung auch im Rahmen des Art. 15 DS-GVO Geltung beanspruche;[21] Art. 12 Abs. 5 DS-GVO zieht das Gericht dagegen nicht heran. Das LG Wuppertal weist in seiner Entscheidung darauf hin, dass ein Rechtsmissbrauch nach § 242 BGB es voraussetzt, dass der Anspruchsinhaber eine formale Rechtsstellung ausnutzt oder etwas geltend macht, an dem er kein schützenswertes Eigeninteresse hat.[22] Für Verantwortliche, die sich auf § 242 BGB berufen wollen, wird es daher empfehlenswert sein, vor Geltendmachung des Einwands eines Rechtsmissbrauchs (zumindest) das Vorliegen dieser beiden Voraussetzungen zu überprüfen.

Darüber hinaus stützt sich auch das LG Wuppertal unter Berufung auf ErwG 63 DS-GVO darauf, dass der Kläger im Rahmen seines Auskunftsbegehrens ausschließlich Leistungsansprüche und damit vollkommen DS-GVO-fremde Zwecke verfolge.[23] In den vorstehenden Entscheidungen war es stets so, dass der Auskunftsteller im Rahmen des Rechtsstreits ausdrücklich Zwecke verfolgte, die mit Blick auf ErwG 63 S. 1 DS-GVO nicht einer Überprüfung der Datenverarbeitung durch den Verantwortlichen und auch nicht deren Rechtmäßigkeitskontrolle dienten. Allerdings wird auch ErwG 63 S. 1 DS-GVO nach Ansicht der Verfasser keine hinreichende Grundlage für die Feststellung eines Rechtsmissbrauchs sein, wenn der Auskunftsteller den Zweck der Auskunft nicht offenlegt. Zumindest in diesem Fall sollte der Einwand des Rechtsmissbrauchs durch den Verantwortlichen mit Bedacht eingesetzt werden.

e) ArbG Neumünster

Das ArbG Neumünster hielt bei der Frage des Rechtsmissbrauchs in Zusammenhang mit einem Auskunftsanspruch nach Art. 15 DS-GVO ebenfalls § 242 BGB für anwendbar.[24] Bemerkenswert ist, dass das Gericht zur Begründung darauf verwies, dass es sich bei § 242 BGB um einen allgemeinen rechtsstaatlichen Rechtsgrundsatz handelt, „der auch auf EU-Ebene gilt (vgl. Art. 8 Abs. 2 S. 1 EU-Grundrechts-Charta, Art. 5 Abs. 1 Buchst a DS-GVO)".[25] Diese Verknüpfung des Grundsatzes von Treu und Glauben nach § 242 BGB (insbesondere) mit dem Verarbeitungsgrundsatz Treu und Glauben gemäß Art. 5 Abs. 1 lit. a) DS-GVO ist nach Ansicht der Verfasser positiv hervorzuheben und ein alternativer Begründungsansatz, da er eine dogmatische Verbindung zwischen der rein nationalen Norm des § 242 BGB und Art. 15 DS-GVO herstellt. Der Grundsatz der Verarbeitung nach Treu und Glauben aus Art. 5 Abs. 1 lit. a) DS-GVO adressiert nach Ansicht der Literatur (ausschließlich) den Verantwortlichen und den Auftragsverarbeiter,[26] nicht aber den Betroffenen. Da sich der Einwand des Rechtsmissbrauchs auf eine Handlung des Betroffenen (= rechtsmissbräuchliche Geltendmachung von Betroffenenrechten) bezieht, wird der den Verantwortlichen adressierende Art. 5 Abs. 1 lit. a) DS-GVO die (dogmatische) Frage, ob § 242 BGB als Rechtsmissbrauchseinwand im Rahmen der Art. 15 ff. BGB herangezogen werden kann, nach Ansicht der Verfasser daher nicht vollends beantworten können. Gleichwohl ließe sich entgegnen, dass sich der Verantwortliche als Auskunft erteilende Stelle auf den Einwand des Rechtsmissbrauchs berufen will, nicht aber der Betroffene.

Neben diesem Aspekt ist besonders bemerkenswert, dass ein Rechtsmissbrauch nach Ansicht des ArbG Neumünster vorgelegen hätte, „wenn der Kläger seinen Schadensersatzanspruch allein und deshalb mit seinem Begehr, eine Abfindung für den Verlust des Arbeitsplatzes zu erhalten, verknüpft hätte".[27] Diese Formulierung lässt den Schluss zu, dass der Zweck der Geltendmachung als solcher zumindest nach Ansicht des ArbG Neumünster nicht den Einwand des Rechtsmissbrauchs ausgelöst hätte. Daraus folgt die bereits zuvor aufgeworfene Frage, ob die Verfolgung geldwerter Ansprüche im Rahmen der Art. 15 ff. DS-GVO tatsächlich als rechtsmissbräuchlich zu betrachten ist.

f) BGH

Besonders hervorzuheben ist, dass sich auch der BGH am Rande einer Entscheidung[28] zu dieser Thematik geäußert hat. So verweist der BGH darauf, dass er auf der Grundlage der getroffenen Feststellungen nicht beurteilen könne, ob vorliegend unter dem Gesichtspunkt anderer vom Kläger verfolgter Zwecke die datenschutzrechtlichen Ansprüche desselben aus Art. 15 DS-GVO – etwa nach den Vorschriften in Art. 12 Abs. 5 S. 2, 15 Abs. 4 DS-GVO oder Art. 23 Abs. 1 DS-GVO i.V.m. § 29 Abs. 1 S. 2 BDSG – beschränkt werden oder sogar entfallen könnten.[29] Bemerkenswert ist also, dass der BGH für die Beschränkung des Auskunftsrechts nach Art. 12 Abs. 5 S. 2 DS-GVO wegen Verwendung anderer nicht von Art. 15 DS-GVO verfolgter Zwecke offen zu sein scheint; das Gericht hat darüber bisher jedoch noch nicht entschieden.

2. Behördenansichten

Auch die Datenschutzaufsichtsbehörden haben sich des hier besprochenen Themas bereits mehrfach angenommen.

a) LDA Brandenburg

So äußerte die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (LDA Branden-

19 Siehe II.a.i.

20 LG Wuppertal, Urt. v. 29.07.2021 – 4 O 409/20, BeckRS 2021, 25249 Rn. 30 ff.

21 LG Wuppertal, Urt. v. 29.07.2021 – 4 O 409/20, BeckRS 2021, 25249 Rn. 31.

22 Siehe ebenda.

23 LG Wuppertal, Urt. v. 29.07.2021 – 4 O 409/20, BeckRS 2021, 25249, Rn. 32 f. mwN.

24 ArbG Neumünster, Urt. v. 11.08.2020 – 1 Ca 247 c/20, BeckRS 2020, 29998 Rn. 36.

25 Siehe ebenda.

26 So z.B. Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 5 Rn. 1.

27 ArbG Neumünster, Urt. v. 11.08.2020 – 1 Ca 247 c/20, BeckRS 2020, 29998 Rn. 36.

28 BGH, Urt. v. 15.06.2021 – VI ZR 576/19, NJW 2021, 2726.

29 BGH, Urt. v. 15.06.2021 – VI ZR 576/19, NJW 2021, 2726 Rn. 33.

burg), dass das Recht auf Auskunft ohne Begründungserfordernis bestehe.[30] Eine Absicht, die auf dem Wege der Auskunft erhaltenen Daten zu einem späteren Zeitpunkt in einem Zivilprozess zu verwenden, könne dem Auskunft Begehrenden somit nicht entgegengehalten werden.

b) LfD Bremen

In gleicher Weise vertritt etwa die Landesbeauftragte für Datenschutz Bremen (LfD Bremen), dass das Motiv der Geltendmachung des Auskunftsanspruchs rechtlich irrelevant sei.[31] Nur im rechtlichen Ausnahmefall eines offenkundigen Missbrauchs der Auskunftsrechtsposition soll hiervon eine Ausnahme zu machen sein. Jedoch spezifiziert die LfD nicht weiter, wann ein solcher Ausnahmefall angenommen werden kann.

III. Ansicht des EuGH zum Missbrauch von Rechtspositionen

Zur Beantwortung der Frage, ob ein Rechtsmissbrauch im vorstehend beschriebenen deutschen Verständnis denkbar ist, wird die Rechtsprechung des EuGH auf entsprechende Anhaltspunkte untersucht.

1. Rechtssache C-597/19 – M.I.C.M.

Im Schlussantrag der Rs. C-597/19 äußerte der Generalanwalt Szpunar, dass im Unionsrecht der allgemeine Grundsatz gelte, dass man sich nicht betrügerisch oder missbräuchlich auf das Unionsrecht berufen kann.[32] So könnten Vorgänge geschützt werden, die zu dem Zweck durchgeführt werden, betrügerisch oder missbräuchlich in den Genuss von im Unionsrecht vorgesehenen Vorteilen zu gelangen. Dies ist nach der Ansicht des Generalanwalts der Fall, wenn Vorschriften des Unionsrechts nicht geltend gemacht würden, um die Ziele der Vorschriften zu verwirklichen, sondern um in den Genuss eines im Unionsrecht vorgesehenen Vorteils zu gelangen, obwohl die entsprechenden Voraussetzungen lediglich formal erfüllt sind.[33] Auch der Generalanwalt geht also davon aus, dass die rein formale Geltendmachung unionsrechtlicher Vorschriften rechtsmissbräuchlich sein kann, wenn damit ein ganz anderer Zweck verfolgt wird, als durch die bemühte EU-Rechtsnorm intendiert. Da der Generalanwalt zudem betont, dass das Verbot des Rechtsmissbrauchs in vielerlei Rechtsgebieten des Unionsrechts Anwendung finde,[34] kann dieser Schlussantrag als erstes Indiz dafür herangezogen werden, dass die Verweigerung des Auskunftsrechts nach Art. 15 DS-GVO aus rechtsmissbräuchlichen Gründen ebenfalls möglich ist. Denn das Argument des Rechtsmissbrauchs greift der EuGH anschließend auch in seinem Urteil zu der Rechtssache auf.[35]

2. Rechtssache C-115/16 – N Luxembourg 1

Diesen allgemeinen Grundsatz des Verbots des Rechtsmissbrauchs greift der EuGH z.B. auch in einer steuerrechtlichen Entscheidung auf.[36] Der EuGH betont in diesem Zusammenhang, dass „der Grundsatz des Missbrauchsverbots einen allgemeinen Grundsatz des Unionsrechts darstellt, der unabhängig davon gilt, ob die betreffenden Rechte und Vorteile ihre Grundlage in den Verträgen, in einer Verordnung oder in einer Richtlinie haben".[37] Letzteres spricht deutlich dafür, dass der Grundsatz des Missbrauchsverbots als allgemeiner Grundsatz des Unionsrechts auch Eingang in die DS-GVO findet und bei deren Auslegung und Anwendung zu berücksichtigen ist.

3. Rechtssache C-434/16 – Nowak

Dass der Grundsatz des Verbots des Rechtsmissbrauchs auch im Datenschutzrecht Berücksichtigung findet, zeigt der Schlussantrag der Generalanwältin Kokott in der Rechtssache Nowak. Dort führt die Generalanwältin (noch zu der alten EU Datenschutz-Richtlinie[38]) aus, dass die missbräuchliche oder betrügerische Berufung auf Unionsrecht nicht gestattet sei.[39] Die Feststellung eines solchen missbräuchlichen Verhaltens verlange das Vorliegen eines objektiven und eines subjektiven Tatbestandsmerkmals.[40] Hinsichtlich des objektiven Tatbestands müsse eine Gesamtwürdigung der objektiven Umstände ergeben, dass trotz formaler Einhaltung der von der Unionsregelung vorgesehenen Bedingungen das Ziel dieser Regelung nicht erreicht wird.[41] Zudem muss das subjektive Tatbestandsmerkmal aus einer Reihe objektiver Anhaltspunkte ersichtlich sein, wonach wesentlicher Zweck der fraglichen Handlungen die Erlangung eines ungerechtfertigten Vorteils ist.[42] So greife das Missbrauchsverbot nicht, wenn die fraglichen Handlungen eine andere Erklärung haben können als nur die Erlangung eines (ungerechtfertigten) Vorteils.[43] Unklar bleibt insoweit, welcher vom Auskunftsteller verfolgte Vorteil das allgemeine unionsrechtliche Missbrauchsverbot konkret auslöst und welcher nicht. Das Vorhandensein anderer mitgliedstaatlicher Regelungen, die ebenfalls eine Auskunft (hier: über Prüfungsarbeiten) zum Gegenstand haben, soll nach dem Schlussantrag der Generalanwältin jedenfalls noch nicht eine Zweckverfehlung hinsichtlich des datenschutzrechtlichen Auskunftsanspruchs indizieren.[44]

30 LDA Brandenburg, Tätigkeitsbericht 2020 Datenschutz, S. 51.

31 LfD Bremen, 3. Jahresbericht nach der Europäischen Datenschutzgrundverordnung (Berichtsjahr 2020), 12.3.

32 Generalanwalt beim EuGH, Schlussantrag v. 17.12.2020 – C-597/19, GRUR-RS 2020, 35419 Rn. 77.

33 Siehe ebenda.

34 Generalanwalt beim EuGH, Schlussantrag v. 17.12.2020 – C-597/19, GRUR-RS 2020, 35419 Rn. 78.

35 EuGH, Urt. v. 17.06.2021 – C-597/19, GRUR 2021, 1067 Rn. 78.

36 EuGH, Urt. v. 26.02.2019 – verb. Rs. C-115/16, C-118/16, C-119/16, C-299/16, IStR 2019, 308 Rn. 98.

37 EuGH, Urt. v. 26.02.2019 – verb. Rs. C-115/16, C-118/16, C-119/16, C-299/16, IStR 2019, 308 Rn. 101.

38 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 (ABl. 1995, L 281, S. 31) in der Fassung der Verordnung (EG) Nr. 1882/2003 des Europäischen Parlaments und des Rates vom 29. September 2003 (ABl. 2003, L 284, S. 1).

39 Generalanwältin beim EuGH, Schlussantrag v. 20.07.2017 – C-434/16, BeckRS 2017, 118086 Rn. 43 mwN.

40 Generalanwältin beim EuGH, Schlussantrag v. 20.07.2017 – C-434/16, BeckRS 2017, 118086 Rn. 44.

41 Siehe ebenda.

42 Siehe ebenda.

43 Siehe ebenda.

44 Generalanwältin beim EuGH, Schlussantrag v. 20.07.2017 – C-434/16, BeckRS 2017, 118086 Rn. 49.

Ein Missbrauch im hiesigen Sinn sei jedenfalls dann nicht gegeben, wenn man über den Auskunftsanspruch Informationen erhält, zu denen man andernfalls keinen Zugang hätte.[45]

IV. Normgebungshistorie zu Art. 12 Abs. 5 DS-GVO

Abgesehen von den vorstehenden Entscheidungen bleibt zuletzt zu untersuchen, ob sich ein allgemeiner Rechtsmissbrauchstatbestand (insbesondere) unter Art. 12 Abs. 5 DS-GVO subsumieren lässt. Ebenso wie das deutsche Recht, kennt auch das Unionsrecht die historische Auslegungsmethode,[46] die nachfolgend als Grundlage der Bewertung dient.

Im Rahmen der Verhandlungen zur DS-GVO und zum damaligen Art. 12 Abs. 4 DS-GVO (nunmehr: Art. 12 Abs. 5 DS-GVO) plädierten mehrere Delegationen im Rahmen der Verhandlungen des Rats der Europäischen Union dafür, anstelle des Begriffs „offenkundig unbegründet" vielmehr „missbräuchlich" in den Normtext aufzunehmen.[47] Dieser Vorschlag wurde abgelehnt. Allerdings enthielt die Ratsfassung der DS-GVO auch noch bis zum 11. Juni 2015 in ErwG 47 Abs. 2 DS-GVO zum Rechtsmissbrauch einen Passus, der beispielsweise bei der Angabe von falschen oder irreführenden Angaben anwendbar sein sollte.[48] Dieser ErwG 47 Abs. 2 DS-GVO ließe sich durchaus auch so verstehen, dass der Missbrauch ein Unterfall des offenkundig unbegründeten Antrags i.S.v. Art. 12 Abs. 5 DS-GVO ist. In der Folge könnte man den Missbrauchstatbestand auch in den jetzigen Art. 12 Abs. 5 DS-GVO und die Formulierung „offenkundig unbegründet" hineinlesen und als Ausnahme von der Pflicht zur Beantwortung von Betroffenenanfragen zulassen. Für dieses Verständnis könnte außerdem sprechen, dass die portugiesische Delegation im Rahmen der Verhandlung die Verständnisfrage stellte, ob denn nicht „offenkundig unbegründet" ohnehin mit „offenkundig missbräuchlich" gleichzusetzen bzw. davon erfasst wäre.[49] Da man im Rahmen der Ratsverhandlungen diese Frage also offensichtlich sah, könnte man dies als Argument dafür anführen, dass der Rechtsmissbrauch auch von Art. 12 Abs. 5 DS-GVO erfasst ist.

Gleichwohl wurde ErwG 47 Abs. 2 DS-GVO im Rahmen der Ratsverhandlungen schließlich gestrichen.[50] Daraus ergeben sich zwei alternative Ableitungen: Mit Blick auf die vorstehende Frage der portugiesischen Delegation könnte man einerseits annehmen, dass ErwG 47 Abs. 2 DS-GVO gestrichen wurde, da die Delegationen des Rates den Missbrauchstatbestand ohnehin für von Art. 12 Abs. 5 DS-GVO umfasst hielten. Andererseits könnte die letztendliche Streichung von ErwG 47 Abs. 2 DS-GVO dafür sprechen, dass sich der Rat am Ende gegen einen solchen Missbrauchstatbestand in der DS-GVO aussprechen wollte.

V. Fazit

Unabhängig davon, welche Positionen man hinsichtlich der Verankerung des Rechtsmissbrauchstatbestands in der DS-GVO einnimmt, lässt sich nach Ansicht der Verfasser nicht bestreiten, dass ein allgemeiner unionsrechtlicher Grundsatz zum Verbot des Rechtsmissbrauchs existiert, der auch im geltenden Datenschutzrecht Anwendung findet. Die vorstehende Streitfrage, ob ein solcher Rechtsmissbrauchstatbestand unter Art. 12 Abs. 5 DS-GVO subsumierbar oder § 242 BGB hier anwendbar ist, kann zumindest unter praktischen Gesichtspunkten dahinstehen bleiben. Denn letztlich handelt es sich dabei eher um eine dogmatische Frage. Nach Ansicht der Verfasser sprechen gute Gründe dafür, dass sich Verantwortliche im Rahmen der Auskunftserteilung nach den Art. 15 DS-GVO auf den Einwand des Rechtsmissbrauchs über die in Art. 12 Abs. 5 und Art. 15 Abs. 4 DS-GVO festgeschriebenen Fälle hinaus berufen können. Dafür spricht neben der Rechtsprechung des EuGH auch, dass sich der BGH offen für diese Interpretation zeigt bzw. bisher nicht ablehnend entschieden hat. Gleichwohl sollten die Anforderungen an die Geltendmachung dieses Einwands in der Praxis nicht unterschätzt werden. Verantwortliche sollten diesen Einwand daher objektiv und subjektiv fundiert begründen, bevor sie ihn erheben. Dabei gilt es zu beachten, dass Betroffene die Geltendmachung ihres Betroffenenrechts ohnehin nicht begründen müssen. Führt der Betroffene also z.B. nicht aus, zu welchen Zwecken die Unterlagen beauskunftet werden sollen, wird der Einwand des Rechtsmissbrauchs zugunsten des Verantwortlichen aus Nachweisgründen regelmäßig eher.

Dr. Carlo Piltz
Rechtsanwalt und berät als Partner in der auf Datenschutz-, IT- und IT-Sicherheitsrecht spezialisierten Kanzlei Piltz Legal in Berlin.

Johannes Zwerschke
Rechtsanwalt und berät als Senior Associate in der auf Datenschutz-, IT- und IT-Sicherheitsrecht spezialisierten Kanzlei Piltz Legal in Berlin.

45 Generalanwältin beim EuGH, Schlussantrag v. 20.07.2017 – C-434/16, BeckRS 2017, 118086 Rn. 50.

46 Pieper, in: Dauses/Ludwigs EU-WirtschaftsR-HdB, 53. EL, Stand: Juli 2021, B. B.I. Rechtsquellen Rn. 8.

47 Rat der Europäischen Union, Ratsdokument 7978/1/15 REV 1, Fn. 59, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-7978-2015-REV-1/de/pdf (zuletzt abgerufen am: 17.12.2021).

48 Rat der Europäischen Union, Ratsdokument 9565/15, S. 26, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf (zuletzt abgerufen am: 17.12.2021).

49 Rat der Europäischen Union, Ratsdokument 7586/1/15 REV 1, S. 58, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-7586-2015-REV-1/en/pdf (zuletzt abgerufen am: 17.12.2021) (nur in Englisch verfügbar).

50 Rat der Europäischen Union, Ratsdokument 10391/15, S. 75, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-7586-2015-REV-1/en/pdf (zuletzt abgerufen am: 17.12.2021) (nur in Englisch verfügbar).

Online-Kompaktkurse Termine

März & April 2022

Thema	Referent/-in	Termin*
Update Telefonwerbung – Aktuelle Rechtsfragen und Dauerbrenner im Telemarketing	Sebastian Schulz	09.03.2022
Datenschutz in der Kita	Georg Karl Bittorf	15.03.2022
Datenschutz-Leit- und Richtlinien	Thomas Müthlein, Dr. Frank Fenner	15.03.2022
Unbeabsichtigte Datenschutz-Verstöße im Personalbereich	Petra Eul-Löh	16.03.2022
Pauschalversteuerung bei Sachzuwendungen nach § 37b EStG	Christian Günther	17.03.2022
Datenschutz-Fehler beim Umgang mit Bewerbungen	Petra Eul-Löh	29.03.2022
Awareness schaffen – Datenschutz-Richtlinien zum Leben erwecken	Dr. Frank Fenner	05.04.2022
Datenschutz im Seniorenzentrum	Georg Karl Bittorf	26.04.2022

* Änderungen bei Terminen bleiben vorbehalten; Preise zzgl. MwSt.

Jetzt anmelden: www.datakontext.com/datenschutz-okk

NUR 119,– €

GDD-Datenschutz Akademie Praxis-Reihe

Online-Kompaktkurse im Datenschutz

90 Minuten praxisgerecht aufbereitetes Datenschutzwissen

Alle aktuellen Kursangebote finden Sie unter:
www.datakontext.com/datenschutz-okk

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Kurzbeiträge

Praxisfälle zum Datenschutzrecht XIV: Datenschutz bei Unternehmensverkauf und Due Diligence

RAin Yvette Reif, LL.M.*

I. Sachverhalt

Unternehmer U betreibt ein erfolgreiches IT- und Softwareberatungsunternehmen mit 150 Mitarbeitern. Da er sich demnächst zur Ruhe setzen will, schaut er sich aktuell nach potenziellen Käufern für das Unternehmen um. Einer der Kaufinteressenten möchte zwecks Durchführung einer Due Diligence nach Abschluss einer Vertraulichkeitsvereinbarung folgende Informationen zu allen Beschäftigten einsehen: Kopien der Arbeitsverträge, alle gehaltsrelevanten Daten sowie Daten zur betrieblichen Altersversorgung, Alter, Dauer der Betriebszugehörigkeit und jeweiliger Arbeitsort.[1]

Darf U dem Wunsch des Interessenten nachkommen?

II. Musterfalllösung

1. Allgemeines

Mit Due Diligence ist die sorgfältige Prüfung und Analyse eines Unternehmens gemeint, insbesondere im Hinblick auf seine wirtschaftlichen, rechtlichen, steuerlichen und finanziellen Verhältnisse, die durch den potenziellen Käufer eines Unternehmens vorgenommen wird.[2] Bei Durchführung eines Due Diligence Verfahrens haben die Beteiligten ein immenses Interesse daran, dass die Prüfung geheim bleibt, denn Informationen, die vor der Unternehmenstransaktion nach außen dringen, können diese blockieren oder zum Scheitern bringen.

Die Datenverarbeitungen im Rahmen einer Due Diligence unterliegen dem Regelungsregime der DS-GVO bzw. des BDSG, sobald Prüfung und Analyse durch den Erwerber sich auch auf zumindest personenbeziehbare Informationen beziehen.

2. Anwendbarkeit des Datenschutzrechts

Da die Beschäftigtendaten, die dem Erwerber bereitgestellt werden, typischerweise aus den HR-Systemen des Veräußerers stammen, ist der sachliche Anwendungsbereich der DS-GVO (Art. 2 Abs. 1) eröffnet. Von § 26 BDSG wird gemäß dessen Abs. 7 im Übrigen auch die nicht automatisierte Verarbeitung personenbezogener Daten erfasst.

3. Mögliche Rechtsgrundlage für eine Offenlegung personenbezogener Beschäftigtendaten gegenüber potenziellen Erwerbern

a) Durchführung des Beschäftigungsverhältnisses (§ 26 Abs. 1 S. 1 BDSG)

Nach § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, sofern dies für dessen Durchführung erforderlich ist. Das Beschäftigungsverhältnis besteht aber aktuell ausschließlich mit dem Verkäufer des Unternehmens und nicht mit den potenziellen Erwerbern, wenn auch das Beschäftigungsverhältnis ggf. in Zukunft im Wege des Betriebsübergangs (§ 613a BGB) auf einen von diesen übergehen mag. Es gehört auch nicht zu den arbeitsvertraglichen Pflichten der Beschäftigten, sich von ihrem Arbeitgeber mit dem Unternehmen an einen anderen Unternehmer „verkaufen" und sich iR eines Due Diligence Verfahrens „durchleuchten" zu lassen. § 26 Abs. 1 S. 1 BDSG scheidet als Rechtsgrundlage damit vorliegend aus.[3]

b) Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) und Kompatibilität (Art. 6 Abs. 4 DS-GVO)

Bei dem Interesse des Unternehmers, sein Unternehmen zu verkaufen, handelt es sich um ein – sogar grundrechtlich geschütztes (Art. 14 GG) – berechtigtes Interesse. Die Weitergabe personenbezogener Daten an den Erwerber bzw. die Bereitstellung von Informationen zur Einsichtnahme könnte insofern über Art. 6 Abs. 1 lit. f DS-GVO gestattet sein. Nach dieser Regelung ist eine Verarbeitung personenbezogener Daten rechtmäßig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, hier der Beschäftigten, überwiegen. Wie sich aus dem Wortlaut des Art. 6 Abs. 1 lit. f DS-GVO ergibt, kann dieser nicht nur Verarbeitungen im Interesse des Verantwortlichen legitimieren, sondern auch solche im Interesse eines Dritten. Die Preisgabe von Beschäftigtendaten im Zusammenhang mit dem Unternehmensverkauf liegt im Interesse des Verkäufers wie auch des Käufers. Mitarbeiter sind das wichtigste Asset eines Unternehmens. Für den potenziellen Käufer eines Unternehmens ist die Personalstruktur beim zur Veräußerung stehenden Unternehmen und die Expertise der dort arbeitenden Personen von zentraler Bedeutung.

Fraglich ist allerdings zunächst, inwiefern Art. 6 Abs. 1 lit. f DS-GVO neben § 26 BDSG zur Anwendung kommen

---

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

1 Sachverhalt angelehnt an LfDI BW, Ratgeber Beschäftigtendatenschutz, Stand: April 2020 (4. Aufl.), Fall 9.

2 Begriffsbestimmung nach https://wirtschaftslexikon.gabler.de/definition/due-diligence-35668.

3 Weitergehend Schröder in Forgó/Helfrich/Schneider, Betr. Datenschutz, 3. Aufl. (2019), Teil VI. Kap. 4 Rn. 14, der Unternehmenstransaktionen „als Teil der Lebenswirklichkeit von Unternehmen" verstehen und daher den Beschäftigungskontext weiterfassen will.

kann und ob nicht die Gefahr besteht, dass über einen Rückgriff auf die Interessenabwägung die Anforderungen des § 26 BDSG unterlaufen werden, nämlich die Erforderlichkeit der Verarbeitung der Beschäftigtendaten für die Durchführung des Beschäftigungsverhältnisses. Die Gefahr, dass § 26 BDSG unterlaufen wird, ergibt sich allerdings nur dann, wenn Zwecke verfolgt werden, die im Zusammenhang mit dem Beschäftigungsverhältnis stehen. Wie vorstehend unter a) ausgeführt, liegt das Interesse des Arbeitgebers, sein Unternehmen zu verkaufen, jedoch außerhalb der Zwecke des Beschäftigungsverhältnisses. Es entspricht der herrschenden Ansicht, dass private Arbeitgeber für sog. „beschäftigungsfremde Zwecke" auf Art. 6 Abs. 1 lit. f DS-GVO zurückgreifen können.[4]

Die Anwendbarkeit von Art. 6 Abs. 1 lit. f DS-GVO in Fällen des Unternehmensverkaufs ist jedoch vor dem Hintergrund fraglich, dass die betroffenen Beschäftigtendaten ursprünglich für die Zwecke des Beschäftigungsverhältnisses erhoben wurden, es sich also um eine Weiterverarbeitung zu neuen Zwecken handelt. Nach Art. 5 Abs. 1 lit. b DS-GVO gilt das Prinzip der Zweckbindung personenbezogener Daten. Nach Art. 6 Abs. 4 DS-GVO setzt eine zweckändernde Verarbeitung, sofern keine Einwilligung der betroffenen Person und keine spezielle gesetzliche Erlaubnis vorliegt, eine Prüfung der Kompatibilität, also der Vereinbarkeit des neuen Verarbeitungszwecks mit dem ursprünglichen Erhebungszweck voraus.

Art. 6 Abs. 4 DS-GVO wirft zahlreiche Fragen auf. Fraglich ist u.a., ob noch ein Rückgriff auf die allgemeine Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO möglich ist, sofern festgestellt wurde, dass ein geplanter neuer Verarbeitungszweck mit dem ursprünglichen Erhebungszweck inkompatibel ist. Ein Umkehrschluss aus Art. 6 Abs. 4 DS-GVO und der dort vorgenommenen Beschränkung auf die Einwilligung bzw. spezifische Erlaubnisse wird wohl zu dem Ergebnis führen, dass im Falle der Inkompatibilität eine Weiterverarbeitung auf Grundlage der allgemeinen Interessenabwägung gerade nicht zulässig sein soll.[5]

Entscheidend ist damit hier die Frage der Vereinbarkeit des neuen Verarbeitungszwecks der Beschäftigtendaten („Unternehmensverkauf und Due Diligence") mit dem ursprüngli-chen Erhebungszweck („Begründung und Durchführung des Beschäftigungsverhältnisses"). Art. 6 Abs. 4 sieht einen nicht abschließenden („unter anderem") Katalog von Aspekten vor, die bei der Kompatibilitätsprüfung zu berücksichtigen sind. Dazu gehören:

- jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung (lit. a),
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen (lit. b),
- die Art der personenbezogenen Daten, insbesondere ob Daten gem. Art. 9 f. DS-GVO verarbeitet werden (lit. c),
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (lit. d) sowie
- das Vorhandensein geeigneter Garantien, wozu etwa Verschlüsselung oder Pseudonymisierung gehören können (lit. e).

Nach den vor Geltung der DS-GVO auf Basis der allgemeinen Interessenabwägung entwickelten Grundsätzen wurde neben der Bereitstellung von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form im Rahmen einer Due Diligence grundsätzlich auch die Preisgabe von Klardaten als zulässig erachtet, sofern ausgewählte Experten oder Beschäftigte in Schlüsselpositionen betroffen waren und eine Offenlegung dem jeweiligen Marktstandard bei Transaktionen vergleichbarer Größe und Bedeutung entsprach.[6] Personenbezogene Informationen über Führungskräfte sind für den Erwerber unentbehrlich. Eine Anonymisierung oder Pseudonymisierung wird dem Informationsinteresse des Erwerbers in aller Regel nicht gerecht.[7] Nach herrschender Literatur soll sich an diesem Umfang zulässiger Datenpreisgabe an potenzielle Unternehmenserwerber seit Geltung der DS-GVO und insbesondere des Art. 6 Abs. 4 im Grundsatz nichts geändert haben.

Zwischen der Nutzung von Daten für ein Beschäftigungsverhältnis und der Prüfung derselben Informationen zum Zweck des Unternehmenserwerbs bestehe ein „naher Zweckzusammenhang" i.S.v. Art. 6 Abs. 4 lit. a DS-GVO.[8] Eine Due Diligence Prüfung sei nach dem relevanten objektiven Erwartungshorizont für Beschäftigte ein allgemein vorhersehbares Ereignis. Dass ihre Daten im Laufe des Beschäftigungsverhältnisses für eine Unternehmenstransaktion relevant werden können, sei objektiv möglich wie vorhersehbar.[9] Wie bei der Erlaubnis nach Art. 6 Abs. 1 lit. f DS-GVO sei auch nach Art. 6 Abs. 4 lit. e DS-GVO das Risiko für die betroffenen Personen durch eine weitestmögliche Anonymisierung der Daten, eine Verschlüsselung der Übermittlung sowie eine Vereinbarung von Geheimhaltungs- und Löschpflichten für den Fall einer gescheiterten Unternehmenstransaktion möglichst gering zu halten.[10] Die bei Einrichtung und Betrieb des virtuellen bzw. physischen Datenraums einzuhaltenden technisch-organisatorischen Anforderungen stiegen mit zunehmender Schutzbedürftigkeit der dort vorgehaltenen Daten.[11]

Auch wenn die Kompatibilitätsprüfung nach Art. 6 Abs. 4 DS-GVO im Ergebnis einer Interessenabwägung also nicht unähnlich sein mag, gibt es aber doch einen entscheidenden Unterschied zur Rechtslage vor Geltung der DS-GVO,

4 Gola, Handbuch Beschäftigtendatenschutz, 8. Aufl., Rn. 752 ff.; LfDI BW, Ratgeber Beschäftigtendatenschutz, Stand: April 2020 (4. Aufl.), S. 59 f.; explizit zur Verarbeitung von Beschäftigtendaten bei Due Diligence im Rahmen eines Unternehmenskaufvertrages Taeger/Gabel/Zöll, 3. Aufl. (2019), BDSG § 26 Rn. 15.

5 Schulz, in: Gola DS-GVO, Art. 6 Rn. 213.

6 Göpfert/Meyer, NZA 2011, 486 (488).

7 Sander/Schumacher/Kühne, ZD 2017, 105 (110).

8 Schröder, in: Forgó/Helfrich/Schneider, Betr. Datenschutz, 3. Aufl. (2019), Teil VI. Kap. 4 Rn. 17.

9 Schmidt, in: WHWS, Arbeitnehmerdatenschutz, 2. Aufl. (2019), Teil B. XIV. Rn. 34.

10 Schröder, in: Forgó/Helfrich/Schneider, Betr. Datenschutz, 3. Aufl. (2019), Teil VI. Kap. 4 Rn. 17; Sander/Schumacher/Kühne, ZD 2017, 105 (109); Schulz, in: Gola, DS-GVO Art. 6 Rn. 262 f.

11 Schulz, in: Gola, DS-GVO, Art. 6 Rn. 263.

nämlich die Informationspflicht aus Art. 13 Abs. 3 DS-GVO gegenüber den Experten bzw. Schlüsselpersonen, deren Daten im Klartext an potenzielle Erwerber fließen sollen. Beabsichtigt nämlich der Verantwortliche, personenbezogene Daten für einen anderen Zweck weiterzuverarbeiten als den, für den diese ursprünglich erhoben wurden, so hat er nach Art. 13 Abs. 3 DS-GVO der betroffenen Person vor der Weiterverarbeitung Informationen über diesen neuen Zweck und alle anderen maßgeblichen Informationen nach Art. 13 Abs. 2 DS-GVO zur Verfügung zu stellen. Ungeachtet dieser Pflicht zur Information bei Zweckänderung sieht außerdem Art. 14 DS-GVO für den Datenempfänger eine Verpflichtung zur Information der Betroffenen über die Speicherung der erhaltenen Daten vor. Sofern potenzielle Erwerber personenbezogen über Beschäftigte des Veräußerers informiert werden sollen, führen die DS-GVO-Transparenzpflichten damit zur Gefährdung der Geheimhaltung der Vertragsverhandlungen.[12] Vor diesem Hintergrund wird empfohlen, durch Anonymisierung auf den Austausch von personenbezogenen Informationen so weit als möglich zu verzichten.[13]

c) Einwilligung

Zwar ist es nicht ausgeschlossen, dass auch Beschäftigte eine datenschutzrechtliche Einwilligung freiwillig erteilen. Nach § 26 Abs. 2 S. 1 BDSG bedarf es aber aufgrund der im Beschäftigungsverhältnis bestehenden Abhängigkeit der beschäftigten Personen bei Einwilligungen von Beschäftigten stets der besonderen Prüfung der Freiwilligkeit der Erklärung. Nach § 26 Abs. 2 S. 2 BDSG kann eine Freiwilligkeit insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Letzteres ist hier nicht anzunehmen. In den meisten Fällen sehen Beschäftigte einen potenziellen Verkauf des Unternehmens durch den Arbeitgeber eher skeptisch, als dass sie sich hiervon Vorteile versprechen. Vielfach ist die Zukunft des Unternehmens unter der Hand des potenziellen Erwerbers im Detail unklar und der Verkauf für die Beschäftigten mit Sorgen verbunden. Als Rechtsgrundlage für die Weitergabe von Daten „einfacher" Beschäftigter an potenzielle Erwerber des Unternehmens dürfte die Einwilligung damit regelmäßig ausscheiden.

Abhängig von der konkreten Funktion kann bei Führungskräften demgegenüber ein klares Ungleichgewicht ggf. zu verneinen sein. Da Führungskräfte oftmals maßgeblich an Unternehmenstransaktionen beteiligt sind, müssen auch Geheimhaltungsinteressen des Veräußerers nicht zwingend einer Einholung entsprechender Erklärungen entgegenstehen.

d) Betriebsvereinbarung

Nach § 26 Abs. 4 BDSG ist die Verarbeitung personenbezogener Beschäftigtendaten, einschließlich besonderer Kategorien personenbezogener Daten, auch auf der Grundlage von Kollektivvereinbarungen zulässig. Dem Abschluss einer Kollektivvereinbarung wird allerdings in der Praxis typischerweise das Geheimhaltungsinteresse des Erwerbers und Veräußerers entgegenstehen.[14] Auch wird der Betriebsrat der Preisgabe personenbezogener Daten der Arbeitnehmer in der Regel nicht ohne Weiteres zustimmen.[15]

III. Ergebnis

Auf den Austausch von personenbezogenen Informationen über Beschäftigte sollte im Rahmen des Due Diligence Verfahrens nach Möglichkeit verzichtet werden. Ausnahmen sind für Schlüsselpersonen und Führungskräfte denkbar. Als Grundlage der Preisgabe von Informationen über diese Personen kommt entweder eine kompatible Weiterverarbeitung nach Art. 6 Abs. 4 DS-GVO oder aber eine Einwilligung der Personen in Betracht. Im ersten Fall bedarf es der Vorabinformation nach Art. 13 Abs. 3 DS-GVO.

12 Sander/Schumacher/Kühne, ZD 2017, 105 (110); Schnebbe, DSRITB 2021, 57 (61).

13 Schröder, in: Forgó/Helfrich/Schneider, Betr. Datenschutz, 3. Aufl. (2019), Teil VI. Kap. 4 Rn. 18; Sander/Schumacher/Kühne, ZD 2017, 105 (110).

14 Sander/Schumacher/Kühne, ZD 2017, 105 (108).

15 Sander/Schumacher/Kühne, ZD 2017, 105 (108).

Hacker-Tools für Datenschutzbeauftragte

11. April 2022 | Frankfurt
Referent: Prof. Dr. Rainer W. Gerling

Schwerpunkte:
✓ Netzwerkscanner
✓ TLS-Analyse
✓ Passworte knacken
✓ Sniffen

Jetzt anmelden: www.datakontext.com

GDD DATAKONTEXT

Aus den aktuellen Berichten der Aufsichtsbehörden (58): TLfDI, 3. TB (2020) nach der DS-GVO: Vier Fälle einwilligungsbedürftiger Verarbeitungen

Zusammengestellt und erläutert von Prof. Peter Gola*

I. Unzulässige Wahlwerbung eines Versicherungsmaklers (TLfDI; 3. TB, 2020, S. 133 ff.)

Die personenbezogenen Daten einer betroffenen Person, die im Rahmen privater oder geschäftlicher Beziehungen erhoben wurden, sind ohne eine Einwilligung und eine Information über die beabsichtigte Zweckänderung nach Art. 13 Abs. 2 DS-GVO nicht für die Versendung von Wahlwerbung des Verantwortlichen nutzbar.

Der TLfDI hat einen Immobilienmakler, der Namen und Adressen von Kunden für die Übersendung von Wahlwerbung für seine Kommunalwahlkandidatur genutzt hatte, gemäß Art. 58 Abs. 2 lit. b DS-GVO verwarnt.

Dabei ging der LfDI zunächst davon aus, dass die Werbung im Rahmen einer Kommunalwahl nicht zur Ausübung ausschließlich rein persönlicher oder familiärer Tätigkeiten zählt (§ 2 Abs. 2 lit. c DS-GVO). In der Verwendung der Daten zur Wahlwerbung erkannte der LfDI zunächst einen Verstoß gegen Art. 5 Abs. 1 lit. a und b DS-GVO: Daten müssen für festgelegte Zwecke erhoben werden und dürfen nicht für andere mit diesen Zwecken nicht vereinbare Zwecke weiterverarbeitet werden. Gemäß Art. 6 Abs. 1 DS-GVO ist eine Verarbeitung nur dann rechtmäßig, wenn ein Erlaubnistatbestand nach Art. 6 Abs. 1 DS-GVO vorliege, was sodann verneint wurde. Das gelte auch für den allein in Betracht zu ziehenden Erlaubnistatbestand des Art. 6 Abs. 1 S. 1 lit. f DS-GVO. Dies ergab sich aus folgender Abwägung: Der Betroffene musste nicht damit rechnen, dass er mit Wahlwerbung von Personen angesprochen wird, mit denen er geschäftlichen bzw. geschäftlich privaten Umgang pflegt. Die Verwendung der Daten für die Übersendung von Wahlwerbung sei daher keine mit dem Erhebungszweck zu vereinbarende Art und Weise.

Zudem hätte der Makler nach dem Transparenzgebot des Art. 5 Abs. 1 lit. a DS-GVO gemäß Art. 13 Abs. 3 DS-GVO die betroffenen Personen von der Absicht, ihre Adressen für einen anderen Zweck weiterzuverarbeiten, nach Art. 13 Abs. 2 DS-GVO informieren müssen.

II. Aufforderungs-E-Mails zur Bewertung eines Online-Shops bedürfen der Einwilligung des Betroffenen (TLfDI, 3. TB, 2020, S. 137)

Die Versendung einer E-Mail zum Zwecke der Aufforderung um Bewertung des vorher durch den Betroffenen genutzten Online-Shops stellt einen Verstoß gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO dar, solange dafür keine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO vorliegt.

Ein Thüringer Unternehmen, welches auch einen Online-Shop betreibt, hat einem Kunden nach Abschluss eines Onlinekaufes eine E-Mail mit der Aufforderung zur Bewertung des Online-Shops zugesandt. Als Zweck dieser E-Mail wurden die Analyse und Verbesserung des Online-Shops angegeben. Der Kunde hat im Rahmen seines Kaufgeschäftes dazu keinerlei Einwilligungen abgegeben. Der TLfDI stellt dazu fest: „Bei der Aufforderung zur Bewertung eines Shops handelt es sich um eine Werbemaßnahme. Werbung wird definiert als „jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern“ (Art. 2 Buchstabe a) der EU-Richtlinie 2006/114/EG über irreführende und vergleichende Werbung vom 12. Dezember 2006). Eine Rechtsgrundlage für die Beurteilung der Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung findet sich in der Datenschutz-Grundverordnung (DS-GVO), abgesehen von einer Einwilligung der betroffenen Person nach Art. 6 Abs. 1 Satz 1 lit a DS-GVO, nur in Art. 6 Abs. 1 Satz 1 lit f DS-GVO. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein, sofern nicht die Interessen der betroffenen Person überwiegen. Anhaltspunkte für die zu treffende Abwägungsentscheidung enthält Erwägungsgrund 47 DS-GVO, der unter anderem ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“ In diesem Fall wäre eine Datenverarbeitung aufgrund eines berechtigten Interesses des Verantwortlichen möglicherweise gerechtfertigt, wenn sie erforderlich wäre, um ein berechtigtes wirtschaftliches Interesse des Verantwortlichen zu wahren und keine schutzwürdigen Interessen der Betroffenen höher gewichtet werden müssten. Zur Förderung des Produktabsatzes ist es grundsätzlich ein legitimes wirtschaftliches Interesse des Verantwortlichen, Werbemaßnahmen durchzuführen. Vorliegend handelte es sich aber aufgrund des Kontaktweges per E-Mail um eine im Rahmen der Bewertung der Zulässigkeit zu berücksichtigende Besonderheit. Hierzu regelt das Wettbewerbsrecht in § 7 UWG, in welchen Fällen von einer unzumutbaren Belästigung der Beworbenen auszugehen und eine Werbung dieser Art unzulässig ist. Weil Art. 6 Abs. 1 Satz 1 lit f DS-GVO eine Verarbeitung personenbezogener Daten nur für zulässig erklärt, soweit die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, sind auch bei der datenschutzrechtlichen Beurteilung einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung die Wertungen in den Schutzvorschriften des UWG für die jeweilige Werbeform mit zu berücksichtigen. Wenn für den werbenden Verantwortlichen ein bestimmter Kontaktweg zu einer betroffenen Person danach nicht erlaubt ist, kann die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit f DS-GVO auch nicht zugunsten der Zulässigkeit einer Verarbeitung dieser Kontaktdaten für Zwecke der Direktwer-

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

bung ausfallen (siehe dazu auch Orientierungshilfe Direktwerbung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: https://www.datenschutzkonferenz-online.de/media/oh/20181107_oh_werbung.pdf). Die Werbung per E-Mail stellt eine unzumutbare Belästigung im Sinne des § 7 Abs. 1 UWG dar, da nach § 7 Abs. 2 Nr. 3 UWG eine Werbung unter Verwendung elektronischer Post ohne vorherige ausdrückliche Einwilligung des Adressaten vorliegt. Es greift auch nicht die Privilegierung des § 7 Abs. 3 UWG, der hiervon abweichend regelt, dass bei Vorliegen der dort genannten Voraussetzungen keine unzumutbare Belästigung vorliegt, da die Werbung auch nicht für eigene ähnliche Waren oder Dienstleistungen des Verantwortlichen erfolgte.

Eine Zufriedenheitsabfrage per E-Mail nach einem Onlineverkauf dient nur der Verbesserung des Online-Shops und ist für das weitere Bewerben von Produkten nicht erforderlich. Demzufolge ist die Zusendung einer solchen Bewertungs-E-Mail nur über den Tatbestand der Einwilligung gemäß Art. 6 Abs. 1 Satz 1 lit a DS-GVO zu rechtfertigen. Eine solche wurde allerdings vom Unternehmen im Rahmen des Kaufvorgangs nicht abgefordert."

Der TLfDI hat nach Anhörung des verantwortlichen Unternehmens diesem gegenüber eine Verwarnung im Verwaltungsverfahren ausgesprochen. Gleichzeitig hat das verantwortliche Unternehmen eine technische Umstellung vorgenommen.

III. Beschäftigtendatenweitergabe wegen betrieblicher Zusatzkrankenversicherung nur mit Einwilligung (3. TB, S. 169)

Beabsichtigt ein Arbeitgeber im Rahmen des betrieblichen Gesundheitsmanagements eine betriebliche Zusatzkrankenversicherung zu Gunsten seiner Beschäftigten abzuschließen hat er vor der Weiterleitung der personenbezogenen Daten der Beschäftigten an eine private Krankenversicherung eine Einwilligung der Beschäftigten in diese Datenweitergabe einzuholen. Hieran ändert nichts, dass der Arbeitgeber zuvor eine Betriebsvereinbarung über das Anbieten einer solchen Zusatzversicherung abgeschlossen hatte.

Vorliegend hatten der Arbeitgeber zwecks Durchführung einer Betriebsvereinbarung über die Einführung einer privaten Zusatzversicherung mit einer Versicherung einen Gruppenversicherungsvertrag abgeschlossen.

Nach Ansicht des TLfDI eine gute Sache, wenn der Arbeitgeberdabei nicht vorschnell die personenbezogenen Daten der Beschäftigten weitergeleitet hätte, ohne diese zu fragen, ob sie die angebotene Versicherung überhaupt wünschten. Der Arbeitgeber ging vielmehr davon aus, dass die Betriebsvereinbarung die Datenverarbeitung rechtfertigen würde. Dies sah der TLfDI anders.

Die Betriebsvereinbarung enthielt zwar eine Klausel, nach der Beschäftigte zwar berechtigt waren, der Datenweitergabe zu widersprechen. Dies reiche zum einen für die Übermittlungsbefugnis nicht aus. Vielmehr habe es an der Erforderlichkeit der Übermittlung (Art. 88 Abs. 1 DS-GVO i.V.m. § 26 Abs. 1 S. 1 BDSG) gefehlt. Dies begründet der TLfDI wie folgt: „Ist eine betriebliche Zusatzversicherung zugunsten der Beschäftigten erforderlich zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses? Klare Antwort: Nein." Auch wenn das Angebot der Zusatzversicherung gut gemeint und für die meisten eine solche Versicherung auch sinnvoll sei, begründe das nicht die Erforderlichkeit der angefragten Datenweitergabe. Daran ändere nichts, dass der Arbeitgeber die Beiträge für die betriebliche Krankenversicherung im vollen Umfang zu übernehmen bereit war. Zwar sehe § 26 Abs. 1 Halb. 2 BDSG vor, dass Beschäftigtendaten auch dann verarbeitet werden dürfen, wenn dies zur Ausübung oder Erfüllung der sich aus einer Betriebsvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung erforderlich ist, wobei nach § 26 Abs. 4 BDSG die Betriebsvereinbarung selbst Erlaubnistatbestand sein kann, Jedoch seien Arbeitgeber und Betriebsrat dabei nicht von den Vorgaben der DS-GVO frei. Die in der Betriebsvereinbarung getroffene Widerspruchslösung rechtfertige keine Interessenabwägung zu Gunsten des Arbeitgebers. Nur eine Einwilligung der Beschäftigten hätte die Weitergabe rechtfertigen können.

Der LfDI ahndete den Verstoß mit einer Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO.

IV. Keine wirksame Einwilligung in die Weitergabe von detaillierten Angaben des Arbeitgebers an Auftraggeber über die Beschäftigtenvergütung zum Nachweis der Einhaltung des gesetzlichen Mindestlohns (TLfDI, 3. TB, 2020, S. 177)

Weder § 13 Mindestlohngesetz bzw. § 14 AEntG noch Art. 6 DS-GVO iVm § 26 BDSG bieten dem Arbeitgeber eine Rechtsgrundlage für eine Weitergabe von detaillierten Beschäftigtengehaltsdaten an seinen Auftraggeber.

Ein Unternehmen aus dem Baugewerbe wurde vor der Auftragsvergabe vom potentiellen Auftraggeber gebeten, sich zu verpflichten, – als Muster vorgelegte – schriftliche Bestätigungen der Beschäftigten über den Erhalt des Mindestlohns vorzulegen. Die Musterbestätigung endete mit der Erklärung des Einverständnisses der Beschäftigten mit der Weitergabe der Erklärung an den Auftraggeber.

Der TLfDI sah keine Rechtsgrundlage für die gewünschte umfassende Datenweitergabe. Das galt auch für die Wirksamkeit der Einwilligung, die abgesehen von Formulierungsfragen und der nicht aufgezeigten Ermöglichung des Widerrufs daran scheitere, dass den Beschäftigten keinerlei rechtlicher oder wirtschaftlicher Vorteil durch die ausführliche Datenweitergabe entstehe. Dass ggf. der auch im Interesse der Beschäftigten liegende Auftrag ohne die gewünschte Datenübermittlung nicht erteilt würde, ließ der TLfDI nicht als Rechtfertigungsargument gelten.

Schließlich verneinte der TLfDI die Erforderlichkeit der Übermittlung der gewünschten Daten, da es für den Auftraggeber andere Möglichkeiten gebe, sich die Einhaltung der Zahlung des staatlichen Mindestlohns nachweisen zu lassen und damit seiner Haftung nach § 14 AEngt zu begegnen, ohne detaillierte Informationen zu erheben. Hierzu zählen nicht vollständige Namenslisten mit Wohnanschriften, Passnummern etc. Vielmehr würden z.B. von einem Wirtschaftsprüfer bestätigte Lohn- und Arbeitszeitlisten genügen, in denen Beschäftigte teilweise anonymisiert (Anfangsbuchstaben mit Vor- und Nachname, ggf. Geburtsdatum) benannt würden.

Rechtsprechung

Zu den Grenzen der Internet-Werbung für ärztliche Fernbehandlungen (Ls)

(**Bundesgerichtshof**, Urteil vom 9. Dezember 2021 – I ZR 146/20 –)

1. **Eine Werbung auf einer Internetseite mit der Aussage „Erhalte erstmals in Deutschland Diagnosen, Therapieempfehlung und Krankschreibung per App" für die von einer privaten Krankenversicherung angebotene Leistung eines „digitalen Arztbesuchs" mittels einer App bei in der Schweiz ansässigen Ärzten verstößt gegen das Verbot der Werbung für Fernbehandlungen nach § 9 HWG.**
2. **Da es sich bei dieser Vorschrift um eine – dem Gesundheitsschutz dienende – Marktverhaltensregelung im Sinne von § 3a UWG handelt, ist die Beklagte nach § 8 Abs. 1 Satz 1 UWG zur Unterlassung der Werbung verpflichtet.**
3. **Nach § 9 Satz 2 HWG ist zwar die Werbung für Fernbehandlungen, die unter Verwendung von Kommunikationsmedien und somit auch Apps erfolgt, nicht untersagt. Das gilt aber nur, wenn nach allgemein anerkannten fachlichen Standards ein persönlicher ärztlicher Kontakt mit dem zu behandelnden Menschen nicht erforderlich ist. Diese Voraussetzung ist hier nicht erfüllt.**
4. **Der Begriff der allgemein anerkannten fachlichen Standards ist unter Rückgriff auf den entsprechenden Begriff in § 630a Abs. 2 BGB, der die Pflichten aus einem medizinischen Behandlungsvertrag regelt, und die dazu von der Rechtsprechung entwickelten Grundsätze auszulegen. Danach können sich solche Standards auch erst im Laufe der Zeit entwickeln und etwa aus den Leitlinien medizinischer Fachgesellschaften oder den Richtlinien des Gemeinsamen Bundesausschusses gemäß §§ 92, 136 SGB V ergeben. Dies ist bis dato nicht der Fall.**

(Nicht amtliche Leitsätze)

Zu den Voraussetzungen und der Annahme einer Kennzeichnungspflicht bei Instagram Posts von Influencern (Influencer I) (Ls)

(**Bundesgerichtshof**, Urteil vom 9. September 2021 – I ZR 90/20 –)

1. **Geht ein klagender Wettbewerbsverband gegen geschäftliche Handlungen der Beklagten zugunsten des eigenen Unternehmens sowie zugunsten fremder Unternehmen vor, muss der Kläger sowohl über eine erhebliche Zahl an Mitgliedern verfügen, die in einem Wettbewerbsverhältnis im Sinne des § 8 Abs. 3 Nr. 2 UWG zu der Beklagten stehen, als auch über solche, die in einem entsprechenden Wettbewerbsverhältnis zu den geförderten Drittunternehmen stehen.**
2. **Eine Influencerin, die Waren und Dienstleistungen anbietet und über ihren Auftritt in sozialen Medien (hier: Instagram) bewirbt, nimmt mit ihren in diesem Auftritt veröffentlichten Beiträgen regelmäßig geschäftliche Handlungen zugunsten ihres eigenen Unternehmens vor.**
3. **Erhält eine Influencerin für einen werblichen Beitrag in sozialen Medien eine Gegenleistung, stellt diese Veröffentlichung eine geschäftliche Handlung zugunsten des beworbenen Unternehmens dar.**
4. **Erhält eine Influencerin für einen in sozialen Medien veröffentlichten Beitrag mit Bezug zu einem Drittunternehmen keine Gegenleistung, stellt diese Veröffentlichung eine geschäftliche Handlung zugunsten des Drittunternehmens dar, wenn der Beitrag nach seinem Gesamteindruck übertrieben werblich ist, also einen werblichen Überschuss enthält, so dass die Förderung fremden Wettbewerbs eine größere als nur eine notwendigerweise begleitende Rolle spielt.**
5. **Ob ein Beitrag einer Influencerin in sozialen Medien einen zur Annahme einer geschäftlichen Handlung zugunsten eines fremden Unternehmens erforderlichen werblichen Überschuss enthält, ist aufgrund einer umfassenden Würdigung der gesamten Umstände des Einzelfalls unter Berücksichtigung des Zusammenwirkens der Gestaltungsmerkmale zu beurteilen. Der Umstand, dass die Influencerin Bilder mit „Tap Tags" versehen hat, um die Hersteller der abgebildeten Waren zu bezeichnen, genügt als solcher nicht, um einen werblichen Überschuss der Instagram-Beiträge anzunehmen. Die Verlinkung auf eine Internetseite des Herstellers des abgebildeten Produkts beinhaltet hingegen regelmäßig einen werblichen Überschuss, auch wenn auf der verlinkten Seite des Herstellers der Erwerb von Produkten nicht unmittelbar möglich ist.**
6. **Der nach § 5a Abs. 6 UWG erforderliche Hinweis auf den kommerziellen Zweck einer geschäftlichen Handlung muss so deutlich erfolgen, dass er aus der Sicht des durchschnittlich informierten, situationsadäquat aufmerksamen und verständigen Verbrauchers, der zur angesprochenen Gruppe gehört, auf den ersten Blick und zweifelsfrei hervortritt. Der im Textteil eines in sozialen Medien veröffentlichten Beitrags erscheinende Hinweis auf den kommerziellen Zweck reicht regelmäßig nicht aus, um den kommerziellen Zweck eines auf der neben dem Text angeordneten Abbildung erscheinenden „Tap Tags" als Werbung zu kennzeichnen.**
7. **Der kommerzielle Zweck eines in sozialen Medien veröffentlichten werblichen Beitrags einer Influencerin**

zugunsten eines Drittunternehmens ergibt sich nicht im Sinne des § 5a Abs. 6 UWG unmittelbar aus dem Umstand, dass die Influencerin nicht nur zu rein privaten Zwecken, sondern auch zugunsten ihres eigenen Unternehmens handelt. Es reicht nicht aus, dass sich für die Adressaten aus den Umständen überhaupt eine kommerzielle Zweckverfolgung ergibt, sondern es muss jeder mit einem Kommunikationsakt verfolgte kommerzielle Zweck erkennbar sein.

8. Das Nichtkenntlichmachen des kommerziellen Zwecks eines die Verlinkung auf die Internetseite eines Drittunternehmens enthaltenden „Tap Tags" ist regelmäßig geeignet, den Verbraucher zu einer geschäftlichen Entscheidung – das Anklicken des Links – zu veranlassen, die er andernfalls nicht getroffen hätte.

Erschütterung des Beweiswerts einer Arbeitsunfähigkeitsbescheinigung

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

Wird ein Arbeitnehmer, der sein Arbeitsverhältnis kündigt, am Tag der Kündigung arbeitsunfähig krankgeschrieben, kann dies den Beweiswert der Arbeitsunfähigkeitsbescheinigung insbesondere dann erschüttern, wenn die bescheinigte Arbeitsunfähigkeit passgenau die Dauer der Kündigungsfrist umfasst.

(Amtlicher Leitsatz)

Aus den Gründen:

1. Ein Arbeitnehmer hat nach § 3 Abs. 1 Satz 1 EFZG Anspruch auf Entgeltfortzahlung im Krankheitsfall durch den Arbeitgeber für die Zeit der Arbeitsunfähigkeit bis zur Dauer von sechs Wochen, wenn er durch Arbeitsunfähigkeit infolge Krankheit an seiner Arbeitsleistung verhindert ist, ohne dass ihn ein Verschulden trifft.

a) Nach allgemeinen Grundsätzen trägt der Arbeitnehmer die Darlegungs- und Beweislast für die Anspruchsvoraussetzungen des § 3 Abs. 1 Satz 1 EFZG (BAG 11. Dezember 2019 – 5 AZR 505/18 – Rn. 16, BAGE 169, 117).

aa) Der Beweis krankheitsbedingter Arbeitsunfähigkeit wird in der Regel durch die Vorlage einer ärztlichen Arbeitsunfähigkeitsbescheinigung iSd. § 5 Abs. 1 Satz 2 EFZG geführt. Die ordnungsgemäß ausgestellte Arbeitsunfähigkeitsbescheinigung ist das gesetzlich ausdrücklich vorgesehene und insoweit wichtigste Beweismittel für das Vorliegen krankheitsbedingter Arbeitsunfähigkeit. Nach § 7 Abs. 1 Nr. 1 EFZG reicht die Vorlage einer ärztlichen Bescheinigung iSd. § 5 Abs. 1 Satz 2 EFZG aus, um dem Arbeitgeber das Recht zur Leistungsverweigerung zu entziehen. Diese gesetzgeberische Wertentscheidung strahlt auch auf die beweisrechtliche Würdigung aus (Staudinger/Oetker [2019] § 616 Rn. 540). Der ordnungsgemäß ausgestellten Arbeitsunfähigkeitsbescheinigung kommt daher aufgrund der normativen Vorgaben im Entgeltfortzahlungsgesetz ein hoher Beweiswert zu. Der Tatrichter kann normalerweise den Beweis einer krankheitsbedingten Arbeitsunfähigkeit als erbracht ansehen, wenn der Arbeitnehmer im Rechtsstreit eine Arbeitsunfähigkeitsbescheinigung vorlegt (so die st. Rspr. vgl. BAG 26. Oktober 2016 – 5 AZR 167/16 – Rn. 17, BAGE 157, 102; 15. Juli 1992 – 5 AZR 312/91 – zu II 1 der Gründe, BAGE 71, 9; ebenso MHdB ArbR/Greiner 5. Aufl. Bd. 1 § 82 Rn. 28; MüKoBGB/Müller-Glöge 8. Aufl. EFZG § 3 Rn. 79; Reinecke DB 1989, 2069 (unter 5.1.2); ErfK/Reinhard 21. Aufl. EFZG § 5 Rn. 14; Schmitt/Küfner-Schmitt, in: Schmitt EFZG 8. Aufl. § 5 EFZG Rn. 111; NK-GA/Sievers EFZG § 5 Rn. 66 f., jeweils mwN).

bb) Die ärztliche Arbeitsunfähigkeitsbescheinigung begründet jedoch keine gesetzliche Vermutung einer tatsächlich bestehenden Arbeitsunfähigkeit iSd. § 292 ZPO mit der Folge, dass nur der Beweis des Gegenteils zulässig wäre (st. Rspr. BAG 11. August 1976 – 5 AZR 422/75 – zu 2 c der Gründe, BAGE 28, 144; 11. Oktober 2006 – 5 AZR 755/05 – Rn. 35; BGH 16. Oktober 2001 – VI ZR 408/00 – zu II der Gründe, BGHZ 149, 63; zust. MHdB ArbR/Greiner 5. Aufl. Bd. 1 § 82 Rn. 28; MüKoBGB/Müller-Glöge 8. Aufl. EFZG § 3 Rn. 79; ErfK/Reinhard 21. Aufl. EFZG § 5 Rn. 14; Schmitt/Küfner-Schmitt, in: Schmitt EFZG 8. Aufl. § 5 EFZG Rn. 111). Aufgrund des normativ vorgegebenen hohen Beweiswerts der Arbeitsunfähigkeitsbescheinigung genügt jedoch ein „bloßes Bestreiten" der Arbeitsunfähigkeit mit Nichtwissen durch den Arbeitgeber nicht, wenn der Arbeitnehmer seine Arbeitsunfähigkeit mit einer ordnungsgemäß ausgestellten Arbeitsunfähigkeitsbescheinigung nachgewiesen hat. Vielmehr kann der Arbeitgeber den Beweiswert der Arbeitsunfähigkeitsbescheinigung nur dadurch erschüttern, dass er tatsächliche Umstände darlegt und im Bestreitensfall beweist, die Zweifel an der Erkrankung des Arbeitnehmers ergeben mit der Folge, dass der ärztlichen Bescheinigung kein Beweiswert mehr zukommt. Der Arbeitgeber ist dabei nicht auf die in § 275 Abs. 1a SGB V aufgeführten Regelbeispiele ernsthafter Zweifel an der Arbeitsunfähigkeit beschränkt (MHdB ArbR/Greiner aaO Rn. 30; Staudinger/Oetker [2019] § 616 Rn. 367; ErfK/Reinhard aaO Rn. 17; Schmitt/Küfner-Schmitt, in: Schmitt aaO Rn. 124). Hierfür gibt es weder nach Wortlaut, Systematik und Zweck der Regelung, der in der Bekämpfung eines Missbrauchs der Entgeltfortzahlung im Krankheitsfall liegt (vgl. BT-Drs. 12/5263 S. 10), hinreichende Anhaltspunkte. Diese Bestimmung gibt ihm lediglich ein zusätzliches Instrument zur Erschütterung des Beweiswerts an die Hand, um einem missbräuchlichen Verhalten des Arbeitnehmers begegnen zu können. Den Beweiswert erschütternde Tatsachen können sich auch aus dem eigenen Sachvortrag des Arbeitnehmers (dazu bspw. BAG 26. Oktober 2016 – 5 AZR 167/16 – Rn. 18, BAGE 157, 102) oder aus der Arbeitsunfähigkeitsbescheinigung selbst ergeben.

cc) Bei der näheren Bestimmung der Anforderungen an die wechselseitige Darlegungslast der Parteien ist zu berücksichtigen, dass der Arbeitgeber in aller Regel keine Kenntnis von den Krankheitsursachen hat und nur in eingeschränktem Maß in der Lage ist, Indiztatsachen zur Erschütterung des Beweiswerts der Arbeitsunfähigkeitsbescheinigung vorzutragen. In Anbetracht dieser Schwierigkeiten hat das Bundesarbeitsgericht bereits erkannt, dass dem Arbeitgeber, der sich auf eine Fortsetzungserkrankung iSd. § 3 Abs. 1 Satz 2 EFZG beruft, hinsichtlich der ihn insoweit treffenden Darlegungs- und Beweislast Erleichterungen zuzubilligen sind (vgl. BAG 13. Juli 2005 – 5 AZR 389/04 – zu I 6 der Gründe, BAGE 115, 206; im Anschluss hieran BAG 10. September 2014 – 10 AZR 651/12 – Rn. 27, BAGE 149, 101). Ebenso hat es entschieden, dass in Bezug auf die vom Arbeitgeber im Rahmen von § 3 Abs. 1 Satz 1 EFZG vorzutragenden Indizien für das Vorliegen eines einheitlichen Verhinderungsfalls der Unkenntnis des Arbeitgebers von den Krankheitsursachen angemessen Rechnung zu tragen ist (vgl. BAG 11. Dezember 2019 – 5 AZR 505/18 – Rn. 20, BAGE 169,

117). Da die Vorlage der Arbeitsunfähigkeitsbescheinigung keine gesetzliche Vermutung oder eine Beweislastumkehr auslöst, dürfen an den Vortrag des Arbeitsgebers, der ihren Beweiswert erschüttern will, keine – unter Berücksichtigung seiner eingeschränkten Erkenntnismöglichkeiten – überhöhten Anforderungen gestellt werden. Der Arbeitgeber muss gerade nicht, wie bei einer gesetzlichen Vermutung, Tatsachen darlegen, die dem Beweis des Gegenteils zugänglich sind.

b) Gelingt es dem Arbeitgeber, den Beweiswert der ärztlichen Arbeitsunfähigkeitsbescheinigung zu erschüttern, so tritt hinsichtlich der Darlegungs- und Beweislast wieder derselbe Zustand ein, wie er vor Vorlage der Bescheinigung bestand. Es ist dann Sache des Arbeitnehmers, konkrete Tatsachen darzulegen und im Bestreitensfall zu beweisen, die den Schluss auf eine bestehende Erkrankung zulassen. Hierzu ist substantiierter Vortrag z.B. dazu erforderlich, welche Krankheiten vorgelegen haben, welche gesundheitlichen Einschränkungen bestanden haben und welche Verhaltensmaßregeln oder Medikamente ärztlich verordnet wurden (vgl. BAG 17. Juni 2003 – 2 AZR 123/02 – Rn. 30; 26. August 1993 – 2 AZR 154/93 – BAGE 74, 127). Der Arbeitnehmer muss also zumindest laienhaft bezogen auf den gesamten Entgeltfortzahlungszeitraum schildern, welche konkreten gesundheitlichen Beeinträchtigungen mit welchen Auswirkungen auf seine Arbeitsfähigkeit bestanden haben. Soweit er sich für die Behauptung, aufgrund dieser Einschränkungen arbeitsunfähig gewesen zu sein, auf das Zeugnis der behandelnden Ärzte beruft, ist dieser Beweisantritt nur ausreichend, wenn er die Ärzte von ihrer Schweigepflicht entbindet. Ob dies konkludent, z.B. durch die Benennung als Zeuge, geschehen kann, erscheint mit Blick auf die höchstpersönliche Natur des Schutzinteresses des Arztgeheimnisses nicht frei von Zweifeln (vgl. MüKoZPO/Damrau/Weinland 6. Aufl. § 385 Rn. 13; aA BAG 8. Mai 2014 – 2 AZR 75/13 – Rn. 40, BAGE 148, 129; Musielak/Voit/Huber ZPO 18. Aufl. § 385 Rn. 8).

2. Ausgehend hiervon hat die Klägerin die Voraussetzungen eines Anspruchs auf Entgeltfortzahlung für die streitgegenständliche Zeit nach § 3 Abs. 1 Satz 1 EFZG nicht dargetan.

a) Die Annahme des Landesarbeitsgerichts, die Klägerin sei im maßgeblichen Klagezeitraum infolge Krankheit an ihrer Arbeitsleistung verhindert gewesen, beruht auf einer fehlerhaften Würdigung des Beweiswerts der von der Klägerin vorgelegten Arbeitsunfähigkeitsbescheinigung.

aa) Grundsätzlich ist die Würdigung der Beweise gem. § 286 ZPO dem Tatrichter vorbehalten. Revisionsrechtlich ist nur zu überprüfen, ob die Beweiswürdigung in sich widerspruchsfrei und ohne Verletzung von Denkgesetzen und allgemeinen Erfahrungssätzen erfolgt ist, ob sie rechtlich möglich ist und ob das Berufungsgericht alle für die Beurteilung wesentlichen Umstände berücksichtigt hat (vgl. BAG 11. Dezember 2019 – 5 AZR 505/18 – Rn. 25, BAGE 169, 117).

bb) Dieser Überprüfung hält die Entscheidung des Landesarbeitsgerichts nicht stand. Es ist hinsichtlich der Arbeitsunfähigkeitsbescheinigung vom 8. Februar 2019 davon ausgegangen, dass sich ernsthafte Zweifel an deren Richtigkeit nicht daraus ergäben, dass sie auf der Diagnose „Sonstige und nicht näher bezeichnete Bauchschmerzen" beruhe und sich über einen Zeitraum von zwei Wochen und damit bis zum Kündigungstermin erstrecke. Die Beklagte habe keine konkreten Umstände aufgezeigt, weshalb eine solche Diagnose generell oder jedenfalls vorliegend die Krankschreibung auch mit der konkreten Dauer nicht rechtfertigen könne. Sie habe lediglich „ins Blaue" hinein behauptet, eine medizinisch begründbare Prognose für eine vierzehntägige Arbeitsunfähigkeit könne nicht vorgelegen haben. Abgesehen davon, dass sich die Arbeitsunfähigkeitsbescheinigung auf einen Zeitraum von 15 Tagen erstreckte, hat das Landesarbeitsgericht damit die Anforderungen an den arbeitgeberseitigen Vortrag zur Erschütterung des Beweiswerts der Arbeitsunfähigkeitsbescheinigung überspannt und zugleich einen von der Beklagten eingewandten und sich bereits aus der Bescheinigung selbst ergebenden wesentlichen Umstand nicht ausreichend berücksichtigt. Das Landesarbeitsgericht hat nicht genügend gewürdigt, dass die Arbeitsunfähigkeitsbescheinigung vom 8. Februar 2019, die zugleich mit der Kündigung vom 8. Februar 2019 bei der Arbeitgeberin eingereicht wurde, passgenau die nach dieser Kündigung noch verbleibende Dauer des Arbeitsverhältnisses bis zum 22. Februar 2019 abdeckte. Das Landesarbeitsgericht hat sich zwar mit der Diagnose befasst, die dem Arbeitgeber üblicherweise gar nicht bekannt sein wird, die zeitliche Koinzidenz aber außer Acht gelassen.

cc) Das Berufungsurteil unterliegt deshalb der Aufhebung (§ 562 Abs. 1 ZPO). Einer Zurückverweisung der Sache an das Landesarbeitsgericht bedarf es nicht. Da die maßgeblichen Tatsachen festgestellt sind und ergänzender Sachvortrag hierzu nicht zu erwarten ist, kann der Senat selbst entscheiden. Auf der Grundlage des festgestellten Sachverhalts ist davon auszugehen, dass der Beweiswert der vorgelegten Arbeitsunfähigkeitsbescheinigung erschüttert ist. Aufgrund der zeitlichen Koinzidenz zwischen bescheinigter Arbeitsunfähigkeit sowie Beginn und Ende der Kündigungsfrist bestehen ernsthafte Zweifel am Bestehen der Arbeitsunfähigkeit.

b) In der Folge trägt die Klägerin (wieder) die volle Darlegungs- und Beweislast für das Bestehen krankheitsbedingter Arbeitsunfähigkeit als Voraussetzung eines Entgeltfortzahlungsanspruchs nach § 3 Abs. 1 EFZG. Es wäre an ihr gewesen, konkrete Tatsachen darzulegen und im Bestreitensfall zu beweisen, die den Schluss auf eine in der streitgegenständlichen Zeit bestehende Erkrankung zulassen. Hierzu reicht ihr vom Landesarbeitsgericht festgestellter Vortrag nicht aus. Die Klägerin hat lediglich pauschal ausgeführt, es habe ein „psychosomatischer Hintergrund" bestanden. Sie sei im Einsatzbetrieb einem massiven Mobbing ausgesetzt gewesen, das zu Schlafstörungen und weiteren psychisch-körperlichen Beeinträchtigungen geführt habe und in absehbarer Zeit wahrscheinlich in ein Burn-Out eingemündet wäre. Sie hat aber keine näheren Angaben zur Intensität der von ihr geschilderten Schlafstörungen oder zur Art und vor allem Schwere der weiteren gesundheitlichen Beeinträchtigungen gemacht und auch nicht vorgetragen, dass die Beschwerden im gesamten Klagezeitraum anhielten. Es fehlte damit an substantiiertem Vortrag zu den während des streitgegenständlichen Zeitraums konkret bestehenden gesundheitlichen Beschwerden und Einschränkungen, deren Intensität und ihren Auswirkungen auf die Arbeitsfähigkeit der Klägerin für die geschuldete Tätigkeit. Die Klägerin ist damit ihrer primären Darlegungslast zu einer im Klagezeitraum objektiv bestehenden krankheitsbedingten Arbeitsunfähigkeit nicht nachgekommen.

II. Das Landesarbeitsgericht hat die Klägerin zwar – folgerichtig – nicht auf die Erschütterung des Beweiswerts der von ihr vorgelegten Arbeitsunfähigkeitsbescheinigung und die sich daraus ergebenden Anforderungen an ihren Sachvortrag hingewiesen. Der Senat kann dennoch nach § 563 Abs. 3 ZPO abschließend entscheiden, weil die Klägerin – trotz entsprechender Hinweise während des Revisionsverfahrens – keine ordnungsgemäß begründete verfahrensrechtliche Gegenrüge erhoben hat. Ein Verstoß des Landesarbeitsgerichts gegen die Hinweispflicht aus § 139 Abs. 3 ZPO kann deshalb in der Revision nicht berücksichtigt werden, § 557 Abs. 3 Satz 2, § 551 Abs. 3 Satz 1 Nr. 2 Buchst. b ZPO (BAG 23. März 2016 – 5 AZR 758/13 – Rn. 39, BAGE 154, 337).

1. Die Klägerin war als Revisionsbeklagte nicht gehindert, wegen einer Verletzung der Hinweispflicht durch das Landesarbeitsgericht bis zum Schluss der mündlichen Verhandlung vor dem Revisionsgericht eine auf § 139 Abs. 3 ZPO gestützte Verfahrensrüge („Gegenrüge") zu erheben (vgl. BAG 23. März 2016 – 5 AZR 758/13 – Rn. 39 mwN, BAGE 154, 337).

2. Sie hat jedoch – trotz entsprechenden Hinweises des Senats – keine ausreichend begründete verfahrensrechtliche Gegenrüge nach § 551 Abs. 3 Satz 1 Nr. 2 Buchst. b ZPO erhoben.

a) Besteht ein Verfahrensmangel darin, dass das Landesarbeitsgericht den Anspruch auf rechtliches Gehör verletzt hat, weil es der Hinweispflicht aus § 139 Abs. 3 ZPO nicht nachgekommen ist, muss konkret dargelegt werden, welchen Hinweis das Gericht hätte geben müssen und welche Reaktion auf einen entsprechenden Hinweis erfolgt wäre (BAG 18. September 2014 – 6 AZR 145/13 – Rn. 34). Wer die Verletzung des § 139 ZPO durch das Berufungsgericht rügt, muss im Einzelnen vortragen, was er auf einen entsprechenden Hinweis vorgebracht hätte. Der zunächst unterbliebene Vortrag muss vollständig nachgeholt und über die Rüge aus § 139 ZPO schlüssig gemacht werden. Hierzu ist vorzutragen, welcher tatsächliche Vortrag gehalten oder welche für die Entscheidung erheblichen rechtlichen Ausführungen gemacht worden wären (vgl. BAG 16. Dezember 2010 – 2 AZR 770/09 – Rn. 10; 16. Oktober 2013 – 10 AZR 9/13 – Rn. 46). Nur so kann das Revisionsgericht feststellen, ob die gerügte Verletzung für das Urteil kausal war (BAG 24. März 2009 – 9 AZR 983/07 – Rn. 32, BAGE 130, 119; 19. Oktober 2010 – 6 AZR 120/10 – Rn. 24).

b) Derartiger Vortrag der Klägerin ist – auch auf entsprechenden Hinweis – nicht erfolgt. Sie hat sich im Wesentlichen lediglich auf ihren zuvor erfolgten, nicht ausreichenden Vortrag berufen. Konkreten Vortrag zu den während des Zeitraums, für den Entgeltfortzahlung verlangt wird, im Einzelnen bestehenden gesundheitlichen Beschwerden und Einschränkungen, deren Intensität und ihren Auswirkungen auf ihre Arbeitsfähigkeit hat sie weiterhin nicht gehalten.

III. Die Rechtsprechung des Gerichtshofs der Europäischen Union zur Bindungswirkung von in einem Mitgliedstaat der Europäischen Union von der dort zuständigen Stelle (vgl. Art. 27 Abs. 5 der Verordnung (EG) Nr. 987/2009 i.V.m. Art. 1 der Verordnung (EG) Nr. 883/2004, vormals Art. 18 Abs. 3 der Verordnung (EWG) Nr. 574/72 iVm. Art. 1 der Verordnung (EWG) Nr. 1408/71) getroffenen ärztlichen Feststellungen über den Eintritt und die Dauer der Arbeitsunfähigkeit (EuGH 3. Juni 1992 – C-45/90 –; 2. Mai 1996 – C-206/94 –) und die sich daraus ergebenden Folgen für die Verteilung der Darlegungs- und Beweislast im Entgeltfortzahlungsprozess (vgl. dazu BAG 19. Februar 1997 – 5 AZR 747/93 – BAGE 85, 140) zwingen nicht zu einer Änderung der Grundsätze der Überprüfung inländischer Arbeitsunfähigkeitsbescheinigungen. Liegen von der im EU-Ausland ansässigen zuständigen Stelle getroffene ärztliche Feststellungen zur Arbeitsunfähigkeit vor, trägt der Arbeitgeber nach Auffassung des Gerichtshofs die Beweislast dafür, dass der Arbeitnehmer entgegen diesen Feststellungen nicht arbeitsunfähig krank war. Es reicht dann – anders als bei im Inland ausgestellten Arbeitsunfähigkeitsbescheinigungen – nicht aus, dass der Arbeitgeber Umstände beweist, die nur zu ernsthaften Zweifeln an der krankheitsbedingten Arbeitsunfähigkeit Anlass geben.

Hierin liegt im Verhältnis zu den oben angewandten Grundsätzen, wie sie für im Inland ausgestellte Arbeitsunfähigkeitsbescheinigungen gelten, keine mit Art. 3 Abs. 1 GG nicht vereinbare Ungleichbehandlung. Eine Bescheinigung nach Art. 27 Abs. 5 der Verordnung (EG) Nr. 987/2009 (vormals Art. 18 Abs. 3 der Verordnung (EWG) Nr. 574/72) enthält Feststellungen, die aufgrund einer von der im EU-Ausland zuständigen Stelle angeordneten oder durchgeführten ärztlichen Kontrolluntersuchung getroffen wurden. Dieser Unterschied zu einer Arbeitsunfähigkeitsbescheinigung iSv. § 5 Abs. 1 EFZG rechtfertigt die unterschiedliche beweisrechtliche Behandlung der Bescheinigungen (ebenso MüKoBGB/Müller-Glöge 8. Aufl. EFZG § 3 Rn. 84; Staudinger/Oetker [2019] § 616 Rn. 550; Schmitt/Küfner-Schmitt, in: Schmitt EFZG 8. Aufl. § 5 EFZG Rn. 128; aA Wedde/Kunz EFZG 4. Aufl. § 5 EFZG Rn. 47).

Darüber hinaus erscheint es fraglich, ob überhaupt eine grundrechtlich relevante Ungleichbehandlung vergleichbarer Sachverhalte angenommen werden kann. Denn auch ein im Inland arbeitender EU-Ausländer, der im Inland erkrankt, wird bei Vorlage einer inländischen Arbeitsunfähigkeitsbescheinigung behandelt wie ein Inländer mit einer entsprechenden Bescheinigung. Ebenso erfährt ein Inländer, wenn er – z.B. im Urlaub – im in der Europäischen Union gelegenen Ausland erkrankt, die gleiche Behandlung wie ein im Inland arbeitender EU-Ausländer, wenn er eine Bescheinigung nach Art. 27 Abs. 5 der Verordnung (EG) Nr. 987/2009 vorlegt. Die besonderen Beweisschwierigkeiten des anspruchsberechtigten Arbeitnehmers, mit denen der Gerichtshof der Europäischen Union die Bindung des Arbeitgebers an die vom Träger des Wohn- oder Aufenthaltsorts getroffenen ärztlichen Feststellungen begründet, hängen mit der Erkrankung im Ausland zusammen. Diese Sachverhalte sind mit Fällen einer Erkrankung im Inland und dort ausgestellter Arbeitsunfähigkeitsbescheinigung nicht vergleichbar.

Vorlagebeschluss: Verarbeitung von Gesundheitsdaten im Arbeitsverhältnis (Ls)

(**Bundesarbeitsgericht**, Beschluss vom 26. August 2021 – 8 AZR 253/20(A) –)

Der Gerichtshof der Europäischen Union wird gemäß Art. 267 AEUV um Vorabentscheidung über die Fragen ersucht:

1. **Ist Art. 9 Abs. 2 Buchstabe h der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung; im Folgenden DS-GVO) dahin auszulegen, dass es einem Medizinischen Dienst einer Krankenkasse untersagt ist, Gesundheitsdaten seines Arbeitnehmers, die Voraussetzung für die Beurteilung der Arbeitsfähigkeit dieses Arbeitnehmers sind, zu verarbeiten?**

2. **Für den Fall, dass der Gerichtshof die Frage zu 1. verneinen sollte mit der Folge, dass nach Art. 9 Abs. 2 Buchstabe h DS-GVO eine Ausnahme von dem in Art. 9 Abs. 1 DS-GVO bestimmten Verbot der Verarbeitung von Gesundheitsdaten in Betracht käme: Sind in einem Fall wie hier über die in Art. 9 Abs. 3 DS-GVO bestimmten Maßgaben hinaus weitere, gegebenenfalls welche Datenschutzvorgaben zu beachten?**

3. **Für den Fall, dass der Gerichtshof die Frage zu 1. verneinen sollte mit der Folge, dass nach Art. 9 Abs. 2 Buchstabe h DS-GVO eine Ausnahme von dem in Art. 9 Abs. 1 DS-GVO bestimmten Verbot der Verarbeitung**

von Gesundheitsdaten in Betracht käme: Hängt in einem Fall wie hier die Zulässigkeit bzw. Rechtmäßigkeit der Verarbeitung von Gesundheitsdaten zudem davon ab, dass mindestens eine der in Art. 6 Abs. 1 DS-GVO genannten Voraussetzungen erfüllt ist?

4. **Hat Art. 82 Abs. 1 DS-GVO spezial- bzw. generalpräventiven Charakter und muss dies bei der Bemessung der Höhe des zu ersetzenden immateriellen Schadens auf der Grundlage von Art. 82 Abs. 1 DS-GVO zulasten des Verantwortlichen bzw. Auftragsverarbeiters berücksichtigt werden?**

5. **Kommt es bei der Bemessung der Höhe des zu ersetzenden immateriellen Schadens auf der Grundlage von Art. 82 Abs. 1 DS-GVO auf den Grad des Verschuldens des Verantwortlichen bzw. Auftragsverarbeiters an? Insbesondere, darf ein nicht vorliegendes oder geringes Verschulden auf Seiten des Verantwortlichen bzw. Auftragsverarbeiters zu dessen Gunsten berücksichtigt werden?**

Weg vom Bett ins Homeoffice ist gesetzlich unfallversichert (Ls)

(**Bundessozialgericht**, Urteil vom 8. Dezember 2021 – B 2 U 4/21 R –)

Ein Beschäftigter, der auf dem morgendlichen erstmaligen Weg vom Bett ins Homeoffice stürzt, ist durch die gesetzliche Unfallversicherung geschützt; Sofern das Beschreiten der Treppe ins Homeoffice allein der erstmaligen Arbeitsaufnahme dient, ist es als Verrichtung im Interesse des Arbeitgebers als Betriebsweg versichert.

(Nicht amtlicher Leitsatz)

Auskunftsrecht nach Art. 15 DS-GVO und Immaterieller Schadensersatz nach Art. 82

(**Landesarbeitsgericht Niedersachsen**, Urteil vom 22. Oktober 2021 – 16 Sa 761/20 –)

Wenn der Auskunftsverpflichtung nach Art. 15 DS-GVO zeitlich und inhaltlich nicht hinreichend nachgekommen wird und der Betroffene keine zeitgerechten, ausreichenden Kenntnisse über die Verarbeitung seiner personenbezogenen Daten erlangt und damit einen Kontrollverlust erleidet, der ihm die Möglichkeit der Überprüfung der Rechtmäßigkeit der Verarbeitung seiner personenbezogenen Daten unmöglich macht oder erschwert, liegt ein entschädigungsplichtiger immaterieller Schaden ge-mäß Art. 82 DS-GVO vor.

(Nicht amtlicher Leitsatz)

Aus den Gründen:

Es liegt zudem ein kausaler, immaterieller Schaden vor. Es ist hierbei von einem weiten Schadensverständnis auszugehen.

(a)

Der Schadensbegriff wird in Rechtsprechung und Literatur nicht einheitlich beantwortet.

So verlange Erwägungsgrund 146 S. 3 eine weite Auslegung des Schadensbegriffs im Lichte der Rspr. des EuGH, die den Zielen der DS-GVO in vollem Umfang entspricht (vgl. BVerfG 14. Januar 2021 – 1 BvR 2853/19 – Rn. 19; ArbG Neumünster, 11. August 2020 – 1 Ca 247 c/20 – Rn. 38). Die Forderung einer schwerwiegenden Persönlichkeitsrechtsverletzung vertrage sich nicht mit Art. 82 DS-GVO, da sie weder von dessen Ziel und Entstehungsgeschichte gedeckt sei (LG Lüneburg 14. Juli 2020 – 9 O 145/19 – Rn. 49), dies wirke sich nur noch bei der Höhe des Anspruchs aus (vgl. ArbG D-Stadt 5. März 2020 – 9 Ca 6557/18 – Rn. 84, m.w.N). Ein immaterieller Schaden entstehe auch, wenn die betroffene Person um ihre Rechte und Freiheiten gebracht oder daran gehindert ist, die sie betreffenden personenbezogen Daten zu kontrollieren (vgl. ArbG Dresden 26. August 2020 – 13 Ca 1046/20 – Rn. 14). Weder der DS-GVO noch ihren Erwägungsgründen lasse sich entnehmen, dass der Schadensersatzanspruch einen qualifizierten Verstoß gegen die DS-GVO voraussetzt. Für die Annahme einer Erheblichkeitsschwelle oder anders – herum formuliert – die Ausnahme von Bagatellfällen, gebe es keinen Anhaltspunkt (vgl. LAG Hamm 11. Mai 2021 – 6 Sa 1260/20 – Rn. 50). Soweit es nicht um reine Formfehler wie Verstöße gegen Dokumentationspflichten geht, gehe mit der Verletzung datenschutzrechtlicher Normen letztlich immer ein immaterieller Schaden einher (vgl. Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18a). Erwägungsgrund 146 S. 6 spreche gegen die Einschränkung des Entschädigungsanspruchs auf schwere Beeinträchtigungen, die Schwere der Beeinträchtigung sei nur bei der Frage der Höhe des Anspruchs zu berücksichtigen, wobei Bagatellfälle außer Betracht bleiben können (vgl. Gola DS-GVO/Gola/Piltz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 13). Damit könne eine betroffene Person nun mehr für jede Verletzung der DS-GVO durch Verarbeitung ihrer personenbezogenen Daten auch ein angemessenes Schmerzensgeld verlangen (vgl. Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 13).

Nach anderer Meinung führe nicht jeder Verstoß zu einem Schadensersatzanspruch. Allein die Verletzung des Datenschutzrechts als solche begründe nicht bereits für sich gesehen einen Schadensersatzanspruch für betroffene Personen. Die Verletzungshandlung müsse in jedem Fall auch zu einer konkreten, nicht nur unbedeutenden oder empfundenen Verletzung von Persönlichkeitsrechten der betroffenen Person geführt haben (vgl. LG Landshut 6. November 2020 – 51 O 513/20 – Rn. 18). Die Anwendung von Strafschadenersatz sei aufgrund Art. 82 nicht zugelassen (vgl. Spindler/Schuster/Spindler/Horváth, 4. Aufl. 2019, DS-GVO Art. 82 Rn. 8). Daher werde man im Grundsatz weiterhin davon ausgehen können, dass immaterielle Schäden im vorliegenden Zusammenhang nur entstehen, wenn das allgemeine Persönlichkeitsrecht der betroffenen Person nicht unerheblich verletzt wurde (vgl. EuArbRK/Franzen, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 22). Es müsse auch bei einem immateriellen Schaden eine Beeinträchtigung eingetreten sein, die unabhängig von einer Erheblichkeitsschwelle wenigstens spürbar sein muss. Andernfalls scheide ein „Schaden" begrifflich schon aus (vgl. LG Bonn 1. Juli 2021 – 15 O 372/20 – Rn. 42). Der Schaden müsse – wie auch der Anwendungsbereich mancher Norm des EU-Rechts – weit verstanden werden; gleichwohl muss er „erlitten" (ErwGr 146 S. 6), maW „spürbar", objektiv nachvollziehbar, von gewissem Gewicht sein (vgl. Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 10).

(b)

Die Kammer folgt den Erwägungen, wonach unabhängig von dem Erreichen einer Erheblichkeitsschwelle bei Verstößen gegen Regelungen der DS-GVO ein immaterieller Schadensersatz in Betracht kommt. Hierbei ist zu berücksichtigen, dass gerade ausgehend von Erwägungsgrund 146 Satz 3 eine weite Auslegung geboten ist, um den Zielen der Verordnung in vollem Umfang zu entsprechen. Hiermit wäre es unvereinbar, würde eine Schadensersatzpflicht nur bei erheblichen Rechtsverstößen eintreten, da dann eine Vielzahl von Fallgestaltungen denkbar wäre, in denen Betroffene trotz Verstößen gegen die Regelungen der DS-GVO keine Kompensation erhielten. Ferner kann, um die Regelungen der DS-GVO effektiv durchzusetzen, auch auf eine abschreckende Wirkung des Schadensersatzes abgestellt werden (vgl. EuGH 17. Dezember 2015 – C-407/14 – Rn. 44). Zudem sollen die betroffenen Personen nach Erwägungsgrund 146 Satz 3 einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Dass ein Schaden erlitten ist, ergibt sich nicht erst bei Überschreiten einer gewissen Erheblichkeitsschwelle – der Schwere der Pflichtverstöße und damit einhergehenden Beeinträchtigungen kann vielmehr effektiv auf Ebene der Höhe des Schadensersatzes begegnet werden.

Indem die Beklagte ihrer Auskunftsverpflichtung zeitlich und inhaltlich nicht hinreichend nachgekommen ist, hat der Kläger keine zeitgerechten, ausreichenden Kenntnisse über die Verarbeitung seiner personenbezogenen Daten erlangt – insofern ist ein Kontrollverlust eingetreten und ihm wird die Möglichkeit der Überprüfung der Rechtmäßigkeit der Verarbeitung seiner personenbezogenen Daten unmöglich gemacht oder erschwert.

(6)

Dem Kläger ist in Anbetracht der Pflichtverstöße der Beklagten nach richterlichem Ermessen gem. § 287 Abs. 1 ZPO ein immaterieller Schadensersatz in Höhe von 1.250,-- Euro zuzusprechen.

(a)

Den Schadensersatzansprüchen soll generell eine Abschreckungswirkung innewohnen (Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 10, mwN).). Unter Berücksichtigung des Erwägungsgrundes 146 (Satz 6) zur DS-GVO soll die betroffene Person einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten (LAG Hamm 11. Mai 2021 – 6 Sa 1260/20 – Rn. 50). Verstöße müssen effektiv sanktioniert werden. Schadenersatz bei Datenschutzverstößen sollen eine abschreckende Wirkung haben, um der Datenschutzgrundverordnung zum Durchbruch zu verhelfen (effet utile) (ArbG Dresden 26. August 2020 – 13 Ca 1046/20 – Rn. 16).

(b)

Gemessen an der Zweckrichtung des Schadensersatzes hält die Kammer unter Berücksichtigung und Abwägung der Umstände des vorliegenden Falls einen immateriellen Schadensersatz in Höhe von 1.250,– Euro angemessen, aber auch ausreichend. Hierbei ist zu berücksichtigen, dass die verspätete Auskunft der Beklagten erfolgte, weil sie nicht innerhalb des ersten Monats die Inanspruchnahme der Verlängerung um zwei Monate begründet mitteilte. Im Ergebnis wurde die Auskunft jedoch innerhalb von gut zwei Monaten nach Geltendmachung des Auskunftsbegehrens und somit noch vor dem Ablauf von drei Monaten erteilt, die der Gesetzgeber dem Verantwortlichen grundsätzlich maximal zubilligt. Hierbei ist auch zu berücksichtigen, dass der Kläger im September 2018 sein Begehren präzisierte und die Beklagte dem in ihrer Antwort Rechnung trug. Andererseits ist erkennbar, dass der Beklagten die einmonatige Frist durchaus bewusst war, da deren Prozessbevollmächtigte im Schreiben vom 20.08.2018 mitteilte, dass eine Erledigung innerhalb dieser Frist erfolgen würde. Insgesamt ist in Anbetracht dieser Gesamtumstände, die dazu führten, dass der Kläger nur für einen vergleichsweise kurzen Zeitraum nach Antragstellung über die Datenverarbeitung im Unklaren war, ein immaterieller Schadensersatz von 250,– Euro zuzuerkennen. Schwerer wiegt demgegenüber der Verstoß gegen Art. 15 Abs. 1 DS-GVO. Da durch die unzureichende Auskunft der Erkenntnisgewinn des Klägers über die Verarbeitung seiner personenbezogenen Daten nicht umfassend war und die Beklagte hierfür keine ausreichend nachvollziehbare Begründung angeben konnte, erscheint der Kammer ein Schadensersatz in Höhe von 1.000,– Euro angemessen. Hierdurch wird ausreichend sichergestellt, dass durch die Zahlung eines spürbaren Betrages der Regelung des Art. 15 DS-GVO zur Geltung verholfen wird und die Verpflichteten angehalten werden, die entsprechenden Maßgaben einzuhalten. In die Überlegung einzustellen ist, dass die Beklagte nicht versehentlich die Auskunft hinsichtlich bestimmter Informationen mit personenbezogenen Daten unterlassen hat, sondern diese bewusst zurückgehalten hat, ohne dass ein Grund hierfür nachvollziehbar dargelegt wurde. Anzuknüpfen ist hierbei nach Sicht der Kammer weder an den Verdienst des Klägers noch die finanzielle Leistungsfähigkeit der Beklagten, da beide Komponenten in keinem Zusammenhang mit den datenschutzrechtlichen Verstößen stehen.

D.

Gründe für eine Revisionszulassung nach § 72 Abs. 2 ArbGG bestanden nur teilweise.

I.

Eine Zulassung hatte zu erfolgen, soweit datenschutzrechtliche Ansprüche des Klägers betroffen waren. Insoweit liegt eine grundsätzliche Bedeutung iSd. § 72 Abs. 2 Nr. 2 ArbGG vor, da die Voraussetzungen des Geldentschädigungsanspruchs nach Art. 82 Abs. 1 DS-GVO und das Verständnis dieser Vorschrift bislang nicht höchstrichterlich geklärt ist und sich nicht unmittelbar aus den Regelungen der DS-GVO ergibt (vgl. auch BVerfG 14. Januar 2021 – 1 BvR 2853/19 – Rn. 20). Auch die Frage der Einschränkungen nach §§ 29, 34 BDSG und Art. 15 Abs. 4 DS-GVO und die Reichweite des Art. 15 Abs. 3 DS-GVO sind solche grundsätzlicher Bedeutung.

Offenlegung von Gesundheitdaten im Betrieblichen Eingliederungs-Management

(**Landesarbeitsgericht Baden-Württemberg**, Urteil vom 20. Oktober 2021 – 4 Sa 70/20 –)

1. **Aus § 167 Abs. 2 Satz 3 SGB IX (in der bis zum 09.06.2021 geltenden Fassung, seit 10.06.2021: Satz 4) folgt nicht nur, dass der Arbeitnehmer auf die Art und den Umfang der im betrieblichen Eingliederungsmanagement (bEM) erhobenen und verwendeten Daten hinzuweisen ist. Vielmehr ergibt sich hieraus auch, dass die Datenverarbeitung datenschutzkonform zu erfolgen hat.**

2. **Die Erreichung der Ziele des bEM erfordert nicht, dass nicht im bEM-Verfahren beteiligten Vertretern des Arbeitgebers vom Arbeitnehmer im Verfahren mitge-**

teilte Diagnosedaten bekanntzumachen wären. Wenn dem Arbeitnehmer im Rahmen des § 167 Abs. 2 Satz 3 SGB IX (in der bis zum 09.06.2021 geltenden Fassung, seit 10.06.2021: Satz 4) dennoch eine Einwilligung in eine solche Datenoffenlegung abverlangt wird, ist im besonderen Maße auf die Freiwilligkeit hinzuweisen.

3. **Wird in dem Hinweis über die Datenerhebung und Datenverwendung der fälschliche Eindruck erweckt, dass Gesundheitsdaten an Vertreter des Arbeitgebers weitergegeben werden können, die nicht am bEM-Verfahren beteiligt sind, geht dies zu Lasten des Arbeitgebers. Die vom Arbeitgeber verursachte Fehlvorstellung steht einer ordnungsgemäßen Einleitung des bEM entgegen.**

(Bestätigung und Fortentwicklung von LAG Baden-Württemberg 28.07.2021 – 4 Sa 68/20 –)

Tenor:

1. Die Berufung der Beklagten gegen das Urteil des Arbeitsgerichts Reutlingen vom 19.11.2020 (1 Ca 108/20) wird zurückgewiesen.
2. Die Beklagte hat die Kosten der Berufung zu tragen.
3. Die Revision wird zugelassen.

Tatbestand:

Die Parteien streiten über die Wirksamkeit einer ordentlichen arbeitgeberseitigen, krankheitsbedingten Kündigung des Arbeitsverhältnisses des Klägers sowie hilfsweise über eine Weiterbeschäftigung des Klägers.

Der am 00.00.0000 geborene, ledige und kinderlose Kläger ist bei der Beklagten in deren Betrieb in R. seit 11. August 2014 beschäftigt als Produktionsfacharbeiter (EG 7 ERA) zu einem durchschnittlichen Bruttomonatsentgelt iHv. zuletzt 3.442,73 Euro.

Die Beklagte beschäftigt in ihrem Betrieb in R. ca. 8.000 Mitarbeiter. Ein Betriebsrat ist in diesem Betrieb gebildet.

Die Beklagte kündigte das Arbeitsverhältnis mit dem Kläger mit Schreiben vom 5. März 2020, dem Kläger am selben Tag zugegangen, ordentlich zum 30. Juni 2020. Gegen diese Kündigung richtet sich die vorliegende Kündigungsschutzklage, die am 25. März 2020 beim Arbeitsgericht einging.

Die Beklagte stützt die Kündigung auf krankheitsbedingte Gründe.

Der Kläger war im Jahr 2016 an insgesamt 31,7 Arbeitstagen, im Jahr 2017 an insgesamt 51 Arbeitstagen, im Jahr 2018 an insgesamt 42 Arbeitstagen und im Jahr 2019 an insgesamt 43 Arbeitstagen arbeitsunfähig krank. Für sämtliche Fehltage war die Beklagte entgeltfortzahlungspflichtig. Im Jahr 2020 bis zum Ausspruch der Kündigung war der Kläger erneut arbeitsunfähig krank von 6. Januar bis 10. Januar 2020. Auch hierfür hatte die Beklagte Entgeltfortzahlung zu leisten.

Die Beklagte hat den Kläger mit Schreiben vom 20. Januar 2020 (Bl. 58 und 59 der arbeitsgerichtlichen Akte) zu einem betrieblichen Eingliederungsmanagement (bEM) eingeladen. Auf diese Einladung hat der Kläger, wie auch schon auf vergangene Einladungen, nicht reagiert.

Bei der Beklagten besteht eine zwischen ihr und dem Gesamtbetriebsrat abgeschlossene Betriebsvereinbarung über das betriebliche Eingliederungsmanagement (BV-bEM) (Bl. 110-115 der arbeitsgerichtlichen Akte), ergänzt durch eine zwischen der Beklagten und dem örtlichen Betriebsrat R. abgeschlossene „Vereinbarung zum BEM-Verfahren am Standort R." (Bl. 116 der arbeitsgerichtlichen Akte). Zu den Beteiligten des bEM heißt es in der BV-bEM auszugsweise:

3. Beteiligte

3.1 Betriebliches Eingliederungsteam

Das betriebliche Eingliederungsteam (BET) besteht aus benannten Vertretern der Personalabteilung, des Betriebsrats, der Schwerbehindertenvertretung, des MED und des HSS. Der angeschriebene Mitarbeiter kann zusätzlich zum betreuenden HR BP aus den Mitgliedern des BET grundsätzlich eine weitere Person hinzuziehen.

3.2 Integrationsteam

Wenn Anpassungen des Arbeitsplatzes, -prozesses oder der -bedingungen erforderlich sind, kann das Integrationsteam – sofern vorhanden – hinzugezogen werden. Hierfür ist das Einverständnis des MA notwendig (Anlage 4). Erteilt der MA sein Einverständnis nicht, führt das BET das BEM mit den dem BET möglichen Maßnahmen fort. Das Integrationsteam besteht aus Vertretern des Betriebsrats, der Schwerbehindertenvertretung, der Arbeitsplanung, der örtlichen Standortleitung, dem Arbeitgeberbeauftragten für Schwerbehinderte, HRL, MED, HSS, HSE.

Ausweislich Nr. 10 der BV-bEM ist dem Einladungsschreiben grundsätzlich zugleich eine Datenschutzerklärung entsprechend einer Anlage 3c (Bl. 89 der LAG-Akte) beizufügen. In dieser Anlage heißt es auszugsweise:

„Ich bin damit einverstanden, dass die Angaben, die im Rahmen des BEM erhoben werden, den am Prozess Beteiligten (insbesondere dem betrieblichen Eingliederungsteam (BET) und ggf. dem Vorgesetzten, dem Übersetzer, und bei erforderlichen Veränderungen des Arbeitsplatzes HSE, TEF, Standortleitung) bekannt gemacht werden. Zweck der Datenerhebung ist es, Arbeitsunfähigkeit zu überwinden und/oder erneuter Arbeitsunfähigkeit vorzubeugen sowie den Arbeitsplatz zu erhalten."

Der Betriebsrat wurde zur beabsichtigten Kündigung angehört mit Anhörungsschreiben vom 17. Februar 2020 (Bl. 62-66 der arbeitsgerichtlichen Akte).

Der Kläger hielt die Kündigung für unwirksam.

Er meinte, ihm könne schon keine negative Gesundheitsprognose gestellt werden. Diverse Krankheitsbilder seien wegen Ausheilung nicht prognosefähig.

Er rügte die Ordnungsgemäßheit der bEM-Einleitung. Er behauptete hierbei, die im Einladungsschreiben benannten Anlagen (Antwortschreiben, Datenschutzunterrichtung und Liste der BET-Mitglieder) nicht erhalten zu haben.

Er rügte zudem die Ordnungsgemäßheit der Betriebsratsanhörung. Er bestritt mit Nichtwissen, dass dem Betriebsrat als Anhang zum Anhörungsschreiben eine Fehlzeitenaufstellung vorgelegt worden sei.

Der Kläger beantragte:

1. Es wird festgestellt, dass das Arbeitsverhältnis der Parteien durch die Kündigung der Beklagten vom 05.03.2020 nicht beendet wird.

2. Im Falle des Obsiegens mit dem Antrag zu 1 wird die Beklagte verurteilt, den Kläger bis zum rechtskräftigen Abschluss des Kündigungsschutzverfahrens zu unveränderten arbeitsvertraglichen Bedingungen weiterzubeschäftigen.

Die Beklagte beantragt, die Klage abzuweisen.

Die Beklagte vertrat die Auffassung, dem Kläger müsse eine negative Gesundheitsprognose gestellt werden. Angesichts der Entgeltfortzahlungsbelastungen sei ihr eine Weiterbeschäftigung nicht mehr zumutbar.

Das bEM sei ordnungsgemäß eingeleitet worden. Die benannten Anlagen seien beigefügt gewesen.

Der Betriebsrat sei ordnungsgemäß angehört worden. Die Fehlzeitenliste sei dem Betriebsrat ebenfalls vorgelegt worden.

Das Arbeitsgericht hat mit Urteil vom 19. November 2020 festgestellt, dass das Arbeitsverhältnis nicht durch die streitgegenständliche Kündigung aufgelöst wurde. Die Beklagte wurde zur Weiterbeschäftigung des Klägers verurteilt. Das Arbeitsgericht schloss einzelne Fehlzeiten aus der Prognosefähigkeit aus und kam zum Ergebnis, dass die weiterhin verbleibende geringfügige Überschreitung des Sechswochenzeitraumes von Arbeitsunfähigkeitszeiten pro Kalenderjahr nicht so gravierend sei, um eine Unzumutbarkeit der Weiterbeschäftigung des Klägers begründen zu können. Jedenfalls sei es nicht davon überzeugt, dass eine sich bereits anbahnende Abnahme der Fehlzeiten keine Fortsetzung finden könne.

Dieses Urteil wurde der Beklagten am 30. November 2020 zugestellt. Hiergegen richtet sich die vorliegende Berufung der Beklagten, die am 22. Dezember 2020 beim Landesarbeitsgericht einging und innerhalb der bis 1. März 2021 verlängerten Begründungsfrist am 26. Februar 2021 begründet wurde.

Die Beklagte hält das Urteil für fehlerhaft.

Sie meint, insbesondere die Erkrankung des Klägers wegen eines Impingementsyndroms aus dem Jahr 2017 hätte nicht aus der Prognosebeurteilung ausgeschieden werden dürfen. Die vom Arbeitsgericht angenommene Abnahme von Fehlzeiten sei im Tatsächlichen nicht erkennbar.

Die Beklagte beantragt:

Das Urteil des Arbeitsgerichts Reutlingen vom 19. November 2020 (1 Ca 108/20) wird abgeändert.

Die Klage wird abgewiesen.

Der Kläger beantragt, die Berufung zurückzuweisen.

Er verteidigt das arbeitsgerichtliche Urteil unter Wiederholung und Vertiefung seines erstinstanzlichen Vorbringens.

Wegen der weiteren Einzelheiten des Sach- und Streitstands wird gem. § 64 Abs. 6 ArbGG iVm. § 313 Abs. 2 Satz 2 ZPO auf den Inhalt der zwischen den Parteien gewechselten Schriftsätze nebst Anlagen sowie auf das Protokoll der mündlichen Verhandlung verwiesen.

Entscheidungsgründe:

Die statthafte, form- und fristgerecht eingelegte und begründete und auch im Übrigen zulässige Berufung der Beklagten ist nicht begründet.

I.

Das Arbeitsgericht hat zumindest im Ergebnis zu Recht der Kündigungsschutzklage stattgegeben.

Das Arbeitsverhältnis zwischen den Parteien wurde nicht durch die streitgegenständliche Kündigung aufgelöst. Die Kündigung ist nicht sozial gerechtfertigt iSd. § 1 Abs. 2 KSchG.

1. Die Wirksamkeit einer auf häufige Kurzerkrankungen gestützten ordentlichen Kündigung setzt zunächst eine negative Gesundheitsprognose voraus. Im Kündigungszeitpunkt müssen objektive Tatsachen vorliegen, die die Besorgnis weiterer Erkrankungen im bisherigen Umfang befürchten lassen. Häufige Kurzerkrankungen in der Vergangenheit können indiziell für eine entsprechende künftige Entwicklung sprechen (erste Stufe). Die prognostizierten Fehlzeiten sind nur dann geeignet, eine krankheitsbedingte Kündigung zu rechtfertigen, wenn sie zu einer erheblichen Beeinträchtigung der betrieblichen Interessen führen. Dabei können neben Betriebsablaufstörungen auch wirtschaftliche Belastungen, etwa durch zu erwartende, einen Zeitraum von mehr als sechs Wochen pro Jahr übersteigende Entgeltfortzahlungskosten, zu einer solchen Beeinträchtigung führen (zweite Stufe). Ist dies der Fall, ist im Rahmen der gebotenen Interessenabwägung zu prüfen, ob die Beeinträchtigungen vom Arbeitgeber billigerweise nicht mehr hingenommen werden müssen (dritte Stufe) (BAG 24. April 2018 – 2 AZR 6/18 –; BAG 16. Juli 2015 – 2 AZR 15/15 –; BAG 20. November 2014 – 2 AZR 755/13 –).

2. Dem Kläger kann auf der ersten Stufe eine negative Gesundheitsprognose gestellt werden.

a) Der Kläger war im Jahr 2016 an insgesamt 31,7 Arbeitstagen arbeitsunfähig krank. Zu den diesen Fehlzeiten zugrunde liegenden Diagnosen oder deren Ausheilung trug der Kläger nichts vor. Soweit sich aus der vorgelegten Diagnosenaufstellung der Krankenkasse Erkrankungen wegen lumbaler Bandscheibenschäden, Radikulopathie, Tonsillitis, chronisch-obstruktive Lungenkrankheit und Gastroenteritis/Kolitis ergeben, ist nicht ersichtlich, weshalb diese Erkrankungen dauerhaft und ohne Wiederholungsmöglichkeiten ausgeheilt sein sollten.

b) Zugunsten des Klägers kann davon ausgegangen werden, dass die Erkrankung wegen eines Impingementsyndroms ausgeheilt ist. Jedenfalls ist ein solches Krankheitsbild später nicht mehr aufgetreten, was, wenn es verschleißbedingt wäre, zumindest untypisch wäre. Selbst unter Abzug der hierauf entfallenden 14 Arbeitsunfähigkeitstage verblieben für 2017 37 arbeitsunfähigkeitbedingte prognosefähige Fehltage. Ein Ausscheiden der übrigen Fehlzeiten, die im Wesentlichen auf Atemwegserkrankungen oder Erkrankungen wegen Gastritis/Kolitis beruhen, kommt nicht in Betracht. Sie sind zumindest im Hinblick auf eine allgemeine Krankheitsanfälligkeit berücksichtigungsfähig.

c) Im Jahr 2018 sind ausschließlich Fehlzeiten wegen Atemwegserkrankungen oder Gastritis/Kolitis angefallen. Es sind sämtliche 42 Fehltage berücksichtigungsfähig.

d) Von den Fehlzeiten des Jahres 2019 können für die Prognose vier Arbeitstage in Abzug gebracht werden wegen einer Handgelenksprellung. Hierbei handelt es sich um ein einmaliges und abgeschlossenes Ereignis. Zugunsten des Klägers kann zudem unterstellt werden, dass die zwei Fehltage wegen einer Gichterkrankung nicht prognosefähig sind. Es verblieben dann immer noch 37 Fehltage. Die übrigen Fehlzeiten wegen Atemwegserkrankungen und Gastritis/Kolitis bleiben prognosefähig.

e) Entgegen der Auffassung des Klägers ist für die Prognosebeurteilung nicht starr auf den Zeitraum der letzten drei Jahre vor Zugang der Kündigung abzustellen. Es können vielmehr auch längere Zeitspannen einbezogen werden (BAG 20. November 2014 – 2 AZR 755/13 –). Zusammenfassend kann festgestellt werden, dass selbst bereinigt in den letzten vier Jahren vor Ausspruch der Kündigung ca. 37 Fehltage pro Jahr angefallen sind, in den letzten drei Jahren gar ca. 38,5 Fehltage. Angesichts von 37 berücksichtigungsfähigen Fehltagen im Jahr 2019 kann entgegen der Auffassung des Arbeitsgerichts auch nicht von einer abnehmenden Tendenz die Rede sein.

3. Diese Fehlzeiten führen bei der Beklagten auf der zweiten Stufe zu erheblichen Beeinträchtigungen betrieblicher Interessen. Die Beklagte hat ausgehend von dieser Prognose auch weiterhin mit deutlichen Entgeltfortzahlungsbelastungen zu rechnen, die über die zumutbare Sechswochengrenze hinausgehen. Es waren nämlich auch in der Vergangenheit sämtliche Fehlzeiten mit Entgeltfortzahlungsbelastungen belegt.

4. Die Kündigung erweist sich jedoch im Rahmen der gebotenen Interessenabwägung auf der dritten Stufe als nicht sozial gerechtfertigt. Sie ist unverhältnismäßig. Die Beklagte hat nämlich trotz Notwendigkeit der Durchführung eines bEM ein solches nicht ordnungsgemäß eingeleitet.

a) Es ist dabei von folgenden Grundsätzen auszugehen.

aa) Die Durchführung des bEM ist zwar keine formelle Wirksamkeitsvoraussetzung für eine Kündigung. § 84 Abs. 2 SGB IX ist dennoch kein bloßer Programmsatz. Die Norm konkretisiert den Verhältnismäßigkeitsgrundsatz. Mit Hilfe des bEM können möglicherweise mildere Mittel als die Kündigung erkannt und entwickelt werden. Möglich ist, dass auch ein tatsächlich durchgeführtes bEM kein positives Ergebnis hätte erbringen können. In einem solchen Fall darf dem Arbeitgeber kein Nachteil daraus entstehen, dass er es unterlassen hat. Will sich der Arbeitgeber hierauf berufen, hat er die objektive Nutzlosigkeit des bEM darzulegen und ggf. zu beweisen. Dazu muss er umfassend und detailliert vortragen, warum weder ein weiterer Einsatz auf dem bisherigen Arbeitsplatz, noch dessen leidensgerechte Anpassung oder Veränderung möglich gewesen seien und der Arbeitnehmer auch nicht auf einem anderen Arbeitsplatz bei geänderter Tätigkeit habe eingesetzt werden können, warum also ein bEM im keinem Fall dazu hätte beitragen können, neuerlichen Krankheitszeiten vorzubeugen und das Arbeitsverhältnis zu erhalten. Ist es dagegen denkbar, dass ein bEM ein positives Ergebnis erbracht, das gemeinsame Suchen nach Maßnahmen zum Abbau der Fehlzeiten also Erfolg gehabt hätte, muss sich der Arbeitgeber regelmäßig vorhalten lassen, er habe „vorschnell“ gekündigt (BAG 20. November 2014 – 2 AZR 755/13 –).

bb) Die Durchführung eines bEM ist auf verschiedene Weisen möglich. § 167 Abs. 2 SGB IX schreibt weder konkrete Maßnahmen noch ein bestimmtes Verfahren vor. Das bEM ist ein rechtlich regulierter verlaufs- und ergebnisoffener „Suchprozess“, der individuell angepasste Lösungen zur Vermeidung zukünftiger Arbeitsunfähigkeit ermitteln soll. Allerdings lassen sich aus dem Gesetz gewisse Mindeststandards ableiten. Zu diesen gehört es, die gesetzlich dafür vorgesehenen Stellen, Ämter und Personen zu beteiligen und zusammen mit ihnen eine an den Zielen des bEM orientierte Klärung ernsthaft zu versuchen. Ziel des bEM ist es festzustellen, aufgrund welcher gesundheitlichen Einschränkungen es zu den bisherigen Ausfallzeiten gekommen ist, und herauszufinden, ob Möglichkeiten bestehen, sie durch bestimmte Veränderungen künftig zu verringern, um so eine Kündigung zu vermeiden. Es ist Sache des Arbeitgebers, die Initiative zur Durchführung des bEM zu ergreifen. Bei der Durchführung muss er eine bestehende betriebliche Interessenvertretung, das Einverständnis des Arbeitnehmers vorausgesetzt, hinzuziehen. Kommt es darauf an, ob der Arbeitgeber eine solche Initiative ergriffen hat, kann davon nur ausgegangen werden, wenn er den Arbeitnehmer zuvor nach § 167 Abs. 2 Satz 3 SGB IX auf die Ziele des bEM sowie Art und Umfang der dabei erhobenen Daten hingewiesen hat. Der Hinweis erfordert eine Darstellung der Ziele, die inhaltlich über eine bloße Bezugnahme auf die Vorschrift des § 167 Abs. 2 Satz 1 SGB IX hinausgeht. Zu diesen Zielen rechnet die Klärung, wie die Arbeitsunfähigkeit möglichst überwunden, erneuter Arbeitsunfähigkeit vorgebeugt und wie das Arbeitsverhältnis erhalten werden kann. Dem Arbeitnehmer muss verdeutlicht werden, dass es um die Grundlagen seiner Weiterbeschäftigung geht und dazu ein ergebnisoffenes Verfahren durchgeführt werden soll, in das auch er Vorschläge einbringen kann. Daneben ist ein Hinweis zur Datenerhebung und Datenverwendung erforderlich, der klarstellt, dass nur solche Daten erhoben werden, deren Kenntnis erforderlich ist, um ein zielführendes, der Gesundung und Gesunderhaltung des Betroffenen dienendes bEM durchführen zu können. Dem Arbeitnehmer muss mitgeteilt werden, welche Krankheitsdaten – als sensible Daten i.S.v. Art. 9 Abs. 1, 4 Nr. 15 DS-GVO – erhoben und gespeichert und inwieweit und für welche Zwecke sie dem Arbeitgeber zugänglich gemacht werden. Nur bei entsprechender Unterrichtung kann vom Versuch der ordnungsgemäßen Durchführung eines bEM die Rede sein (BAG 20. November 2014 – 2 AZR 755/13 –).

cc) Bezogen auf den erforderlichen Hinweis zur Datenerhebung und Datenverwendung ist noch Folgendes zu berücksichtigen:

Die Klärung von Möglichkeiten zur Beendigung gegenwärtiger und Vermeidung neuer Arbeitsunfähigkeiten sowie zum Erhalt des Arbeitsplatzes ist nur möglich, wenn die beteiligten Akteure im möglichen Umfang Informationen über die Ausgangssituation haben. Daher ist das Erfassen dieser Ausgangssituation denknotwendig Bestandteil eines bEM. Zu beachten ist dabei aber, dass berechtigte Interessen des Beschäftigten gegen eine umfassende Informationssammlung sprechen können. Nicht zuletzt, weil es in der Regel um besonderer Kategorien personenbezogener Daten iSd. Art. 9 EU-DS-GVO, insbesondere Gesundheitsdaten nach Art. 4 Nr. 15 EU-DS-GVO geht, gehört zu den Pflichten des Arbeitgebers auch die Beachtung des Datenschutzes. Die Beachtung des Datenschutzes ist in § 167 Abs. 2 SGB IX zwar verklausuliert, aber dennoch ausdrücklich vorgeschrieben. Ihre Notwendigkeit ergibt sich zudem aus dem besonderen Spannungsfeld der in wesentlichen Teilen auch schon rechtlich geregelten Interessen, in dem das bEM notwendig angesiedelt ist. Dies sind insbesondere das Erkenntnisinteresse des

Arbeitgebers an allen für die Leistungsfähigkeit des Beschäftigten relevanten Informationen und das Interesse des Beschäftigten am Erhalt seines Arbeitsplatzes auch bei gesundheitlicher Einschränkung. Auch ganz allgemein ist die Einhaltung datenschutzrechtlichen Anforderungen für eine vertrauensvolle und effektive Zusammenarbeit im Rahmen des bEM unerlässlich (FRR/Ritz/Schian SGB IX § 167 Rn. 29 und 30).

Bei der Organisation des Datenschutzes sind folgende Leitlinien einzuhalten. Der Arbeitgeber – und in Anlehnung an den Rechtsgedanken des § 35 Abs. 1 Satz 3 SGB I jede andere Person, die Personalentscheidungen treffen kann – darf ohne ausdrückliche Zustimmung des Betroffenen Zugang nur zu solchen Daten haben, die für den Nachweis der Erfüllung der Pflicht zum bEM erforderlich sind oder ohne die er seine Zustimmung zu geplanten Maßnahmen etc nicht erteilen kann. Diagnosen und ähnlich sensible Daten dürfen dem Arbeitgeber ohne ausdrückliche schriftliche Zustimmung des Betroffenen nicht zugänglich sein (FRR/Ritz/Schian SGB IX § 167 Rn. 44a und 45).

b) In Anwendung dieser Grundsätze kann nicht von einer ordnungsgemäßen Einleitung des bEM-Verfahrens ausgegangen werden.

aa) Eine Einleitung eines bEM war gemäß § 167 Abs. 2 Satz 1 SGB IX geboten. Der Kläger war innerhalb des Jahres vor Ausspruch der Kündigung an 37 Arbeitstagen, somit länger als sechs Wochen (wiederholt) arbeitsunfähig krank.

bb) An der Ordnungsgemäßheit des Einladungsschreibens selbst bestehen keine Zweifel.

cc) Ob dem Einladungsschreiben entsprechend der Behauptung der Beklagten das Hinweisblatt über die Datenerhebung und Datenverwendung als Anlage beigefügt war, kann dahinstehen. Eine Beweiserhebung hierüber konnte unterbleiben.

dd) Denn selbst wenn man unterstellen wollte, dass das Hinweisblatt dem Kläger zusammen mit dem Einladungsschreiben zugegangen sein sollte, wären die Voraussetzungen für eine ordnungsgemäße Unterrichtung über die Datenverwendung nicht erfüllt.

(1) Die erkennende Kammer (LAG Baden-Württemberg 28. Juli 2021 – 4 Sa 68/20 –) hat in einem anderen Verfahren, ebenfalls die Beklagte betreffend, zu dem hier streitgegenständlichen Unterrichtungsschreiben bereits wie folgt ausgeführt:

Vorliegend hat die Beklagte in der „Datenschutzerklärung“ versucht, von der Klägerin (hier: vom Kläger) eine Einwilligung nicht nur zur „Erhebung“ und „Nutzung“ (auch) von Gesundheitsdaten zu erlangen, sondern gemäß dem ersten Absatz auch zur „Bekanntmachung“ dieser Daten unter anderen gegenüber dem „Vorgesetzten“ und der „Standortleitung“. Die Einwilligung in die „Bekanntgabe“ von Gesundheitsdaten gegenüber dem „Vorgesetzten“ mag man vielleicht noch einschränkend auslegen können, dass dies nur gelten solle, wenn der Vorgesetzte als Teilnehmer des betrieblichen Eingliederungsteams (BET) herangezogen wurde. Im beigefügten Antwortschreiben hätte die Klägerin (hier: der Kläger) eine solche Beteiligung des Vorgesetzten ankreuzen können. Für eine „Bekanntmachung“ jedenfalls aller offenbarter Gesundheitsdaten (insb. Diagnosen) gegenüber der Standortleitung besteht dagegen kein nachvollziehbarer Grund. Hier reicht es aus, wenn der Arbeitgeber weiß, auf welche Einschränkungen er bei einer etwa gebotenen Umgestaltung von Arbeitsplätzen zu achten hat. Einer Kenntnis, auf welcher Diagnose diese Einschränkung beruht, bedarf er nicht. Es ist zwar nicht ausgeschlossen, dass ein Arbeitnehmer auch dem nicht im BET beteiligten Standortleiter freiwillig seine Gesundheitsdaten überlassen möchte i.S.d. Art. 9 Abs. 2 a; 7 EU-DS-GVO. Dann muss dem Arbeitnehmer aber im besonderem Maße deutlich gemacht werden, dass dieser Teil der Einwilligung nur freiwillig ist, weil sie für die Zwecke der Durchführung des bEM nicht erforderlich ist, vergleiche Art. 7 Abs. 4 EU-DS-GVO. Das ist vorliegend nicht der Fall.

Hieran hält die Kammer fest.

(2) Daran ändert sich auch nichts, weil nach dem ergänzenden Vorbringen der Beklagten das Einladungsschreiben und die Unterrichtung über die Datenerhebung und Datenverwendung in Zusammenhang gelesen werden müssten mit der BV-bEM. Dem Kläger wurde nämlich als Ausgangssituation im Einladungsschreiben lediglich mitgeteilt, dass das bEM mit Mitgliedern des BET durchgeführt werde. Dafür soll dem Kläger eine Anlage mit einer Liste der BET-Mitglieder zugeleitet worden sein. Auf dieser Liste befanden sich aber nur Namen von Mitarbeitern der Personalabteilung, von Mitgliedern des Betriebsrats und der Schwerbehindertenvertretung, der Werkärzte und der Mitarbeiter der Sozialberatung. Der/die Standortleiter/in war auf dieser Liste nicht benannt. Zwar kann gemäß Nr. 3.2 der BV-bEM, wenn Anpassungen des Arbeitsplatzes, -prozesses oder der -bedingungen erforderlich sind, mit Einverständnis des Mitarbeiters auch ein sog. Integrationsteam zum bEM hinzugezogen werden mit einem gegenüber dem BET erweiterten Teilnehmerkreis, der ua. die örtliche Standortleitung umfasst. Jedoch ist diese Erweiterungsmöglichkeit im Einladungsschreiben nicht erwähnt. Der Kläger hätte anhand des Einladungsschreibens somit nicht erkennen können, dass die im Datenschutzhinweis benannte „Bekanntgabe“ seiner Gesundheitsdaten an die Standortleitung nur bei einem zusätzlichen Einverständnis in eine Verfahrenserweiterung und nur innerhalb des bEM-Verfahrens und seiner Zwecksetzung erfolgen sollte. Er musste unter bloßer Zugrundelegung der Datenschutzunterrichtung vielmehr davon ausgehen, dass seine Gesundheitsdaten, insbesondere seine Diagnosen, gegebenenfalls an die Standortleitung bekannt gemacht werden könnten, obwohl diese gar nicht in das Verfahren eingebunden wären. Eine solche unzureichende Darstellung der Ausgangslage wäre zumindest geeignet gewesen, einen Arbeitnehmer – so auch den Kläger – in Abwägung mit seinen Datenschutzinteressen von einer freiwilligen Teilnahme am bEM Abstand nehmen zu lassen. Diese potentielle Fehlvorstellung kann nicht dadurch überbrückt werden, weil im Betreff des Einladungsschreibens die BV-bEM benannt wurde. Arbeitnehmer sind nicht gehalten, neben dem ausdrücklichen Einladungsschreiben eine in dessen Betreff benannte Betriebsvereinbarung parallel zu lesen, um etwaige Irritationen und Unklarheiten zu beseitigen.

(3) Die Kammer hatte die unzureichende Einleitung des bEM im Verfahren zu beachten, obwohl der Kläger eine inhaltliche Fehlerhaftigkeit der Unterrichtung gar nicht gerügt hat, sondern nur den Zugang des Unterrichtungsschreibens über die Datenerhebung und -verwendung bestritt. Es mag für die Beklagte misslich sein, dass die Vorlage der Datenschutzunterrichtung im Prozess nur erforderlich wurde, weil der Kläger dessen Zugang überhaupt bestritt und es deshalb zum Zwecke einer Beweiserhebung über den Zugang notwendig war, zu wissen, welches Schreiben überhaupt zugegangen sein soll. Durch die Vorlage des Schreibens wurde dieses aber zum Gegenstand des Verfahrens und des Prozessvortrags der Beklagten gemacht. Dieser Prozessvortrag war dann jedoch – unter Beachtung des Streitgegenstands – unter allen in Betracht kommenden Gründen zu prüfen. Lediglich bedurfte es eines rechtlichen Hinweises des Gerichts gemäß § 139 ZPO (BAG 13. Dezember 2012 – 6 AZR 5/12 –). Dieser Hinweis wurde im Berufungstermin erteilt.

c) Es kann vorliegend nicht ausgeschlossen werden, dass bei einer ordnungsgemäßen Unterrichtung über das bEM der Kläger an einem solchen teilgenommen hätte und im Rahmen des Verfahrens Möglichkeiten gefunden worden wären, die Fehlzeiten des Klägers zu reduzieren. Jedenfalls hat die Beklagte nicht aufgezeigt, dass ein bEM vorliegend entbehrlich gewesen wäre.

II.

Der Kläger hat im Bestandsschutzstreit obsiegt. Es überwiegt somit sein Beschäftigungsinteresse gegenüber den gegenläufigen Interessen der Beklagten. Dem Kläger steht daher ein allgemeiner Weiterbeschäftigungsanspruch zu.

III.

1. Die Kostenentscheidung beruht auf § 97 Abs. 1 ZPO.

2. Die Revision war für die Beklagte gemäß § 72 Abs. 2 Nr. 1 ArbGG wegen grundsätzlicher Bedeutung zuzulassen.

Schadensersatz bei verzögerter Datenauskunft

(**Landesarbeitsgericht Hamm**, Urteil vom 11. Mai 2021 – 6 Sa 1260/20 n.rk. –)

Für die Bemessung des einer betroffenen Person zustehenden immateriellen Schadensersatzes nach Art. 82 DS-GVO ist im Rahmen des dem Gericht eröffnetem weitem Ermessens eine Orientierung an dem Kriterienkatalog für die Bemessung von Bußgeldern in Art. 83 Abs. 2 S. 2 DS-GVO naheliegend (so auch ArbG Düsseldorf vom 05.03.2020 – 9 Ca 6557/18 –)

Aus den Gründen:

I. Die Berufung ist teilweise begründet, soweit die Klägerin die Zahlung eines immateriellen Schadensersatzes begehrt. Sie hat aus Art. 82 Abs. 1 DS-GVO einen Anspruch auf Zahlung eines solchen Schadensersatzes in Höhe von 1.000,00 Euro.

1. Der Klageantrag ist zunächst bestimmt genug, § 253 Abs. 2 Nr. 2 ZPO. Bei einem Schadensersatzanspruch auf Geldentschädigung, bei dem die Bestimmung des Betrages von der Ermittlung der Schadenshöhe durch Beweisaufnahme oder durch gerichtliche Schätzung oder vom billigen Ermessen des Gerichts abhängt, ist es ausreichend, wenn die zahlenmäßige Feststellung der Klageforderung dem Gericht überlassen wird, sofern dem Gericht zugleich die tatsächlichen Grundlagen gegeben werden, die ihm die Feststellung der Höhe des gerechtfertigten Klageanspruchs ermöglichen (vgl. BGH vom 13.03.1967 – III ZR 8/66 m.z.N.). Selbes gilt, wenn – wie hier – die ziffernmäßige Festlegung der Schadenshöhe entscheidend von der Ausübung des richterlichen Ermessens oder einer richterlichen Schätzung nach § 287 Abs. 1 ZPO abhängt (BGH vom 13.03.1967 – III ZR 8/66 m.z.N.). Vorliegend hat die Klägerin zudem angegeben, dass sie einen Mindestschaden von 6.000,00 Euro (vgl. Berufungsbegründung vom 21.12.2020) für angemessen erachtet.

2. Nach Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen.

Die DS-GVO, die seit dem 25.05.2018 in Kraft getreten ist (Art. 99 Abs. 2 DS-GVO) gilt gemäß Art. 288 AEUV unmittelbar in jedem Mitgliedsstaat der Europäischen Union, ohne dass es einer weiteren Umsetzung durch nationales Recht bedarf.

a) Verantwortlicher im Sinne des Art. 82 Abs. 1 DS-GVO ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Ziff. 7 DS-GVO), mithin die Beklagte.

b) Die Beklagte hat vorliegend gegen ihre Auskunftspflicht gegenüber der Klägerin aus Art. 15 Abs. 1 DS-GVO verstoßen. Der Auskunftsanspruch besteht auch in einem Arbeitsverhältnis. Die allgemeinen Bestimmungen der EU-DSVO enthalten eine Vollregelung, auch zum Beschäftigtendatenschutz (vgl. LAG Baden-Württemberg vom 20.12.2018 – 17 Sa 11/18 –). Der Auskunftsanspruch ist ein Grundrecht (Art. 8 Abs. 2 GRCh, Art. 6 Abs. 1 EUV) und gehört zur „Magna Charta" der Betroffenenrechte (Lemke, der Datenschutzrechtliche Auskunftsanspruch im Arbeitsverhältnis, NJW 2020, 1841 ff).

Nach Art. 15 Abs. 1 DS-GVO hat die betroffene Person (Art. 4 Ziff. 7 DS-GVO) das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden und – soweit dies der Fall ist – das weitere Recht auf die unter lit. a) bis h) der Vorschrift benannten Informationen. Nach der Vorgabe des Art. 12 Abs. 3 S. 1-3 DS-GVO ist ein solches Auskunftsbegehren binnen eines Monats nach Eingang, nach einer Unterrichtung über eine Fristverlängerung binnen zwei weiterer Monate zu beantworten.

(1) Ein solches Verlangen hat die Klägerin vorliegend mit außergerichtlichem Schreiben ihres heutigen Prozessbevollmächtigten vom 30.01.2020 gestellt. Darin hat sie unter Bezugnahme auf die Datenschutzgrundverordnung Auskunft über „sämtliche bei Ihnen gespeicherten Daten, insbesondere die Daten der Arbeitszeiterfassung" begehrt. Das Auskunftsbegehren unterliegt nach den Bestimmungen der DS-GVO keinen besonders geregelten Anforderungen an Form und Inhalt. Es kann dahinstehen, ob sich der Anspruch der Klägerin inhaltlich auf den gesamten Umfang der mit dem Schreiben geltend gemachten Daten bezieht. Aus diesem Verlangen konnte die Beklagte hinreichend konkret erkennen, auf welche Rechtsgrundlage die Klägerin ihr begehren stützt. Aus Art. 4 Ziff. 2 DS-GVO ergibt sich zudem, dass sich die Verarbeitung, die Gegenstand des Auskunftsanspruchs nach Art. 15 DS-GVO ist, auf jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten bezieht. Eine

Einschränkung auf einen bestimmten Auskunftsteil hat die Klägerin nicht vorgenommen. Sie hat nur formuliert, dass sich ihr Begehren „insbesondere“, aber nicht erkennbar nicht ausschließlich auf die Daten der Zeiterfassung beziehe.

(2) Der Auskunftsanspruch bezieht sich inhaltlich auf personenbezogene Daten. Dabei handelt es sich nach Art. 4 Ziff. 1 DS-GVO um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Zur Verarbeitung gehört nach Art. 4 Ziff. 2 DS-GVO insbesondere das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung und die Verwendung solcher Daten. In einem Arbeitsverhältnis verarbeitet der Arbeitgeber zwangsläufig personenbezogene Daten der bei ihm beschäftigten Arbeitnehmer. Bei diesen Daten kann es sich neben den Kontaktdaten der Person etwa um Informationen über das Bestehen und die Dauer einer Arbeitsunfähigkeit, über die Gewährung von Urlaubsansprüchen oder auch über Leistungs- und Verhaltensdaten handeln. Die Beklagte hat bis heute keine Auskunft darüber erteilt, ob und zu welchem Verarbeitungszweck (Art. 15 Abs. 1 lit. a)) und nach welchen Kategorien (Art. 15 Abs. 1 lit. b)) sie entsprechende Daten der Klägerin verarbeitet. Die Beklagte hat auf das gestellte Auskunftsverlangen erstmals unter dem 13.08.2020 reagiert und der Klägerin – offenbar auch im Hinblick auf den zu diesem Zeitpunkt klageweise rechtshängig gemachten und auf den Umfang der geleisteten Arbeitszeit im Arbeitsverhältnis beschränkten Auskunftsantrag – Arbeitszeitnachweise zugesendet. Eine weitere Auskunft ist – bis heute – nicht erfolgt.

(3) Eine Haftung für die Verstöße könnte nur entfallen, wenn die Beklagte für diese nicht verantwortlich wäre, Art. 83 Abs. 3 DS-GVO. Dies hat die Beklagte nicht dargetan.

c) Entgegen der Auffassung der Beklagten ist der Klägerin durch die fehlende Erteilung der Auskunft ein immaterieller Schaden entstanden.

Das zutreffende Verständnis des Schadensbegriffs ist in der Rechtsprechung des Gerichtshofs der Europäischen Union bislang nicht geklärt. Der Begriff kann auch nicht in seinen einzelnen, für die Beurteilung des vorliegenden Sachverhalts notwendigen Voraussetzungen unmittelbar aus der DS-GVO bestimmt werden. Auch in der bislang vorliegenden Literatur, die sich unter Bezugnahme auf den Erwägungsgrund 146 überwiegend für ein weites Verständnis des Schadensbegriffs ausspricht, sind die Details und der genaue Umfang des Anspruchs noch unklar (vgl. dazu: BVerfG vom 14.01.2021 – 1 BvR 2853/19 – mit zahlreichen Nachweisen).

Weder der DS-GVO noch ihren Erwägungsgründen lässt sich indes entnehmen, dass der Schadensersatzanspruch einen qualifizierten Verstoß gegen die DS-GVO voraussetzt. Für die Annahme einer Erheblichkeitsschwelle oder – anders herum formuliert – die Ausnahme von Bagatellfällen, gibt es keinen Anhaltspunkt (so auch BVerfG vom 14.01.2021 – 1 BvR 2853/19 –).

Unter Berücksichtigung des Erwägungsgrundes 146 S. 3 zur DS-GVO soll der Begriff des Schadens im Lichte der Rechtsprechung des Europäischen Gerichtshofes weit und auf eine Weise ausgelegt werden, die den Zielen der Verordnung in vollem Umfang entspricht. Die Ziele der DS-GVO bestehen dabei u.a. darin, den Risiken für die Rechte und Freiheit natürlicher Personen zu begegnen, die – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – aus einer Verarbeitung personenbezogener Daten hervorgehen und zu einem immateriellen Schaden führen können. Dabei kann ein immaterieller Schaden nicht nur in einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen liegen. Er kann (bereits) entstehen, wenn die von der Verarbeitung personenbezogener Daten betroffenen Personen daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren (vgl. Erwägungsgrund 75).

In jedem Arbeitsverhältnis verarbeitet der Arbeitgeber zwangsläufig personenbezogene Daten seiner Mitarbeiter. Jeder Arbeitgeber wird mindestens die Kontaktdaten, die Bankdaten zwecks Überweisung des Entgelts sowie Anwesenheits- und Fehlzeitendaten seiner Mitarbeiter erheben, speichern und verwenden. In welchem Umfang und in welchen Kategorien eine solche Verwendung erfolgt, ist Arbeitnehmern nicht ohne weiteres ersichtlich. Ebenso können Arbeitnehmer nicht von sich aus erkennen, ob Daten auch Dritten zur Verfügung gestellt und für welche Dauer – ggf. auch nach Beendigung des Arbeitsverhältnisses – diese Daten gespeichert bleiben. Die Beklagte wendet vorliegend nicht ein, dass sie über die der Klägerin im August 2020 übersendeten Arbeitszeitnachweise keine weiteren personenbezogenen Daten der Klägerin verarbeitet. Eine Kontrolle über diese Daten hat die Klägerin indes nicht, solange die Beklagte ihrer Auskunftspflicht – in erster Stufe zumindest hinsichtlich der Bestätigung des „Ob“ der Verarbeitung personenbezogener Daten – nicht nachkommt. Der Klägerin fehlt dabei nicht nur die Kenntnis, welche Kategorien von Daten die Beklagte formalisiert oder nicht formalisiert verarbeitet. Sie kann ebenso nicht beurteilen, wie lange solche Daten nach Beendigung des Arbeitsverhältnisses weiter gespeichert bleiben und an welche Dritte die Beklagte solche Daten ggf. weiterreicht. Die Schwere des immateriellen Schadens, mithin das Gewicht der Beeinträchtigung, das die Klägerin – subjektiv – wegen der bestehenden Unsicherheit und des Kontrollverlustes empfinden mag, ist für die Begründung der Haftung nach Art. 82 Abs. 1 DS-GVO und mithin für die Frage des „ob“ eines entstandenen Schadens nicht erheblich (so auch ArbG Düsseldorf vom 05.03.2020 – 9 Ca 6557/18).

d) Die Klägerin hat die Bemessung der Höhe des immateriellen Schadensersatzes in das Ermessen des Gerichts gestellt, § 287 Abs. 1 S. 1 ZPO. Unter Würdigung aller Umstände des Einzelfalles geht die Berufungskammer davon aus, dass der Klägerin zur Abgeltung des immateriellen Schadens ein Geldanspruch in Höhe von 1.000,00 Euro zusteht.

(1) Unter Berücksichtigung des Erwägungsgrundes 146 (Satz 6) zur DS-GVO soll die betroffene Person einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten. Insoweit erscheint eine Orientierung an dem Kriterienkatalog für die Bemessung von Bußgeldern in Art. 83 Abs. 2 S. 2 DS-GVO naheliegend (so auch ArbG Düsseldorf vom 05.03.2020 – 9 Ca 6557/18 –). Danach sind für die Ermittlung der Höhe einer Geldbuße u.a. die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens, frühere einschlägige Verstöße sowie die Kategorien der betroffenen personenbezogenen Daten zu betrachten. Bei der Bemessung der Entschädigung für immaterielle Schäden kommt den Gerichten grundsätzlich ein weites Ermessen zu, § 287 Abs. 1 S. 1 ZPO. Es müssen mithin sowohl sämtliche Auswirkungen des konkreten Datenschutzverstoßes für die geschädigte Person als auch sämtliche in der Person des Schädigers liegenden, insbesondere die Tatsituation und den Verschuldensgrad betreffenden, Umstände berücksichtigt werden (vgl. Oetker, in: MüKoBGB, 8. Aufl. 2019, § 253 ZPO Rz. 36 ff).

2) In Anwendung des zuvor dargestellten Maßstabs ist unter Berücksichtigung und Abwägung aller Umstände des Einzelfalls ein Schadensersatz in Höhe von 1.000,00 Euro angemessen.

Dabei hat die Kammer zu Lasten der Beklagten berücksichtigt, dass diese die Auskunft nach Art. 5 Abs. 1 DS-GVO bis zum heutigen Tag nicht erteilt hat. Die Beklagte hat der Klägerin lediglich im August 2020 Arbeitszeitnachweise übermittelt. Damit hat die Beklagte den Auskunftsanspruch allenfalls rudimentär erfüllt. Schriftsätzlich hat sich die Beklagte auf den Standpunkt gestellt, dass die Klägerin in dem Schreiben vom 30.01.2020 zu Unrecht Auskunft über „sämtliche Daten" gefordert habe, obgleich ein Anspruch sich allenfalls auf solche Daten beziehe könne, die die Klägerin persönlich betreffen. Soweit die Beklagte darin eine Rechtfertigung erblickt, einem aus ihrer Sicht unklaren oder überzogenen Begehren nicht nachkommen zu müssen, kann dies nur zu ihren Lasten berücksichtigt werden. Zum einen erscheint eine derart weite Auslegung des Begehrens der Klägerin im Kontext des Schreibens bereits fernliegend. So erläutert der Prozessvertreter in dem Schreiben vom 30.01.2020, dass die Beklagte nach Auskunft seiner Mandantin, die Arbeitszeit elektronisch erfasse, dass es sich bei der Erfassung dieser Daten um personenbezogene Daten handele und die Mandantin daher „ihren" Auskunftsanspruch nach der Datenschutz-Grundverordnung geltend mache. Auch für einen unbefangenen Leser ist erkennbar, dass die Klägerin keine Auskunft über Daten begehrt, die mit ihrer Person nicht in Zusammenhang stehen. Von dieser Auslegung ist die Beklagte indes auch im Kammertermin nicht abgerückt. Ein Problembewusstsein der Beklagten im Hinblick auf die Verletzung eines Rechts, dass der Europäischen Verordnungsgeber, wie sich bereits aus Art. 8 Abs. 2 der Grundrechtscharta zeigt, als sehr bedeutsam einordnet, vermochte die Berufungskammer nicht zu erkennen. Es ist auch nicht ersichtlich, dass die Klägerin die tatsächliche Erteilung der Auskunft in der Zukunft noch außergerichtlich erreichen wird. Zugunsten der Beklagten kann insoweit nur unterstellt werden, dass einschlägige frühere Verstöße nicht vorliegen.

Obwohl das vorgehend dargestellte Verhalten die Annahme nahelegt, dass die Beklagte den Umfang und die Bedeutung ihrer Verpflichtung aus der Datenschutzgrundverordnung jedenfalls fahrlässig grob verkennt, ist zu Lasten der Klägerin zu berücksichtigen, dass sie die tatsächliche Erlangung der ihr nach Art. 15 Abs. 1 DS-GVO zustehenden Informationen in Erkennung des Umstandes, dass die Beklagte diesem Auskunftsbegehren nicht ohne weiteres nachkommen wird, bislang nicht konsequent verfolgt hat. Nachdem die Beklagte im August 2020 Arbeitsnachweise erteilt hat, hat die Klägerin den Auskunftsanspruch insoweit für erledigt erklärt. Sie hat aber in der Folgezeit davon abgesehen, ihr Auskunftsverlangen im Weiteren gerichtlich geltend zu machen, um eine tatsächliche Durchsetzung zu erreichen. Vielmehr hat die Klägerin sich darauf beschränkt, unter Berufung auf die fehlende Auskunft einen immateriellen Schadensersatzanspruch gerichtlich einzuklagen. Ihr Prozessverhalten deutet für die Berufungskammer darauf hin, dass die tatsächliche Erlangung einer Kontrolle über die von ihr verarbeiteten personenbezogenen Daten nicht ihr primäres Ziel ist. Es drängt sich vielmehr für die Berufungskammer der Eindruck auf, dass es ihr in dem außergerichtlichen Schreiben vom 30.01.2020 maßgeblich um die Herausgabe der Arbeitsaufzeichnungen zum Zwecke der Bezifferung einer beabsichtigten Überstundenklage ging. Obwohl sie durch die nach wie vor ausstehende Auskunft nach wie vor keine Kontrolle über ihre personenbezogenen Daten hat, die bei der Beklagten – auch nach Beendigung des Arbeitsverhältnisses – gegebenenfalls weiter verwendet werden, lässt das Verhalten der Klägerin nicht erkennen, dass dieser Umstand als solcher eine besondere Belastung für sie darstellt, die nicht jedenfalls mit der Zahlung eines Schadensersatzbetrages kompensiert werden könnte. Insbesondere ist nicht erkennbar, dass die Klägerin beabsichtigt, die tatsächliche Erteilung der Auskunft auch im Falle der Zahlung eines Schadensersatzes durch die Beklagte weiterzuverfolgen. Dies deutet darauf hin, dass ihre persönliche Betroffenheit im Hinblick auf die fehlende Möglichkeit der Kontrolle ihrer personenbezogenen Daten überschaubar ist und Zweifel an der Nachhaltigkeit des Auskunftsverlangens berechtigt erscheinen. Dieser Umstand ist bei der Bemessung der Höhe des immateriellen Schadensersatzes – anders als bei der Frage des Entstehens eines solchen – zu berücksichtigen.

Inwieweit die Höhe des Schadensersatzes auch von dem nach Art. 4 Ziffer 7 DS-GVO Verantwortlichen und dessen Finanzkraft abhängen mag (so ArbG Düsseldorf 5. März 2020 – 9 Ca 6557/18), kann dahinstehen. Keine der Parteien hat vorliegend Angaben diesbezüglich getätigt. Der Umstand, dass es sich bei der Beklagten um einen Kleinbetrieb handelt, hat für sich genommen keine Aussagekraft hinsichtlich der Finanzkraft des Unternehmens.

Unter Berücksichtigung all dessen hat die Kammer für den Verstoß der Beklagten gegen Art. 15 Abs. 1 DS-GVO insgesamt einen Schadensersatzanspruch in Höhe von 1.000,00 Euro angesetzt.

Keine Zuständigkeit der Aufsichtsbehörde bei abgeschalteten Überwachungskameras (Ls)

(**Oberverwaltungsgericht Koblenz**, Urteil vom 25. Juni 2021 – 10 A 10302/21 –)

Eine abgeschaltete Kamera unterfällt nicht dem Anwendungsbereich der Datenschutz-Grundverordnung. Darüber hinaus ermächtigt Art. 58 Abs. 2 lit. f DS-GVO nicht zur Anordnung des Abbaus einer abgeschalteten Überwachungskamera.

Keine Diskriminierung bei Nichtaufnahme von Mädchen im Knabenchor (Ls)

(**Oberverwaltungsgericht Berlin-Brandenburg**, Urteil vom 21. Mai 2021 – 5 B 32.19 –)

1. **Es liegt keine geschlechtsbezogene Diskriminierung vor, wenn ein Mädchen nicht in den nur von Jungen besetzten Staats- und Domchor Berlin aufgenommen wird. Insbesondere die „Orientierung daran, ob die Bewerberinnen und Bewerber zusätzlich zum hohen Ausbildungsstand stimmlich zum Klang eines Knabenchores passen", ist nicht zu beanstanden.**
2. **Dies gilt jedenfalls solange, wie es im Land Berlin auch Mädchen möglich ist, eine hochwertige musische Bildung zu erhalten.**

(Nicht amtliche Leitsätze)

Kein Anspruch auf Aufhebung des Entzugs der DSB-Funktion wegen eventueller Inkompatibilität im vorläufigen Rechtsschutzverfahren

(**Verwaltungsgerichtshof Baden-Württemberg**, Beschluss vom 26. Juli 2021 – 4 S 1225/21 –)

1. **Wird eine behördliche Datenschutzbeauftragte unter Widerruf ihrer Aufgaben als DSB umgesetzt, weil eine Inkompatibiliät mit der gleichzeitig wahrgenommenen Aufgabe als Leiterin des Rechnungsprüfungsamts vorliegen soll, spricht viele dafür, dass die Entziehung der Aufgabe als DSB aller Voraussicht nach rechtswidrig ist, weil kein genereller Interessenkonflikt im Sinne des Art. 38 Abs. 6 Satz 1 DS-GVO ersichtlich ist.**

2. **Der Klägerin steht jedoch im vorläufigen Rechtsschutzverfahrens kein Anspruch auf Aufhebung der Maßnahme zu, weil es jedenfalls an der für die Annahme eines Anordnungsgrundes geforderten Offensichtlichkeit der Rechtswidrigkeit fehlt. Denn dass der Entzug der Aufgaben als Datenschutzbeauftragte rechtsgrundlos erfolgte, sich insbesondere nicht auf Art. 38 Abs. 6 Satz 2 DS-GVO stützen lässt, lässt sich bei summarischer Prüfung gerade nicht mit dem mit Blick auf das grundsätzliche Verbot einer Vorwegnahme der Hauptsacheentscheidung erforderlichen hohen Grad an Wahrscheinlichkeit feststellen.**

(Nicht amtliche Leitsätze)

Sachverhalt:

I. Die Antragstellerin steht als Leiterin des Rechnungsprüfungsamts in den Diensten der Antragsgegnerin. Mit Schreiben des Oberbürgermeisters der Antragsgegnerin vom 11.12.2017 wurde ihr ab 01.01.2018 die Funktion der Datenschutzbeauftragten nach Art. 37 VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DS-GVO -) übertragen.

Nachdem Zweifel an der Rechtmäßigkeit ihrer Bestellung aufgekommen waren, setzte der Oberbürgermeister die Antragstellerin mit Schreiben vom 19.01.2021 darüber in Kenntnis, dass sie mangels Gemeinderatsbeschlusses nicht wirksam zur Datenschutzbeauftragten bestellt worden sei; hilfsweise widerrief er ihre Bestellung unter Berufung darauf, dass ein Interessenkonflikt zwischen ihrer Tätigkeit als Leiterin des Rechnungsprüfungsamts und ihrer Aufgabe als Datenschutzbeauftragte bestehe.

Das Verwaltungsgericht hat den Antrag der Antragstellerin, sachdienlich gerichtet darauf, der Antragsgegnerin im Wege der einstweiligen Anordnung aufzugeben, ihr bis zur Entscheidung in der Hauptsache die Funktion der behördlichen Datenschutzbeauftragten der Antragsgegnerin zu übertragen, abgelehnt. Zwar habe die Antragstellerin einen Anordnungsanspruch glaubhaft gemacht. Denn sie sei nach summarischer Prüfung auch ohne Gemeinderatsbeschluss ordnungsgemäß zur behördlichen Datenschutzbeauftragten berufen worden. Die Entziehung dieser Aufgabe erweise sich aller Voraussicht nach auch als rechtswidrig, weil kein genereller Interessenkonflikt im Sinne des Art. 38 Abs. 6 Satz 1 DS-GVO zwischen ihrer Tätigkeit als Leiterin des Rechnungsprüfungsamts und ihrer Aufgabe als Datenschutzbeauftragter ersichtlich und auch das im gerichtlichen Verfahren erstmals angeführte zerrüttete Vertrauensverhältnis zwischen ihr und dem Oberbürgermeister bei summarischer Prüfung nicht zu erkennen sei. Es fehle allerdings an einem Anordnungsgrund. Denn eine – wie hier – bloße Umsetzung führe grundsätzlich nicht zu Nachteilen, die ein Abwarten einer Entscheidung in der Hauptsache unzumutbar erscheinen ließen, und drohende, schlechthin unzumutbare Nachteile, die eine Vorwegnahme der Hauptsache verlangten, seien weder hinreichend dargetan noch ersichtlich.

Die Antragstellerin beruft sich in ihrer Beschwerdebegründung darauf, dass die Voraussetzungen für das Vorliegen eines Anordnungsgrunds gegeben seien, weil die Entscheidung über ihre Abberufung als Datenschutzbeauftragte offensichtlich rechtswidrig und willkürlich sei und sie grundlos degradiere.

Aus den Gründen:

II. Mit diesem Vortrag hat die Antragstellerin keinen Erfolg. Auch der Senat hält einen Anordnungsgrund für nicht glaubhaft gemacht.

1. Zutreffend hat das Verwaltungsgericht die durch den Widerruf der Bestellung der Antragstellerin zur Datenschutzbeauftragten erfolgte Entziehung von Teilaufgaben als eine der beamtenrechtlichen Umsetzung gleichstehende Maßnahme eingestuft, weil sich damit ein Teilbereich ihres Dienstpostens, d.h. der ihr konkret übertragenen Aufgaben, ändert (vgl. dazu Bay. VGH, Beschluss vom 25.11.2010 – 3 CE 10.1806 -, Juris Rn. 31).

2. Soll die Umsetzung eines Beamten auf einen anderen Dienstposten oder eine dieser gleichstehende Maßnahme wie etwa eine teilweise Aufgabenentziehung durch eine einstweilige Anordnung im Sinne von § 123 VwGO vorläufig rückgängig gemacht werden, so ist ein Anordnungsgrund für eine solche Regelung nur im besonderen Einzelfall gegeben. Grundsätzlich kann ein Betroffener insoweit auf den Rechtsschutz im Hauptsacheverfahren verwiesen werden, weil eine Umsetzung im Grundsatz jederzeit rückgängig gemacht werden kann, er mithin in der Zwischenzeit keinen endgültigen Rechtsverlust erleidet. Ein Anordnungsgrund besteht deswegen in Fällen solcher Art nur, wenn dem betroffenen Beamten in sonstiger Weise ohne die Gewährung vorläufigen Rechtsschutzes schwere, unzumutbare Nachteile drohen, die sich auch bei einem späteren Erfolg im Hauptsacheverfahren nicht mehr ausgleichen lassen (Senatsbeschluss vom 09.10.2018 – 4 S 1773/18 -, Juris Rn. 6; Sächs. OVG, Beschluss vom 14.10.2020 – 2 B 271/20 -, Juris Rn. 23; OVG NRW, Beschluss vom 21.03.2019 – 6 B 1459/18 -, Juris Rn. 18).

a. Allein der Umstand, dass ohne die beantragte einstweilige Anordnung nach Auffassung des von einer Umsetzung Betroffenen ein rechtswidriger und seinem Ansehen abträglicher Zustand bis zur Entscheidung über die Hauptsache aufrechterhalten würde, begründet noch keinen solchen schweren, unzumutbaren Nachteil, sondern ist regelmäßige Folge des Verbots der Vorwegnahme der Hauptsache (ebenso Sächs. OVG, Beschluss vom 14.10.2020 – 2 B 271/20 -, Juris Rn. 25; OVG NRW, Beschluss vom 15.12.2014 – 6 B 1220/14 -, Juris Rn. 10; Schnellenbach, Beamtenrecht in der Praxis, 8. Aufl., 2013, § 4 Rn. 71). Ein unzumutbarer Nachteil kann allerdings, worauf die Antragstellerin im Grundsatz zurecht hinweist, anzunehmen sein, wenn sich die Umsetzung als materiell offensichtlich rechtswidrig erweist; in diesem Fall hätte der Verweis des Beamten auf den Ausgang eines unter Umständen mehrere Jahre andauernden Hauptsacheverfahrens zur Folge, dass er einen durch die Umsetzung bewirkten materiell offensichtlich rechtswidrigen Eingriff in seine Rechtssphäre während eines gegebenenfalls beträchtlichen Zeitraums hinnehmen müsste. Die Rechtsschutzga-

rantie des Art. 19 Abs. 4 GG gebietet es, dem Beamten die Hinnahme einer solchen offensichtlich rechtswidrigen, insbesondere willkürlichen Maßnahme auch nicht für die Dauer des Rechtsschutzverfahrens zuzumuten (vgl. Senatsbeschluss vom 07.03.1996 – 4 S 2546/95 -, Juris Rn. 4 f.; OVG S.-A., Beschluss vom 14.09.2020 – 1 B 92/20 -, Juris Rn. 16; OVG NRW, Beschluss vom 21.03.2019 – 6 B 1459/18 -, Juris Rn. 22 ff.).

Vorliegend hat die Antragsgegnerin ihren unter dem 19.01.2021 erfolgten Widerruf der Bestellung der Antragstellerin zur Datenschutzbeauftragten damit begründet, dass, wie das eingeholte Rechtsgutachten aufzeige, zwischen der Tätigkeit der behördlichen Datenschutzbeauftragten auf der einen und ihrer Funktion als Leiterin des Fachbereichs Revision auf der anderen Seite wegen der in Revisionsabteilungen erfolgenden Auswertung großer Datenmengen Interessenskonflikte bestünden.

Ob diese Auffassung im Ergebnis einer rechtlichen Überprüfung standhält, ob also die Wahrnehmung der mit der Leitung des Rechnungsprüfungsamts der Antragsgegnerin verbundenen Aufgaben und Pflichten tatsächlich zu einem Interessenkonflikt im Sinne von Art. 38 Abs. 6 Satz 2 DS-GVO mit den Aufgaben und Pflichten eines Datenschutzbeauftragten führt oder ob, wie das Verwaltungsgericht unter Berufung auf die Einschätzung des Landesbeauftragten für den Datenschutz in dessen Schreiben vom 29.01.2021 meint, vorliegend nicht von einer Inkompatibilität der beiden Tätigkeiten auszugehen ist, kann im Rahmen des vorläufigen Rechtsschutzverfahrens dahinstehen, weil es jedenfalls an der für die Annahme eines Anordnungsgrundes geforderten Offensichtlichkeit fehlt.

Die Frage eines Interessenkonflikts gemäß Art. 38 Abs. 6 Satz 2 DS-GVO wird insbesondere im Zusammenhang mit der – mit der Leitung des Rechnungsprüfungsamts inhaltlich vergleichbaren – Tätigkeit der betrieblichen internen Revision ausgesprochen kontrovers diskutiert. Überwiegend wird die Bestellung jedenfalls des Leiters der Revisionsabteilung zum Datenschutzbeauftragten bereits im Grundsatz abgelehnt, weil die Revisionsabteilung typischerweise selbst in größerem Umfang personenbezogene Daten verarbeite und es überdies zu einer Kollision zwischen der Berichtspflicht des Revisors und der Schweigepflicht des Datenschutzbeauftragten kommen könne (Forgó/Helfri/Schneider, Betrieblicher Datenschutz, 3. Aufl., 2019, Teil II Kapitel 3 Rn. 63; ausführl. [zu § 4f BDSG a.F.] Ernst, NJOZ 2010, 2443, 2444 ff. m.w.N. auch zur Gegenauffassung; ähnlich [sollte vermieden werden] auch Plath, DS-GVO/BDSG, 3. Aufl., 2018, Art. 38 Rn. 35). Nach anderer Auffassung ist der Innenrevisor zwar von seinem Aufgabengebiet und seinen damit verbundenen Kenntnissen her zunächst gut geeignet, um die Aufgaben als Datenschutzbeauftragter zu erfüllen (darauf hinweisend etwa Schaffland/Wiltfang, DS-GVO/BDSG, Stand 04/21, Art. 37 Rn. 51 f.); ungeachtet dieser Eignung wird aber eine Einzelfallbetrachtung dahingehend für erforderlich gehalten, ob und in welchem Maße Interessenkonflikte daraus resultieren können, dass der Datenschutzbeauftragte im Rahmen seiner Tätigkeit in der Revision selbst Datenauswertungen durchführt oder verantwortet (Kühling/Buchner, DS-GVO /BDSG, 3. Aufl., 2020, Art. 38 Rn. 42; BeckOK Wolff/Brück, Datenschutzrecht, Stand 01.11.2019, Art. 38 DS-GVO Rn. 36; Schaffland/Wiltfang, DS-GVO/BDSG, Stand 04/21, Art. 37 Rn. 52).

Vor diesem Hintergrund lässt sich im Rahmen der im einstweiligen Rechtsschutzverfahren vorzunehmenden summarischen Prüfung nicht feststellen, dass sich die Rechtswidrigkeit des mit Schreiben vom 19.01.2021 erfolgten Widerrufs der Bestellung der Antragstellerin als Datenschutzbeauftragter geradezu aufdrängt, der Widerruf damit offensichtlich rechtswidrig ist, wie es für die ausnahmsweise Annahme eines Anordnungsgrundes im Sinne von § 123 Abs. 1 VwGO erforderlich wäre.

b. Auch soweit die Antragstellerin einwendet, die Abberufung als Datenschutzbeauftragte führe zu ihrer „grundlosen Degradierung“, kann sie hier damit keinen Erfolg haben.

Eine Degradierung im Sinne einer nicht (mehr) amtsangemessenen Aufgabenzuweisung infolge ihrer Abberufung liegt nicht vor; dass die Funktion der Leiterin des Rechnungsprüfungsamtes der Antragsgegnerin auch ohne die zusätzlichen Aufgaben als Datenschutzbeauftragte dem statusrechtlichen Amt einer Stadtoberverwaltungsrätin entspricht, wird zurecht nicht infrage gestellt. Auf die Beibehaltung bestimmter Aufgaben oder Funktionen aber hat ein Beamter auch dann keinen Anspruch, wenn diese etwa mit einem besonderen Ansehen in Gemeindeverwaltung oder Kommune oder einer weitergehenden Personalverantwortung verbunden sind; umso weniger begründet deren Entzug einen Anordnungsgrund im Rahmen des § 123 Abs. 1 VwGO.

Ob im Einzelfall etwas anderes gilt, wenn, wie es die Antragstellerin formuliert, der Aufgabenentzug „ohne sachlich einleuchtende rechtlich zulässige Gründe“ erfolgt und zudem Gegenstand öffentlicher Berichterstattung war, weil auch in diesem Fall ohne die Gewährung vorläufigen Rechtsschutzes schwere, unzumutbare Nachteile drohen könnten, die sich auch bei einem späteren Erfolg im Hauptsacheverfahren nicht mehr ausgleichen lassen, bedarf vorliegend keiner Entscheidung. Denn dass der Entzug der Aufgaben als Datenschutzbeauftragte rechtsgrundlos erfolgte, sich insbesondere nicht auf Art. 38 Abs. 6 Satz 2 DS-GVO stützen lässt, lässt sich, wie gesehen, bei summarischer Prüfung gerade nicht mit dem mit Blick auf das grundsätzliche Verbot einer Vorwegnahme der Hauptsacheentscheidung erforderlichen hohen Grad an Wahrscheinlichkeit feststellen.

Zur Rechtsgrundlage des Auskunftsrechts gegenüber einem in kirchlichen Besitz befindlichen Krankenhaus

(**Landgericht Siegen**, Beschluss vom 26. November 2021 – 2 O 236/21 –)

1. **Eine Patientin kann sich für ihren Datenauskunftsanspruch gegenüber einer als GmbH organisierten Klinik in Trägerschaft der Evangelischen Kirche nicht auf Art. 15 DS-GVO berufen, sondern nur auf § 19 DSG-EKD.**
2. **Aus dem gleichen Grund stehen der Patientin bei verweigerter Datenauskunftserteilung keine Schadensersatzansprüche gem. Art. 82 Abs. 1 DS-GVO gegen die Klinik zu.**

(Leitsätze des Einsenders)

Sachverhalt:

Die Parteien streiten über ärztliche Behandlungsfehler bei einer Wirbelsäulenoperation und deren Vor- und Nachsorge im Hause der Antragsgegnerin, dem Diakonie xxx-Krankenhaus, in den Jahren 2017-2018.

Des Weiteren begehrt die Antragstellerin eine vollständige Datenauskunft nach Art. 15 der Europäischen Datenschutzgrundverordnung (Vo (EU) 2016/679, im Folgenden DS-GVO), welche sie erstmals am 18.01.2019 von der Antragsgegnerin eingefordert hat, sowie wegen bislang nicht erteilter Auskunft ein Schmerzensgeld auf Basis von Art. 82 Abs. 1) DS-GVO.

Die Antragstellerin ist der Ansicht, die DS-GVO greife vorliegend ein, da es sich bei dem Betrieb des Krankenhauses um eine rein wirtschaftliche Betätigung der Beklagten handele, die sich nicht vom Betrieb anderer, nicht konfessioneller Krankenhäuser unterscheide.

Die Beklagte ist der Ansicht, in datenschutzrechtlicher Hinsicht sei nicht die DS-GVO, sondern das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (im Folgenden: DSG-EKD) anwendbar, da sie gem. Art. 91 DS-GVO als kirchliche Einrichtung deren Anwendbarkeit nicht unterliege.

Aus den Gründen:

1. Der Antragstellerin stehen gegen die Antragsgegnerin keine Ansprüche gem. Art. 15, 82 DS-GVO zu, da die DS-GVO auf sie nicht anwendbar ist. Gem. Art. 91 DS-GVO dürfen, wenn eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher personen bei der Verarbeitung anwendet, diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.

Daraus folgt, dass die kirchenrechtlichen Datenschutzregeln vorrangig anwendbar sind, wenn sie mit der DS-GVO in Einklang gebracht werden können und bereits vor Inkrafttreten der DS-GVO bestanden. Dies ist bei dem DSG-EKD der Fall. Die Antragsgegnerin als Trägerin von diakonischen Krankenhäusern fällt zudem aufgrund ihres Bezugs zur Evangelischen Kirche unter das Merkmal „Kirche“, auch wenn es sich bei ihr um eine selbstständige, privatrechtlich (nämlich als GmbH) organisierte Einrichtung der Kirche handelt.

a) Ob öffentlich-rechtliche und privatrechtliche Religionsgesellschaften sowie ihre in Privatrechtsrechtsform organisierten Einrichtungen Normadressaten der DS-GVO bzw. des BDSG und der Landesdatenschutzgesetze sind, wurde – weil konkrete diesbezügliche Aussagen in den genannten Normen fehlen – bisher von Literatur und Aufsichtsbehörden unterschiedlich gesehen. Aussagekräftige Rechtsprechung dazu ist bislang nicht veröffentlicht. Die Meinungen reichen von der generellen Ausnahme der Anwendung der staatlichen Datenschutzgesetze (sog. Exemtionslösung) über ihre Anwendung mit der Ausnahme der Kerntätigkeit religiöser Betätigung (sog. Subsumtionslösung) bis zur vollen Anwendung (vgl. Gola, DS-GVO, 2. Aufl. 2019, Art. 91 Rn. 5).

aa) Für die weite Auslegung des Art. 91 DS-GVO wird angeführt, dass Art. 91 DS-GVO seinem Wortlaut nach keinen Zusammenhang der Verarbeitung von Daten mit der spezifisch religiösen Aufgabe erfordere. Daraus sei zu entnehmen, dass sich autonome Regeln für die Verarbeitung von Daten nicht notwendig nur auf die Daten von Mitgliedern beziehen müssten. Es genüge vielmehr, wenn die Verarbeitung den Status gemäß Art. 17 Abs. 1 AEUV berühre. Dies könne insbesondere im Beschäftigungskontext auch der Fall sein, wenn es um Daten von Nichtmitgliedern gehe. Auch die Teilnahme am Privatrechtsverkehr und die damit zusammenhängende Verarbeitung von Daten könnten den Status berühren. Ein Beispiel sei etwa der Vertrieb religiöser Schriften durch eine GmbH als Teil des selbst definierten Auftrags einer Kirche, religiösen Vereinigung oder Gemeinschaft. Dies wiederum unter der Voraussetzung, dass das Staatskirchenrecht des jeweiligen Mitgliedstaates dies abdecke. Es bestehe deshalb kein Anlass, die Frage, welches Datenschutzrecht auf selbstständige kirchliche Einrichtungen anwendbar ist, im Licht von Art. 91 DS-GVO neu zu stellen. Diese Frage beantworte sich nach dem Staatskirchenrecht des jeweiligen Mitgliedstaates. Die Auffassung von Dammann (ZD 2016, 307 (311, 312)), dass Art. 91 für selbständige Einrichtungen wirtschaftlicher, kultureller und sozialer Art wie Krankenhäuser und Lehreinrichtungen von Kirchen, religiösen Vereinigungen und Gemeinschaften nicht gelte, sei mit der Zielsetzung von Art. 17 Abs. 1 AEUV, deren Umsetzung Art. 91 DS-GVO diene, nicht in Einklang zu bringen. Dafür spreche auch die vom EuGH vertretene Auffassung, dass der Begriff der Religion auch das forum externum umfasse, also die Bekundung des religiösen Glaubens in der Öffenilichkeit (EuGH, Urt. v. 14.03.2017 – c-157/15,ECLI:EU:C:2017:203 – G4S Secure Solutions, Rn. 28, wobei einzuräumen sei, dass es bei diesem „Kopftuchfall“ um die Religionsausübung einer Einzelperson ging, nicht dagegen um die Betätigung einer religiösen lnstitution) (zum gesamten Absatz Ehmann/Selmayr/Ehmann/Kranig, 2. Aufl. 2019, DS-GVO Art. 81 Rn. 18). Weiter wird darauf abgestellt, dass unter den Begriff der Religionsgemeinschaft nach der Rechtsprechung des BVerfG nicht nur die organisierten Kirchen und deren rechtlich selbstständige Teile fielen, sondern weitere ihnen zugeordnete Einrichtungen, „wenn sie nach kirchlichem Selbstverständnis ihrer Aufgabe oder ihrem Zweck entsprechend berufen sind, ein Stück Auftrag in dieser Welt wahrzunehmen und zu erfüllen“ (Tinnefeld, ZD 2020,145 mit Verweis auf BVerfGE 46, 73, 88; BVerfGE 53, 366, 391).

bb) Für die sog. Subsumtionslösung wird vorgebracht, dass sich Art. 17 AEUV, wonach die Europäische Union den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, achtet und ihn nicht beeinträchtigt, an korporativ-institutionelle Organisationen mit religiösem bzw. weltanschaulichem Proprium (Waldhoff, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, Art. 1Z AEUV Rn. 18) richte. Gemeint seien damit die Religionsgesellschaften selbst. Zudem beziehe sich Art. 17 AEUV in erster Linie auf den Status und nicht auf Tätigkeiten von Religionsgesellschaften.

Wenn jedoch nur der Status solcher Gemeinschaften anerkannt würde, die Verwirklichung ihrer Zwecke jedoch ohne weiteres eingeschränkt werden könnte, liefen die Schutzpflichten, die Art. 17 Abs. 1 AEUV der EU auferlegt, leer. Folglich seien auch Tätigkeiten, wenn auch nur in sehr restriktivem Maße, von Religionsgemeinschaften von Art. 17 Abs. 1 AEUV umfasst (Classen, in: Grabitz/Hilf/Nettesheim. Das Recht der Europäischen Union, 61. EL April 2017, Art. 17 AEUV Rn. 30). Eine typische Tätigkeit von Religionsgemeinschaften sei bspw. der Betrieb von karitativen Krankenhäusern. Träger dieser kirchlichen Krankenhäuser sei jedoch zumeist eine GmbH. Folglich handele es sich um privatrechfliche Einrichtungen einer Religionsgesellschaft. Es lasse sich demnach vertreten, dass auch privatrechtliche Einrichtungen von Religionsgemeinschaften in den Schutzbereich des Art. 17 AEUV fielen und damit auch nach Art. 91 DS-GVO vom Anwendungsbereich der DS-GVO ausgenommen und dem kirchlichen Datenschutz unterstellt seien. Auf Grund der angezeigten restriktiven Auslegung des Art. 17 AEUV werde dies jedoch nur im Bereich der Kerntätigkeiten religiöser Betätigung möglich sein und nicht bei reinen Wirtschaftsbetrieben von Kirchen (Seifert, in: NK-DatenschutzR, DS-GVO Art. 91 Rn. 10) (zum gesamten Absatz Paal/Paulyl/Pauly, 3. Aufl. 2021, DS-GVO Art. 91 Rn. 10). Auch der Bundesbeauftragte für den

Datenschutz und die lnformationsfreiheit Prof. Dr. Kelber führt aus, dass zwar auf den ersten Blick DS-GVO und BDSG immer dann gelten würden, wenn öffentlich-rechtliche Religionsgemeinschaften in Form von privaten Wirtschaftsunternehmen (z.B. Krankenhäuser, Pflegedienste oder Kindertagesstätten) tätig würden, weil es sich in diesem Fall um nicht-öffentliche Stellen im Sinne von § 2 Abs. 4 BDSG handele, mit Blick auf das verfassungsrechtlich garantierte Selbstbestimmungsrecht von Religionsgemeinschaften jedoch eine differenzierte Betrachtungsweise notwendig sei. Nach dieser unterliege privatrechtliches Handeln der Kirchen als kircheneigene Angelegenheit grundsätzlich nicht der DS-GVO und dem BDSG. Auch bei einem Handeln der Kirche im privaten Bereich müsse danach unterschieden werden, ob es sich bei dieser Tätigkeit um eine kircheneigene Angelegenheit handele oder nicht. Das Selbstverwaltungsrecht erstrecke sich nämlich auf alle der Kirche in bestimmter Weise zugeordneten Einrichtungen ohne Rücksicht auf ihre Rechtsform. Voraussetzung sei nur, dass diese nach kirchlichem Selbstverständnis ihrem Zweck oder ihrer Aufgabe entsprechend berufen seien, ein Stück Auftrag der Kirche wahrzunehmen und zu erfüllen. Die Zugehörigkeit der Einrichtung zur Kirche werde auch nicht dadurch aufgehoben, dass sich die Kirche einer Organisationsform des staatlichen Rechts bediene. Erst recht würde dies im Falle einer organisatorischen Anbindung der Einrichtung an die Kirche deutlich, wenn beispielsweise leitende Mitarbeiter des Krankenhauses gegenüber der Amtskirche verantwortlich wären, sei es auf Grund eines kirchlichen Dienstverhältnisses, sei es auf Grund einer Rechenschaftspflicht. Immer dann, wenn die Tätigkeit einer Einrichtung dem kirchlichen Verkündigungsauftrag zuzurechnen sei, gelte ausschließlich das kirchliche Datenschutzrecht. Etwas anderes müsse gelten, wenn die Kirchen außerhalb des karitativen oder sonst zum kirchlichen Auftrag gehörenden Bereichs in Formen des Privatrechts tätig würden (z.B. Brauereien) oder wenn Daten durch die Teilnahme am allgemeinen Rechtsverkehr anfielen (z.B. im Rahmen der Vermietung von Wohnungen). In diesen Fällen sei die Anwendbarkeit der DS-GVO und des BDSG ohne Zweifel zu bejahen. Wenn eine institutionelle Verbindung zur Kirche völlig fehle, könne nicht mehr vom kircheneigenen Bereich gesprochen werden. Dies sei bei eigenständigen Praxen, die sich nur in das kirchliche Krankenhaus eingemietet hätten, ebenso der Fall wie bei externen Firmen, die privatwirtschaftliche Dienstleistungen erbrächten. Für diese Einrichtungen müssten die DS-GVO und das BDSG ausnahmslos gelten. Für die Übermittlung von Daten durch den kircheneigenen Teil des Krankenhauses an diese Einrichtungen gelte allerdings noch das kirchliche Datenschutzrecht (zum gesamten Absatz: https://www.bfdi.bund.de/DE/Buerger/lnhalte/Allgemein/Datenschutz/Kirchen_Religionsgemeinschaften.html).

Eine weitere differenzierte Ansicht in Bezug auf konfessionelle Krankenhäuser nimmt indes eine Trennung danach vor, ob die konkrete Datenverarbeitung den „kirchlichen" oder den „weltlichen" Bereich betreffe. Denn das „Kirchenprivileg" gelte prinzipiell nur für den kirchlichen Kernbereich. Wenn ein Krankenhaus mit kirchlichem Träger aber voll am Wirtschaftswettbewerb teilnehme, dürfte es sich für nicht kirchliche Krankenhäuser unter Umständen als Wettbewerbsnachteil darstellen, wenn die kirchlichen Krankenhäuser in den rein „weltlichen" Konstellationen unterschiedlich behandelt würden. Insofern erscheine es sachgerecht, den Gedanken des § 2 Abs. 5 BDSG von öffentlichen Institutionen, die am privaten Wettbewerb teilnehmen und dadurch nicht die „behördlichen" privilegien genießen, auch auf diese kirchlichen Einrichtungen zu übertragen. Denn wenn sie voll am Wirtschaftsleben teilnähmen, erbrächten sie keine originären Leistungen aus dem kirchlichen Bereich, weshalb es auch nicht sachgerecht sei, ihnen die kirchlichen Privilegien für Datenverarbeitungstätigkeiten, die aber den welilichen Bereich betreffen, zuzugestehen (Spyra, Münchener Anwaltshandbuch Medizinrecht, Clausen/schroeder-Printzen 3. Aufl. 2020, g 23 Rn. 12, Bl.1gs f. d.A.).

cc) Weiterhin wird vertreten, dass die Verordnungsregelung des Art. 91 DS-GVO generell nur für Kirchen, religiöse Vereinigungen und Gemeinschaften als solche gelte, nicht aber für deren selbstständige Einrichtungen wirtschaftlicher, kultureller oder sozialer Art, wie etwa Krankenhäuser und Lehreinrichtungen (Dammann, ZD 2016, 307). Eine abweichende Behandlung führe zu Rechtsunsicherheit, ob im Einzelfall eine der Kirche zuzuordnende Tätigkeit betroffen sei. Die Belange der kirchlichen Einrichtungen ließen sich hinreichend i.R.d. BDSG berücksichtigen, etwa bei der nach § 28 Abs. 2 Nr. 1 i.V.m. § 28, Abs. 1 Satz 1 Nr. 2 BDSG vorzunehmenden Abwägung (Preuß, ZD 2014, 2017 zum BDSG m.w.N.). Ein Einschreiten der staatlichen Aufsichtsbehörden komme jedoch bei Datenschutzverstößen seitens der kirchlichen Einrichtungen auf Grund einer Reduzierung des Entschließungsermessens auf null nicht in Betracht (Preuß a.a.O.)

b) Nach Ansicht der Kammer ist, da sich aus Art. 91 DS-GVO selbst keine Einschränkung ableitet und die Schutzpflichten, die Art. 17 Abs. 1 AEUV der EU auferlegt, nicht leer laufen dürfen, mit der differenzierenden Ansicht darauf abzustellen, ob es sich bei der Tätigkeit der Antragsgegnerin um eine solche aus dem Kernbereich der Kirche handelt, was vorliegend zu bejahen ist. Die Beurteilung richtet sich danach, ob nach kirchlichem Selbstverständnis durch den Betrieb des Krankenhauses eine dem religiösen Auftrag der Kirche entsprechende und dem Zweck kirchlicher Fürsorge gegenüber den Menschen dienende Aufgabe erfüllt werden soll. Dabei ist zu berücksichtigen, dass nicht nur dann Kernbereiche kirchlicher Aufgaben betroffen sind, wenn es um direkte Seelsorge geht. Es kommt deshalb nicht darauf an, ob ein Patient in einem konfessionellen Krankenhaus spürbar und auf den ersten Blick ersichtlich anders behandelt wird als ein Patient in einem beispielsweise öffentlichrechtlich organisierten Krankenhaus. Vielmehr ist entscheidend, ob die Kirche mit der Einrichtung ihren Aufgaben gerecht werden will. Zu diesen Aufgaben gehören nach dem Selbstbild der Kirche insbesondere auch karitative Aufgaben, wobei damit nicht nur ehrenamtliche bzw. unentgeliche Betreuungsaufgaben gemeint sind, sondern auch der wirtschaffliche Betrieb von Betreuungsangeboten für Hilfe bedürftige Menschen, wie z.B. von Kindergärten, Alten- und Pflegeheimen und Krankenhäusern. Diese Tätigkeiten können heutzutage nicht mehr ohne wirtschaftlichen Fokus betrieben werden, was jedoch nach Ansicht der Kammer nicht dazu führt, dass deshalb bei jeglicher wirtschaftlicher Tätigkeit der Bezug zu einer Kernaufgabe der Kirche zu verneinen ist. Die Antragsgegnerin bezeichnet auf ihrer Krankenhaus-Homepage unter der Rubrik „über uns" die persönliche Zuwendung als eine ihrer besonderen Stärken, wobei sich aus dem grundlegenden christlichen Selbstverständnis – dem Dienst am Menschen – die hohe Qualität von Pflege und Medizin ableite. Daran zeigt sich der karitative Aspekt der kirchlichen Trägerschaft. Soweit die Antragstellerin auf die Ausführungen des Generalanwalts des EuGH (vgl. Fuhlrott: Generalanwalt EuGH: Kündigung eines katholischen Chefarztes wegen Wiederheirat verstößt gegen das Diskriminierungsverbot, GWR 201g, 241) Bezug nimmt, wonach die Tatsache, dass der Gesellschaftszweck der Verwirklichung von Aufgaben der Caritas diene, nicht ausreiche, um eine pri-

vate Organisation anzunehmen, deren Ethos auf religiösen Grundsätzen beruhe, steht dies der vorgenannten Würdigung nicht entgegen. Im dortigen Fall ging es nämlich nicht um die Frage der Anwendbarkeit der kirchlichen Datenschutzgesetze, sondern darum, ob sich die beklagte katholische Klinik, die ihrem Chefarzt aufgrund Wiederheirat nach Scheidung gekündigt hatte, auf die nach deutschem Verfassungsrecht und der Antidiskriminierungs-RL verbriefte Sonderstellung berufen konnte, da nach der Richtlinie eine Ungleichbehandlung wegen der Religion nur dann keine Diskriminierung sei, wenn Art der Tätigkeit und ihre Ausübung eine wesenliche, rechtmäßige und gerechtfertigte Anforderung angesichts des Ethos darstelle. Vorliegend geht es indes nicht um die Frage einer ungerechtfertigten Diskriminierung, sondern um die Frage, welches Datenschutzrecht auf die Antragstellerin anwendbar ist, wobei zu betonen ist, dass die Nichtanwendung der DS-GVO ohnehin nur dann in Betracht kommt, wenn die kirchenrechflichen Datenschutzregeln mit der DS-GVO „in Einklang" gebracht werden können. Aus dieser Voraussetzungen ergibt sich, dass es keine wesentlichen Unterschiede zwischen den Gesetzen geben darf, weshalb sich aus dem Streit um die Anwendbarkeit im Wesentlichen lediglich Unterschiede hinsichilich der Aufsichtsbehörde und dem zu beschreitenden Rechtsweg ergeben.

2. Die Anträge der Antragstellerin konnten auch nicht in ein Auskunftsbegehren nach § 19 DSG-EKD ausgelegt werden. Zum einen hat die Antragstellerin deutlich gemacht, dass sie eine Auskunft nach dem DSG-EKD nicht begehrt, zum anderen wäre ein darauf gerichteter Prozesskostenhilfeantrag als mutwillig zu erachten, weil die Antragsgegnerin mehrfach betont hat, dass sie bei Vorlage einer Vollmacht nach DSG-EKD bereit ist, die geforderte Auskunft zu erteilen. Darüber hinaus wäre für ein Begehren nach DSG-EKD nicht der Rechtsweg zur Zivilgerichtsbarkeit, sondern gem. § 47 Abs. 1 Nr. 3 DSG-EKD zu den kirchlichen Verwaltungsgerichten eröffnet.

(Eingesandt von RA Dr. Martin Riemer, Brühl)

Ein immaterieller Schadensersatz nach Art. 82 DS-GVO muss konkretisiert sein (Ls)

(**Landgericht Bremen**, Beschluss vom 16. Juli 2021 – 1 W 18/21 –)

1. **Ein Anspruch auf Schadensersatz nach Art. 82 DS-GVO setzt den Eintritt eines materiellen oder immateriellen Schadens voraus. Auch zur Geltendmachung eines Anspruchs auf Ersatz immaterieller Schäden genügt die Behauptung eines Verstoßes gegen die Vorschriften der DS-GVO ohne Vorbringen zu einem hierdurch entstandenen immateriellen Schaden nicht.**

2. **Im Verfahren über die Bewilligung von Prozesskostenhilfe besteht keine Pflicht der einzelstaatlichen Gerichte zur Vorlage an den Europäischen Gerichtshof für ein Vorabentscheidungsverfahren nach Art. 267 Abs. 3 AEUV.**

Schadensersatzanspruch aus Art. 82 DS-GVO wegen der unberechtigten Nutzung einer anwaltlichen E-Mail-Adresse zwecks Werbung

(**Amtsgericht Pfaffenhoven**, Urteil vom 9. September 2021 – 2 C 133/21 –)

1. **Die Werbung mittels E-Mail-Marketing setzt für die Zulässigkeit außerhalb der Fälle des § 7 Abs. 3 UWG eine – vorherige und ausdrückliche – Einwilligung voraus, mithin eine Willenserklärung, die ohne Zwang für den konkreten Fall in Kenntnis der Sachlage erfolgt.**

2. **Auf eine Erheblichkeitsschwelle kommt es bei dem Schadensersatzanspruch des Art. 82 DS-GVO nicht an, da eine solche in der DS-GVO nicht erkennbar wird; zudem spricht für einen weiten Schadensbegriffs auch die Zielsetzung der DS-GVO.**

3. **Die Schwere des immateriellen Schadens ist für die Begründung der Haftung nach Art. 82 Abs. 1 DS-GVO irrelevant und wirkt sich nur auf die Höhe des Anspruchs aus.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien streiten über Ansprüche wegen Verletzung von Datenschutzvorschriften.

Am 25.01.2021 erhielt der Kläger von der Beklagten eine Werbe-E-Mail, unstreitig, ohne dass er zuvor eine Anfrage an die Beklagte gerichtet hatte.

Der Kläger bat daraufhin mit Antwort-E-Mail die Beklagte um Mitteilung, wann sie seine Adresse gespeichert habe und woher sie sie erhalten habe, und um Übersendung einer Unterlassungserklärung verbunden mit einem Vertragsstrafeversprechen.

Es kam zu weiterer Kommunikation der Parteien. Zur Herkunft der Adresse teilte die Beklagte mit Email vom 06.02.2021 mit, sie habe sich bezüglich einer Rechtsberatung im Heimatort umgesehen und darunter die Dienstleistung bzw. Kontaktdaten des Klägers entdeckt; da sich die Fragestellungen klären konnten, habe es keinen weiteren Bedarf für eine Kontaktaufnahme gegeben. Die Mailing-Aktion habe ausschließlich auf Kontaktdaten basiert, die manuell erfasst wurden.

Die Beklagte gab die vom Kläger erbetene Unterlassungsverpflichtung ab.

Der Kläger machte geltend, es bedürfe einer gerichtlichen Klärung, da der Kläger ein besonderes Interesse habe, dass die anwaltlich genutzte Adresse nicht missbräuchlich angesprochen werde. und forderte des Weiteren ein Schmerzensgeld von mindestens 300,00 €.

Der Kläger erhob daher zunächst Klage mit dem Antrag:

die Beklagte wird verurteilt, dem Kläger Auskunft zu erteilen über die Herkunft der E-Mail Adresse des Klägers und über den Zeitpunkt der Speicherung durch die Beklagte.

Der Kläger trug sodann vor, die Adresse sei zwischenzeitlich mit weiteren Angeboten bespamt worden mit ähnlichen Produkten, und es sei nicht nachzuvollziehen, woher der Absender die Adresse erhalten habe.

Der Kläger führt insofern aus, es sei gemäß Art. 82 DS-GVO immaterieller Schadenersatz zu zahlen. Er meint, dass der Vortrag datenschutzwidriger Verwendung ohne Einwilligung als ausreichend anzusehen sei. Die Werbung der Beklagten sei eindeutig ein rechtswidriger Eingriff gewesen. Die Beklagte habe auch gegen Art. 14 DS-GVO verstoßen.

Durch die rechtswidrige Werbung auf die Kanzlei-Adresse habe sich der Kläger nicht nur mit der Frage der Abwehr der Werbung auseinander setzen müssen, sondern auch damit, wie die Beklagte an die Adresse kam. Die Werbeansprache sei daher nicht nur lästig oder ärgerlich gewesen sondern habe den Kläger beschäftigt und belastet, auch die Nichterteilung der Auskünfte sei ein Verstoß gegen den Datenschutz, insbesondere Art. 15 DS-GVO.

Dies sei ausreichend für die Festsetzung eines Schmerzensgeldes. Berücksichtigt sei, dass die Beklagte sich vorsätzlich, zumindest aber grob fahrlässig über die DS-GVO hinweg gesetzt habe.

Aus den Gründen:

I.

Dem Kläger steht gem. Art. 82 DS-GVO ein Anspruch auf Ersatz immateriellen Schadens zu, den das Gericht wie tenoriert bemisst.

Die Beklagte hat gegen Bestimmungen der DS-GVO verstoßen, die Verstöße haben nach dem – insoweit auch unwidersprochen gebliebenen und damit zugestandenen (§ 138 Abs. 3 ZPO) Vorbringen des Klägers kausal zu einem immateriellen Schaden geführt.

Die Beklagte hat zum einen die Email-Adresse des Klägers ohne Rechtfertigung i.S.d. Art. 6 DS-GVO verarbeitet, zum anderen dem Kläger verspätet bzw. zunächst nicht vollständig Auskunft erteilt.

a.

Die Beklagte hat unstreitig i.S.d. Art. 4 DS-GVO die Email-Adresse des Klägers verarbeitet (erhoben, erfasst und gespeichert, und durch ihr Anschreiben weiter verwendet).

Hierfür – jedenfalls für die Speicherung und Verwendung wie erfolgt – konnte die Beklagte keinen rechtfertigenden Tatbestand i.S.d. Art. 6 Abs. 1 DS-GVO darlegen. Die Beklagte behauptet insbesondere schon selbst nicht (geschweige denn belegt dies), dass der Kläger hierin eingewilligt hätte. Sie behauptet im Prozess schon selbst nicht, dass der Kläger ihr etwa seine Email-Adresse (und dies mit entsprechender Einwilligung) mitgeteilt hätte oder (auch wenn dies in der streitgegenständlichen Email so angegeben gewesen war) der Kläger eine Anfrage an die Beklagte gesandt hätte (Fall der Nachfragewerbung, vgl. Eckhardt, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl., § 25 b) Rdnr. 82 m.N.w., zit. nach beck-online) oder etwa ein Fall des § 7 Abs. 3 UWG vorgelegen hätte (dies würde u.a. voraussetzen, dass ein Unternehmer – hier die Beklagte – im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von einem Kunden dessen elektronische Postadresse erhalten hat; dies war unstreitig ebenfalls nicht der Fall). Die Beklagte trug vielmehr vor, die Email-Adresse des Klägers aus frei zugänglicher Quelle im Internet gefunden zu haben, bei der Suche nach einer Rechtsberatung. Sie hat die Email-Adresse jedoch – selbst wenn die ursprüngliche Erfassung zu einem berechtigten Zweck erfolgt sein sollte, wie die Beklagte wohl behauptet – unstreitig nicht hierfür gespeichert und verwendet, sondern (als auch nach ihrem eigenen Vorbringen der ursprüngliche Zweck längst entfallen gewesen wäre) zum Zwecke der Werbung, die jedoch mangels vorheriger Einwilligung des Klägers gegen § 7 Abs. 2 Nr. 3 UWG und Art. 6 Abs. 1 S. 1 verstieß.

Die Werbung mittels E-Mail-Marketing setzt für ihre Zulässigkeit außerhalb der Fälle des § 7 Abs. 3 UWG eine – vorherige und ausdrückliche – Einwilligung voraus, mithin eine Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt (vgl. Eckhardt a.a.O. Rdnr. 86 m.Nw.). Eine solche wird schon durch die Beklagte – welche insoweit darlegungs- und beweisbelastet wäre – nicht im Ansatz behauptet oder vorgetragen.

Ebenso wenig ist aus dem Vorbringen einer – auch nur z.B. konkludent – erteilten Einwilligung iSd Art. 6 Abs. 1 S. 1 lit a. DS-GVO zu entnehmen. Auch keiner der weiteren Fälle der Vorschrift ist zu erkennen, insbesondere auch nicht ein Fall des Art. 6 Abs. 1 S. 1 lit. f. DS-GVO (überwiegende berechtigte Interessen des Verwantwortlichen oder eines Dritten). Gem. Erwägungsgrund 47 ist im Rahmen der Interessenabwägung nach lit. f zu prüfen, „ob eine betroffene Person zum Zeitpunkt der Datenerhebung und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird“ (vgl. Gola DS-GVO/Schulz, 2. Aufl. 2018, DS-GVO Art. 6 Rn. 61). Im Rahmen der Interessenabwägung ist zunächst der vom Datenverarbeiter verfolgte Zweck mit der Art, dem Inhalt sowie der Aussagekraft der Daten gegenüberzustellen; zu berücksichtigen sind sodann insbesondere die vernünftige Erwartungshaltung der betroffenen Person bzw. die Absehbarkeit (Branchenüblichkeit) der Verarbeitung sowie ihre Beziehung zu dem Verantwortlichen (BeckOK DatenschutzR/Albers/Veit, 36. Ed. 01.05.2020, DS-GVO Art. 6 Rn. 53). Vorliegend führt bereits vor diesem Hintergrund die Abwägung hier zu dem Ergebnis, dass die schutzwürdigen Interessen des Klägers – welcher unstreitig in keinerlei vorheriger Beziehung zur Beklagten gestanden und auch sonst nicht nachweisbar seine Email-Adresse selbst in einer Weise, die solche Verwendung absehbar gemacht hätte, mitgeteilt oder veröffentlich hatte – die Interessen der Beklagten an einer Werbemaßnahme für von ihr vertriebene Masken überwogen. Zudem spricht viel dafür, auch insoweit die Maßstäbe des § 7 Abs. 2 UWG zu berücksichtigen. Das OVG Saarlouis (B.v. 16.02.2021, 2 A 355/19, NJW 2021, 2225) führte in einem Fall der unerlaubten Telefonwerbung hierzu aus, „dass die Bewertungsmaßstäbe des § 7 II Nr. 2 UWG, welcher der Umsetzung RL 2002/58/EG dient, auch im Rahmen des Art. 6 I Buchst. f DS-GVO zu berücksichtigen wären. Es ist zwar zutreffend, dass auch die Verarbeitung personenbezogener Daten für Direktwerbung ein berechtigtes Interesse nach dem Erwägungsgrund 47 DS-GVO darstellen kann. Aber auch in diesem Zusammenhang ist zu berücksichtigen, dass die Ziele, die mit der Verarbeitung verfolgt werden, unionrechtskonform sein müssen. Daher gilt auch in diesem Zusammenhang die Wertung des § 7 II Nr. 2 UWG Geltung beanspruchen, mit der Folge, dass sich die Kl. nicht auf ein „berechtigtes“ Interesse berufen kann. Für dieses Ergebnis spricht im Übrigen auch die Forderung, für die Auslegung des Art. 6 I Buchst. f DS-GVO als Ausgangspunkt konkret gefasste Erlaubnitatbestände aus dem nationalen Recht heranzuziehen, um dem allgemeinen Erlaubnistatbestand Konturen zu verleihen und Rechtssicherheit herzustellen“. Diese Ausführungen überzeugen und gelten ebenso für den hier vorliegenden Fall der Direktwerbung per Email, der ebenfalls von Art. 13 der Richtlinie 2002/58/EG erfasst und in § 7 Abs. 2 Nr. 3 UWG konkret geregelt ist.

Zudem hat die Beklagte auch gegen Art. 14 sowie 15 DS-GVO verstoßen. Gemäß Art. 14 DS-GVO hat der Verantwortliche in dem Fall, dass die Erhebung der Daten nicht bei der betroffenen Person selbst erfolgt ist – was hier unstrittig der Fall war – eine Informationspflicht gegenüber dem Betroffenen über die in Art. 14 Abs. 1, 2 genannten Einzelheiten, welche gem. Art. 14 Abs. 3 lit, a, b DS-GVO unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats, bzw. falls die personenbezogenen Daten zur Kommunikation mit der

betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie (auch in diesem Fall jedoch spätestens innerhalb eines Monats, vgl. Kühling/Buchner/Bäcker, 3. Aufl. 2020, DS-GVO Art. 14 Rn. 33; Paal/Pauly/Paal/Hennemann, 3. Aufl. 2021, DS-GVO Art. 14 Rn. 34) zu erfüllen ist. Eine Erfüllung dieser Pflicht – insbesondere innerhalb der Frist (die Beklagte speicherte die Daten ihrer eigenen Einlassung nach bereits ab 25.12.2020) – wurde nicht ersichtlich.

Des Weiteren hat der Betroffene gem. Art 15 DS-GVO ein Auskunftsrecht bzgl. der personenbezogenen Daten sowie über

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Jedenfalls hinsichtlich der Herkunft (oben lit. g) hat die Beklagte auf entsprechende Aufforderung des Klägers außergerichtlich keine Auskunft erteilt. Der Kläger hatte hinreichend präzise danach gefragt, woher die Beklagte seine Email-Adresse erhalten habe; die Beklagte teilte hierzu zunächst nur mit, es habe sich um „manuell erfasste" Daten gehandelt, und sie habe sich wegen einer Rechtsberatung in ihrem Heimatort umgesehen und darunter seine „Kontaktdaten entdeckt"; eine Angabe, wo sie diese denn „entdeckt" oder erhalten hat, um diese dann manuell zu erfassen, fehlt völlig, war jedoch ohne weiteres erkennbar das, wonach der Kläger gefragt hatte. Erst im Prozess mit der Klageerwiderung vom 30.03.21 (somit über 3 Monate nach der Datenerhebung und v.a. erst 2 Monate nach der Aufforderung des Klägers) ließ die Beklagte erkennen, dass sie offenbar – so ist ihr Vorbringen zu verstehen – öffentlich zugängliche Internetseiten als Quelle verwendet hatte.

b.

Des Weiteren kann dahinstehen, ob eine Haftung gem. Art. 82 DS-GVO von vornherein als verschuldensunabhängig zu sehen ist oder von einer Verschuldensvermutung oder Beweislastumkehr auszugehen ist (vgl. Paal/Pauly/Frenzel, Art. 82 DS-GVO, Rdnr. 6 m.Nw.); vorliegend ist jedenfalls schon nichts vorgetragen oder ersichtlich, was gegen ein Verschulden der Beklagten spräche.

c.

Die genannten Verstöße haben unter Berücksichtigung des klägerischen Vorbringens – welches insoweit nicht bestritten wurde – zu einem immateriellen Schaden des Klägers geführt (welcher entgegen der Ansicht des Klägers allerdings nicht in dem Verstoß allein als solchem liegt, sondern der Verstoß muss – dies auch kausal – zu einem Schaden geführt haben; Gegenteiliges ist auch der Entscheidung des BVerfG nicht zu entnehmen, dort wurde letztlich beanstandet, dass die Vorinstanz auf eine „Erheblichkeit" abgestellt hatte, jedoch nicht vorgegeben, dass ein kausaler Schaden als solcher gar nicht mehr vorliegen bzw. festgestellt werden müsste). Auf eine „Erheblichkeitsschwelle" kommt es insofern nicht an, da eine solche in der DS-GVO nicht erkennbar wird und für einen weiten Schadensbegriff auch die Zielsetzung der DS-GVO spricht; Verstöße müssen wirksam sanktioniert werden, damit die DS-GVO wirken kann (vgl. Frenzel a.a.O. Rdnr. 10). Die Schwere des immateriellen Schadens ist daher zutreffend für die Begründung der Haftung nach Art. 82 Abs. 1 DS-GVO irrelevant und wirkt sich nur noch bei der Höhe des Anspruchs aus (vgl. ArbG Düsseldorf Urt. v. 05.03.2020 – 9 Ca 6557/18, BeckRS 2020, 11910, Rdnr. 84, m.w.N.).

Der Schaden kann auch bereits etwa in dem unguten Gefühl liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind, insbesondere wenn nicht ausgeschlossen ist, dass die Daten unbefugt weiterverwendet werden, auch bereits in der Ungewissheit, ob personenbezogene Daten an Unbefugte gelangt sind. Unbefugte Datenverarbeitungen können zu einem Gefühl des Beobachtetwerdens und der Hilfslosigkeit führen, was die betroffenen Personen letztlich zu einem reinen Objekt der Datenverarbeitung degradiert. Den Kontrollverlust nennt EG 75 ausdrücklich als „insbesondere" zu erwartenden Schaden. Des Weiteren kommen etwa Ängste, Stress, Komfort- und Zeiteinbußen in Betracht. (vgl. Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18b)

Die Höhe des Anspruchs ist dabei nicht willkürlich, sondern auf der Grundlage der inhaltlichen Schwere und Dauer der Rechtsverletzung zu beurteilen, unter Berücksichtigung des Kontexts, der Umstände eines Verstoßes. Genugtuungs- und Vorbeugungsfunktion können bei der Bezifferung eine Rolle spielen. Einerseits darf die Höhe des Schadensersatzes keine Strafwirkung entfalten. Andererseits reicht ein künstlich niedrig bezifferter Betrag mit symbolischer Wirkung nicht aus, um die praktische Wirksamkeit des Unionsrechts sicherzustellen (vgl. Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 12a).

So sprach etwa das AG Hildesheim (U.v. 05.10.2020, 43 C 145/19, ZD 2021, 384) 800,00 € zu in einem Fall, in dem auf einem wiederaufbereiteten und weiterveräußerten PC private Daten des ursprünglichen Besitzers noch vorhanden und somit an den Dritten gelangt waren.

Das LG Lüneburg (Urteil vom 14.7.2020 – 9 O 145/19, ZD 2021, 275) etwa sprach 1.000,00 € zu in einem Fall eines rechtswidrigen Schufa-Eintrags.

Vorliegend berücksichtigt das Gericht, dass der Kläger (der selbst zunächst von der Beklagten 300,00 € gefordert hatte, im Rahmen der prozessualen Geltendmachung dann einen Bereich von nicht unter 100,00 € für angemessen hielt) nicht nur von einem, sondern von mehreren Verstößen der Beklagten gegen Vorschriften der DS-GVO betroffen war (s.o.). Andererseits blieben die Auswirkungen für den Kläger – anders als etwa in den beiden o.g. Fällen des AG Hildesheim und des LG Lüneburg im „eigenen Bereich" des Klägers, es wurde von den Verstößen kein Bereich tangiert (jedenfalls wurde derartiges nicht erkennbar), der Beziehungen des Klägers zu anderen Dritten betraf, etwa (auch nur potentiell) die Gefahr einer

Schädigung seines Ansehens, seiner Kreditwürdigkeit o.ä. bot. Die erkennbaren Auswirkungen lagen vielmehr darin, dass der Kläger sich – wie er unwidersprochen vortrug – sich mit der Abwehr der von ihm unerwünschten Werbung und der Herkunft der Daten auseinandersetzen musste. Gerade letzteres – zumal unter Berücksichtigung der Dauer des Verstoßes und der zunächst nicht ansatzweise zielführend erfolgten Auskunftserteilung – ist geeignet, zu einem durchaus belastenden Eindruck des Kontrollverlusts zu führen, zumal dies auch die Auseinandersetzung mit dem Verstoß und auch die Abwehr ggf. drohender anderweitiger Verstöße erschwert (die Quelle der Daten kann ja – und wird erfahrungsgemäß – auch die Quelle für andere sein, die ggf. unter Verstoß gegen die DS-GVO diese Daten verarbeiten). Vor diesem Hintergrund ist insbesondere die bestenfalls als zögerlich zu bezeichnende Information durch die Beklagte (die insoweit auch im Prozess recht vage blieb, wenn auch der Kläger dies nicht mehr weiter verfolgte) im Interesse einer effektiven Abschreckung als schmerzensgelderhöhend zu berücksichtigen. Soweit die Beklagte mit ihrem letzten Vorbringen möglicherweise behaupten will, nur zur Versorgung ihrer Mitmenschen agiert zu haben (quasi altruistisch), erscheint dies im Übrigen wenig lebensnah. Nicht zu berücksichtigen war dagegen, dass der Kläger zwischenzeitlich weitere unerwünschte Emails erhalten haben mag; eine Verantwortung der Beklagten hierfür wird schon nicht behauptet oder ersichtlich.

Das Gericht erachtet – auch im Vergleich mit den o.g. Entscheidungen, denen noch deutlich gravierendere (zumindest potentielle) Auswirkungen zugrundelagen – vorliegend im Ergebnis eine Entschädigung von 300,00 € für angemessen.

Die Entscheidung über die Zulassung der Berufung wegen grundsätzlicher Bedeutung der sich stellenden Rechtsfragen beruht auf § 511 Abs. 4 S. 1 Nr. 1 Alt. 1 ZPO.

Schmerzensgeld auf Grund der Verwendung eines diskriminierenden Fotos einer Beschäftigen zwecks Firmenwerbung (Ls)

(**Arbeitsgericht Münster**, Urteil vom 25. März 2021 – 3 Ca 391/20 –)

1. **Der Arbeitgeber verwendet ein Foto einer Mitarbeiterin in einer Werbebroschüre – unter Verstoß gegen die Datenschutzgrundverordnung und das Kunsturhebergesetz – dann unbefugt und in diskriminierender Weise, wenn er das Foto der Mitarbeiterin in einem auf ihre Hautfarbe bezogenen Kontext ohne deren schriftliches Einverständnis veröffentlicht.**

2. **Als Folge ist der der Mitarbeiterin ein Betrag eines Gehalts in Höhe von 5.000 Euro zu zahlen. Der Anspruch ergibt sich als Entschädigung nach § 15 AGG oder als Schmerzensgeld nach Art 82 I DS-GVO, § 823 BGB i.V.m. § 22 KUG.**

(Nicht amtliche Leitsätze)

Polizei darf Bahnreisenden nicht allein wegen Hautfarbe kontrollieren

(**Verwaltungsgericht Dresden**,Urteil vom 18. Januar 2022 – 6 K 438/19 –)

Die polizeiliche Kontrolle eines Bahnreisenden ist verfassungswidrig, wenn sie allein aufgrund seiner Hautfarbe erfolgt. Eine Verweigerung der Herausgabe des Personalausweis ist gerechtfertigt und darf nicht erzwungen werden.

(Nicht amtlicher Leitsatz)

Zur Speicherung des Geburtsdatums und der Anrede eines Apotheken-Online-Kunden

(**Verwaltungsgericht Hannover**, Urteil vom 9. November 2021 – 10 A 502/19 –)

Eine Online-Versandapotheke darf im Bestellvorgang das Geburtsdatum und die Anrede nicht bei jedem Produkt verarbeiten

Tatbestand:

Die Klägerin betreibt eine Online-Versandapotheke und wendet sich gegen eine datenschutzrechtliche Anordnung, die unter anderem auf die Unterlassung der Erhebung und Verarbeitung bestimmter Daten im Bestellprozess auf ihrer Webseite gerichtet ist.

Am 06.10.2018 gab eine Privatperson bei dem Bayerischen Landesamt für Datenschutzaufsicht (im Folgenden: BayLDA) eine Online-Beschwerde hinsichtlich der von der Klägerin betriebenen Online-Versandapotheke ein und rügte die Art und den Umfang der Datenerhebung während des Bestellprozesses. Das BayLDA leitete diese Beschwerde mit E-Mail vom 15.10.2021 zur Bearbeitung in eigener Zuständigkeit an die Beklagte weiter.

Die Beklagte stellte am 01.11.2018 fest, dass die Klägerin auf der Webseite „www.E..de“ im Rahmen des Bestellvorgangs, wenn sich der Kunde für die Option „Bestellung ohne Registrierung“ entscheidet und sodann das Feld „weiter ohne Kundenkonto“ auswählt, ein Bestellformular angezeigt bekommt, welches als verpflichtende Angaben (gekennzeichnet durch ein *) unter anderem die Anrede (mit den Auswahloptionen „Frau“ oder „Herr“) und das Geburtsdatum abfragt. Daraufhin wandte sich die Beklagte im Rahmen eines aufsichtsbehördliches Prüfungsverfahren nach Art. 57 Abs. 1 lit. a) und lit. f) und Art. 58 Abs. 1 lit b) Datenschutzgrundverordnung (im Folgenden: DS-GVO) mit einem Anhörungsschreiben vom 02.11.2018 an die Klägerin. Die Erhebung und Verarbeitung von Anrede und Geburtsdatum verstoße gegen die datenschutzrechtlichen Prinzipien der Rechtmäßigkeit und Datenminimierung.

Mit Schreiben vom 14.11.2018 teilte die Klägerin der Aufsichtsbehörde mit, dass nach ihrer Auffassung die Erhebung der Anrede und des Geburtsdatums der Kunden zur Erfüllung des Vertrages mit den Kunden sowie aufgrund gesetzlicher Vorgaben zwingend erforderlich sei. Die Erhebung und Verarbeitung des Geburtsdatums diene unter anderem dazu zu erfahren, ob der Vertragspartner eingeschränkt oder voll geschäftsfähig sei, weil im Falle einer eingeschränkten Geschäftsfähigkeit die Sorgeberechtigten des Bestellers den Vertrag genehmigen müssten. Die Erhebung dieser personenbezogenen Daten sei auch aufgrund einer Interessenabwägung für den Verantwortlichen zulässig, weil mit der Einnahme von Medikamenten in der Regel gesundheitliche Risiken/Nebenwirkungen verbunden seien. Vor diesem Hintegrund sei die Altersabfrage unumgänglich. Der Apotheker müsse soweit erforderlich, Medikamente altersgerecht dosieren bzw. entsprechende Altersempfehlungen der Hersteller berücksichtigen können. Unterließen Apotheker eine solche Prüfung, liefen sie Gefahr, nicht altersgerecht dosierte Medikamente an Kunden abzugeben und damit Pflichten aus dem Vertragsverhältnis erheblich zu verletzen. Die Abfrage der Anrede diene einer freundlichen und kundenangemessenen Ansprache und begründe daher ein überwiegendes berechtigtes Interesse der Klägerin an der Datenverarbeitung.

Mit Schreiben vom 06.12.2018 wies die Beklagte die Klägerin darauf hin, dass auch unter Berücksichtigung der erfolgten Stellungnahme noch Datenschutzrechtsverstöße festzustellen seien. Die Erhebung des Geburtsdatums sei nicht in jedem Fall erforderlich. So müsse die entsprechende Abfrage unterbleiben, soweit sie für eine altersgerechte Dosierung oder zur Berücksichtigung von Altersempfehlungen des Herstellers nicht notwendig sei. Auch die pauschale Erhebung der Anrede unabhängig davon, ob das bestellte Medikament im Einzelfall einen geschlechtsspezifischen Anwendungsbereich habe, verstoße gegen die datenschutzrechtlichen Prinzipien der Rechtmäßigkeit und Datensparsamkeit. Zudem liege ein Verstoß gegen das Transparenzgebot vor, soweit die Erhebung der Anrede auf ein berechtigtes Interesse zur freundlichen Ansprache gestützt werde. Dieses berechtigte Interesse werde als Rechtsgrundlage weder in der Datenschutzerklärung noch im Bestellformular genannt.

Die Klägerin reagierte hierauf mit Schreiben vom 28.12.2018 und vertiefte ihren Vortrag aus dem Anhörungsverfahren.

Mit Bescheid vom 08.01.2019 wies die Beklagte die Klägerin an, es ab dem 23.01.2019 zu unterlassen, auf der Webseite mit der URL https://www.E..de im Bestellprozess unabhängig von der Art des bestellten Medikaments das Geburtsdatum des Bestellers bzw. der Bestellerin zu erheben und/oder erheben zu lassen und zu verarbeiten und/oder verarbeiten zu lassen (Ziffer 1 des Bescheides). Außerdem wies die Beklagte die Klägerin an, es ab dem 23.01.2019 zu unterlassen, die Anrede, die auf der Webseite mit der URL https://www.E..de im Bestellprozess erhoben worden ist, zur Vertragserfüllung zu verwenden, wenn und soweit Gegenstand der Bestellung Medikamente sind, die nicht geschlechtsspezifisch zu dosieren und/oder einzunehmen sind (Ziffer 2 des Bescheides). Schließlich wies die Beklagte die Klägerin an, ab dem 23.01.2019 die Rechtsgrundlage für die Erhebung und Verarbeitung der Anrede im Bestellprozess, eine freundliche und kundenangemessene Ansprache und Kommunikation zu ermöglichen, auf der Webseite mit der URL https://www.E..de zu nennen (Ziffer 3 des Bescheides). Zur Begründung führte die Beklagte aus: Die Gestaltung des Bestellprozesses widerspreche der DS-GVO. Es liege eine Verletzung des Prinzips der Datensparsamkeit vor. So sei die Erhebung und Verarbeitung des Geburtsdatums ohne Rücksicht darauf, ob es sich im Einzelfall um ein Medikament handele, das altersgerecht zu dosieren sei, datenschutzrechtlich unzulässig. Soweit ein Medikament unabhängig vom Alter einzunehmen sei, sei die Erhebung des Geburtsdatums nicht erforderlich, um den Kaufvertrag mit dem Besteller ordnungsgemäß zu erfüllen. Die Erhebung und Verarbeitung des Geburtsdatums könne auch nicht auf die Wahrung eines berechtigten Interesses gestützt werden. Die Gewissheit darüber, ob jemand beschränkt geschäftsfähig sei oder nicht und damit die Einwilligung oder Genehmigung der Eltern bzw. sonstiger Inhaber der Vermögenssorge abzufragen sei, sei zwar ein berechtigtes Interesse. Hierfür sei es aber ausreichend, die Volljährigkeit als solche abzufragen. Die Verarbeitung der Anrede sei nicht in jedem Fall zur Vertragserfüllung notwendig. Soweit ein Medikament unabhängig vom Geschlecht einzunehmen sei, sei die Verarbeitung der Anrede nicht erforderlich. Eine freundliche und kundenangemessene Ansprache und Kommunikation sei zwar ein ideelles Interesse an Selbstdarstellung, und damit bestünde für die Klägerin grundsätzlich ein berechtigtes Interesse im Sinne der DS-GVO. Dieses werde aber weder in der Datenschutzerklärung und im Bestellformular noch im Übrigen auf der klägerischen Webseite genannt, sodass ein Verstoß gegen das Transparenzgebot vorliege.

Die Klägerin hat zwischenzeitlich in ihrem Bestellformular hinsichtlich der Anrede „Herr/Frau“ die Auswahloption „ohne Angabe“ eingefügt und ihre Datenschutzerklärung dahingehend ergänzt, dass die Abfrage dieses Datums zum Zweck einer freundlichen und kundenangemessenen Ansprache und Kommunikation sowie auf Grundlage von Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO erfolge.

Die Klägerin hat gegen diesen Bescheid am 22.01.2019 Klage erhoben. Zur Begründung wiederholt und vertieft sie ihre Darlegung aus dem Verwaltungsverfahren. Ergänzend trägt sie im Wesentlichen noch vor, dass sich die Rechtmäßigkeit der Erhebung und Verwendung des Geburtsdatums auch aus § 2 Abs. 1 Nr. 3 der Verordnung über die Verschreibungspflicht von Arzneimitteln (im Folgenden: AMVV) ergebe. Hiernach dürften Apotheker gemäß einer ärztlichen Verschreibung Arzneimittel nur dann an Besteller abgeben, wenn die entsprechende Verschreibung bestimmte Daten enthalte. Hierzu gehöre auch das Geburtsdatum. Die Erhebung und Verarbeitung des Geburtsdatums folge aus dieser Regelung verpflichtend. Zudem ergebe sich aus § 1 der Berufsordnung der Apothekerkammer Niedersachsen eine Beratungsplicht zur altersgerechten Dosierung von Medikamenten, sodass auch hiernach die Erhebung und Verarbeitung des Geburtsdatums erforderlich sei und keinen datenschutz-

rechtlichen Verstoß darstelle. Hierfür sei es auch nicht ausreichend, lediglich eine Altersspanne abzufragen. Zudem sei grundsätzlich davon auszugehen, dass die das Medikament erwerbende Person auch die Person sei, die es später konsumieren werde. Anders als in der Apotheke könne der Onlinehändler aber nicht an den Äußerlichkeiten der Person abschätzen, wie alt die das Medikament bestellende Person sei und welcher Beratungsumfang gegebenenfalls erforder-lich sei. Dem werde durch die Abfrage des Geburtsdatums entgegengewirkt. Die Entscheidung eines Apothekers, welche Daten aus seiner Sicht für eine qualitativ hochwertige, sorgfältige und umfassende Beratung notwendig seien, sei Teil seines durch Art. 12 GG geschützten Berufsrechts. Die Klägerin habe auch ein berechtigtes Interesse daran, das Geburtsdatum abzufragen, um die Volljährigkeit des Kunden abzufragen und damit die Wirksamkeit des Vertrages beurteilen zu können. Dies sei über die Abfrage des konkreten Geburtsdatums zuverlässiger möglich. Denn die Hemmschwelle hier gleich drei falsche Daten (Tag, Monat und Jahr) anzugeben, sei geringer, als wenn man einfach nur ein Häkchen zur Bestätigung der Volljährigkeit setzen müsste. Im Hinblick auf die Erhebung des Geschlechts/der Anrede benenne die Klägerin in ihrer Datenschutzerklärung nunmehr, dass die Verarbeitung der geschlechtsspezifischen Angaben zum Zwecke einer freundlichen und kundenangemessenen Kommunikation diene. Da dies aber für Besteller offensichtlich sei, habe hierzu rechtlich keine Pflicht bestanden. Darüber hinaus müssten Apotheker nach § 20 Apothekenbetriebsordnung (ApBetrO) bei der Information und Beratung über Arzneimittel insbesondere die Aspekte der Arzneimittelsicherheit berücksichtigen. Hierzu gehöre auch, über etwaige Neben- und Wechselwirkungen mit anderen Medikamenten zu beraten. Unabhängig davon, ob das bestellte Medikament eine Geschlechtsbezogenheit aufweise, könne die Geeignetheit eines Medikamentes nur dann zutreffend beurteilt werden, wenn der Apotheker das Geschlecht kenne und demnach abschätzen könne, welche anderen Medikamente der Patient unter Umständen einnehme, um gegebenenfalls entsprechende Rückfragen stellen zu können. Die Anordnungen der Beklagten seien schließlich auch unverhältnismäßig. Der Klägerin werde in unzumutbarer Weise die Änderung ihrer Bestellabläufe auferlegt.

Aus den Gründen:

II. Der Bescheid der Beklagten vom 08.01.2019 ist hinsichtlich der unter Ziffer 1 tenorierten Untersagungsverfügung rechtmäßig und verletzt die Klägerin nicht in ihren Rechten (§ 113 Abs. 1 Satz 1 VwGO).

1. Rechtsgrundlage für die noch streitgegenständliche Anordnung ist Art. 58 Abs. 2 lit. d) der Datenschutzgrundverordnung (DS-GVO), Verordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Abl. L 119) i.V.m. § 20 Abs. 1 Niedersächsisches Datenschutzgesetz (NDSG). Hiernach verfügt jede Aufsichtsbehörde über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten, den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen.

2. Die Anordnung in Ziffer 1 des Bescheides der Beklagten vom 08.01.2019 ist formell rechtmäßig. Die Beklagte ist insbesondere aufgrund von Art. 51 Abs. 1 DS-GVO i.V.m. § 40 Abs. 1 Bundesdatenschutzgesetz (BDSG), § 22 Abs. 1 Nr. 1 NDSG zuständige Aufsichtsbehörde für die Überwachung von nichtöffentlichen Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen. Insoweit weist Art. 51 Abs. 1 DS-GVO die Mitgliedstaaten der Europäischen Union an, eine unabhängige Behörde für die Überwachung der Anwendung der Verordnung zu schaffen. Aufgrund dieser Regelung hat der Bundesgesetzgeber mit Wirkung zum 25.05.2018 § 40 Abs. 1 BDSG neu gefasst und den Ländern die Überwachung des Anwendungsbereiches der DS-GVO für nichtöffentliche Stellen übertragen (vgl. Art. 1 und Art. 8 Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 30.06.2017; BGBl. I 2017, S. 2097). Der niedersächsische Gesetzgeber hat die Wahrnehmung dieser Aufgaben in § 22 Abs. 1 Nr. 1 NDSG der Landesbeauftragten für den Datenschutz überantwortet.

3. Die Anordnungen sind auch materiell rechtmäßig.

a) Die Anordnung der Beklagten in Ziffer 1 des Bescheides vom 08.01.2019 zur Verarbeitung des Geburtsdatums genügt dem aus dem Rechtsstaatsprinzip folgenden Bestimmtheitsgebot. Der Bestimmtheitsgrundsatz verlangt, dass der Inhalt der behördlichen Entscheidung für den Adressaten verständlich ist. Der Adressat muss erkennen können, was von ihm gefordert wird. Der Wille der Behörde muss vollständig und eindeutig zum Ausdruck kommen. Allerdings genügt es, wenn sich der Inhalt des Verwaltungsakts anhand seiner Begründung und unter Heranziehung von Umständen, die den Beteiligten bekannt sind, durch Auslegung bestimmen lässt (vgl. Bayerischer VGH, Beschl. v. 26.02.2007 – 1 z.B. 06.2296 –, juris m.w.N.). In der streitgegenständlichen Anordnung heißt es zwar nur, dass angeordnet werde, es zu unterlassen, im Bestellprozess „unabhängig von der Art des bestellten Medikaments“ das Geburtsdatum zu erheben und zu verarbeiten. Im Zusammenhang mit der Begründung des Bescheides ergibt sich aber eindeutig, dass eine Unterlassung der Datenerhebung nur für diejenigen Produkte angeordnet wird, die auf der Webseite der Klägerin bestellbar sind und keine altersabhängige Dosierung erfordern. So heißt es in der Begründung zu dieser Ziffer im Bescheid wörtlich: „Die pauschale Erhebung und Verarbeitung des Geburtsdatums ohne Rücksicht darauf, ob es sich im Einzelfall um ein Medikament handelt, das altersgerecht zu dosieren ist, ist datenschutzrechtlich unzulässig.“

b) Das Geburtsdatum als allgemeines Personendatum stellt ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO dar. Bei der Abfrage dieses Datums im Bestellformular auf der klägerischen Homepage handelt es sich auch um einen Verarbeitungsvorgang im Sinne der DS-GVO. Denn nach der in Art. 4 Nr. 2 DS-GVO enthaltenen Begriffsbestimmung bezeichnet der Ausdruck „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vor-

gang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

c) Die Erhebung und Verarbeitung des Geburtsdatums unabhängig davon, welches Produkt bestellt wird, verstößt gegen das in Art. 5 Abs. 1 lit. a DS-GVO normierte Prinzip der Rechtmäßigkeit und steht somit im Widerspruch zur DS-GVO.

Nach Art. 5 Abs. 1 lit. a DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Dies entspricht der Vorgabe von Art. 8 Abs. 2 Satz 1 Grundrechtecharta der EU (GRC), wonach personenbezogene Daten nur mit Einwilligung der betroffenen Person oder auf Basis sonstiger gesetzlich geregelter legitimer Grundlagen verarbeitet werden dürfen. Diesen Grundsatz nimmt Art. 6 Abs. 1 DS-GVO durch die Anforderung auf, dass eine der dort geregelten Rechtsgrundlagen zur Datenverarbeitung vorliegen muss (vgl. Schantz, in: BeckOK Datenschutzrecht, 37. Ed., Stand 01.05.2020, Art. 5 DS-GVO, Rn. 5).

Die Erhebung und Verarbeitung des Geburtsdatums im Bestellprozess auf der streitgegenständlichen Homepage der Klägerin – auch für solche Produkte, die altersunabhängig zu dosieren sind – kann auf keine der in Art. 6 DS-GVO genannten Rechtsgrundlagen gestützt werden.

aa) Nachdem die Klägerin sich im Bestellprozess unstreitig keine Einwilligung des Bestellers zur Datenverarbeitung einholt, kann die Verarbeitung des Geburtsdatums nicht auf Art. 6 Abs. 1 lit. a) DS-GVO gestützt werden.

bb) Die Abfrage des Geburtsdatums kann nicht auf Art. 6 Abs. 1 lit. b) DS-GVO gestützt werden. Hiernach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Dies ist vorliegend nicht der Fall. Die Formulierung „zur Erfüllung eines Vertrages“ darf nicht im rechtstechnischen Sinne zu eng verstanden werden. Neben der „Erfüllung“ im engeren Sinne sind die Vorbereitung und Anbahnung des Vertrages, dessen Durchführung sowie auch dessen Abwicklung insbesondere zur Erfüllung von Gewährleistungspflichten oder sekundären Leistungspflichten erfasst (vgl. Plath, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, Art. 6 DS-GVO, Rn. 11). Auch vorvertragliche Maßnahmen können eine Verarbeitung legitimieren, allerdings nur, wenn sie „auf Anfrage der betroffenen Person erfolgen“. Liegt ein Vertrag i.S.d. Art. 6 Abs. 1 lit. b) DS-GVO vor, so muss die Verarbeitung zur Durchführung des Vertrages bzw. der Vertragsanbahnung objektiv erforderlich sein, damit der Erlaubnistatbestand zur Anwendung kommen kann. Ist dies der Fall, ist eine weitere Interessenabwägung grundsätzlich entbehrlich (Plath, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, Art. 6 DS-GVO, Rn. 16). Die DS-GVO definiert den Begriff der Erforderlichkeit nicht ausdrücklich. Einen Anhaltspunkt gibt aber der Erwägungsgrund 39. Hier heißt es: „Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.“ Die Verwendung des Begriffs „Zumutbarkeit“, lässt den Rückschluss zu, dass für die Feststellung der Erforderlichkeit grundsätzlich keine übermäßig strengen Maßstäbe angesetzt werden dürfen. Demnach wird vertreten, dass die Datenverarbeitung bereits dann erforderlich ist, wenn kein milderes, wirtschaftlich gleich effizientes Mittel zur Verfügung steht, um den entsprechenden Zweck mit gleicher Sicherheit zu verwirklichen (Plath, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, Art. 6 DS-GVO, Rn. 18). Eine Verarbeitung von personenbezogenen Daten wird auch dann als erforderlich angesehen, wenn sie zwar nicht unumgänglich für den Vertragsschluss ist, jedoch für die Erreichung des Geschäftszwecks als förderlich angesehen werden kann. Demnach gilt, dass die Erforderlichkeit auch dann anzunehmen ist, wenn zwar ein milderes Mittel zur Verfügung steht, also das Rechtsgeschäft auch ohne die konkrete Verwendung der Daten durchgeführt werden könnte, die Wahl eines solchen Mittels jedoch mit Nachteilen für den Verantwortlichen und/oder die betroffenen Personen verbunden wäre. Dies gilt umso mehr, wenn die Verwendung der Daten auch im Interesse der betroffenen Person geschieht, etwa um einen besseren Service oder eine schnellere Abwicklung zu ermöglichen. Neben der Verarbeitung der sogenannten „Stammdaten“, wie den Namen, die Anschrift und der Zahlungsinformationen, können grundsätzlich je nach Einzelfall zusätzlich die Verarbeitung von „weiteren Daten“, etwa die Verarbeitung des Geburtsdatums, zumindest des Geburtsjahrs, zur Verifizierung der Geschäftsfähigkeit bzw. eines Mindestalters oder zur Unterscheidung mehrerer gleichnamiger Kunden zulässig sein. Im Rahmen dieser Einzelfallentscheidung ist mit dem Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DS-GVO abzuwägen (Plath, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, Arti-kel 6 DS-GVO, Rn. 21).

Legt man diesen Maßstab zugrunde, ist die Erhebung und Verarbeitung des genauen Geburtsdatums, welches sich aus Tag, Monat und Jahr zusammensetzt, nicht zur Erfüllung des Vertrages über altersunabhängig zu dosierende Produkte erforderlich. Typischerweise schließen die Klägerin und die von ihrer Webseite bestellenden Personen einen Kaufvertrag über das bestellte Produkt ab. Die Klägerin ist zur Erfüllung dieses Vertrages dazu verpflichtet, dem Besteller das Produkt zu übergeben und das Eigentum daran zu verschaffen, während der Besteller dazu verpflichtet ist das bestellte Produkt zu bezahlen. Hierfür ist die Abfrage des Geburtsdatums grundsätzlich nicht erforderlich. Der Klägerin ist zwar darin zuzustimmen, dass ihr als Apothekenversandhandel besondere Beratungs-, Informations- und Aufklärungspflichten zukommen und diese (wohl) auch als vertragliche Nebenpflichten zu qualifizieren sind. So hat der Apotheker Patienten und andere Kunden sowie die zur Ausübung der Heilkunde, Tierheilkunde oder Zahnheilkunde berechtigten Personen über Arzneimittel und apothekenpflichtige Medizinprodukte hinreichend zu beraten und zu informieren. Die Information und Beratung über Arzneimittel muss insbesondere Aspekte der Arzneimittelsicherheit berücksichtigen sowie die sachge-

rechte Anwendung des Arzneimittels umfassen. Der Apotheker hat auch über eventuelle Nebenwirkungen oder Wechselwirkungen, die sich aus den Angaben auf der Verschreibung und den Angaben des Patienten oder Kunden ergeben sowie über die sachgerechte Aufbewahrung oder Entsorgung des Arzneimittels zu informieren und zu beraten, soweit dies erforderlich ist. Er hat bei Patienten und anderen Kunden gewissenhaft zu ermitteln, inwieweit diese gegebenenfalls weiteren Informations- und Beratungsbedarf haben, und ihnen eine entsprechende Beratung anzubieten. Im Falle der Selbstmedikation ist auch festzustellen, ob das gewünschte Arzneimittel zur Anwendung bei der vorgesehenen Person geeignet erscheint oder in welchen Fällen anzuraten ist, gegebenenfalls einen Arzt aufzusuchen (vgl. § 20 ApBetrO, entsprechende Regelungen enthalten auch die Berufsordnungen der verschiedenen Apothekerkammern, vgl. für Niedersachsen § 9 Berufsordnung der Apothekerkammer Niedersachsen).

Die Kammer zweifelt nicht daran, dass im Rahmen dessen auch eine Beratung zur altersgerechten Dosierung erforderlich sein kann. Unabhängig davon, ob zum Zwecke einer altersgerechten Beratung die Abfrage des Geburtsdatums des Bestellers tatsächlich das richtige Mittel ist – insoweit teilt die Kammer die Ansicht der Beklagten, dass konsequenterweise das Alter derjenigen Person abgefragt werden müsste, für die das bestellte Produkt zur Anwendung/Einnahme bestimmt ist, welche nicht unbedingt mit der des Bestellers personengleich sein muss – zeigt ein Blick in die klägerische Produktpalette, dass auf der streitgegenständlichen Webseite ein großes Sortiment an Waren angeboten wird, welche offensichtlich altersunabhängig angewendet oder konsumiert werden. Die entsprechenden Produkte können dementsprechend klassischerweise auch in einer Drogerie, in der grundsätzlich nicht die Möglichkeit einer Beratung durch einen Apotheker besteht, erworben werden. Beispielhaft seien hier nur die folgenden Produktfelder genannt: Pflaster, Verbandsmaterial, Gesichts- und Körperpflegecremes, Fußbäder, Einlegesohlen, Parfums, Raumdüfte, Hand- und Nagelpflegeprodukte sowie Haarpflegeprodukte. Ein besonderer altersabhängiger Beratungsbedarf ist bei diesen Produkten nicht erkennbar, besondere altersbedingte Nebenpflichten wie eine Beratungsobliegenheit zum Vertrag lassen sich für diese Produkte demnach nicht konzipieren.

Im Übrigen spricht einiges dafür, dass die Klägerin das Argument der altersgerechten Beratung nur vorschiebt. Sollte die Abfrage des Geburtsdatums tatsächlich einer altersgerechten Beratung dienen, leuchtet nicht ein, weshalb andere Daten, die für eine adäquate Beratung erforderlich sind – wie etwa Fragen nach einer Schwangerschaft/Einnahme anderer Medikamente –, nicht abgefragt werden.

Die Klägerin dringt auch nicht mit dem Argument durch, sie müsse zur Überprüfung der Geschäftsfähigkeit des Bestellers das Geburtsdatum abfragen. Dem Risiko einer Rückabwicklung bei schwebend-unwirksamen Verträgen kann mit der einfachen Abfrage der Volljährigkeit gleichermaßen begegnet werden. Soweit die Klägerin meint, die Hemmschwelle, unwahre Angaben zu machen, sei bei dieser Abfrageart geringer als wenn das gesamte Geburtsdatum abgefragt wird, folgt die Kammer dem nicht. Es ist vielmehr davon auszugehen, dass Personen, die die Anonymität des „Online-Shoppens“ missbräuchlich ausnutzen wollen, hiervon auch nicht dadurch abgehalten werden, dass sie ein volles Geburtsdatum angeben müssen. Zudem ist darauf hinzuweisen, dass die Abfrage des Geburtsdatums zumindest in den Fällen, in denen sich die Geschäftsunfähigkeit nicht aus dem Alter, sondern aus dem Gesundheitszustand des Bestellers ergibt, auch nicht dazu geeignet ist, die Klägerin vor (schwebend) unwirksamen Vertragsabschlüssen zu schützen.

Soweit das Geburtsdatum bei Online-Bestellvorgängen in Einzelfällen als Identifizierungskriterium erforderlich sein könnte, hat die Klägerin schon nicht geltend gemacht, das Geburtsdatum für diesen Zweck zu benötigen.

cc) Die Abfrage des Geburtsdatums kann nicht auf Art. 6 Abs. 1 lit. c) DS-GVO gestützt werden. Hiernach ist die Datenverarbeitung zulässig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist. In Abgrenzung zu Art. 6 Abs. 1 lit. b DS-GVO meint Art. 6 Abs. 1 lit. c DS-GVO mit „rechtlicher Verpflichtung“ nicht eine auf einer privatautonomen Entscheidung beruhende vertragliche Obligation, sondern eine Verpflichtung kraft Rechts der Union oder eines Mitgliedstaates. Eine solche rechtliche Verpflichtung ist für die Produktpalette der Klägerin, die eine altersabhängige Dosierung nicht erfordern, nicht ersichtlich.

Insbesondere ergibt sie sich nicht aus § 2 Abs. 1 Nr. 3 Arzneimittelverschreibungsordnung. Nach dieser Norm muss eine Verschreibung den Namen und das Geburtsdatum der Person, für die das Arzneimittel bestimmt ist, enthalten.

Die Klägerin kann sich auf diese Vorschrift bereits nicht berufen, weil vorliegend streitgegenständlich nur der Bestellprozess über rezeptfreie Produkte auf der Webseite der Klägerin ist. Schließlich können nur solche über den von der Beklagten geschilderten Bestellprozess ohne Registrierung geordert werden. Die Bestellung von rezeptpflichtigen Medikamenten über die Webseite der Klägerin erfolgt auf gesondertem Wege und erfordert die Einsendung des Rezepts auf dem postalischen Weg.

Sollte man die bereits benannten Informations- und Beratungspflichten von Apothekern nicht als vertragliche Neben-, sondern als gesetzliche Pflichten qualifizieren, so ist für diejenigen von der Klägerin angebotenen Produkte, die altersunabhängig zu dosieren/anzuwenden sind, auf die unter bb) dargelegten Ausführungen zu verweisen.

dd) Die Abfrage des Geburtsdatums für altersunabhängig zu dosierende Produkte kann schließlich auch nicht auf Art. 6 Abs. 1 lit. f) DS-GVO gestützt werden. Hiernach ist die Datenverarbeitung rechtmäßig, wenn die Verarbeitung 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, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Die Erforderlichkeit der Verarbeitung wird auch hier wie unter lit. b) dann ange-

nommen, wenn kein milderes, wirtschaftlich gleich effizientes Mittel zur Verfügung steht, den entsprechenden Zweck mit gleicher Sicherheit zu verwirklichen (Plath, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, Art. 6 DS-GVO, Rn. 56).

Soweit die Klägerin vorträgt, ein berechtigtes Interesse daran zu haben, in Erfahrung bringen zu können, ob der Besteller aufgrund seines Alters (beschränkt) geschäftsfähig ist, so bedarf es einer Abwägung zu dem diesem Interesse gegenüberstehenden Recht auf informationelle Selbstbestimmung des jeweiligen Bestellers aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vorliegend schon nicht, weil es bereits an der Erforderlichkeit der Datenerhebung zu diesem Zweck scheitert. Die Klägerin muss sich diesbezüglich – wie bereits dargelegt – auf das mildere gleich effiziente Mittel der Abfrage der Volljährigkeit verweisen lassen.

d) Die getroffene Anordnung stellt sich auch nicht als unverhältnismäßig dar. Sie ist geeignet, den Widerspruch zur DS-GVO zu unterbinden. Es ist auch kein milderes gleich effizientes Mittel zur Beseitigung des rechtswidrigen Zustandes ersichtlich – insbesondere musste die Beklagte sich nicht auf das Mittel der Verwarnung beschränken, nachdem die Klägerin im behördlichen Anhörungsverfahren schon zu erkennen gegeben hatte, dass sie einen Datenrechtsverstoß hinsichtlich der Verarbeitung des Geburtsdatums nicht anerkenne. Es ist auch nicht erkennbar, dass es der Klägerin unzumutbar wäre bzw. sie unverhältnismäßig stark belasten würde, technisch ihre Webseite so zu konzipieren, dass das Geburtsdatum nur bei denjenigen Produkten abgefragt wird, bei denen eine altersabhängige Beratung erforderlich ist. Dies ist der Kammer auch von anderen Online-Händlern bekannt, die beispielsweise Videospiele mit einer Altersbeschränkung oder Spirituosen anbieten und auf deren Webseite für nur diese Produkte eine besondere Abfrage erfolgt. Die Kammer geht auch nicht davon aus, dass eine entsprechende Umstellung der Webseite mit erheblichen wirtschaftlichen Einbußen – wenngleich mit einem gewissen Arbeitsaufwand – einhergeht, den die Klägerin aber zugunsten des informationellen Selbstbestimmungsrechts ihrer Kunden aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hinzunehmen hat.

III. Die Kostenentscheidung ergibt sich als gemischte Kostenentscheidung (§ 155 Abs. 1 Satz 1 VwGO) zum einen aus § 154 Abs. 1 VwGO, soweit die Klage aufrechterhalten wurde und die Klägerin unterlegen ist, und zum anderen aus § 161 Abs. 2 VwGO als Entscheidung des Gerichts unter Berücksichtigung des bisherigen Sach- und Streitstandes nach billigem Ermessen, soweit die Beteiligten das Verfahren für erledigt erklärt haben. Billigem Ermessen entspricht es, wenn die Klägerin auch für diesen Teil die Kosten trägt.

Die Klägerin hat den Rechtsstreit hinsichtlich der Ziffern 2 und 3 des streitgegenständlichen Bescheides für erledigt erklärt, nachdem sie selbst ihr Bestellformular und ihre Datenschutzerklärung angepasst hat. So besteht hinsichtlich der Anrede im Bestellformular nunmehr neben den Auswahloptionen „Herr/Frau“ auch die Möglichkeit, „keine Angabe“ zu tätigen. Zudem hat die Klägerin ihre Datenschutzerklärung um die Information ergänzt, dass die Anrede zum Zweck einer freundlichen und kundenangemessenen Ansprache und Kommunikation verarbeitet wird und die Verarbeitung auf Grundlage von Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO erfolgt. Dementsprechend ist davon auszugehen, dass sie den Bescheid der Beklagten diesbezüglich faktisch akzeptiert hat und aus diesem Grund die Klage nicht mehr weiterverfolgt. Dies kommt einer versteckten Klagerücknahme gleich.

Ihre Klage hätte diesbezüglich aber auch keine Aussicht auf Erfolg gehabt. Die Erhebung und Verarbeitung des Geschlechts/der Anrede zur Vertragserfüllung im Bestellprozess auf der streitgegenständlichen Homepage der Klägerin – auch für solche Produkte, die geschlechtsunabhängig zu dosieren bzw. einzunehmen/anzuwenden sind – kann nicht auf Art. 6 Abs. 1 lit. b DS-GVO gestützt werden.

Auch diesbezüglich gilt, dass die Kammer grundsätzlich anerkennt, dass Apothekern besondere Informations- und Beratungspflichten als vertragliche Nebenpflichten zu erfüllen haben. Bei bestimmten Produkten wird Apothekern auch eine geschlechtsspezifische Beratungsobliegenheit zukommen. Allerdings gilt auch hier, dass ein Blick auf die streitgegenständliche Webseite der Klägerin zeigt, dass eine Vielzahl der von ihr angebotenen Produkte eine besondere geschlechtsspezifische Beratung nicht erfordern. Hinsichtlich dieser Produkte kann die Datenverarbeitung demnach auch nicht auf Art. 6 Abs. 1 lit. b DS-GVO gestützt werden. Wie bei den altersunabhängig zu dosierenden Produkten gilt auch hier, dass es der Klägerin zuzumuten ist, den Bestellprozess so auszugestalten, dass eine Abfrage des Geschlechts/der Anrede nur für solche Produkte erfolgt, die eine geschlechtsspezifische Beratung erfordern. Ein solches Vorgehen hätte zudem den Vorteil, dass dem Besteller bzw. der Bestellerin auch deutlich werden dürfte, dass es zum einen auf das biologische Geschlecht und zum anderen auf das Geschlecht derjenigen Person ankommt, für die das Produkt in der späteren Anwendung auch tatsächlich gedacht ist.

Soweit die Anrede zur Wahrung eines berechtigten Interesses der Klägerin im Sinne des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO im Bestellprozess auf der klägerischen Webseite erhoben und verarbeitet werden darf, verstieß die Nichtnennung der Rechtsgrundlage für diese Datenverarbeitung gegen das in Art. 5 Abs. 1 lit. a i.V.m. Art. 12 Abs.1 und Art. 13 Abs. 1 lit. c DS-GVO normierte Transparenzprinzip. Art. 5 Abs. 1 Satz 1 lit. a DS-GVO verlangt, dass die betroffene Person die Datenverarbeitung nachvollziehen können muss. Erwägungsgrund 39 Satz 2 stellt dahingehend klar, dass die betroffene Person bereits prospektiv über zukünftige Datenverarbeitungen Klarheit haben muss, denn nur so wird der betroffenen Person ermöglicht, die Kontrolle über ihre personenbezogenen Daten (vgl. Erwägungsgrund 7 Satz 2) zu behalten (Schantz, in: BeckOK Datenschutzrecht, 37. Ed., Stand 01.05.2020). Eine Konkretisierung findet dieses Prinzip in Art. 12 DS-GVO, der wiederum auf Art. 13, 14 und 15-22 sowie Art. 34 DS-GVO verweist. Art. 13 Abs. 1 DS-GVO sieht in lit. c dahingehend vor, dass die Zwecke der

beabsichtigten Datenverarbeitung sowie die Rechtsgrundlage hierfür anzugeben sind. Hierfür ist es ausreichend, wenn im Hinblick auf den Zweck ein entsprechendes Schlagwort genannt und im Hinblick auf die Rechtsgrundlage eine oder gegebenenfalls mehrere der in Art. 6 Abs. 1 genannten Fallgruppen zitiert wird (Kamlah, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, Art. 13 DS-GVO, Rn. 11). Zum maßgeblichen Entscheidungszeitpunkt des Erlasses des Bescheides vom 08.01.2019 wurde weder in der Datenschutzerklärung der Klägerin noch in dem Bestellformular selbst darauf hingewiesen, dass die Abfrage der Anrede zur Ermöglichung einer freundlichen und kundenangemessenen Ansprache sowie Kommunikation erhoben und verarbeitet wird und damit einem berechtigten Interesse der Klägerin i.S.d. Rechtsgrundlage des Art. 6 Abs. 1 lit. f DS-GVO dient.

Die Klägerin kann sich diesbezüglich auch nicht auf Art. 13 Abs. 4 DS-GVO berufen. Hiernach bedarf es der Benennung des Zwecks und der Rechtsgrundlage der Datenverarbeitung nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt. Die bereits vorhandene Kenntnis kann grundsätzlich auch dadurch begründet sein, dass es sich um offen-sichtliche Umstände handelt (vgl. Kamlah, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, Art. 13 DS-GVO, Rn. 31d). Im Hinblick darauf, dass Kunden in Bestellbestätigungen regelmäßig auch ohne besondere oder mittels geschlechtsneutraler Ansprache adressiert werden (beispielsweise „Sehr geehrter Kunde, sehr geehrte Kundin“) und die Erhebung der Anrede/des Geschlechts auch noch andere Gründe – wie die von der Klägerin selbst benannte geschlechtsspezifische Beratung – haben kann, drängt es sich vorliegend gerade nicht auf, dass der Zweck der entsprechenden Datenverarbeitung die kundenfreundliche und angemessene Ansprache ist, welche auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden kann.

Anwaltliches Berufsgeheimnis contra Informationszugangsanspruch (Ls)

(**Verwaltungsgericht Baden-Württemberg**, Urteil vom 22. Juni 2021 – 10 S 320/20 –)

1. **Das anwaltliche Berufsgeheimnis kann einem Informationszugangsanspruch entgegenstehen, wenn der Zugangsanspruch auf Informationen gerichtet ist, die selbst der anwaltlichen Schweigepflicht unterliegen oder die jedenfalls Rückschlüsse auf solchermaßen geschützte Informationen zulassen.**
2. **Die Vertraulichkeit von Beratungen und Entscheidungsprozessen kann einem Informationszugangsanspruch, der auf Informationen aus einer rechtsanwaltlichen Beratung gerichtet ist, im Einzelfall entgegenstehen, wenn die Beratungsleistung durch eine besondere inhaltliche Nähe zu einzelnen Personen zuzuordnenden Meinungen oder zu den Beratungen und Entscheidungsprozesse kennzeichnenden Dynamiken geprägt ist.**

E-LEARNING

Mitarbeiter online sensibilisieren:

In 45 Minuten Unternehmensrisiken mindern

- Datenschutz
- IT-Sicherheit
- Compliance
- Antidiskriminierung

nur 14,90 € Einstiegspreis (netto) pro Schulung

Jetzt informieren:
elearning-mit-zertifikat.de

UNIVADO

DATAKONTEXT

Berichte, Informationen, Sonstiges

BlnLfDI: TTDSG trat in Kraft: Klare Regeln für Cookies und ähnliche Technologien

Am 1. Dezember 2021 trat das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft. Das Gesetz regelt unter anderem den Schutz der Vertraulichkeit und Privatsphäre bei der Nutzung von internetfähigen Endgeräten wie Webseiten, Messengern oder Smart-Home-Geräten.

„Mit dem TTDSG ändert sich auch der rechtliche Rahmen für den Einsatz von Cookies und vergleichbaren Technologien", erklärt Volker Brozio, kommissarischer Dienststellenleiter der Berliner Beauftragten für Datenschutz und Informationsfreiheit. „Das Gesetz schafft Klarheit und bestätigt die Auffassung der Datenschutzbehörde: Für den Einsatz von Cookies und ähnlichen Technologien braucht es im Regelfall eine Einwilligung der Nutzer/innen. Infolgedessen müssen Anbieter/innen von Telemedien überprüfen, ob Anpassungsbedarf unter anderem auf ihren Webseiten oder Apps besteht."

Auf den meisten Webseiten und Apps werden Technologien wie Cookies eingesetzt, um Informationen auf den Geräten der Nutzenden abzulegen und zu verwalten. Damit einher geht regelmäßig die Verarbeitung von personenbezogener Daten, mindestens der IP-Adresse der Nutzer/innen.

Dies dient häufig nicht nur dazu, das Verhalten von Nutzer:innen zu verfolgen, sondern auch Persönlichkeitsprofile über die gesamte Internetnutzung zu erstellen und anzureichern.

Die rechtlichen Rahmenbedingungen für das Setzen und Auslesen von Informationen aus Endgeräten sind in der europäischen ePrivacy-Richtlinie geregelt. Mit dem TTDSG hat der Bundesgesetzgeber nach über einem Jahrzehnt Verzögerung nunmehr die Vorgaben der ePrivacy-Richtlinie in nationales Recht umgesetzt. Die anschließende Verarbeitung der so erhobenen personenbezogenen Daten richtet sich wiederum nach den Anforderungen der Datenschutz-Grundverordnung (DS-GVO). Wer Cookies und ähnliche Technologien verwendet, muss daher in der Regel beide Gesetze beachten.

Betreibende von Webseiten und anderen Telemedien benötigen grundsätzlich eine Einwilligung der Nutzer/innen, wenn sie Informationen auf dem Endgerät speichern oder darauf zugreifen wollen. Einer Einwilligung bedarf es ausnahmsweise nur dann nicht, wenn die Speicherung von und der Zugriff auf Informationen in den Endgeräten unbedingt erforderlich sind, damit ein von den Nutzenden ausdrücklich gewünschter Telemediendienst zur Verfügung gestellt werden kann. Das ist zum Beispiel der Fall bei einem Cookie, der dazu dient, Artikel eines Online-Shops in einem Warenkorb zu speichern.

Um Verantwortliche bei der Umsetzung der neuen Anforderungen behilflich zu sein, erarbeiten die deutschen Datenschutz-Aufsichtsbehörden derzeit eine Orientierungshilfe. Diese soll Anfang des Jahres 2022 veröffentlicht werden.

Zu guter Letzt: BVerwG: Entfernung aus dem Beamtenverhältnis bei Leugnung der Existenz der Bundesrepublik Deutschland

Der Betroffene war Regierungsobersekretär beim Bundesnachrichtendienst. Im Juli 2015 beantragte er beim Landratsamt Starnberg einen Staatsangehörigkeitsausweis und gab dabei u.a. als Geburts- und Wohnsitzstaat jeweils „Königreich Bayern" an, wobei er auf das „RuStaG Stand 1913" (= Reichs- und Staatsangehörigkeitsgesetz in der Fassung von 1913) bezogen hat.

4 Jahre später zieht das BVerwG mit Urteil vom 02.12.2021 – 2 A 7.21 die Konsequenz. Ein Beamter, der die Existenz der Bundesrepublik Deutschland dadurch leugnet, dass er in einem Antrag auf Erteilung eines Staatsangehörigkeitsausweises durchgehend „Königreich Bayern" statt „Bundesrepublik Deutschland" angibt, verletzt in schwerwiegender Weise seine Verfassungstreuepflicht und kann deshalb im Disziplinarwege aus dem Beamtenverhältnis entfernt werden.

Literaturhinweise

Diermann, Patrick, **Datenschutzaufsicht über die Tätigkeit der Finanzverwaltung,** Schriften zum Steuerrecht (SSR), Duncker & Humblot, Berlin 2022, Band 170, 226 S., 74,90 €

Nach der grundlegenden Neugestaltung des Datenschutzrechts durch die DS-GVO und die darauf bezogenen Folgeänderungen durch den deutschen Steuergesetzgeber unterliegen auch Finanzbehörden der Aufsicht durch eine unabhängige (nationale) Behörde. Dieses Aufsichtskonzept ist für Finanzbehörden neu. Die Arbeit hat es sich zur Aufgabe gemacht, die Datenschutzaufsicht über Finanzbehörden mit einem breiten Zugriff auf die Thematik zu erarbeiten. Sie hat vor allem die praktische Rechtsanwendung im Blick und ist dem Rechtsanwender eine Hilfestellung, das komplexe Normgeflecht zu durchdringen. Sie präsentiert Lösungsansätze für die vielfältigen Rechtsfragen, die sich bei der Datenschutzaufsicht über Finanzbehörden stellen. Dabei zeigt die Arbeit unter anderem, dass die DS-GVO nicht pauschal für alle Steuerarten gilt und die Konzentration der Aufsicht beim BfDI über Landesfinanzbehörden gegen die Kompetenzordnung des Grundgesetzes verstößt.

(Redaktion)

Harte-Bavendamm, Henning/Henning-Bodewig, Frauke/Goldmann, Michael/Tollmitt, Jan (Hrsg.), **Gesetz gegen den unlauteren Wettbewerb – Mit Preisangabenverordnung und Geschäftsgeheimnisgesetz**, Beck-Verlag, München 2021, 5. Aufl., 3234 S., 319,00 €

In dem großen Praktikerkommentar erläutern dreizehn erfahrene Richter, Wissenschaftler und Praktiker das deutsche und europäische Wettbewerbsrecht. Als Fazit kann man vorweg festhalten, dass es sich bei der umfangreichen Kommentierung um eine geschlossene Darstellung des deutschen und europäischen Lauterkeitsrechts und der Bezüge zu angrenzenden Rechtsgebieten mit u.a. einer präzisen und praxisnahen Darstellung des Verfahrensrechts, insbesondere zur Abmahnung, Unterwerfung und Vertragsstrafe sowie zum Verfügungs- und Erkenntnisverfahren handelt.

Bei der nunmehr erfolgten Aktualisierung der Kommentierung wurden ausführlich berücksichtigt das Gesetz zur Stärkung des fairen Wettbewerbs vom 02.12.2020, sowie auch schon teilweise das zum 28.5.2022 in Kraft tretende Gesetz zu Stärkung des Verbraucherschutzes sowie das Gesetz für faire Verbraucherverträge. In der Kommentierung sind von besonderem Interesse die folgenden neuen bzw. neukonzipierten Stichworte:

- Starke Einschränkung des „fliegenden Gerichtsstands“
- Aktivlegitimation von Mitbewerbern und Wirtschaftsverbänden
- Missbrauch der Aktivlegitimation
- Voraussetzungen einer wirksamen Abmahnung
- Einschränkung des Aufwendungsersatzes
- Gegenansprüche des Abgemahnten
- Neuer Schadenersatzanspruch des Verbrauchers
- Neue Vorschrift zur Telefonwerbung
- Darstellung des neugeordneten Geheimnisschutzes („Know-how“)
- Eingehende Erörterung der Preisangabenverordnung

Bei zahlreichen dieser Themen bestehen Verbindungen zu Datenschutzrecht; sei es bei der Zulässigkeit der Telefonwerbung oder beim Schadensersatz für Verbraucher.

Zusammengefasst: Das Werk benötigen alle, die sich auf höchstem Niveau mit dem Wettbewerbsrecht aber auch mit Datenschutzfragen zu befassen haben.

(Schriftleitung)

Krimphove, Dieter, **Werberecht**, Kohlhammer, Stuttgart 2021, 2. Aufl., 150 S., broschiert, 23,00 €

Mit dem Begriff „Werberecht“ beschreibt der Autor das Verbot irreführender, vergleichender, diskriminierender und aufdringlicher Werbung, Das Thema umfasst die vorverkaufliche Tätigkeit eines Vertreibers und greift somit in das gesamte Vertriebsgeschehen stark ein. Anhand zahlreicher Beispiele und Übersichten erläutert das Werk die komplexe Materie (und dabei auch neuartige Vertriebsformen). Tipps für Klausur und Praxis sowie Schaubilder erleichtern das Verständnis und den Umgang mit dem Werberecht in Studium und täglicher Praxis. Wichtige Entscheidungen zu den im Buch behandelten Themen, interaktive Fälle und ein Multiple-Choice-Test stehen auf der Verlagshomepage als Download zur Verfügung. Erstaunlich ist, dass bei Erörterung des UWG als eine Basis der Regelungen ein Hinweis auf datenschutzrechtliche Einschränkungen werblicher Aktivitäten fehlen. Das Wort Datenschutz findet man nicht und auch nicht das datenschutzrechtliche Widerspruchsrecht des Art. 21 DS-GVO.

(Schriftleitung)

Anton Barrein, **Das Recht auf Home-Office-Handlungsspielräume und Grenzen des Arbeits- und Sozialversicherungsgesetzes für die digitalisierte Arbeitswelt 4.0**, Duncker & Humblodt, Schriften zum Sozial- und Arbeitsrecht (SAR), Band 369, 2022. 3 Tab.; 467 S., (X) 119,90 €

Das Home-Office ist für einen Großteil der Bevölkerung durch die Corona-Pandemie eine sehr reale Erfahrung geworden. Die Praxis zeigt, dass die rechtlichen Grundlagen jedoch noch wenig aufbereitet sind. Der Regelungsrahmen des Arbeits- und Sozialversicherungsrechts erscheint daher für die Arbeitsvertragsparteien als eine Herausforderung, sodass dieser zu Beginn dargestellt wird. Im Mittelpunkt der Untersuchung steht die Rechtslage de lege lata, die schon in bestimmten Einzelfällen Anspruchskonzeptionen auf Home-Office bereithält. Gleichwohl plant das Bundesministerium für Ar-

beit und Soziales – weiterhin – einen Rechtsanspruch auf Home-Office. De lege ferenda muss dafür der unions- und verfassungsrechtliche Rahmen mit einbezogen werden. Ein an § 8 TzBfG orientierter Rechtsanspruch auf Home-Office entpuppt sich als für beide Arbeitsvertragsparteien sehr kompliziert und daher nur bedingt nützlich. Der Gesetzgeber sollte im Gegensatz dazu betriebliche und tarifvertragliche Regelungen fördern.

Das Buch endet mit einer guten zum Einlesen gut zusammenfassenden Übersicht und einem Literaturverzeichnis.

(Redaktion)

9. HAMBURGER DATENSCHUTZTAGE

1.–3.6.2022

Alle Macht den Daten

Ein Blick in die Zukunft des Datenschutzes

Jetzt anmelden: **www.datakontext.com**

IBS data protection

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Hausrecht statt Rausschmiss: Regeln für Messenger-Chats

Chats per Messenger-Gruppen sind auch in Schulklassen an der Tagesordnung. Ein Schüler eröffnet eine Gruppe, und die ganze Stufe tritt bei. Man kann im Chat die Angelegenheiten der Stufe organisieren, jeder kann alles mitbekommen, und auf Wunsch der Lehrer werden auch Hausaufgaben & Co. verbreitet. Wenn viele Schüler chatten, kann sich auch mal einer im Ton vergreifen. Darf man ihn dann rausschmeißen? Nicht einfach so, denn rechtlich betrachtet, ist ein Zusammenschluss von mehreren Personen, die einen gemeinsamen Zweck verfolgen, eine Gesellschaft des Bürgerlichen Rechts. Man kann die Entfernung aus der Gruppe als Kündigung begreifen. Grundsätzlich kann jeder Gesellschafter die gesamte Gesellschaft kündigen, wenn ein wichtiger Grund vorliegt. Dann muss sie aber aufgelöst werden. Man kann dann einen neuen Stufenchat ohne die Person eröffnen, die man ausschließen will. Hohe Hürden also, für den Rausschmiss aus dem Klassenchat. So oder so bietet es sich an, wenn der Administrator bei Gründung des Chats gleich in der ersten Nachricht Regeln für das kommuniziert, was erwünscht ist. Themen der „Gruppen-Policy“ sind: Freundlicher Umgangston, keine ellenlangen Diskussionen, sondern Daumen hoch oder runter, wenn es was zu entscheiden gibt. Und ein wichtiger Hinweis: Streitfragen klärt man im persönlichen Gespräch.

Datenschutz kompakt

27.–28. April 2022 I Berlin
Referent: RA Andreas Jaspers

Schwerpunkte:

- ✓ Datenschutzrecht: Grundlagen, Beschäftigtendatenschutz, Haftung und Sanktionen
- ✓ Datenschutzorganisation: Datenschutz-Management, Datenschutz-Folgenabschätzung

Jetzt anmelden: **www.datakontext.com**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

powered by GDD

Foto: peshkova - Adobe Stock

Der einfache Weg zum organisierten Datenschutz!

DA DATA AGENDA

Datenschutz Manager

Der Experte an Ihrer Seite!

- ✓ webbasiert, On Premise oder PC-/Laptop Installation
- ✓ professionelle Schritt-für-Schritt Anleitung mit vielen Vorlagen
- ✓ einfaches Erfassen und Dokumentieren aller Datenschutzmaßnahmen
- ✓ effektive Zusammenarbeit aller verantwortlichen Stellen
- ✓ besonders für externe DSBs geeignet: Alle Mandanten in einem System

Jetzt informieren: **www.DataAgenda.de/datenschutzmanager**

DATAKONTEXT