

Zeitschrift für
Datenschutz-,
Informations- und
Kommunikationsrecht

RDV

6/2022

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

STERZ/WERNER/RAABE, Intelligente Verkehrssysteme – IT-Sicherheit
in offenen Infrastrukturen – Teil 1

MEYER, Rechtsmissbräuchliche Schadensersatzforderungen

GOLA, Mitarbeitervertretungen und Datenschutzbeauftragte als
„Gewährleister“ des Datenschutzes der Beschäftigten

Kurzbeiträge

SÖBBING, DS-GVO: Wer trägt die Kosten einer anlasslosen Inspektion
bei einem Auftragsdatenverarbeiter?

GOLA, Aus den Berichten und Informationen der Aufsichtsbehörden
(63): GPS-Ortung von Beschäftigten (27. Tätigkeitsbericht
der LfDI Niedersachsen (2021) vom 03.09.2020

REIF, Praxisfälle zum Datenschutzrecht XIX: Sonderkonditionen für
Auszubildende bei Versicherungsunternehmen aus dem Konzernverbund

Rechtsprechung

Aus dem Inhalt

EUGH zu Bekanntmachungen nach der Geldwäscherichtlinie

EUGH, Zur Regelung einer allgemeinen und unterschiedslosen
Speicherung der Verkehrsdaten durch die Anbieter von
Diensten der elektronischen Kommunikation (Ls)

BGH legt EuGH erneut Frage zur Klagebefugnis von
Verbraucherschutzverbänden bei Datenschutzverstößen
durch Facebook vor

BGH, Prüfpflichten eines Bewertungsportals (Ls)

BAG, BAG-EuGH-Anfrage zu immateriellen Schadensersatz
wegen bei der Übermittlung personenbezogener Daten
an die vormalige Konzernmutter der Arbeitgeberin in
den USA auf Grund einer Betriebsvereinbarung

38. Jahrgang
Dezember 2022
Seiten 289–342



Gesellschaft für Datenschutz
und Datensicherheit e.V.


DATAKONTEXT
www.rdv-online.de



11. GDD-Winter-Workshop

für Datenschutzbeauftragte und -berater
sowie Datenschutzdienstleister

30.-31. Januar 2023 | Garmisch Partenkirchen

Schwerpunkte:

- ✓ Aktuelle Entwicklungen im Datenschutz
- ✓ Neuer transatlantischer Datenschutzrahmen
- ✓ Verhaltensregeln für Auftragsverarbeiter - »Trusted Data Processor«
- ✓ Zivilrecht und Datenschutz
- ✓ Datenschutz und künstliche Intelligenz

Jetzt anmelden: www.datakontext.com

Inhaltsverzeichnis

Editorial	289	Beweislast bei Geltendmachung eines Berichtigungsanspruchs (Ls) (BVerwG, Urteil vom 02.03.2022)	326
Veranstaltungen	290	Anspruch auf Berichtigung des Geburtsdatums im Melderegister (Ls) (BVerwG, Urteil vom 02.03.2022)	326
Aufsätze		Zur Anwendung der Datenschutzgesetzen der Kirchen bei von ihnen als GmbH betriebenen Kliniken (OLG Hamm, Beschluss vom 23.09.2022)	327
Leonie STERZ/Christop WERNER/Prof. Dr. Oliver RAABE Intelligente Verkehrssysteme – IT-Sicherheit in offenen Infrastrukturen – Teil 1	291	Kein Ausschluss aus Vergabeverfahren wegen Einbindung der luxemburgischen Tochtergesellschaft eines US-amerikanischen Unternehmens (OLG Karlsruhe, Beschluss vom 07.09.2022)	328
Dr. Sebastian MEYER Rechtsmissbräuchliche Schadensersatzforderungen	300	Zur Berechtigung einer Abmahnung bei Datenschutzvernachlässigung (LAG Sachsen, Urteil vom 07.04.2022)	328
Prof. Peter GOLA Mitarbeitervertretungen und Datenschutzbeauftragte als „Gewährleister“ des Datenschutzes der Beschäftigten	306	Datenzugangsrechte von Betriebsrats-Wahlinitiatoren fehlen (Ls) (AG Berlin, Beschluss vom 26.08.2022)	337
Kurzbeiträge		Selbstbestimmung Minderjähriger gegenüber Auskunftserteilung an den Vater (Ls) (Interdiözesanes Datenschutzgericht, Beschluss vom 25.02.2022)	337
Thomas SÖBBING DS-GVO: Wer trägt die Kosten einer anlasslosen Inspektion bei einem Auftragsdatenverarbeiter?	315	Verpflichtung zur Aufbewahrung von Beistandsakten (Ls) (Interdiözesanes Datenschutzgericht, Beschluss vom 25.04.2022)	337
Prof. Peter GOLA Aus den Berichten und Informationen der Aufsichtsbehörden (63): GPS-Ortung von Beschäftigten (27. Tätigkeitsbericht der LfDI Niedersachsen (2021) vom 03.09.2020	317	Berichte, Informationen, Sonstiges	
RAin Yvette REIF LL.M. Praxisfälle zum Datenschutzrecht XIX: Sonderkonditionen für Auszubildende bei Versicherungsunternehmen aus dem Konzernverbund	318	Bitkom-Umfrage: Nur 22 Prozent der Unternehmen setzen DS-GVO vollständig um	339
Rechtsprechung		Literaturhinweise	
EuGH zu Bekanntmachungen nach der Geldwäscherichtlinie (EuGH, Urteil vom 22.11.2022)	322	<i>Buchbesprechungen</i>	
Zur Regelung einer allgemeinen und unterschiedslosen Speicherung der Verkehrsdaten durch die Anbieter von Diensten der elektronischen Kommunikation (Ls) (EuGH, Urteil vom 20.09.2022)	323	<i>Carla-Charlotte Schmidt</i> , Regelungsoptionen des deutschen Gesetzgebers zum Whistleblower-Schutz in Umsetzung der EU-Richtlinie 2019/1937 (REDAKTION)	340
BGH legt EuGH erneut Frage zur Klagebefugnis von Verbraucherschutzverbänden bei Datenschutzverstößen durch Facebook vor (BGH, Beschluss vom 10.11.2022)	323	<i>Jonas Michael Schnelling</i> , Auskunft im Familienrecht zwischen Anspruch und Informationspflicht – Ein Beitrag zum extensiven Verständnis der Pflicht zur ungefragten Information (REDAKTION)	340
Prüfpflichten eines Bewertungsportals (Ls) (BGH, Urteil vom 09.08.2022)	324	<i>Peter Gola/Dirk Heckmann</i> , Datenschutz-Grundverordnung, BDSG: DS-GVO (REDAKTION)	340
BAG-EuGH-Anfrage zu immateriellen Schadensersatz wegen bei der Übermittlung personenbezogener Daten an die vormalige Konzernmutter der Arbeitgeberin in den USA auf Grund einer Betriebsvereinbarung (BAG, Beschluss vom 22.09.2022)	325	<i>Peter Gola</i> , Recht bei der Personalgewinnung – Datenschutz-, Wettbewerbs- und Arbeitsrecht in der Praxis (REDAKTION)	341
Kein Initiativrecht des Betriebsrats zur Einführung eines Systems der Arbeitszeiterfassung (Ls) (BAG, Beschluss vom 13.09.2022)	325	<i>Detlef Grimm/Jonas Singraven (Hrsg.)</i> , Digitalisierung und Arbeitsrecht (SCHRIFTLEITUNG)	341
BAG-Vorabanfrage an den EuGH nach ordentlicher Kündigung durch kirchliche Einrichtung wegen Kirchenaustritt vor Beginn des Arbeitsverhältnisses (Ls) (BAG, Beschluss vom 21.07.2022)	325	Josef Haverkamp, Datenschutz – Grundlagen, Empfehlungen und Arbeitshilfen für Betriebs- und Personalräte (REDAKTION)	341
Anordnung von Coronatests durch den Arbeitgeber (BAG, Urteil vom 01.06.2022)	326	Nachgefasst	342
Darlegungslast bei Überstundenvergütung (Ls) (BAG, Urteil vom 04.05.2022)	326		

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

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

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

in Kooperation mit der

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

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

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

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

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

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

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

Prof. Dr. Karl LINNENKOHLE, Universität Kassel

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

Dr. Alexander OSTROWICZ, Präsident des Landesarbeitsgerichts
Schleswig-Holstein a.D.

Prof. Dr. Michael RONELLENFITSCH, Hessischer Datenschutzbeauftragter

Prof. Dr. Friedhelm ROST, Vorsitzender Richter am Bundesarbeitsgericht a.D.

Peter SCHAAR, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D.

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

Prof. Dr. Dres. h.c. Spiros SIMITIS, Universität Frankfurt

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irimi VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 6/2022

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-Secktem

Druck

Grafisches Centrum Cuno GmbH & Co. KG

Gewerbering West 27, 39240 Calbe (Saale)

Anzeigenverwaltung

DATAKONTEXT GmbH, Frechen

Wolfgang Scharf

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

wolfgang.scharf@datakontext.com

www.datakontext.com

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
38. Jahrgang 2022 Heft 6
Seiten 289-342

RDV

Recht der Datenverarbeitung

38. Jahrgang · Dezember 2022 · Seiten 289–342

Editorial

Hinweisgeberschutz und Datenschutz

Das Hinweisgeberschutzgesetz ist kurz vor der Zielgeraden. Es wurde auch Zeit. Die europäische Richtlinie hätte man eigentlich bis zum 17. Dezember vergangenen Jahres umsetzen müssen. Nun strebt man ein Inkrafttreten Anfang nächsten Jahres an. Es ist zunächst einmal gut, dass der Gesetzgeber erkannt hat, wie wichtig der Schutz von Hinweisgebern ist. Er handelt jetzt freilich nicht aus eigenem Antrieb, sondern weil europarechtliche Vorgaben ihn dazu drängen.

Nicht alles an diesem Gesetz ist gut. Ärgerlich ist insbesondere die Haftungsregelung, wonach der Hinweisgeber, der fahrlässig unrichtige Informationen verbreitet, nicht schadensersatzpflichtig sein soll demjenigen gegenüber, dessen Ruf ggfs. ruiniert wird – egal wie groß der Schaden ist und selbst dann, wenn die Information gezielt erfolgte, um den Betroffenen zu schädigen. Das birgt Risiken und Gefahren. Die Begründung des Gesetzes führt dazu aus, das müsse so sein, weil das Europarecht dies vorschreibt. Das ist falsch. Dem Europarecht geht es um den Schutz vor Repression, nicht um Privilegierung im Irrtum oder schuldhaft falscher Denunziation.

Solche und ähnliche Monita können dem Ziel, einen angemessenen und effektiven Hinweisgeberschutz zu schaffen, entgegenstehen. Das Gesetz geht von der vollständigen Gleichwertigkeit der internen und externen Meldewege aus. Ein Arbeitnehmer oder wer auch immer eine Meldung vornehmen will, hat also die freie Wahl, ob er sich zunächst an das Unternehmen und die dortigen

Compliance-Kanäle hält oder ob er sich an eine externe Behörde wendet. Der Gesetzgeber hätte gut daran getan, Anreize zu setzen, zunächst die interne Meldestelle zu nutzen. Das entspräche auch der bisherigen Rechtsprechung, sowohl des Bundesarbeitsgerichts als auch des Europäischen Gerichtshofs für Menschenrechte und auch die Richtlinie fordert die Mitgliedsstaaten ausdrücklich auf, sich dafür einzusetzen, dass die Meldung über interne Meldekanäle gegenüber den Meldungen über externe Meldekanäle in den Fällen bevorzugt wird, in denen intern wirksam gegen den Verstoß vorgegangen werden kann und der Hinweisgeber keine Repressalien befürchtet. Dieses Bemühen fehlt gänzlich und das ist ein großer Fehler. Das aber ist zentral zum Schutze aller Beteiligten. Denn ein geäußerter Verdacht ist eben zunächst nur ein Verdacht und der Hinweisgeber wird ja ermutigt, auch dann Hinweise zu geben, wenn er nicht sicheres Wissen hat. Dann aber ist eine valide Klärung der Vorwürfe notwendig zu einem Stadium, bevor der Vorwurf noch keine weiteren Kreise gezogen hat. Denn was berichtet wird, das muss nach der Vorstellung des Gesetzesentwurfs gar nicht wahr sein, solange der Berichtende gutgläubig ist. Und mehr noch: Der Sachverhalt muss auch nicht unter den Anwendungsbereich des Gesetzes fallen, solange der Berichtende hinreichende Gründe für die Annahme hat, dass dem doch der Fall ist. Er ist selbst dann geschützt, selbst wenn er schuldhaft irrt, solange das nicht grob fahrlässig ist. Das alles ist sehr, sehr weit gefasst und

oftmals zu weit, um Rechtssicherheit im Unternehmen und auch demjenigen zu geben, dessen Verhalten Gegenstand der Meldung ist. Der Datenschützer runzelt nachdenklich die Stirn. Semper aliquid haeret. Das Persönlichkeitsrecht des Betroffenen sollte ernster genommen werden.

Hinweisgeberinnen und Hinweisgeber leisten einen wichtigen Beitrag zur Aufdeckung und Ahndung von Missständen“ betont die Gesetzesbegründung. Es ist zu hoffen, dass trotz dieser Kritik das Gesetz seinen Beitrag zu einer guten Unternehmenspraxis leisten wird, dass tatsächlich – wie es die Gesetzesbegründung ausführt – „Hinweisgeberschutz in der Bundesrepublik Deutschland ... wirksam und nachhaltig verbessert“ wird. Hoffen wir das Beste. Alle sind aufgerufen, hieran mitzuwirken.

Prof. Dr. Gregor Thüsing



Prof. Dr. Gregor Thüsing

ist 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
30.-31.01.2023	GDD-Winter-Workshop	Garmisch-Partenkirchen	GDD e.V. und DATAKONTEXT
01.02.2023	Konzerndatenschutz	Online	GDD e.V. und DATAKONTEXT
02.02.2023	Datenschutz und Betriebsrat unter der DS-GVO	Online	GDD e.V. und DATAKONTEXT
07.02.2023	Websites datenschutzkonform gestalten	Online	GDD e.V. und DATAKONTEXT
08.-09.02.2023	Datenschutz kompakt	Köln	GDD e.V. und DATAKONTEXT
13.02.2023	Beschäftigtendatenverarbeitung nach DS-GVO und BDSG	Köln	GDD e.V. und DATAKONTEXT
14.02.2023	Die Aufgaben und der Tätigkeitsbericht des betrieblichen DSB praxisnah im Unternehmen	Köln	GDD e.V. und DATAKONTEXT
15.02.2023	Datenschutz-Folgenabschätzung	München	GDD e.V. und DATAKONTEXT
27.02.-03.03.2023	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
06.03.2023	Hacker-Tools für Datenschutzbeauftragte	Berlin	GDD e.V. und DATAKONTEXT
07.03.2023	Datenschutz aktuell	Online	GDD e.V. und DATAKONTEXT
08.03.2023	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Online	GDD e.V. und DATAKONTEXT
09.03.2023	Datenschutz-Management light	Köln	GDD e.V. und DATAKONTEXT
13.-14.03.2023	Basiswissen IT-Sicherheit	Stuttgart	GDD e.V. und DATAKONTEXT
15.03.2023	TTDSG: Onlinedatenschutz auf dem Weg zur ePrivacy-Verordnung	Köln	GDD e.V. und DATAKONTEXT
16.03.2023	Datenschutz in medizinischen Einrichtungen	Hamburg	GDD e.V. und DATAKONTEXT
20.-22.03.2023	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Köln	GDD e.V. und DATAKONTEXT
23.03.2023	IT-Sicherheitsmanagement aus Sicht der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
23.03.2023	Grundlagen der Auftragsverarbeitung	Köln	GDD e.V. und DATAKONTEXT
27.03.2023	Forensik für Revisoren, Prüfer und Datenschutzbeauftragte	Hamburg	GDD e.V. und DATAKONTEXT
29.03.2023	Datenschutz International	Hamburg	GDD e.V. und DATAKONTEXT
30.03.2023	Löschen nach DS-GVO	Köln	GDD e.V. und DATAKONTEXT
17.04.2023	Home- und Mobile-Office: Datenschutz-, und IT-Sicherheits- und Notfallkonzepte	Online	GDD e.V. und DATAKONTEXT
18.04.2023	Mobile Endgeräte im Zeitalter von DS-GVO und ePrivacy-Verordnung	Köln	GDD e.V. und DATAKONTEXT
19.04.2023	Big Data-Analysen nach DS-GVO und BDSG	Köln	GDD e.V. und DATAKONTEXT
24.04.2023	Planung und Umsetzung der Überwachungsaufgaben der DSB	Köln	GDD e.V. und DATAKONTEXT

Leonie Sterz/Christoph Werner/Prof. Dr. Oliver Raabe

Intelligente Verkehrssysteme – IT-Sicherheit in offenen Infrastrukturen Teil 1

Der Straßenverkehr wird zunehmend digitalisiert. Dies betrifft sowohl die Fahrzeuge selbst, in denen vermehrt digitale Funktionen wie Assistenzsysteme implementiert werden, als auch die Verkehrsinfrastruktur, in der analoge Verkehrssteuerungsfunktionen wie Straßenschilder und Ampeln durch digitale Systeme ersetzt oder zumindest er-

gänzt werden. Zu diesen Systemen zählen insbesondere intelligente Verkehrssysteme (IVS), bei denen Informations- und Kommunikationstechnologien im Straßenverkehr, d.h. in den Fahrzeugen, der Verkehrsinfrastruktur und ggf. auch in Wearables von Verkehrsteilnehmer/innen (z.B. Smartphones) eingesetzt werden.¹

I. Einleitung

Nach dem gesetzlichen Vorstellungsbild verfolgen IVS eine Vielfalt von Zielsetzungen. Neben der effizienteren Verkehrssteuerung sollen auch die Nutzersicherheit und der Komfort erhöht werden.² Ein denkbare Szenario ist z.B. das Blaulicht von Einsatzfahrzeugen der Polizei, Feuerwehr und anderen Rettungsdiensten³ auch digital umzusetzen („virtuelles Blaulicht“).⁴

Im Recht wird die Einführung von IVS auf europäischer Ebene durch die RL von 2010⁵ (IVS-RL) angestrebt und gefördert. Aus Gründen der dafür notwendigen Kompatibilität und Interoperabilität der an einem IVS beteiligten Systeme wurden delegierte Verordnungen zur Spezifikation erlassen.⁶

Dieser Rechtsrahmen wird durch einen neuen Entwurf zur Änderung der IVS-RL (IVS2-RL-E)⁷ fortentwickelt. Mit diesem soll dem Fortschritt in der Digitalisierung der Mobilität in den letzten Jahren Rechnung getragen werden, der durch zunehmende Automatisierung von Kfz bis hin zu einer erstrebten autonomen Fahrfunktion und digital gestütztem Verkehrsmanagement gekennzeichnet ist.⁸ Während in den delegierten Verordnungen zur bisherigen IVS-RL vorgesehen war, dass die Daten für die jeweiligen IVS zentral über einen nationalen Zugangspunkt kommuniziert werden,⁹ werden die Daten zukünftig vermehrt durch Fahrzeug-Fahrzeug- (V2V), Fahrzeug-Infrastruktur- (V2I) und Infrastruktur-Infrastruktur-Kommunikation (I2I) sowie die Verkehrsvernetzung (V2X)¹⁰ zwischen den Akteuren direkt kommuniziert.¹¹ Entsprechend werden auch die Regelungen für IVS im IVS2-RL-E um Normen zu kooperativen IVS (C-ITS), die sich durch ebendiesen Austausch von Nachrichten der Nutzer untereinander auszeichnen, ergänzt.¹²

Im Hinblick auf die wachsende Echtzeitkritikalität von Daten und die Vernetzung der Akteure scheint die durchgängige Realisierung von Maßnahmen der IT-Sicherheit zunächst eine Selbstverständlichkeit zu sein. Gleichwohl werden normative Ende-zu-Ende Vorgaben zur Gewähr von IT-Sicherheit z.B. durch Rahmensetzungen für IT-Sicherheitsanalysen und Bestimmung von Kriterien für die Wahl

angemessener Schutzmaßnahmen bislang in der geltenden IVS-RL nicht berücksichtigt. Durch den neuen Entwurf der IVS-RL und andere Gesetzesvorhaben¹³ wird die IT-Sicherheit aber zumindest teilweise adressiert.¹⁴

Der zuvor beschriebene Übergang von einer zentralisierten, geschlossenen IVS-Infrastruktur zu offenen IVS mit einem dynamischen Teilnehmerkreis führt zu einem neuen Kommunikationsparadigma mit einem gesteigerten Bedarf einer normativen IT-Sicherheitsregulierung, die gerade und trotz der Rollenvielfalt im IVS eine Ende-zu-Ende Gesamtbeurteilung integriert.

Das IT-Sicherheitsrecht muss dabei insbesondere neben der genannten Echtzeitfähigkeit auch die wachsende Kritikalität der Systeme für vitale Fahrfunktionen und Verkehrssi-

* Diese Untersuchung wurde unterstützt durch Mittel des Topic Engineering Secure Systems (46.23.03) der Helmholtz-Gemeinschaft (HGF) sowie der KASTEL Security Research Labs. Wir bedanken uns bei Frau Julia Straburzynski für ihre Unterstützung bei Recherche und Korrektur.

1 Vgl. Art. 4 Nr. 1 IVS-RL (siehe hierzu unten Fn. 4), § 2 Nr. 1 IVSG.

2 Vgl. Art. 4 Nr. 4 IVS-RL.

3 Vgl. § 38 Abs. 1, 2 StVO.

4 Vgl. Bieker-Walz, Verkehrsmanagement für Einsatzfahrzeuge, S. 15 f.; Spehr, FAZ 23.04.2008, abrufbar unter: <https://www.faz.net/-gyg-x1ua>, Stand 08.11.2022.

5 Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

6 Die sich auf die vorrangigen Bereiche (Art. 2 IVS-RL) und die daraus abgeleiteten vorrangigen Maßnahmen (Art. 3 IVS-RL) beziehen.

7 COM(2021) 813 final, 2021/0419 (COD), Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2010/40/EU zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

8 Dies spiegelt sich datenschutzrechtlich auch in der Einführung des § 63e StVG wider.

9 Vgl. Art. 5 Abs. 2, 3 del. VO (EU) Nr. 885/2013; Art. 7 Abs. 1, 2 del. VO (EU) Nr. 886/2013.

10 Umfasst auch die Vernetzung mit „persönlichen tragbaren Geräten“ wie z.B. Smartphones: Art. 2 Abs. 4 del. VO 2019/1789.

11 Hierfür wird auch der Begriff Mobile Ad-Hoc-Network (MANET) und als Unterbegriff hierzu Vehicle Ad-Hoc-Network (VANET) verwendet, vgl. Plößl, Mehrseitige sichere Ad-hoc Vernetzung von Fahrzeugen, S. 7 f.

12 Vgl. Art. 1 Nr. 3 lit. b IVS2-RL-E.

cherheit sowie die erhöhte Unsicherheit der IT-Verantwortlichen im Hinblick auf Angriffsvektoren und Schutzmaßnahmen reflektieren. Ebenso muss der Rechtsrahmen Herausforderungen aus dem neuen Rollenmodell bewältigen. Einzelne Fahrzeuge unterschiedlicher Hersteller sind konstruktive Bestandteile eines IVS als Datenlieferanten oder -empfänger, treten dem System aber nur temporär bei und verlassen es im nächsten Moment wieder. Über Smartphone-Apps können auch Fußgänger und Radfahrer temporär einbezogen werden.

Eine IT-Sicherheitsregulierung von IVS besteht außerhalb des IVS-Rechts, jedenfalls dem Grunde nach, im Recht kritischer Infrastrukturen (KRITIS-Recht), welches auf europäischer Ebene aus der NIS-RL und auf nationaler Ebene aus dem BSIG und der BSI-KritisV besteht. Dabei sind IVS als kritische Infrastruktur adressiert, wenn das konkrete IVS den Schwellenwert in Ziff. 1.4.3. Anhang 7 der BSI-KritisV von 500.000 angeschlossenen oder durchschnittlich im Versorgungsgebiet versorgter Nutzer erreicht oder überschreitet. Dann greifen für die jeweiligen Betreiber die IT-Sicherheitspflichten aus § 8a BSIG, mithin die Pflicht, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des IVS maßgeblich sind. Aus der Perspektive der erfassten Systemgrenzen und des weiten Fokus auf Dienstangebote scheint das KRITIS-Recht zunächst im Gegensatz zu eher produktbezogenen Regulierungsregimen (s. Typengenehmigungsrecht, del. VO 2019/1789) grundsätzlich geeignet, den geforderten Ende-zu-Ende Schutz leisten zu können.

Es stellt sich jedoch schon hier die Frage, ob die materiellen Regelungsprinzipien des KRITIS-Rechts, welche auf „klassische“ zentrale, geschlossene Infrastrukturen wie die Strom- und Wasserversorgung zugeschnitten sind, für IVS überhaupt geeignet sein können. Allein für die Informationsbasis bei der Wahl von angemessenen Schutzmaßnahmen der IT-Sicherheit nach § 8a BSIG deutet sich bereits an, dass ein Schutzregime, welches für die Herausforderungen in regelmäßig kommunikativ geschlossenen Systemen der klassischen kritischen Infrastrukturen konzipiert ist, diesen Herausforderungen derartig offener Systeme schwerlich gewachsen sein kann.

Weiterhin besteht, allerdings eher produktbezogen, eine IT-Sicherheitsregulierung für Fahrzeuge. Diese ist in Form der UN-R 155¹⁵ im Rahmen von Typengenehmigungs- und Marktüberwachungsverfahren europäisch integriert und stellt so einen Rahmen normativer IT-Sicherheitsregulierung für Kraftfahrzeuge zur Verfügung. Fraglich ist allerdings, ob wegen des produktbezogenen Fokus der UN-R diese wiederum auch die spezifischen Anforderungen der IVS zur Gewähr von Ende-zu-Ende IT-Sicherheit hinreichend in den Fokus nehmen kann.

Vor diesem Hintergrund lohnt sich in diesem ersten Teil des Aufsatzes eine Detailschau der Einzelregelungen und des gesamten Regelungsgefüges bei IVS (II.) auch im Hinblick auf das Zusammenspiel und Lücken bei der Gewähr von Ende-zu-Ende IT-Sicherheit im Rahmen von nationaler, eu-

ropäischer und internationaler Normsetzung. Ein zentrales Defizit ist das Fehlen einer normativen Risikomethodik bzw. eine nicht hinreichend angepasste Verweisung auf private Normung.¹⁶ Diese Herausforderungen und Regelungslücken werden abschließend unter III. in einem Fazit zusammengefasst. Ein entsprechender Lösungsansatz für die Begründung der Verantwortlichkeit sowie die Gewährleistung der Ende-zu-Ende IT-Sicherheit werden im zweiten Teil des Beitrags im nächsten Heft vorgestellt.

II. Regelungsgefüge

Im folgenden Abschnitt wird das KRITIS-Recht (1.), die IVS-RL (2.) sowie das fahrzeugbezogene Typengenehmigungsrecht (3.) betrachtet.

1. KRITIS-Recht

a) Anwendbarkeit auf IVS

Wie zuvor beschrieben können IVS als kritische Infrastrukturen erfasst sein, wenn sie den entsprechenden Schwellenwert erreichen. Der Schwellenwert bezieht sich auf die Anzahl von 500.000 angeschlossenen oder durchschnittlich im Versorgungsgebiet versorgten Nutzern. Ist dieser erreicht, unterliegen die Betreiber von IVS den IT-Sicherheitspflichten nach § 8a BSIG.

Allerdings ist diese Anzahl schwerlich zu erreichen: Es besteht ein Wandel von großflächigen, zentral vernetzten IVS-Dienstangeboten zu verteilten, fahrzeugfokussierten und auf multilateraler Echtzeitkommunikation basierenden Diensten. Dies führt dazu, dass pro Dienstangebot die Anzahl der Nutzer/innen deutlich geringer ausfallen wird. Daher soll im zweiten Teil des Beitrags der Frage nachgegangen werden, ob diese Anwendungsvoraussetzung in Form von nutzerzahlbezogenen Schwellenwerten sachgerecht ist.

b) Wahl von Schutzmaßnahmen

Sofern ein konkretes IVS als kritische Infrastruktur zu werten ist, richten sich gegenwärtig die Anforderungen im Bereich des IT-Sicherheitsrechts nach § 8a BSIG. Die Betreiber des IVS hätten mithin „angemessene“ Schutzmaßnahmen zu ergreifen. Fraglich erscheint jedoch, ob der Maßstab der „Angemessenheit“ hier hinreichend bestimmt ist. Denn es wird grundsätzlich kein Rahmen für Inhalte, Maßstäbe und Methodik bei der Ermittlung der Angemessenheit von tech-

13 Eine von der Kommission verabschiedete delegierte Verordnung (C(2019)1789 final), die insbesondere auch IT-Sicherheitsanforderungen an C-ITS-Stationen/-Dienste und ein Informationssicherheitsmanagementsystem gemäß ISO/IEC 27001 vorsieht, fand allerdings keine Zustimmung des Rats und konnte daher nicht in Kraft treten. Hierzu näher unter Abschnitt II. 2. c).

14 Ausführlich unter 2. b) und c).

15 UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2021/387]

16 Vgl. Ullmann/Strubbe/Wieschebrink, Vernetzter Straßenverkehr: Herausforderungen für die IT-Sicherheit in: Roßnagel/Hornung, Grundrechtsschutz im Smart Car, S. 309.

nisch-organisatorischen Maßnahmen zur IT-Sicherheit bereitgestellt.¹⁷

aa) Notwendigkeit einer methodischen Konkretisierung

Ein solcher konkretisierter Rahmen könnte jedoch aus mehreren Gründen notwendig sein: Einerseits dürfte im Hinblick auf den Eingriffscharakter der gesetzlich geforderten Investitionen in Sicherheitstechnik und Unternehmensorganisation schon aus Art. 12 und 14 GG eine Konkretisierung der Methodik geboten sein, um ein hinreichendes Maß an Normenbestimmtheit zu erreichen.

Andererseits könnte eine Konkretisierung auch erforderlich sein, um den Betreibern die Einhaltung der Vorgaben und damit der Gewährleistung eines angemessenen IT-Sicherheitsniveaus zu ermöglichen. Hierzu enthalten andere bereichsspezifische Regelungen zu KRITIS regelmäßig schon eine verfahrensrechtliche Konkretisierung dieser Maßstäbe für die Wahl von Schutzmaßnahmen.

So verlangt der IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG der BNetzA, dass die Netzbetreiber im Rahmen der Wahl von Schutzmaßnahmen ein Informationssicherheitsmanagementsystem (ISMS) implementieren, das den Anforderungen der ISO/IEC 27001 in der jeweils geltenden Fassung genügt.¹⁸ Für den dem IVS artverwandten Bereich der Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr ist nach § 8a Abs. 2 BStG ein branchenspezifischer Sicherheitsstandard (B3S) eingeführt worden, welcher explizit ein ISMS entsprechend ISO/IEC 27001 fordert.¹⁹ Ebenso wird in Annex IV der o.g. gescheiterten del. VO 2019/1789 verlangt, dass Betreiber einer C-ITS-Station ein ISMS im Einklang mit ISO/IEC 27001 betreiben.²⁰ Ohne einen Verweis auf die ISO/IEC 27001 wartet hingegen in den Art. 5-14 der Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) mit einem vollständig konturierten IKT-Risikomanagementrahmen auf.²¹ Schließlich tendiert auch die kommende NIS-RL 2.0 in Art. 17 f. zu einem Weg für ein granulares, methodisches Grundkonzept risikobasierter Maßnahmenwahl für die IT-Sicherheit.²²

Insgesamt kann man konstatieren, dass das Fehlen einer normativen Risikomethodik für die Betreiber kritischer Infrastrukturen problematisch ist. Dies gilt bei IVS im Besonderen, da es sich hier regelmäßig nicht um statische Client-Server-Architekturen handelt, wie sie klassischen KRITIS-Infrastrukturen zu eigen sind.

Die risikoprägenden Unsicherheiten sind hier zum einen deshalb erhöht, da durch verteilte und offene Kommunikationsarchitekturen die vernetzten Teilnehmer wie Fahrzeuge dem System temporär beitreten und ebenso dynamisch wieder austreten können. Zum anderen besteht auch durch die Ermöglichung neuer Angriffsvektoren in Bezug auf die multidirektionalen Nachrichtenübermittlungen eine erhöhte Unsicherheit. Für einen besonderen Bedarf an normativer Formalisierung des Verfahrens zur Risikobestimmung und Maßnahmenwahl spricht zudem, dass im Verhältnis zu den Kfz-Herstellern und dem Regulierungsregime der UN-R 155²³ die Systemgrenzen und damit die Verantwortlichkeit für die IT-Sicherheit explizit bestimmt werden müssen, um Kollisionen der Schutzregime zu vermeiden.

Deshalb ist für IVS eine normative inhaltliche und methodische Konkretisierung zur risikobasierten Ermittlung der Angemessenheit einer Maßnahmenwahl im Vergleich zu „klassischen“ kritischen Infrastrukturen erst recht geboten.

bb) Ausgestaltung der Konkretisierung

Hierfür wird bislang wie beschrieben häufig auf die private Normung der ISO/IEC 27000-Normfamilie verwiesen. In Betracht kommen neben einem solchen einfachen Verweis sowohl eine bereichsspezifisch angepasste Verweisung als auch eine unmittelbare gesetzliche Verankerung der Grundzüge einer Risikomethodik.

aaa) Einfache Verweisung

Einerseits könnte nach dem Vorbild des IT-Sicherheitskataloges zu § 11 Abs. 1b EnWG eine dynamische Verweisung auf Methoden und Maßstäbe der ISO/IEC 27000-Normfamilie in Betracht gezogen werden. Es besteht aber die Frage, ob der Inkorporation privater Normwerke durch eine Verweisung nicht die geforderte Normenklarheit gesetzlicher Regelungen entgegensteht. Das Gebot der Normenklarheit besagt, dass Rechtsnormen so formuliert sein müssen, dass der/die Betroffene die Rechtslage erkennen und somit sein/ihr Verhalten daran anpassen kann.²⁴ Es wird aus dem Rechtsstaatsprinzip nach Art. 20 Abs. 3 GG abgeleitet.²⁵ Die Verweisungen sollen dem Gebot jedenfalls dann genügen, wenn sie hinreichend klar erkennen lassen, welche – ihrerseits hinreichend klaren und bestimmten Normen – im Einzelnen gelten sollen und wenn dem/der Bürger:in die Rechtslage insgesamt hinreichend klar sein kann.²⁶ Dies ist bei Verweisen auf die ISO/IEC 27000 besonders problematisch, da diese in der Regel dynamisch auf die jeweils aktuelle Fassung der privaten Normung abstellen.

17 Allerdings besteht die Möglichkeit der Verwendung Branchenspezifischer Sicherheitsstandards (B3S) nach § 8a Abs. 2 BStG sowie von Audits, Prüfungen und Zertifizierungen, die durch das BSI festgelegt werden (§§ 8a Abs. 3, 5 BStG).

18 Vgl. BNetzA, IT-Sicherheitskatalog nach § 11 Abs.1a EnWG, S. 10; https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=1, abgerufen am 08.11.2022.

19 Vgl. DIN VDE V 0832-700 VDE V 0832-700:2019-03, Straßenverkehrs-Signalanlagen, Teil 700: Branchenspezifischer Sicherheitsstandard (B3S) für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr, Ziff. 4.3.1., hierzu auch unter Abschnitt 2. c).

20 Vgl. Annex 4 del. VO 2019/1789, S. 3.

21 Vgl. Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 COM(2020) 595 final 2020/0266 (COD).

22 Vgl. Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, COM(2020) 823 final.

23 Bei dem für die Anwendung ebenfalls auf die ISO/IEC 27001 verwiesen wird; vgl. United Nations, ECE/TRANS/WP.29/2021/59, Proposals for Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system), S. 3.

24 Ständige Rechtsprechung des BVerfG, vgl. anstelle vieler BVerfGE 45, 400, 420 = BVerfG NJW 1977, 1723, 1724; BVerfGE 156, 11 = NVwZ 2021, 226 Rn. 87.

25 BVerfGE 45, 400, 420 = BVerfG NJW 1977, 1723, 1724; BVerfGE 156, 11 = NVwZ 2021, 226 Rn. 87.

26 Dürig/Herzog/Scholz/Grzeszick, 98. EL März 2022, GG Art. 20 VII. Rn. 55.

Insofern müssen Verweisungen jedenfalls „begrenzt bleiben und dürfen nicht durch die Inbezugnahme von Normen, die andersartige Spannungslagen bewältigen, ihre Klarheit verlieren und in der Praxis nicht zu übermäßigen Schwierigkeiten bei der Anwendung führen“.²⁷ Gemessen an diesen Maßstäben könnte ein dynamischer gesetzlicher Verweis auf die jeweils gültige Methodik der Risikobewertung und Maßnahmenwahl aus der ISO/IEC 27000-Reihe aus der Perspektive des Rechtsstaatsprinzips allerdings fraglich sein. Ganz grundsätzlich ist diese Normreihe zur Konkretisierung von Methoden, Kriterien und Verfahren zum Risikomanagement der Informationssicherheit bei *privater Geschäftstätigkeit* in Unternehmen bestimmt.

Damit sind aber weitestgehend *andere Spannungslagen*, insbesondere hinsichtlich der Schutzgüter und Risikokriterien, adressiert, als sie der Risikobewertung als Gegenstand von Angemessenheitserwägungen im Rahmen der IT-Sicherheit in IVS zugrunde liegen.

Die für einen Geschäftsbetrieb maßgeblichen Risikokriterien/Schutzgüter wie „Verlust von Finanzmitteln, Beeinträchtigung von Geschäftsplänen und Deadlines“ sind im Hinblick auf die IVS-relevanten Schutzgüter/Schadereignisse regelmäßig unerheblich. Allenfalls in diese Richtung weisend, jedoch unklar im Bedeutungsgehalt, können die genannten Risikokriterien der „Verletzung von rechtlichen oder regulatorischen Anforderungen“ gelten,²⁸ wobei sich letzteres als zirkelschlüssig erweisen könnte, als die private Normung gerade die gesetzlichen Anforderungen konkretisieren sollte.

Zudem implementiert die ISO-Normreihe auch das Kriterium der Risikoakzeptanz.²⁹ Dies ist im Rahmen privatautonomer Entscheidungen, deren Auswirkungen in der Regel auf finanzielle Binnenaspekte gerichtet sind, ein nachvollziehbarer Umstand. Eine gänzlich andere Spannungslage zeigt sich bei den IVS: Hier sind die normativen Schutzgüter der Daseinsvorsorge, des Lebensschutzes und der Verkehrssicherheit maßgeblich. Diesbezüglich existiert kein Spielraum für private Akzeptanzkriterien von Betreibern kritischer Infrastrukturen.

Vor diesem Hintergrund bewältigt die fragliche ISO-Normfamilie offensichtlich andere Spannungslagen zum Risikomanagement als das KRITIS-Recht. Insofern wäre eine nicht angepasste Verweisung auf die jeweils aktuellen Normen der ISO/IEC 27000-Reihe in einer bereichsspezifischen Regelung zu IVS nach dem Rechtsstaatsprinzip aus Art. 20 Abs. 3 GG nicht geeignet, den unbestimmten Rechtsbegriff der Angemessenheit auszufüllen.

aaa) Angepasste Verweisung oder gesetzliche Ausgestaltung

Eine gesetzliche Ausgestaltung einer Risikomethodik für IVS könnte aber durch einen modifizierenden Verweis auf die ISO/IEC 27001 erfolgen. Die gesetzliche Modifikation müsste dann im Hinblick auf die abwägungsrelevanten Schutzgüter der Verkehrssicherheit und das Kriterium der

Risikoakzeptanz erfolgen. Dies würde dem Weg entsprechen, der auf europäischer Ebene durch Anhang IV der del. VO 2019/1789 vorgezeichnet ist. Ebenso könnte aber auch bereichsspezifisch eine vollständige Verfahrensregelung zu einem ISMS für IVS als kritische Infrastruktur beispielsweise im IVSG implementiert werden.³⁰

Die normative Ausgestaltung der Risikomethodik könnte dem Grundgedanken der rechtlichen Privatisierung von ehemaligen Staatsaufgaben folgend zur Gewähr von Straßenverkehrssicherheit durch IVS erforderlich sein. Im KRITIS-Recht entspricht es grundsätzlich dem „Gebot der funktionalen Äquivalenz“, dass die Rücknahme der staatlichen Erfüllungsverantwortung wiederum durch verfahrensrechtliche Instrumente des öffentlichen Rechts auszugleichen sein kann.³¹ Der diesbezügliche Anknüpfungspunkt ist die objektiv-rechtliche Schutzpflichtdimension der Grundrechte. Als grober Maßstab soll gelten: Je stärker sich der Staat bei der Leistungserbringung auf Private verlässt, desto größer deren Gewähr für die ordnungsgemäße Funktionserfüllung im Schutzpflichtenmodell sein muss.³² Im Rahmen der Einführung von IVS findet eine Verlagerung von Verantwortlichkeiten für die Straßenverkehrssicherheit auf private Dienstbetreiber statt. Dies gilt insoweit auch für die hierfür notwendige IT-Sicherheit. Angesichts der hier verwendeten hochkomplexen IKT wiese der Staat ohnehin erhebliche Informationsdefizite und Wissensprobleme auf.³³

Allerdings gilt es bei wissensbasierten Entscheidungsprogrammen, wie bei der Wahl von Schutzmaßnahmen der IT-Sicherheit, zwischen dem Sach-, Erfahrungs- und Regelwissen des Entscheiders zu differenzieren. Das notwendige Sachwissen wird auch schon in klassischen ordnungsrechtlichen Verfahren naturgemäß für die Behörden als instabil angesehen.³⁴ Gerade im Bereich der Regulierung komplexer Technologien und der Dynamisierung von Rechtsgebieten wird beim staatlichen Entscheider zudem grundsätzlich ein Mangel der stabilen Verfügbarkeit des Erfahrungswissens bei Prognoseentscheidungen unter Unsicherheit, wie es dem Konditionalprogramm von Risikoentscheidungen über IT-Schutzbedarfe eigen ist, angenommen.³⁵ Auf der Ebene des notwendigen „Regelwissens“ könnte allerdings im Hinblick

27 BVerfG NJW 2020, 2235, 2256 Rn. 215.

28 ISO/IEC 27005:2008, S. 8.

29 ISO/IEC 27005:2008, S. 21.

30 Es ist zu beachten, dass die IT-Sicherheitsregelungen der del. VO 2019/1789 produktbezogen auf die einzelnen C-ITS-Stationen ausgelegt sind, wohingegen eine KRITIS-Regelung den Zusammenhang des vollständigen Teilsystems bzw. Dienstangebotes in den Fokus der Risikobetrachtung und Maßnahmenwahl nehmen müsste.

31 Burgi, Die Funktion des Verfahrensrechts in privatisierten Bereichen – Verfahren als Gegenstand der Regulierung nach Verantwortungsteilung in: Hoffmann-Riem/Schmidt-Aßmann, Verwaltungsverfahren und Verwaltungsverfahrensgesetz, S. 155, 174 f.

32 Schoch, Gewährleistungsverwaltung: Stärkung der Privatrechtsgesellschaft?, NVwZ 2008, 241, 244.

33 Schoch, Gewährleistungsverwaltung: Stärkung der Privatrechtsgesellschaft?, NVwZ 2008, 241, 242.

34 Vgl. Röhl, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts Bd. I 2012, S. 748 ff.

35 Vgl. Wollenschläger, Wissensgenerierung im Verfahren, S. 31.

auf eine effektive Gestaltung des Verfahrens des Risikomanagements nach wie vor eine deutliche Überlegenheit staatlicher Kompetenzen angelegt sein.

Hinsichtlich der Methoden der Risikobewertung, könnte sich deshalb die gesetzliche Gestaltung des Verfahrensrahmens für IT-Sicherheit in kritischen Infrastrukturen deutlich sachgerechter darstellen als der einfache oder angepasste Verweis auf die internationale Standardisierung der privaten ISO/IEC 27000-Normfamilie.

Vor diesem Hintergrund erscheint eine gesetzliche Konkretisierung des Verfahrensprogramms und die Konturierung der leitenden inhaltlichen und methodischen Vorgaben für die Wahl von Schutzmaßnahmen bei IVS geboten.

c) Zwischenfazit

Das auf IVS anwendbare KRITIS-Recht weist zumindest ein wesentliches Defizit auf: Das KRITIS-Recht lässt eine für IVS passende Risikomethodik zur Gewährleistung der IT-Sicherheit vermissen. Im zweiten Teil des Beitrags wird sich zeigen, ob mit dem die Anwendbarkeit begründenden Schwellenwertkonzept ein weiteres im Hinblick auf IVS bestehendes Defizit hinzukommt.

2. IVS-RL

Anders als im KRITIS-Recht gibt es in der aktuell geltenden IVS-RL keine Regelungen, die dem IT-Sicherheitsrecht zuzuordnen sind (a). Allerdings finden sich in dem Entwurf der neuen IVS-RL vereinzelt Vorgaben zur IT-Sicherheit (b), die durch delegierte Verordnungen konkretisiert werden können. Hierfür könnte sich der EU-Gesetzgeber an der gescheiterten del. VO 2019/1789 orientieren (c).

a) Bisherige IVS-RL

So verweist Art. 10 IVS-RL lediglich deklaratorisch auf das Datenschutzrecht. In den Grundsätzen für die Spezifikationen und die Einführung von IVS in Anhang II findet sich ebenfalls keine Vorschrift dahingehend, dass IVS angemessen gegen Angriffe auf die IT-Sicherheit geschützt werden müssen. Die dort in Buchstabe i geforderte Belegung der technischen Reife³⁶ bezieht sich lediglich auf die Betriebssicherheit.

Das Fehlen von Anforderungen im Rahmen des IT-Sicherheitsrechts ist dem vorrangigen Ziel der IVS-Richtlinie, die Einführung von IVS in der Union zu fördern, geschuldet (vgl. Art. 1 Abs. 1, ErwG. 23 IVS-RL). Dies spiegelt sich auch in den vier delegierten Verordnungen wider, die die EU-Kommission zur Ergänzung der IVS-RL erlassen hat. Diese regeln jeweils Einzelheiten zu bestimmten Arten von IVS-Diensten, wie dem eCall,³⁷ Echtzeitinformationsdiensten,³⁸ Informationsdiensten für LKW-Parkplätze³⁹ und der Bereitstellung eines Mindestniveaus allgemeiner für die Straßenverkehrssicherheit relevanter Verkehrsinformationen.⁴⁰ Anforderungen an die IT-Sicherheit dieser Dienste fehlen auch hier.

b) IVS-2-RL-E

Am 15.12.2021 verabschiedete die EU-Kommission den IVS2-RL-E.⁴¹ Derzeit (Stand 16.11.2022) wird der Entwurf im Rat diskutiert. Der Entwurf behält im Wesentlichen die bisherige Ausrichtung der IVS-RL auf Verbreitung und Verstärkung der Interoperabilität von IVS durch erhöhte Verfügbarkeit der hierfür relevanten Daten und verstärkte Zusammenarbeit der Beteiligten bei.⁴² Neu ist, dass der Gesetzgeber auf den oben unter I. erläuterten Wechsel des Kommunikationsparadigmas von einem zentralen und geschlossenen hin zu einem multidirektionalen, offenen und verteilten System reagiert hat. So werden mit dem Entwurf die bereits erwähnten C-ITS aufgenommen. Auf die in C-ITS erhöhte Unsicherheit hat der Gesetzgeber durch die Aufnahme von IT-Sicherheitsvorschriften reagiert. Neben den IT-Sicherheitsvorschriften zu C-ITS enthält der IVS2-RL-E auch einige wenige allgemeine IT-sicherheitsrechtlichen Regelungen für IVS.

Die IT-sicherheitsrechtlichen Regelungen werden im Folgenden zusammengefasst.

aa) Allgemeine IT-Sicherheitsregelungen für IVS

Für IVS existieren im IVS2-RL-E zwar keine materiellen IT-Sicherheitsvorgaben, aber solche, die die EU-Kommission zu bestimmten behördlichen Maßnahmen ermächtigen.

Nach Art. 7a IVS2-RL-E kann die EU-Kommission in Notfällen, die einen schwerwiegenden Einfluss auf die Straßenverkehrssicherheit, die IT-Sicherheit und die Verfügbarkeit sowie Integrität von IVS-Diensten haben, vorläufige Maßnahmen erlassen. Der Anwendungsbereich beschränkt sich auf die vorrangigen Bereiche gem. Art. 2 IVS-RL. Außerdem müsste der Notfall geeignet sein, das sichere und ordnungsgemäße Funktionieren des Verkehrssystems der EU zu beeinträchtigen. Unklar ist, was unter einem schwerwiegenden Einfluss zu verstehen ist. Die Vorschrift bezieht sich nur auf überregional wirkende Ereignisse, wodurch der Anwendungsbereich erheblich eingeschränkt ist.

36 Art. 5 Abs. 1 i.V.m. Anhang II lit. i IVS-RL „Belegung der technischen Reife: d. h. nach einer angemessenen Risikobewertung die Zuverlässigkeit innovativer IVS anhand ausreichender technischer Entwicklung und betrieblicher Nutzung nachweisen“.

37 Delegierte Verordnung (EU) Nr. 305/2013 der Kommission vom 26. November 2012 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die harmonisierte Bereitstellung eines interoperablen EU-weiten eCall-Dienstes.

38 Delegierte VO 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste.

39 Delegierte VO (EU) Nr. 885/2013 der Kommission vom 15. Mai 2013 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die Bereitstellung von Informationsdiensten für sichere Parkplätze für Lastkraftwagen und andere gewerbliche Fahrzeuge.

40 Delegierte VO (EU) 2022/670 der Kommission vom 2. Februar 2022 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste.

41 COM(2021) 813 final.

42 Vgl. S. 6 des Entwurfs COM(2021) 813 final.

Daneben ist die EU-Kommission nach Art. 6 Abs. 1 i.V.m. Art. 7 Abs. 1 IVS-RL und Anhang I Ziff. 3.4.1 IVS2-RL-E befähigt, Spezifikationen zur Unterstützung der Sicherheit in Bezug auf das Human-Machine-Interface, zur Verwendung mobiler Geräte wie beispielsweise Smartphones und zur Sicherheit der fahrzeuginternen Kommunikation zu erlassen. Da sich insbesondere erstere und letztere Regelungen mit dem fahrzeugspezifischen Recht überschneiden könnten (siehe Abschnitt 3.), gilt die Befugnis zum Erlass der Spezifikationen nur, soweit sie nicht in den Geltungsbereich der einschlägigen fahrzeugspezifischen Verordnungen⁴³ fallen. Inwieweit hierfür neben der umfassenden UN-R 155 überhaupt Raum ist (hierzu unter Abschnitt 3. a), ist unklar.

bb) Besondere IT-Sicherheitsregelungen für C-ITS

Für C-ITS enthält der Entwurf Ermächtigungen zum Erlass von Anforderungen an die Public Key Infrastructure (PKI) und Sicherheitskonzepte für das Risikomanagement bei C-ITS-Diensten.

aaa) Anforderungen an die PKI

Die für C-ITS ausgetauschten V2X-Nachrichten werden unverschlüsselt gebroadcastet, d.h. jede Person mit einem Empfangsgerät kann diese lesen. Die Gefahr der Erstellung von Bewegungsprofilen wird durch die pseudonymisierte Versendung und regelmäßige Änderung des Pseudonyms verringert. Um Vertrauen in die Authentizität und Integrität der Nachrichten herzustellen, werden sie zudem signiert übertragen. Hierfür wird eine PKI verwendet. Da es mehrere PKI geben kann, ist zur Sicherstellung der Interoperabilität und des Vertrauens der PKI untereinander eine übergeordnete Instanz erforderlich. Diesbezüglich kann die EU-Kommission nach Art. 10a IVS2-RL-E und Anhang I Ziff. 4.3 Spezifikationen für ein EU-System für das Management von Sicherheitsberechtigungen nachweisen von C-ITS-Diensten erlassen (EU C-ITS Security Credential Management System – EU CCMS). Hierzu gehört die Festlegung bestimmter Rollen (Anhang I Ziff. 4.3.2. IVS2-RL-E) sowie der Erlass von Regeln für die Verwaltung von Public Key Zertifikaten für C-ITS-Dienste (Anhang I Ziff. 4.3.1. IVS2-RL-E).

Im Rahmen der o.g. del. VO 2019/1789 wurde bereits eine Zertifikatsrichtlinie erarbeitet, die gemeinsame Regeln für den Betrieb einer PKI festlegt.⁴⁴ Auch wenn die del. VO nicht in Kraft getreten ist, wird die Zertifikatsrichtlinie bis heute verwendet und ist verpflichtend, wenn man als Organisation am EU CCMS teilnehmen möchte.⁴⁵ Das BSI hat kürzlich zwei Technische Richtlinien erlassen, die die Anforderungen aus der Zertifikatsrichtlinie zusammenfassen und ergänzen.⁴⁶ Da sich die unverbindliche Zertifikatsrichtlinie in der Praxis bereits durchgesetzt hat, darf angenommen werden, dass sich die EU-Kommission für eine neu erlassene, verbindliche Zertifikatsrichtlinie auf Basis des IVS2-RL-E an der bisherigen Zertifikatsrichtlinie orientieren wird.

Auch die Rollen sollten bereits in der del. VO 2019/1789 festgelegt werden. Danach sollte die EU-Kommission die erforderlichen Rollen übernehmen, bis eine gesonderte Ins-

tanz dafür geschaffen wurde (Art. 24-26 del. VO 2019/1789). Auch hieran könnte sich der EU-Gesetzgeber bei Erlass neuer Spezifikationen auf Basis des IVS2-RL-E orientieren.

aaaa) Sicherheitskonzept für C-ITS-Dienste

Weiterhin ist bei den Spezifikationen im Rahmen des EU CCMS der Erlass eines Sicherheitskonzepts für das Informationssicherheitsmanagement in C-ITS-Diensten vorgesehen (Anhang I Ziff. 4.3.3. IVS2-RL-E). Regelungstechnisch ist dies nicht ganz geglückt, da der Umfang dieses Sicherheitskonzepts nicht klar wird. Weil das Sicherheitskonzept als Unterpunkt zum EU CCMS aufgeführt ist, könnte man wegen der Systematik den Umfang allein auf solches Informationssicherheitsmanagement beziehen, das auf Zertifikaten basiert. Dies würde aber verkennen, dass sich ein umfassendes Informationssicherheitsmanagement nicht in der Verwendung und Verwaltung von Zertifikaten erschöpfen kann. So sind Angriffe denkbar, die sich durch Signaturzertifikate nicht verhindern lassen, wie DoS-Angriffe oder die Verfälschung von Daten durch Manipulation von Sensoren, bevor diese per V2X-Nachricht versendet werden. Auch die Sicherheitsrichtlinie aus der del. VO 2019/1789 (dazu sogleich unter Abschnitt 2.c), die hier wieder als Anhaltspunkt für eine neue delegierte Verordnung herangezogen werden könnte, bezieht sich nicht nur auf Zertifikate, sondern auf ein allgemeines Management der Informationssicherheit in C-ITS. Dies alles spricht dafür, auch das im IVS2-RL-E aufgeführte Sicherheitskonzept allgemein und nicht lediglich in Bezug auf Zertifikate auszulegen. Um dies klarzustellen, hätte die Ziff. 4.3.3. Anhang 1 IVS2-RL-E neben und nicht unter dem EU CCMS aufgeführt werden sollen (beispielsweise als Ziff. 4.4.).

cc) Zwischenfazit

Insgesamt geht der IVS2-RL-E aus Sicht der IT-Sicherheit in die richtige Richtung, indem der EU-Gesetzgeber auf den Wechsel des Kommunikationsparadigmas reagiert hat und insbesondere die IT-Sicherheit von C-ITS behandelt. Es bleibt aber abzuwarten, wie die EU-Kommission die genannten Regelungsbereiche durch den Erlass delegierter Rechtsakte nach In-Kraft-Treten des IVS2-RL-E ausfüllen wird und inwiefern sich diese mit dem fahrzeugspezifischen Recht überschneiden werden.

43 Genauer sind dies VO (EU) 2018/858 („TypengenehmigungsVO“), VO (EU) Nr. 167/2013 (TypengenehmigungsVO bezüglich land- und forstwirtschaftlicher Fahrzeuge), VO (EU) Nr. 168/2013 (TypengenehmigungsVO bezüglich zwei- oder dreirädriger Kraftfahrzeuge und vierrädriger Kraftfahrzeuge).

44 Del. VO 2019/1789 Annex 3.

45 Bräunlich/Matzerath, Vorgaben für den sicheren und interoperablen Betrieb von kooperativen intelligenten Transportsystemen im europäischen Anwendungskontext, in: Cyber-Sicherheit ist Cheffinnen- und Chefsache! Tagungsband zum 18. Deutschen IT-Sicherheitskongress 2022, S. 157, 159 f.; BSI TR 03164-1 (11); <https://cpoc.jrc.ec.europa.eu/Documentation.html>, abgerufen am 09.11.2022; <https://its-norway.no/wp-content/uploads/2021/02/6-Geert-van-der-Linden-C-ITS-21-03-11.pdf>, abgerufen am 09.11.2022.

46 BSI TR 03164-1 und 03164-2.

Da in der gescheiterten del. VO 2019/1789 vor allem hinsichtlich des EU CCMS nahezu dasselbe geregelt werden sollte und da diese trotz ihrer Unverbindlichkeit bereits eine hohe Praxisrelevanz erreicht hat, spricht vieles dafür, dass sich der EU-Gesetzgeber für die zu erlassenden delegierten Rechtsakte an dieser orientieren wird. Angesichts dessen soll die del. VO 2019/1789 in Bezug auf die C-ITS-Sicherheitsrichtlinie im Folgenden kritisch beleuchtet werden.

aaa) Entwurf der del. VO 2019/1789

Die del. VO 2019/1789 sieht in Art. 27 vor, dass jeder Betreiber einer C-ITS-Station ein ISMS nach ISO/IEC 27001 implementiert und dabei die im Anhang IV Abschnitt 1.3.1. enthaltenen Einschränkungen und zusätzlichen Anforderungen berücksichtigt.

Das ISMS umfasst sämtliche C-ITS-Stationen eines Betreibers sowie alle anderen durch ihn betriebenen Informationsverarbeitungssysteme, die die genormten C-ITS Nachrichten verarbeiten (Ziff. 1.3.1. Abs. 1 Annex 4 del. VO 2019/1789). C-ITS-Stationen sind nach Art. 2 Abs. 3 del. VO 2019/1789 alle Software- und Hardwarekomponenten, die die für den C-ITS-Dienst erforderlichen Nachrichten empfangen, senden und verarbeiten. Die del. VO verweist hier auf die EN 302 665 v 1.1.1, die verschiedene Arten von C-ITS-Stationen definiert, namentlich persönliche (z.B. Smartphones), zentrale, straßen- (z.B. RSU) und fahrzeugseitige Stationen.

Mit der Adressierung der C-ITS-Stationen weist die del. VO 2019/1789 weniger eine Dienstperspektive auf, als dies in der übrigen IVS2-RL-E und im KRITIS-Recht üblich ist. Bei beiden Rechtsregimen stehen insoweit der IVS-Dienst bzw. die kritische Dienstleistung (§ 1 Abs. 1 Nr. 3 KritisV) im Vordergrund. Dagegen blickt die del. VO 2019/1789 auf ein C-ITS als Summe einzelner C-ITS-Stationen und nimmt folglich die C-ITS-Station als Produkt in den Fokus. Bei Überschreitung der entsprechenden Schwellenwerte kann die del. VO 2019/1789 daher komplementär zum KRITIS-Recht sein.⁴⁷

Der Betreiber der C-ITS-Stationen in Art. 2 Abs. 16 del. VO 2019/1789 wird nur knapp definiert als jede natürliche oder juristische Person, die für die Inbetriebnahme und den Betrieb von C-ITS-Stationen verantwortlich ist. Wie die Verantwortlichkeit bei mehreren relevanten Personen bestimmt werden soll, wird nicht erläutert. Der Betreiber von C-ITS-Stationen muss im Rahmen des ISMS lediglich andere hierfür relevante Personen und Interessenträger bestimmen. Konkrete Maßnahmen knüpfen hieran jedoch nicht an.

Neben einer erforderlichen Zertifizierung nach der ISO/IEC 27001 hinsichtlich des ISMS (Art. 28 del. VO 2019/1789) bedürfen C-ITS-Stationen einer Zertifizierung nach ISO/IEC 15408, die Evaluationskriterien für die IT-Sicherheit von Produkten und Systemen enthält (Ziff. 1.6.2.2 Abs. 30-32 del. VO 2019/1789). Auch dies zeigt die produktorientierte Sicht der del. VO 2019/1789. Zusätzlich muss eine Konformitätserklärung über die C-ITS-Station abgegeben werden, die besagt, dass die in Art. 5 del. VO 2019/1789 festgesetzten Anforderungen eingehalten wurden (Art. 13 Nr. 1 del. VO 2019/1789 und Annex 5 del. VO 2019/1789). Diese enthalten jedoch keine Anforderungen hinsichtlich der IT-Si-

cherheit, sondern vorrangig hinsichtlich ihrer Interoperabilität.

Als Zwischenfazit lässt sich zunächst positiv festhalten, dass die del. VO 2019/1789 nicht nur einen einfachen Verweis auf die ISO/IEC 27001, sondern an IVS angepasste Einschränkungen und zusätzliche Anforderungen enthält. So werden besonders die Systemgrenzen, bzw. in der Terminologie der del. VO der Anwendungsbereich, in Ziff. 1.3.1. Abs. 3 Annex 4 del. VO 2019/1789 festgelegt. Zudem werden die möglichen Auswirkungen auf Schutzziele im Fall von IT-Sicherheitsvorfällen bezüglich verschiedener Nachrichtentypen aufgelistet und bewertet (Ziff. 1.4. Annex 4 del. VO 2019/1789). Negativ ist hingegen, dass weder der Katalog an Schutzgütern eindeutig auf das normativ relevante Maß beschränkt wurde⁴⁸ noch insoweit die individuelle Risikoakzeptanz ausgeschlossen wurde.

Tendenziell war die del. VO 2019/1789 aus Sicht des IT-Sicherheitsrechts begrüßenswert, weil sie zeigte, dass der europäische Gesetzgeber im Zuge der zunehmenden Vernetzung des Straßenverkehrs das Erfordernis einer IT-sicherheitsrechtlichen Regelung in diesem Bereich erkannt hat. Insofern hat das Scheitern der del. VO 2019/1789 die Entwicklung dieser Rechtsmaterie behindert.

3. Typengenehmigungsrecht

Nach § 2 Nr. 1 IVSG umfassen IVS den Einsatz von IKT im Straßenverkehr, wozu auch die Fahrzeuge gehören.⁴⁹ Die Fahrzeuge sind als Informationsquellen und -senken faktisch vernetzter Bestandteil von IVS. Gleichwohl unterfallen Fahrzeuge daneben auch einer eigenen Regulierung, insbesondere dem Typengenehmigungsrecht.

Das Typengenehmigungsrecht regelt die Berechtigung eines Herstellers, für eine unbestimmte Anzahl von ihm gefertigter, baugleicher Fahrzeuge Übereinstimmungsbescheinigungen auszustellen, die dann wiederum für die Zulassung der Fahrzeuge erforderlich sind.⁵⁰ Das Typengenehmigungsrecht ist mithin durch eine fahrzeugzentrierte Sicht gekennzeichnet, wobei die Anforderungen an das Fahrzeug durch den Hersteller nachzuweisen sind.

Zentrales Gesetz des Typengenehmigungsrechts ist die Typengenehmigungsverordnung (VO 2018/858), die auf die neuere General Safety Regulation II (VO 2019/2144) verweist. In den Anhängen der letztgenannten werden wiederum diverse UN-Regelungen aufgelistet, die ebenfalls Teil der Anforderungen an die Typengenehmigung sind. Hierzu gehört insbesondere die für die vorliegende Untersuchung relevante UN-R 155, welche die Cybersicherheit der Fahrzeuge betrifft und durch die del. VO (EU) 2022/1389 in die VO 2019/2144 eingefügt wurde.

⁴⁷ Erwägungsgrund 6 del. VO 2019/1789.

⁴⁸ Del. VO 2019/1789, Anhang IV, Ziff. 1.4, Abs. 15.

⁴⁹ Vgl. Art. 4 Nr. 1 IVS-RL.

⁵⁰ Siebert, in: Siebert, Die Genehmigungsverfahren für Kraftfahrzeuge, 2. Aufl. 2021, S. 23; daneben besteht die Möglichkeit der Einzelgenehmigung von Fahrzeugen, der in der Praxis aber nur eine untergeordnete Bedeutung zukommt.

a) UN-R 155

Die UN-R 155 schreibt zur Gewährleistung der Cybersicherheit die Durchführung eines Cybersecurity-Managementsystems (CSMS) vor. Hierbei handelt es sich im Kern um ein Risikomanagement, d.h. eine Methodik für den Umgang mit Risiken.

Ein Risiko ist nach UN-R 155, „die Möglichkeit, dass durch eine bestimmte Bedrohung Schwachstellen eines Fahrzeugs ausgenutzt werden und dadurch eine Organisation oder einer Person Schaden zugefügt wird.“ Ergänzend kann die in ISO/SAE 21434 (Road vehicles – Cybersecurity engineering) genannte Definition herangezogen werden,⁵¹ welche Risiko als „die Auswirkung von Ungewissheit auf die Cybersicherheit von Straßenfahrzeugen, ausgedrückt durch die Durchführbarkeit von Angriffen und deren Auswirkungen“, beschreibt.⁵²

Zusammenfassend kann man damit festhalten, dass mit der Möglichkeit der Ausnutzung bzw. der Durchführbarkeit eines Angriffs die Wahrscheinlichkeit eines Ereignisses beschrieben wird und dieses Ereignis bestimmte Auswirkungen haben kann. Bei den Auswirkungen wird nach ISO/SAE 21434 der Schaden oder die physische Beeinträchtigung eines Schadenszenarios betrachtet, welches wiederum als nachteilige Folge oder unerwünschtes Ergebnis aufgrund der Beeinträchtigung einer (oder mehrerer) Cybersicherheitseigenschaft(en) (Schutzziele) eines Assets oder einer Gruppe von Assets definiert ist.

Als Beispiele für Schadensszenarien werden in Ziff. 8.3.2. der ISO/SAE 21434 die Offenlegung von Verbraucherinformationen durch einen Vertraulichkeitsverlust im Infotainment-System sowie das ungewollte Auslösen einer Vollbremsung bei Höchstgeschwindigkeit durch einen Integritätsverlust im Bremssystem genannt. Ein Schadensszenario, bei dem das Fahrzeug dritte Verkehrsteilnehmende durch Falschinformationen (ggf. über ein IVS) schädigt, wird hingegen nicht genannt.

Die Risikomethodik wird fachspezifisch weiter ausgestaltet. Als Hilfestellung für die Risikoidentifikation werden in Anhang 5 etwa die Grundzüge der fachspezifischen Bedrohungen, Schwachstellen und Angriffsmethoden benannt. Im Rahmen der Risikobehandlung mindestens zu treffende Maßnahmen sind abstrakt in Anhang 5 Teil B und C niedergelegt, wobei ein Abweichen durch alternativ-gleichwertige bzw. neuere Maßnahmen zugelassen wird. Im Ergebnis müssen die Maßnahmen nach Ziff. 7.3.4, 7.3.5. „angemessen“ sein, was bedeutet, dass das verbleibende Risiko auf Basis der Risikokriterien für den Hersteller als tolerierbar angesehen werden muss.⁵³

b) Überschneidender Anwendungsbereich

Wie bei der Definition von IVS begründet auch die UN-R 155 einen überschneidenden Anwendungsbereich zwischen IVS und Fahrzeugen: Die Gewährleistung der Cybersicherheit erfordert nach Ziff. 7.3.3 in der Risikobewertung auch die „Wechselwirkungen mit sämtlichen externen Systemen [wie etwa IVS] zu berücksichtigen.“ Die „Risikobewertung“ bildet nach der Definition in Ziff. 2.1 den Oberbegriff für Risikoer-

mittlung, Risikoanalyse und Risikoeinschätzung und damit den Kern des CSMS. Mithin sind diese Wechselwirkungen mit externen Systemen in nahezu der gesamte Risikomethodik zu berücksichtigen.⁵⁴

Mit Blick auf den Lebenszyklus der Fahrzeuge kommt diesem Aspekt auch deshalb besonderes Gewicht zu, da das CSMS nicht nur für die Entwicklungs- und Produktionsphase, sondern auch für die Postproduktionsphase gilt, die nach Ziff. 2.7 bis zum Ende der Lebensdauer aller Fahrzeuge des Fahrzeugtyps andauert, also die vollständige Betriebsphase umfasst. Folglich muss der Hersteller alle Risiken (auch durch Wechselwirkungen mit externen Systemen) berücksichtigen, die in diesem Zeitraum erst noch entstehen, etwa durch das Aufkommen neuer IVS. Durch diese Ausdehnung auf die Betriebsphase der Fahrzeuge wird der Hersteller ähnlich wie der Betreiber eines Systems zur kontinuierlich aktualisierten Risikobewertung (Ziff. 7.2.2.2.) und damit verbundener Risikobehandlung der Fahrzeuge verpflichtet.

c) Unsicherheit

Bezüglich der Bewältigung der Risiken aus Wechselwirkungen mit externen Systemen gilt es jedoch weiterhin zu beachten, dass der Fahrzeughersteller nur Sach- und Erfahrungswissen darüber hat, welche Daten das Fahrzeug von externen Systemen für seine Fahrfunktionen benötigt und wie sich somit auch Manipulationen der Daten auf die Fahrfunktionen auswirken.⁵⁵ Erhebliche Unsicherheit besteht beim Fahrzeughersteller hingegen darüber, welche entfernten Auswirkungen von ihm ausgesendete und ggf. durch Dritte manipulierte Daten haben. Die Risikoabschätzung bzgl. des Datenoutputs an externe Systeme bleibt aus der Perspektive des Herstellers somit zwangsläufig unvollständig; es ist insoweit aus Anhang 5 auch nicht ersichtlich, dass diese entfernten Auswirkungen mitberücksichtigt wurden. Insofern besteht ein Wissensdefizit bei der Betrachtung der Risiken im Überschneidungsbereich. Hierauf wird im zweiten Aufsatzteil vertiefend eingegangen.

d) Zwischenfazit

Die UN-R 155 als Bestandteil des Typengenehmigungsrechts fordert vom Fahrzeughersteller die Einhaltung eines Cybersicherheitsmanagements, mithilfe dessen die Cybersicherheitsrisiken über den gesamten Lebenszyklus der Fahrzeuge betrachtet werden. Diese Methodik entspricht auch den bereits dargestellten Anforderungen, mit Ausnahme der auch hier bestehenden Möglichkeit der individuellen Risikoakzeptanz.⁵⁶

51 Siehe: UN-R 155 Interpretation Document, Ziff. 2.1 und zu Ziff. 5.3.1., part (a) hinsichtlich der Kompetenz des Personals.

52 ISO/SAE 21434, Ziff. 3.1.25.

53 UN R 155 Interpretation Document zu Ziff. 7.2.2.2., part (d).

54 In ISO/SAE 21434, Ziff. 9.3.2. wird insoweit auch darauf hingewiesen, dass die Systemgrenzen (hier: item boundaries) anhand der Schnittstellen zu anderen Objekten und Komponenten innerhalb und/oder außerhalb des Fahrzeugs zu beschreiben sind.

55 Z.B. Daten aus der Cloud, vgl. UN-R 155 Interpretation Document, zu Ziff. 7.3.5., part (b).

Gleichzeitig schließt das CSMS auch Risiken aus Wechselwirkungen mit externen Systemen mit ein, wobei der Fahrzeughersteller insofern nur die Risiken für das Fahrzeug und keine entfernten Risiken für IVS durch manipulierte Daten aus dem Fahrzeug betrachten muss. Diese könnte er auch nur unzureichend behandeln, da für ihn mangels Sach- und Erfahrungswissen hohe Unsicherheit darüber besteht, welche Auswirkungen diese Risiken im Rahmen des IVS auslösen könnten.

III. Fazit

Der untersuchte Rechtsrahmen weist diverse Schwierigkeiten und Defizite auf. Im Rahmen des KRITIS-Rechts wurde auf die Problematik des vollständigen Fehlens einer gesetzlichen Risikomethodik sowie auf die alternative Möglichkeit des angepassten Verweises auf private Normung (ISO/SAE 27000) hingewiesen. Außerdem wurde die Frage aufgeworfen, ob das Schwellenwertkonzept im Hinblick auf IVS sachgerecht ist. Dem soll im zweiten Teil des Beitrags weiter nachgegangen werden.

Bezüglich des IVS-Rechts konnte gezeigt werden, dass dieses insbesondere mit dem neuen Entwurf und der gescheiterten delegierten Verordnung sinnvolle Regelungsansätze für die IT-Sicherheit bietet. Kritisch wurde insofern attestiert, dass bei der modifizierenden Verwendung der ISO/SAE 27000-Risikomethodik nicht alle rechtlich relevanten Aspekte auch hinreichend angepasst wurden; dies gilt insbesondere für die fehlende Beschränkung auf normative Schutzgüter sowie die fortbestehende Möglichkeit individueller Risikoakzeptanz.

Schließlich wurde das für die IT-Sicherheit relevante Typengenehmigungsrecht in Form der UN-R 155 untersucht und dabei dieselbe Problematik bezüglich der individuellen Risikoakzeptanz festgestellt.

Noch entscheidender als die bereits genannten methodischen Defizite ist aber, dass sowohl das IVS-Recht als auch die UN-R 155 in ihrem Anwendungsbereich wechselseitige Überschneidungen aufweisen. Es wurde herausgearbeitet, dass diese Überschneidungen sich sachlich immanent aus dem Charakter der IVS als offene

Systeme mit den Fahrzeugen als informationsempfangende und -bereitstellende Teilnehmer ergeben. Für die Normadressaten beider Systeme (IVS, Fahrzeuge) besteht somit hohe Unsicherheit über die jeweils anderen Systeme. Hierfür fehlt es bislang an einer gesetzlichen Methodik, mit der diese Unsicherheit bewältigt werden kann. Eine Vertiefung dieses Problems sowie entsprechende Lösungsvorschläge werden im zweiten Teil des Aufsatzes geboten.



Leonie Sterz

arbeitet am ZAR/KIT (Zentrum für angewandte Rechtswissenschaft am Karlsruher Institut für Technologie) und forscht schwerpunktmäßig im Datenschutz- und IT-Sicherheitsrecht mit besonderem Fokus auf den Bereich Smart Mobility.



Christoph Werner

arbeitet am ZAR/KIT (Zentrum für angewandte Rechtswissenschaft am Karlsruher Institut für Technologie) und forscht schwerpunktmäßig im Datenschutz- und IT-Sicherheitsrecht.



Prof. Dr. Oliver Raabe

arbeitet am ZAR/KIT (Zentrum für angewandte Rechtswissenschaft am Karlsruher Institut für Technologie) und forscht schwerpunktmäßig im Datenschutz- und IT-Sicherheitsrecht mit Querbezügen zur Rechtsinformatik und besonderem Fokus auf den Bereich Smart Mobility.

Dr. Sebastian Meyer

Rechtsmissbräuchliche Schadensersatzforderungen

Das Landgericht München hat einem Betroffenen einen Betrag in Höhe von 100,00 EUR zugesprochen, weil das beklagte Unternehmen für seine Homepage frei verfügbare Schriften von Google (Webfonts) nicht auf dem eigenen Server hinterlegt hatte, sondern die Schriften direkt bei Seitenaufruf über die Server von Google nachgeladen wur-

den.¹ Auf diese Weise erhielt Google bei jedem Seitenaufruf eines Nutzers zwangsläufig dessen IP-Adresse, da diese zur Auslieferung der nachgeladenen Inhalte erforderlich war. Das Zivilgericht hat hierin einen Datenschutzverstoß gesehen, der es rechtfertigt, dem Betroffenen einen Schadensersatzanspruch zuzusprechen.

I. Ausgangslage bei Google Fonts

Der Ausgangspunkt, die Einstufung des Vorgehens als Datenschutzverstoß, für die Herleitung des Schadensersatzanspruchs wohl nicht zu beanstanden. Die Bereitstellung der Schriftarten von Google wäre für das verklagte Unternehmen auch auf dem eigenen Server rechtlich zulässig und technisch möglich gewesen. Google weist in dem Kontext selbst darauf hin, dass alle Schriftarten unter Open Source Lizenzen veröffentlicht sind und frei genutzt werden können.² Die von dem Unternehmen gewählte Umsetzung des Abrufs über Google war daher unnötig und führt insoweit zu einer überflüssigen Offenlegung der IP-Adresse gegenüber Google. Der richtige Ansatz für die datenschutzrechtliche Bewertung dürfte die Annahme eines Verstoßes gegen die Pflicht zur datenschutzfreundlichen Technikgestaltung gem. Art. 25 Abs. 1 DS-GVO (privacy by design) durch das Unternehmen sein.³ Unter dem Gesichtspunkt der Datenminimierung gem. Art. 5 Abs. 1 lit. c) DS-GVO dürfte die technische Umsetzung ebenfalls zu beanstanden sein, weil die Datenverarbeitung nicht auf das unbedingt notwendige Maß reduziert war.⁴ Das Gericht hat zur Herleitung des Schadensersatzanspruchs darauf abgestellt, dass es an einer erforderlichen Einwilligung des Betroffenen in die Weitergabe der IP-Adresse an Google gefehlt habe und sich hierdurch ein Verstoß gegen das allgemeine Persönlichkeitsrecht ergeben würde.⁵ Weil die Einwilligung nur eine von mehreren möglichen Rechtsgrundlagen zur „Weitergabe“ der IP-Adresse ist, musste das Gericht außerdem herausarbeiten, dass die gewählte Gestaltung auch nicht unter dem Gesichtspunkt des berechtigten Interesses der verantwortlichen Stelle gem. Art. 6 Abs. 1 lit. f) DS-GVO gerechtfertigt werden konnte.⁶ Die Argumentation ist im Ergebnis richtig, wenn auch in den Entscheidungsgründen relativ oberflächlich wiedergegeben. Es gibt durchaus berechnete Interessen für die durch das Unternehmen gewählte Gestaltung, beispielsweise die einfachere Umsetzung durch einen Verweis auf die Server von Google. Es dürften allerdings auch insoweit die schutzwürdigen Interessen der Betroffenen überwiegen. Es hätte also richtigerweise in der Entscheidungsbegründung heißen müssen, dass das Vorliegen berechtigter Interessen dahinstehen kann, weil jedenfalls die schutzwürdigen Interessen der Betroffenen überwiegen. Im Rahmen der Interessenabwägung wären dann die Grundsätze von privacy by design und der Datenminimierung her-

anzuziehen gewesen; außerdem dürfte es maßgeblich darauf ankommen, dass ohne besonderen Mehraufwand relativ einfach eine andere technische Lösung bereitgestanden hätte.⁷

Wenn unter Berücksichtigung der vorstehenden Erwägungen von einem Datenschutzverstoß auszugehen ist, dann stellt sich zwangsläufig die Frage der möglichen Rechtsfolgen. Aus dem Deliktsrecht kann zunächst ein Unterlassungsanspruch hergeleitet werden, wenn von einem Eingriff in das allgemeine Persönlichkeitsrecht auszugehen ist, wozu grundsätzlich auch das Recht auf informationelle Selbstbestimmung gehört.⁸ Eigenständige Unterlassungsansprüche werden unmittelbar durch die datenschutzrechtlichen Bestimmungen nicht gewährt.⁹ Für einen zusätzlichen Anspruch auf Schadensersatz ergibt sich allerdings eine Anspruchskonkurrenz zwischen § 823 BGB und Art. 82 DS-GVO.¹⁰ Nach dem nationalen Schadensersatzrecht kommt es immer auf ein Verschulden an, außerdem ist ein Ersatz für immaterielle Schäden unter dem Gesichtspunkt des Schmerzensgeldes nur in sehr engen Grenzen denkbar.¹¹ Der datenschutzrechtliche Schadensersatzanspruch ist dagegen bewusst an geringere Voraussetzungen geknüpft und sieht ausdrücklich auch den Ersatz von immateriellen Schäden vor.¹² Das datenschutzrechtliche Konzept folgt danach dem politischen Willen, die Rechte der Betroffenen zu stärken und vermeintliche Defizite bei der Rechtsdurchsetzung zu

1 LG München, Urte. v. 20.01.2022 – 3 O 17493/20, GRUR-RS 2022, 612, Google Fonts.

2 Vgl. die Erläuterungen von Google unter <https://developers.google.com/fonts>.

3 Baumgartner/Gausling, ZD 2017, 308 (309).

4 Roßnagel, in: Simitis/Hornung/Spiecker, Art. 5 Rn. 121.

5 LG München, Urte. v. 20.01.2022 – 3 O 17493/20, GRUR-RS 2022, 612, Rn. 7.

6 Veil, NJW 2018, 3337 zur Abgrenzung zwischen Einwilligung und berechtigten Interesse; vgl. auch Frenzel, in: Paal/Pauly, Art. 6 Rn. 8.

7 Der Aufwand für die alternative Gestaltung von Datenverarbeitungsvorgängen kann dabei durchaus ein relevanter Faktor sein, wie sich auch aus Art. 32 DS-GVO ergibt, vgl. etwa Martini, in: Paal/Pauly, Art. 32 Rn. 60.

8 Rixecker, in: MüKo-BGB, Anhang zu § 12 Rn. 12 zur Abgrenzung zwischen dem Persönlichkeitsrecht und dem Datenschutzrecht.

9 Leibold/Laoutoumai, ZD-Aktuell 2021, 05583.

10 Frenzel, in: Paal/Pauly, Art. 82 Rn. 20.

11 Quaas, in: BeckOK Datenschutzrecht, Art. 82 Rn. Zur Ersatzfähigkeit immaterieller Schäden.

12 Buchner/Wessels, ZD 2022, 251 (253); Bergt, in: Kühling/Buchner, Art. 82 Rn. 2.

beseitigen. Vor diesem Hintergrund ist die Bestimmung zum Schadensersatz im Datenschutzrecht bewusst so ausgestaltet, dass alleine die Feststellung eines Datenschutzverstößes genügt, um gestützt hierauf einen immateriellen Schadensersatz verlangen zu können.¹³ Das Verschulden der verantwortlichen Stelle wird insoweit vermutet und es besteht über Art. 82 Abs. 3 DS-GVO lediglich eine Exkulpationsmöglichkeit für die verantwortliche Stelle.¹⁴ Bisher noch nicht geklärt ist allerdings die Frage, ob besondere Anforderungen an die Beeinträchtigung des Betroffenen zu stellen sind, bevor ein immaterieller Schadensersatz verlangt werden kann.¹⁵ Der Umgang mit Ansprüchen auf immateriellen Schadensersatz liegt im Rahmen mehrerer Vorlageverfahren beim EuGH, mit einer kurzfristigen Entscheidung und Klärung ist aber nicht zu rechnen.¹⁶

In dieser Situation hat das LG München entschieden, der Datenschutzverstoß und das von dem Betroffene empfundene individuelle Unwohlsein sei so erheblich, dass ein Schadensersatzanspruch gerechtfertigt sei.¹⁷ Zur Begründung wird unter anderem angeführt, dass die Daten ausgerechnet an Google übermittelt werden, also an einen US-Anbieter, der „bekanntermaßen Daten über seine Nutzer sammelt“ und seinen Hauptsitz in einem potentiell unsicheren Drittland hat.

II. Anspruchsschreiben von Trittbrettfahrern

Es ist natürlich wenig überraschend, dass nach Veröffentlichung der Entscheidung die Argumentation des Gerichts zur Herleitung des Schadensersatzanspruchs von interessierten Kreisen als Anleitung aufgefasst wurde, wie im eigenen Namen Schadensersatzzahlungen verlangt werden können. Auf diese Gefahr wurde früh hingewiesen, und sie hat sich schnell in Form von entsprechenden Aufforderungs- bzw. Abmahnschreiben realisiert.¹⁸ Es wurden dazu gezielt andere Unternehmen gesucht, die ebenfalls für ihre Homepages Google Fonts einsetzen, ohne diese auf den eigenen Servern vorzuhalten. Die Entscheidung des LG München wurde dabei verkürzt so interpretiert, dass ein „allgemeines Unwohlsein“ ausreichend wäre, um als eine Art Entschädigung eine Zahlung von 100,00 EUR zu verlangen. In einer ersten Welle haben sich Einzelpersonen mit vorformulierten Schreiben an eine Vielzahl von Unternehmen gewandt und darauf verwiesen, sie hätten bei Aufruf der jeweiligen Homepage „mit Erschrecken“ feststellen müssen, dass ohne erforderliche Zustimmung Webfonts direkt über Google geladen und hierdurch personenbezogene Daten an Google übermittelt würden, was bei dem Anspruchsteller ein allgemeines Unwohlsein ausgelöst hätte. Dieser Verstoß könnte jetzt nachträglich nur noch durch Zahlung einer Entschädigung kompensiert werden. In den meisten Schreiben dieser Art wurde relativ unverhohlen mit einer „offiziellen Beschwerde“ bei der Aufsichtsbehörde gedroht, wenn die Entschädigung nicht freiwillig gezahlt würde. In Einzelfällen wurde auch versucht, die Entscheidung des LG München in der Weise zu verallgemeinern, dass entweder generell das Nachladen von Schriften von externen Servern oder sogar

jegliche Einbindung von Drittanbieterinhalten ohne Zustimmung als Datenschutzverstoß anzusehen sei und Schadensersatzansprüche auslösen würde.

In einer zweiten Welle haben sich dann fast erwartungsgemäß Rechtsanwälte gefunden, die auf den Zug aufgesprungen sind und angeblich im Auftrag der jeweiligen Mandanten Datenschutzverstöße verfolgen sollen.¹⁹ In klassischer Abmahnmanier wurde dargestellt, dass die dynamische Einbindung der Webfonts einen Datenschutzverstoß darstelle und damit Unterlassungsansprüche auslösen würde, die nur durch Abgabe einer vorbereiteten Unterlassungsverpflichtungserklärung ausgeräumt werden könnten. Neben der Unterlassungserklärung wurde dann die Zahlung eines Schadensersatzbetrages und die Übernahme der angefallenen Rechtsanwaltskosten unter dem Gesichtspunkt der Geschäftsführung ohne Auftrag (GoA) verlangt.

III. Rechtliche Einordnung und Übertragbarkeit der Argumentation

Für die rechtliche Bewertung der von den Anspruchstellern selbst oder über Rechtsanwälte geltend gemachten Ansprüche ist zunächst als Ausgangspunkt festzuhalten, dass der eigentliche Datenschutzverstoß bei der dynamischen Einbindung der Schriftarten von Google nicht mit Aussicht auf Erfolg in Abrede gestellt werden kann. Für die Bewertung kommt es maßgeblich darauf an, dass – wie dargestellt – eine alternative Möglichkeit bestanden hätte, die identischen Schriften ohne das Nachladen über die Server von Google zu realisieren, wodurch dann die IP-Adresse nicht an Google übermittelt worden wäre. Soweit es also in der jeweiligen Auseinandersetzung um die dynamische Einbindung von Webfonts geht, sollte dieses Vorgehen nicht explizit gerechtfertigt werden.

Diese Wertung des konkreten Falls lässt sich aber nicht bzw. nur sehr eingeschränkt auf andere Konstellationen übertragen.²⁰ Selbst im Hinblick auf die Einbindung von Schriftarten anderer Anbieter wäre erst einmal zu prüfen, ob bezogen auf die zur Nutzung vorgesehenen Schriftarten überhaupt eine gleichwertige Möglichkeit zur Bereitstellung auf den eigenen Servern besteht. Die datenschutzrechtliche Unzulässigkeit der dynamischen Einbindung der Webfonts von Google beruht schließlich maßgeblich darauf, dass sie

13 Boehm, in: Simitis/Hornung/Spiecker, Art. 82 Rn. 10.

14 Moos/Schefzig, in: Taeger/Gabel, DS-GVO, 3. Aufl. 2019, Art. 82 Rn. 70.

15 BVerfG, Beschl. v. 14.01.2021 – 1 BvR 2853/19, ZD 2021, 266 zur Vorlagepflicht an den EuGH.

16 OGH Österreich, Beschl. v. 15.04.2021 – 6 Ob 35/21x, ZD 2021, 631; BAG, Beschl. v. 26.08.2021 – 8 AZR 253/20, ZD 2022, 56; LG Saarbrücken, Beschl. v. 22.11.2021 – 5 O 151/19, RDV 2022, 107.

17 LG München, Urte. v. 20.01.2022 – 3 O 17493/20, GRUR-RS 2022, 612 Rn. 12.

18 Skupin, GRUR-Prax 2022, 264.

19 Buchner/Wessels, ZD 2022, 251 (255) zu den Fehlanreizen zur Geltendmachung von Datenschutzverstößen.

20 Fischer, ZD 2022, 291 (292) spricht allerdings davon, dass Urteil sei „exemplarisch“.

von Google kostenfrei auch zur Installation auf den eigenen Servern freigegeben sind. Besteht diese Option bei anderen Anbietern nicht, kann nicht pauschal darauf verwiesen werden, dass diese Schriftarten dann nicht für die eigene Internetseite eingebunden werden dürfen. Der Seitenbetreiber ist in diesem Fall aber verpflichtet, für eine adäquate Absicherung der personenbezogenen Daten der Seitenbesucher zu sorgen. Ein „anonymes“ Nachladen von Inhalten kommt dabei nicht in Betracht, weil die IP-Adresse zumindest kurzzeitig für die korrekte Auslieferung der Inhalte an den Betroffenen technisch erforderlich ist.²¹ Aufgrund der Qualifikation von IP-Adressen als personenbezogene Daten führt damit die Einbindung von Drittanbieterinhalten immer zu einer Offenlegung der IP-Adresse der jeweiligen Seitenbesucher und damit zu einer Verarbeitung personenbezogener Daten.²² Der Seitenbetreiber kann sich aber absichern, indem er vorab den Seitenbesucher um eine Einwilligung bittet, wozu beispielsweise der ohnehin umfassend genutzte Cookie-Banner so gestaltet wird, dass er sich nicht nur auf den Einsatz von Cookies bezieht, sondern generell auf eingebundene Drittanbieterinhalte.²³ Ein solches Vorgehen ist datenschutzrechtlich durchaus denkbar, kann aber zu technischen Hürden führen. Es muss dann insbesondere sichergestellt werden, dass wirklich nur für solche Seitenbesucher Drittanbieterinhalte nachgeladen werden, die die vorgesehene Einwilligung erteilt haben. Für optionale Inhalte wie das Kartenmaterial von Google Maps oder Inhalte von Social Media-Anbietern wie Twitter mag dies ein gangbarer Weg sein.²⁴ In diesen Bereichen bestünde außerdem die Möglichkeit, direkt vor Aufruf der entsprechenden Inhalte den Seitenbesucher zu bitten, zuvor die Einbindung externer Inhalte zu aktivieren. Wenn es dagegen um Standardfunktionalitäten geht, sprechen die besseren Gründe dafür, dass hier keine ausdrückliche Einwilligung erforderlich ist, sondern der Seitenbetreiber sich auf berechnete Interessen berufen kann. Der Seitenbetreiber hat etwa ein Interesse daran, dass im Rahmen eines einheitlichen Corporate Designs seine Informationsangebote immer ähnlich aussehen und sich so ein Wiedererkennungseffekt einstellt, auch bezogen auf die genutzten Schriftarten. Für die datenschutzrechtliche Abwägung kommt es schließlich darauf an, ob schutzwürdige Interessen der Betroffenen überwiegen. Dass aber die Preisgabe der eigenen IP-Adresse so gravierend in geschützte Interessen des Betroffenen eingreift, erscheint sehr fragwürdig, da die Verwendung der IP-Adresse ohnehin zwingend zur Nutzung sämtlicher Internetinhalte erforderlich ist.

Es gibt auch keine allgemeine Wertung in der Form, dass Dienste von Google generell nicht eingesetzt werden dürfen, soweit hierdurch Inhalte von Google nachgeladen werden. Ein Großteil der Kritik gegenüber Google bezieht sich darauf, dass Google bzw. Alphabet als amerikanisches Unternehmen aufgrund der Gesetzeslage in den USA gar nicht effektiv den Schutz von personenbezogenen Daten sicherstellen kann, insbesondere nicht bezogen auf Informations- und Offenlegungspflichten gegenüber staatlichen Stellen. Dieses Risiko besteht tatsächlich, allerdings bezogen auf jedes amerikanische Unternehmen und kann von keinem entsprechenden Unternehmen in letzter Konsequenz ausge-

räumt werden.²⁵ Würde diese Argumentation, die teilweise auch von Aufsichtsbehörden geäußert wird, ernst genommen, dann müssten letztlich alle amerikanischen Anbieter ausgeschlossen werden.²⁶ Das Internet und die IT-Landschaft würde sich deutlich verändern, für die Betroffenen aber nicht unbedingt zum Guten. Die Marktmacht von Google und anderen IT-Unternehmen lässt sich sicherlich unter kartellrechtlichen Gesichtspunkten kritisch bewerten.²⁷ Zur Wahrheit gehört es aber auch, dass die Dienste von Google sich deshalb so großer Beliebtheit erfreuen, weil es regelmäßig kaum Alternativen gibt, die ähnlich einfach eingebunden werden können und ohne größere Kosten umsetzbar sind. Ein Dienst wie Google reCaptcha, der nach komplexen Algorithmen bei Anfragen zwischen menschlichen Seitenbesuchern und automatisierten Aufrufen durch Bots differenziert, lässt sich vermutlich kaum ohne Rückgriff auf die Server von Google realisieren.²⁸ Dennoch kann in solchen Fällen die Einbindung von Google angemessen sein, weil trotz Übermittlung der IP-Adresse das Schutzinteresse des Seitenbetreibers überwiegt.²⁹ Wie bei der Einbindung der Webfonts ist letztlich immer zu fragen, ob es eine gleichwertige Alternative gibt, die ohne die entsprechende Datenübermittlung auskommt.

IV. Fehlende Ansprüche Betroffener trotz eines Datenschutzverstößes

Die Einordnung eines Verhaltens als Datenschutzverstoß führt zunächst nur dazu, dass die verantwortliche Stelle den Verstoß abstellen muss, um sich wenigstens zukünftig rechtskonform und damit compliant zu verhalten. Diese Pflicht besteht natürlich unabhängig davon, ob die Aufsichtsbehörde oder ein Dritter das Thema aufgegriffen haben. Die Aufsichtsbehörden sollen im Rahmen ihrer jeweiligen Zuständigkeiten für eine Einhaltung der datenschutzrechtlichen Vorgaben sorgen, dürfen dabei aber im eigenen Ermessen entscheiden, ob und wie sie im Hinblick auf bestimmte Themen vorgehen.³⁰ Entgegen einer vereinzelt vertretenen Auffassung besteht keine ausschließliche Zuständigkeit der Aufsichtsbehörden zur Verfolgung von Datenschutzverstößen.³¹ Es dürfen demnach auch andere Or-

21 EuGH, Urte. v. 19.10.2016 – C-582/14, MMR 2016, 842, Breyer.

22 EuGH, Urte. v. 19.10.2016 – C-582/14, MMR 2016, 842, Breyer; vgl. dazu auch Ernst, in: Paal/Pauly, Art. 4 Rn. 11; Schmitz, in: Hoeren/Sieber, Teil 16.2 Rn. 64.

23 Haberer, MMR 2020, 810 (815) spricht insoweit von einem „Datenschutz-Banner“.

24 Engeler, ZD 2018, 55 (61).

25 VG Wiesbaden, Beschl. v. 01.12.2021 – 6 L 738/21, ZD 2022, 177.

26 DSB Österreich, Bescheid v. 22.12.2021 – D155.027, 2021-0.586.257, ZD 2022, 215.

27 Meye/Rempe, K&R 2022, 247 (248).

28 Conrad/Hausen, in: Auer-Reinsdorff/Conrad, § 36 Rn 232; vgl. auch AG Nürnberg, Urte. v. 30.06.2017 – 22 C 237/17, BeckRS 2017, 140318 Rn. 28.

29 Conrad/Hausen; in: Auer-Reinsdorff/Conrad, § 36 Rn 233 gehen ebenfalls von einem berechtigten Interesse aus.

30 VG Wiesbaden, Beschl. v. 31.08.2021 – 6 K 226/21, NZI 2022, 527 zum Ermessenspielraum der Aufsichtsbehörden; das Verfahren ist beim EuGH anhängig unter dem Aktenzeichen C-552/21; vgl. ebenfalls dazu VG Wiesbaden, Beschl. v. 10.12.2021 – 1107/21, ZD 2022, 352.

31 Werkmeister, in: Gola, Art. 80 Rn. 17.

ganisationen und Einrichtungen Datenschutzverstöße aufgreifen und gegen sie vorgehen, insbesondere die Verbraucherverbände im Rahmen ihrer Befugnisse nach dem UKlaG.³² Für die Betroffenen sind sogar ausdrücklich umfassende Betroffenenrechte und der Anspruch auf Schadensersatz vorgesehen. Die verantwortliche Stelle muss also grundsätzlich damit leben, dass von interessierte Seite direkt vorgegangen werden kann, selbst wenn die Aufsichtsbehörde untätig bleibt. Bezogen auf die Verbraucherverbände ergibt sich ein Korrektiv durch die Notwendigkeit zur Berücksichtigung als klagebefugte Organisation und Einrichtung; für Betroffene und Wettbewerber gibt es kein vergleichbares Korrektiv.³³ Hieraus ergibt sich das Risiko, dass der Versuch unternommen werden kann, mit vorgeschobenen datenschutzrechtlichen Ansprüchen primär andere Ziele zu verfolgen und damit letztlich die datenschutzrechtlichen Möglichkeiten zu missbrauchen.³⁴ Für Betroffene kann es dabei darum gehen, ihre Verärgerung über das Unternehmen zum Ausdruck zu bringen. Ein typisches Szenario war es insoweit schon in der Vergangenheit, dass ohne echtes Interesse an den gespeicherten Daten Auskunftsansprüche geltend gemacht werden. Bezogen auf den datenschutzrechtlichen Schadensersatzanspruch kommt natürlich vor allem der Versuch in Betracht, Zahlungen von der verantwortlichen Stelle zu erhalten, um hierdurch letztlich sogar von einem Verstoß noch zu profitieren. Selbst ohne ausdrückliche Regelung im datenschutzrechtlichen Kontext können und müssen derartige Aspekte unter dem Gesichtspunkt des Rechtsmissbrauchs berücksichtigt werden.³⁵

V. Unterlassung

Hinsichtlich möglicher Unterlassungsansprüche einzelner Betroffener kann zunächst der Versuch unternommen werden, von einem abschließenden Charakter des datenschutzrechtlichen Sanktionssystems auszugehen, der einem Rückgriff auf § 1004 BGB entgegenstehen könnte.³⁶ Argumentativer Ansatz hierfür ist die Regelung in Art. 79 Abs. 1 DS-GVO, die nicht generell Rechtsschutzmöglichkeiten außerhalb der DS-GVO zulassen soll. Diese Sichtweise ist allerdings umstritten und dürfte sich nur schwer mit dem generellen Grundsatz vereinbaren lassen, dass die DS-GVO für einen effektiven Schutz der Betroffenen sorgen und diesen nicht verhindern soll.³⁷ Selbst wenn aber generell Unterlassungsansprüche bestehen können, gilt im Hinblick auf solche Ansprüche der „das gesamte Rechtsleben durchziehende Grundsatz“, dass die Ausübung eines Rechts nicht erlaubt ist, wenn eine formale Rechtsstellung ausgenutzt wird, ohne dass ein schützenswertes Eigeninteresse besteht.³⁸

Indizien für ein rechtsmissbräuchliches Verhalten ist es etwa, wenn zwischen dem Betroffenen und dem Verantwortlichen keinerlei vorangehende Beziehung besteht.³⁹ Die Geltendmachung gleichartiger Unterlassungsansprüche gegen eine Vielzahl von Anspruchsgegnern deutet ebenfalls auf ein missbräuchliches Verhalten hin.⁴⁰ Einher geht damit häufig eine Gestaltung, wonach bei anwaltlicher Vertretung nicht einmal eine Vollmacht für den konkreten Einzelfall be-

steht, sondern mit einer Blankovollmacht gearbeitet wird. Für den Rechtsmissbrauch spricht ferner die Tatsache, dass eine umfangreiche Ausarbeitung zu der vermeintlichen Rechtsverletzung erfolgt, die in keinem Verhältnis zu dem gerügten Verstoß besteht.

Bezogen auf die Einbindung der Webfonts von Google treffen alle Indizien für die Aufforderungsschreiben der Betroffenen zu. Die Schreiben enthalten umfangreiche Ausführungen zur Rechtslage, warum das Nachladen von Webfonts direkt bei Google unzulässig ist und was das LG München hierzu ausgeführt hat. Zum Nachweis des Rechtsverstoßes werden zumeist noch Screenshots beigefügt, durch die der Sachverhalt gerichtsverwertbar dokumentiert würde. Angesichts dieses Vorgehens drängt sich die Frage auf, wer sich unter normalen Umständen diese Mühe macht. Erschwerend kommt die Tatsache hinzu, dass die Einbindung von Dritthalten wie Webfonts nicht im Rahmen der typischen Nutzung einer Internetseite auffällt. Der Seitenbesucher muss sich also entweder den Quelltext der Seite ansehen oder hierfür entsprechende Tools verwenden. Es kann daher ausgeschlossen werden, dass – wie durch viele Aufforderungsschreiben suggeriert wird – die angegriffene Gestaltung zufällig bemerkt wurde.

Es liegt daher auf der Hand, dass sich einzelne Betroffene ganz gezielt auf die Suche nach Datenschutzverstößen begeben haben. Grundsätzlich ist es dabei nicht zu kritisieren, wenn Betroffene sich nicht mit ihrem Anliegen an den Datenschutzbeauftragten der verantwortlichen Stelle wenden oder die Aufsichtsbehörde selbst informieren, sondern die Angelegenheit selbst in die Hand nehmen. Es stellt sich nur die Frage, was der Betroffene mit seinem Vorgehen erreichen will und überhaupt erreichen kann. Die bei dem erstmaligen Seitenaufruf erfolgte Übermittlung von Daten kann nachträglich ohnehin nicht mehr beseitigt werden. Es ist insbesondere nicht möglich, die Daten von Google „zurückzuholen“. Für die Zukunft hat es der Betroffene aber selbst in der Hand, eine weitere vermeintliche Beeinträchtigung seiner Rechtsposition zu vermeiden, indem die Internetseite nicht mehr aufgerufen wird.

Wird der Betroffene dagegen in der Form tätig, dass er in einem großen Umfang gleichgelagerte Verstöße geltend

32 EuGH, Ur. v. 29.07.2019 – C-40/17 – Fashion ID; EuGH, Ur. v. 28.04.2022 – C-319/20, ZD 2022, 384.

33 Ohly, GRUR 2022, 924 (924) weist zutreffend darauf hin, dass es sich für den EuGH angeboten hätte, auch die Frage der Klagebefugnis von Wettbewerbern ebenfalls zu beantworten.

34 OLG Hamm, Beschl. v. 15.11.2021 – 20 U 269/21, ZD 2022, 237 und LG Wuppertal, Ur. v. 29.07.2021 – 4 O 409/20, ZD 2022, 53 für Beispiele aus der Rechtsprechung.

35 Lembke, NJW 2020, 1841 (1845).

36 LG Wiesbaden, Ur. 20.01.2022 – 10 O 14/21, ZD 2022, 238; VG Regensburg, Bescheid v. 06.08.2020 – RN 9 K 19.1061, ZD 2020, 601.

37 VG Wiesbaden, Beschl. v. 01.12.2021 – 6 L 738/21, ZD 2022, 177; ebenso Martini, in: Paal/Pauly, Art. 79 Rn. 20.

38 LG Wuppertal, Ur. v. 29.07.2021 – 4 O 409/20, ZD 2022, 53.

39 Knippenkötter, GRUR-Prax 2011, 483, listet insgesamt zahlreiche Indizien für eine Bewertung im Wettbewerbsrecht auf; vgl. zur Darlegung im Verfahren auch Barbasch, GRUR-Prax 2011, 486.

40 LG Dessau-Roßlau, Ur. v. 01.12.2012 – 3 O 87/11, wonach hierfür 37 Abmahnungen in drei Monaten ausreichend sind; ähnlich LG Hamburg, Ur. v. 07.02.2017 – 312 O 144/16 für 42 Abmahnungen in einem Jahr.

macht, die einfach zu finden sind, spricht dies für sich genommen schon für ein rechtsmissbräuchliches Verhalten.⁴¹ Es liegt dabei in der Natur der Sache, dass die in Anspruch genommene Stelle nur Indizien für einen Rechtsmissbrauch vortragen kann. Bei einer hinreichend substantiierten Darlegung der Indizien muss dann aber der Anspruchsteller diese Vorwürfe entkräften.

VI. Schadensersatz

Trotz der fehlenden Klärung diverser Vorlagefragen durch den EuGH ist auch jetzt schon bezogen auf die Schadensersatzansprüche klar, dass ein Anspruch auf immateriellen Schadensersatz zwingend immer einen Schaden voraussetzt. Der Schadensersatzbegriff mag weit auszulegen sein und explizit immaterielle Schäden umfassen, es muss aber immer ein konkreter Schaden festgestellt werden, der durch die Datenschutzverletzung verursacht wurde.⁴² Für die Geltendmachung eines Anspruchs kann also bei richtiger Interpretation alleine der Verweis auf den Datenschutzverstoß nicht genügen.⁴³

Wenn es aber dem Betroffenen darum geht, die Datenschutzverletzung dafür zu nutzen, um einen Schadensersatzanspruch geltend zu machen, dann darf hierin kein ersatzfähiger Schaden gesehen werden. Es liegt praktisch ein Fall bewusster Selbstschädigung vor, weil es der Betroffene gerade darauf anlegt, einen Schaden zu erleiden, um diesen dann zum Anlass zu nehmen, immateriellen Schadensersatz zu fordern.

Ein kausal verursachter Schaden dürfte übrigens auch dann nicht vorliegen, wenn durch das Nachladen der Schriftarten überhaupt keine zusätzlichen Informationen des Betroffenen preisgegeben werden. Hat der Betroffene beispielsweise zuvor selbst die Suchmaschine von Google benutzt, wäre die IP-Adresse aufgrund der Suchanfrage bei Google ohnehin schon bekannt. Das Nachladen der Schriftarten würde in diesem Fall überhaupt keinen (weiteren) Schaden anrichten. Wenn der Betroffene die Seiten der verantwortlichen Stelle direkt über einen Link in den Suchergebnissen aufruft, wüsste Google sogar schon, dass sich der Betroffene für das Angebot der verantwortlichen Stelle interessiert. Die Bewertung muss auch gelten, wenn die verantwortliche Stelle für ihr Online-Angebot auch weitere Dienste von Google nutzt, die einen Abruf von Daten über die Server von Google erfordern. In diesen Fällen führt die zusätzliche Einbindung von Webfonts ebenfalls nicht zu einem Schaden, da die Daten dort ohnehin schon vorliegen. Es bliebe zwar der formale Datenschutzverstoß bezogen auf Webfonts bestehen, ein hierdurch kausal verursachter Schaden ist aber ausgeschlossen.

VII. Übernahme von Abmahnkosten

Soweit von dem Betroffenen ein Rechtsanwalt mit der Vertretung seiner Interessen beauftragt wurde, verlangt dieser typischerweise die Übernahme der Kosten der anwaltlichen Mandatierung von dem Anspruchsgegner.⁴⁴ Diese Kosten sind nicht unmittelbar durch die Datenschutzverletzung entstanden, sondern beruhen auf einem eigenständigen Verhalten des Betroffenen. Es hätte ihm freigestanden, die

Ansprüche auch selbst geltend zu machen. Gleichwohl wären die Kosten natürlich nicht entstanden, wenn die verantwortliche Stelle nicht die Ursache für die Mandatierung durch den Datenschutzverstoß gesetzt hätte. In der Konsequenz sind diese Kosten als Schadensposition an sich erstattungsfähig, wenn sie erforderlich waren oder für erforderlich gehalten werden durften.⁴⁵ Vor diesem Hintergrund ist es nicht prinzipiell zu beanstanden, dass die Geltendmachung eines Schadensersatzanspruchs in Höhe von 100,00 EUR Gebühren für die anwaltliche Vertretung in ungefähr gleicher Höhe verursacht.

Es erscheint aber wenig überzeugend, dass ein Betroffener ohne materiellen Schaden zunächst auf eigene Kosten einen Rechtsanwalt beauftragt, damit dieser für ihn einen immateriellen Schadensersatz in Höhe von 100,00 EUR geltend macht. Wenn aber der mandatierte Rechtsanwalt direkt mit seinem Aufforderungsschreiben die Freistellung des Mandanten von den Kosten verlangt, dann beinhaltet dies implizit die Erklärung, dass diese Kosten auch wirklich angefallen sind. Es ist natürlich unzulässig, die Zahlung von Kosten durch den Anspruchsgegner zu verlangen, die so gar nicht angefallen sind. Dies gilt auch für berufsrechtlich fragwürdige Absprachen, wonach der Rechtsanwalt keine Gebühren abrechnet, wenn diese nicht von der Gegenseite übernommen werden. Selbst nach den letzten berufsrechtlichen Lockerungen sind Erfolgshonorare vom Grundsatz gem. § 49b Abs. 2 BRAO weiterhin unzulässig.⁴⁶ Über § 4a RVG gibt es zwar eine Öffnungsklausel, die in der Vergangenheit darauf abstellte, ob der Mandant ohne die Vereinbarung eines Erfolgshonorars ansonsten aufgrund seiner wirtschaftlichen Verhältnisse von der Rechtsverfolgung abgehalten worden wäre.⁴⁷ Selbst nach der Neuregelung mit einer Öffnung für Geldforderungen bis 2.000 Euro fällt die Geltendmachung des immateriellen Schadensersatzes nicht hierunter, wenn zugleich auch Unterlassungsansprüche geltend gemacht werden.⁴⁸ Formal dürften aber üblicherweise die Unterlassungsansprüche ebenfalls verfolgt werden, weil ansonsten die alleinige Verfolgung der Zahlungsansprüche wiederum ein Indiz für den Rechtsmissbrauch wäre.⁴⁹

In strafrechtlicher Hinsicht kann ein versuchter Betrug vorliegen, wenn der Anspruchsgegner unter Vortäuschung des Anfalls entsprechender Kosten zu einer Zahlung bewegt werden sollte, soweit solche tatsächlich angefallen sind.⁵⁰

41 OLG Hamburg, Urf. v. 11.08.2016 – 3 U 56/15 zum Rechtsmissbrauch bei Massenabmahnungen.

42 Boehm, in: Simitis/Hornung/Spiecker, Art. 82 Rn. 11 zum Schadensbegriff unter Verweis auf ErWG 146; vgl. auch Buchner/Wessels, ZD 2022, 251 zur bisherigen Handhabung.

43 Wybitul/Leibold, ZD 2022, 207 (211).

44 OLG Frankfurt, Urf. v. 14.04.2022 – 3 U 21/20, BKR 2022, 534.

45 Domisch/Scharnetzki, VersR 2022, 411 (414) zur generellen Erstattungsfähigkeit von Anwaltskosten im Schadensrecht.

46 Brüggemann, in: Weyland, BRAO, § 49b Rn. 18.

47 Winkler/Teubel, in: Mayer/Kroiß, RVG, § 4a Rn. 27.

48 Rucker/Bell, NJOZ 2022, 545 zur Neuregelung seit dem 01.10.2021.

49 OLG Hamm, Urf. v. 01.04.2008 – 4 U 10/08; dazu Knippenkötter, GRUR-Prax 2011, 483 (484).

50 Perron, in: Schönke/Schröder, StGB, § 263 Rn. 51 zum Prozessbetrug bei gerichtlicher Geltendmachung.

51 Träger, in: Weyland, BRAO, § 43a Rn. 38.

Für den Rechtsanwalt stellt sich nicht nur die Frage der Beteiligung an der Straftat des Mandanten, sondern es ergibt sich auch ein Konflikt mit der Wahrheitspflicht gem. § 43a Abs. 3 BRAO.⁵¹ Der Rechtsanwalt ist an den Gebührenabsprachen im Innenverhältnis mit seinem Mandanten unmittelbar beteiligt und muss daher die Unrichtigkeit und die sich daraus abgeleiteten Konsequenzen erkennen. Tritt ein Rechtsanwalt in größerem Umfang für einen Betroffenen auf, so erscheint es erst recht unwahrscheinlich, dass der Betroffene wirklich bereit ist, in erheblichem Umfang die Kosten seines Rechtsanwaltes für jeden einzelnen Fall zu übernehmen, wenn allenfalls gelegentlich eine Zahlung einer verantwortlichen Stelle erreicht werden kann. Indizien für ein entsprechendes Vorgehen sind pauschale Vollmachten ohne Nennung des Anspruchsgegners und die eigenständige Dokumentation der vermeintlichen Rechtsverletzungen direkt durch den Rechtsanwalt.

Es stellt sich alleine die Frage der Beweisbarkeit entsprechender Absprachen, da die verantwortliche Stelle sich keine sichere Kenntnis darüber verschaffen kann, was der Betroffene und sein Rechtsanwalt vereinbart haben.⁵² In seltenen Fällen ergeben sich bereits Anhaltspunkte durch eine ungeschickte Einlassung des Anspruchstellers, in anderen Fällen muss, wie allgemein beim Rechtsmissbrauch, mit Indizien gearbeitet werden.⁵³

Fazit

Die Nutzung der Schriftarten von Google ist datenschutzkonform nur in der Weise möglich, dass eine Installation auf den eigenen Servern erfolgt, wodurch bei Seitenaufruf keine Offenlegung der IP-Adresse gegenüber Google

erfolgt. Soweit die Schriften dagegen dynamisch nachgeladen werden, ergeben sich aus dem Datenschutzverstoß der verantwortlichen Stelle nicht zwangsläufig rechtliche Ansprüche des Betroffenen. Ein eigenständiger Unterlassungsanspruch ist jedenfalls in der DS-GVO nicht vorgesehen; ein immaterieller Schadensersatzanspruch käme zwar grundsätzlich in Betracht, scheidet im konkreten Fall aber an einem kausal verursachten Schaden. Das gezielte Suchen nach derartigen Rechtsverletzungen kann nämlich nicht zugleich zu einer solchen Beeinträchtigung eigener Rechtspositionen führen, die wiederum einen Schadensersatzanspruch nach sich zieht. Dem Anspruchsteller kann außerdem der Einwand des Rechtsmissbrauchs entgegengehalten werden, wenn die datenschutzrechtlichen Betroffenenrechte als Möglichkeit für einen Nebenverdienst missbraucht werden.



Dr. Sebastian Meyer

ist Rechtsanwalt im Bielefelder Büro der Kanzlei Brandi Rechtsanwälte; er ist zugleich Fachanwalt für IT-Recht, Notar sowie Lehrbeauftragter an der Universität Bielefeld, Fachhochschule Bielefeld und Fernuni Hagen.

52 LG München I, Urt. v. 22.12.2014 – 4 HKO 8107/14 zur Frage der Beweispflicht hinsichtlich der im Innenverhältnis getroffenen Absprachen.

53 Knippenkötter, GRUR-Prax 2011, 483 (484).

Prof. Peter Gola

Mitarbeitervertretungen und Datenschutzbeauftragte als „Gewährleister“ des Datenschutzes der Beschäftigten

Datenschutzbeauftragte und die Mitarbeitervertretungen haben bezogen auf den Beschäftigtendatenschutz parallel laufende Aufgaben, die die Pflicht zur Kooperation quasi vorgeben, ohne auf die Neuregelungen in § 79a BetrVG bzw. § 68 BPersVG zurückgreifen zu müssen. Beiden ist die Überwachung der datenschutzkonformen Verarbeitung der Daten des Kollektivs der Beschäftigten übertragen und zugleich die Pflicht, sich Datenschutzanliegen von Beschäftigten, die sich an die wenden, anzunehmen und ggf. um Abhilfe zu sorgen. Das gilt, wenn Beschäftigte generell auf DS-GVO-widrige Verarbeitungen hinweisen, aber auch,

wenn sie um Unterstützung in einem sie persönlich betreffenden Fall nachsuchen. Insoweit stellt sich dann aber auch die Frage, ob der vom Gesetzgeber etablierte „Doppelschutz“ der Beschäftigten dadurch unzulässig minimiert wird, wenn der Datenschutzbeauftragte zugleich Mitglied der Mitarbeitervertretung oder sogar deren Vorsitzender wäre. Wenngleich dies wohl nicht praktisch geworden ist, ist gleichwohl letztlich zu erörtern, ob Mitarbeitervertretung oder Datenschutzbeauftragte, wenn sie ihrem Schutzauftrag nicht nachkommen, von Beschäftigten haftbar gemacht werden können.

I. Einleitung

1. Die parallel laufenden Aufgabenstellungen

a) Allgemeines

Im Rahmen ihres Schutzauftrag haben Datenschutzbeauftragte und Betriebs-/Personalräte¹ einerseits Kontroll- und Schutzfunktionen bezüglich der mitarbeiterbezogenen Datenverarbeitungen des Arbeitgebers; andererseits wirken bzw. – bei der Mitarbeitervertretung – bestimmen sie mit, ob und für welche Zwecke Beschäftigtendaten verarbeitet werden sollen.²

Zudem obliegt dem Datenschutzbeauftragten und der Mitarbeitervertretung die Pflicht, Beschäftigten in Datenschutzbelangen gegenüber dem Arbeitgeber mit Rat und Unterstützung zur Seite zu stehen. (§ 80 Abs. 2 Ziff. 3 BetrVG, § 62 Nr. 3 BPersVG; § 38 Abs.4 DS-GVO).

Beiden obliegt also nicht nur ein das Kollektiv der Arbeitnehmerschaft betreffender gesetzlicher Schutzauftrag. Sie sind auch verpflichtet, – berechtigtem – individuellen Schutzbedarf einzelner Beschäftigter zu genügen.

Zur Einhaltung von Datenschutznormen sind aber auch Mitarbeitervertretung und Datenschutzbeauftragter selbst bezüglich ihrer Datenverarbeitungen angehalten.³ Für beide gilt nach wie vor das Datengeheimnis, wenngleich es in der DS-GVO nicht mehr ausdrücklich normiert ist, weil die vormalige Regelung in § 5 BDSG a.F. entfallen ist.⁴ Vorrangig verpflichtet § 79 Abs. 1 BetrVG die Mitglieder des Betriebsrats, über Geschäfts- und Betriebsgeheimnisse Verschwiegenheit zu wahren. Auch das GeschGehG ist zu beachten.⁵

Die Folge ist, dass Beweismittel, die ein Betriebsrat unter Verstoß gegen Datenschutzrecht erlangt hat, nicht verwertbar sind⁶ oder Betriebsratsmitglieder, die wiederholt datenschutzrechtswidrig in elektronische Personalakten Einsicht nehmen, aus dem Betriebsrat ausgeschlossen werden können.⁷

Eine Regelung eines permanenten und uneingeschränkten Einsichtsrechts in die elektronisch geführten Personalakten der Arbeitnehmer für den Betriebsratsvorsitzenden ist wegen Verstoßes gegen § 75 Abs. 2 BetrVG unwirksam.

Denn mit einer solchen Regelung wird unverhältnismäßig und damit unzulässig in die Persönlichkeitsrechte der betroffenen Arbeitnehmer eingegriffen.⁸ Der Betriebsrat hat auch kein uneingeschränktes Recht zur Weitergabe elektronisch erfasster, namensbezogener Arbeitszeiten an die Aufsichtsbehörde.⁹ Aus Gründen des Datenschutzes muss er vielmehr im Einzelfall die Erforderlichkeit der Datenweitergabe prüfen und hierbei die Interessen der betroffenen Arbeitnehmer berücksichtigen.¹⁰

Die gleiche Einschränkung gilt für den Datenschutzbeauftragten, bevor er ggf. im Konfliktfall die Aufsichtsbehörde kontaktiert.

b) Kooperation

Bei der Gewährleistung des Beschäftigtendatenschutzes besteht für die Mitarbeitervertretung und den Datenschutzbeauftragten nicht nur grundsätzlich wegen der gemeinsamen Schutzfunktion, sondern auch gemäß gesetzlicher Regelung das Recht und grundsätzlich auch die Pflicht zur Zusammenar-

1 Brink/Joos, Datenschutzrechtliche Verantwortlichkeit der betrieblichen und behördlichen Beschäftigtenvertretungen, NZA 2019, 1395; Hoynningen-Huene, von, Datenüberwachung durch Betriebsrat und Datenschutzbeauftragten, NZA-Beilage 1/1985, 19; Schierbaum, Betriebliche Datenschutzbeauftragte und Betriebsrat. Die zwei Akteure des arbeitnehmer-Datenschutzes, AiB 2001, 512; Wagner, Betriebsrat und betrieblicher Datenschutzbeauftragter. Wer kontrolliert wen? BB 1993, 1729.

2 Vgl. Pötters/Hansen, Datenschutzanforderungen an die Betriebsratsarbeit, bRAktuell 2020, 193; Staben, Die Datenschutzverantwortlichkeit des Betriebsrats, ZfA 2020, 287; Stück, Betriebsrat oder Geheimrat? Beschäftigtendatenschutz beim Betriebsrat, ZD 2019, 256.

3 Vgl. bereits ABmus, Kontrolle des Betriebsrats durch den betrieblichen Datenschutzbeauftragten?; ZD 2011, 27; Kranig/Wybitul/Zimmer-Helfrich, Sind Betriebsräte für den Datenschutz selbst verantwortlich?, ZD 2019, 1.

4 Gola, Handbuch Beschäftigtendatenschutz, Rn. 2563 f.

5 Gola, Recht der Personalgewinnung, S. 155 ff.

6 LAG Berlin-Brandenburg, Beschl. v. 15.05.2014 – 18 TaBV 828/12.

7 LAG Berlin-Brandenburg, Beschl. v. 12.11.2012 – 17 TaBV 1318/12.

8 LAG Düsseldorf, Beschl. v. 23.06.2020 – 3 TaBV 65/19S.

9 BAG, Urt. v. 03.06.2003 – 1 ABR 19/02.

10 Kort, Das Dreiecksverhältnis von Betriebsrat, betrieblichen Datenschutzbeauftragten und Aufsichtsbehörde beim Arbeitnehmerdatenschutz, NZA 2015, 1345.

beit.¹¹ Dies ergibt sich aktuell aus dem in § 79a BetrVG bzw. § 68 BPersVG zum Ausdruck gekommenen Grundgedanken.¹²

Ferner kann für den DSB Art. 39 Abs. 1 lit. a DS-GVO herangezogen werden. Danach hat der DSB den Verantwortlichen zu unterrichten und zu beraten. Die Beratung und Unterstützung umfasst die dem Verantwortlichen zugeordnete Stellen und damit nach der Regelung des § 79a BetrVG/§ 68 BPersVG eindeutig auch die Mitarbeitervertretung.¹³

Zu verweisen ist auch darauf, dass der Betriebsrat den Datenschutzbeauftragten als Sachverständigen in Datenschutzfragen in Anspruch nehmen kann bzw. muss.¹⁴ Das kann zum einem auf der Basis der § 40 BetrVG, § 44 BPersVG geschehen. Der Beauftragte kann aber auch außerhalb der Funktion als sachverständiger Arbeitnehmer im Rahmen seines Sicherstellungsauftrags und als "Anwalt der Betroffenen" gemäß Art. 38 Abs. 4 DS-GVO die Beratung auch ohne Weisung oder Genehmigung des Arbeitgebers wahrnehmen.

c) Unterschiedliche Blickwinkel

Hingewiesen wird darauf, dass der Datenschutzbeauftragte bei der Bewertung von Personaldatenverarbeitungen die Interessen von Arbeitgeber und Beschäftigten gleichermaßen berücksichtigen müsse,¹⁵ während der Betriebsrat zwar Unternehmensinteressen nicht vollständig außer Acht lassen dürfe, seine Tätigkeit aber primär an den Belangen der Belegschaft auszurichten habe.¹⁶ Diese Unterscheidung in der Interessengewichtung kann aber nur zu unterschiedlichen Ergebnissen führen, wenn der Arbeitgeber bei einer Maßnahme einen Handlungsspielraum hat. Ist eine Verarbeitung von Mitarbeiterdaten unzulässig, kann der Handlungsauftrag für die Mitarbeitervertretung und den DSB nur identisch sein. Sie haben im Rahmen ihrer Möglichkeiten auf das Ende der Verarbeitungen hinzuwirken, wozu auch die beiderseitige Information und das Nachsuchen um Unterstützung gehören kann.

d) Kollektiv- und individualbezogene Aufgaben

Beiden obliegen einerseits Kontroll- und Schutzfunktionen bezüglich der mitarbeiterbezogenen Datenverarbeitungen des Arbeitgebers; andererseits wirken sie beratend (für den DSB: Art. 38 Abs. 1 DS-GVO) bzw. – im Falle bei der Mitarbeitervertretung – bestimmend (z.B. bei automatisierter Personaldatenverarbeitung § 87 Abs. 2 Nr. 6 BetrVG; § 80 Abs 1 Nr. 21 BPersVG) dabei mit, ob und für welche Zwecke Beschäftigtendaten verarbeitet werden sollen.¹⁷

Sie haben aber nicht nur diesen das Kollektiv der Arbeitnehmerschaft betreffenden gesetzlichen Schutzauftrag. Vielmehr obliegt es beiden auch individuellen Beschäftigtenschutz zu gewährleisten, indem sie Beschäftigten in Datenschutzbelangen gegenüber dem Arbeitgeber mit Rat und Unterstützung zur Seite zu stehen haben. Dies gilt zum einem, wenn sich ein Beschäftigter an sie wendet (§ 80 Abs 1 Nr. 4 BetrVG; § 62 Nr. 3 BPersVG, Art. 38 Abs. 4 DS-GVO), und zum anderen auch „von Amtswegen“, wenn sie einen einzel-fallbezogenen datenschutzrelevanten Eingriff feststellen.

Zumindest in den letztgenannten Fällen sind sie trotz der gesetzlich verfügten datenschutzrechtlichen Einordnung in

den Betrieb/die Behörde „de facto“ im konkreten Fall auch eine datenverarbeitende Stelle, da sie hier ggf. zur gebotenen vertraulichen Wahrnehmung ihrer Aufgaben auch Beschäftigtendaten in eigener Regie und außerhalb der Kenntnisnahme durch den Arbeitgeber verarbeiten.

2. Informationsrechte und datenschutzrechtliche Grenzen

a) Allgemeines

Bei der Wahrnehmung ihrer Schutzfunktion bestehen für Datenschutzbeauftragte und Mitarbeitervertretungen einerseits spezielle Informationsrechte und andererseits aber auch datenschutzrechtliche Grenzen.

b) Die Mitarbeitervertretung

Arbeitnehmerdatenschutz wird zunächst durch § 75 BetrVG zur Aufgabe des Betriebsrats,¹⁸ § 75 Abs. 1 BetrVG verbietet die Diskriminierung wegen dort aufgelisteter Merkmale, woraus nach § 26 Abs. 1 S. 1 BDSG das Verbot der Verarbeitung diesbezüglicher Daten folgt. Des Weiteren verpflichtet die Norm die Betriebsparteien in Absatz 2 zur aktiven Gewährleistung des Persönlichkeitsschutzes der Beschäftigten.¹⁹ Die Schutzpflicht verlangt insbesondere Regelungen des Arbeitnehmerdatenschutzes und zudem Handlungen, die mit der DS-GVO bzw. dem BDSG kollidieren, zu unterlassen oder zu unterbinden, wobei sich hieraus jedoch kein Mitbestimmungsrecht ableiten lässt.²⁰

Effektiver für den Schutzauftrag ist § 80 Abs. 1 Nr. 1 BetrVG. Hiernach obliegt es dem Betriebsrat, die Einhaltung der zu Gunsten der Arbeitnehmer geltenden Gesetze durch den Arbeitgeber zu überwachen. § 68 Abs. 2 BPersVG und die Personalvertretungsgesetze der Länder enthalten gleiche Regelungen. Die dort statuierte Verpflichtung der Mitarbeitervertretungen, auf die Einhaltung der dem Schutz der Mitarbeiter dienenden Gesetze zu achten, umfasst gewichtig auch alle Regelungen des Beschäftigtendatenschutzes.²¹

11 Vgl. bereits Iraschko-Luscher, Zusammenarbeit des Datenschutzbeauftragten mit dem Betriebsrat, IT-Sicherheit und Datenschutz, 2007, 696

12 Kiesche, Kooperieren beim Datenschutz, AiB Extra, August 2022, 24, Flink, Beschäftigtenschutz als Aufgabe des Betriebsrats, S. 279.

13 Heberlein, in: Ehmann/Selmayr, 2. Aufl., DS-GVO Art. 39 Rn. 9; Flink, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, S. 279

14 Gola, Handbuch Beschäftigtendatenschutz, 8. Aufl., Rn. 2236 ff.

15 Kort, Was ändert sich für Datenschutzbeauftragte, Aufsichtsbehörden und Betriebsrat mit der DS-GVO?, ZD 2017, 3; Kurzböck/Weinbeck, DS-GVO-Verstöße im Betriebsratsbüro – wer haftet?, BB 2018, 1652; Lücke, Die Betriebsverfassung in Zeiten der DS-GVO: „Bermuda-Dreieck“ zwischen Arbeitgeber, Betriebsräten und Datenschutzbeauftragten! NZA 2019, 658.

16 St. Rechtspr. BAG, Urt. v. 28.05.2014 – 7 ABR36/12; Fitting, BetrVG, 31. Aufl., 2022, § 2 Rn. 6.

17 Vgl. Kurzböck/Weinbeck, Die datenschutzrechtliche Verantwortlichkeit des Betriebsrats, BB 2020, 500; Maschmann, Der Betriebsrat als für den Datenschutz Verantwortlicher, NZA 2020, 1207.

18 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07; Seifert, in: Simitis/Hornung/Spiecker, DS-GVO Art. 88 Rn. 231; Maschmann, in: Richardi, BetrVG, § 75 Rn. 60.

19 Flink, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, S. 46 f.

20 Fitting, BetrVG, 31. Aufl., 2022, § 75 Rn. 137.

21 Vgl. BAG, Beschl. v. 17.03.1987 – 1 ABR 59/85: „Das das Bundesdatenschutzgesetz ein zugunsten der Arbeitnehmer geltendes Gesetz im Sinne von § 80 Abs. 1 Nr. 1 BetrVG ist, gilt auch für die DS-GVO.“

Das BAG²² und des BVerwG²³ haben bereits Anfang der 80er Jahre festgehalten, dass demgemäß die Kontrolle der Einhaltung von Datenschutznormen, soweit sie die Verarbeitung von Beschäftigtendaten betreffen, zu den Aufgaben der Mitarbeitervertretung gehört (§ 80 Abs. 1 Nr. 1 BetrVG bzw. § 68 Abs. 2 BPersVG).

Für die Wahrnehmung der Aufgabe wesentlich ist sodann § 80 Abs. 2 BetrVG, der den Arbeitgeber zur umfassenden Unterrichtung des Betriebsrats bezüglich der zur Wahrnehmung seiner Aufgaben benötigten Informationen verpflichtet. Die Mitarbeitervertretung hat im Rahmen des Verhältnismäßigkeitsprinzips das Recht, Unterlagen einzusehen und dies auch mit dem Ziel festzustellen, ob Datenschutzverstöße durch den Arbeitgeber begangen werden.

Spezielle, vorrangige Informationsansprüche enthalten das BetrVG und das EntgTranspG mit dem dem Betriebsrat eingeräumten Einblicksrecht in Lohn- und Gehaltslisten (§ 80 Abs. 2 Halbs. 2 BetrVG oder § 13 Abs. 2 und 3 EntgTranspG). Während das Einsichtsrecht nach dem BetrVG unabhängig von Willen des Betroffenen ausgeübt werden kann,²⁴ setzt die Kontrolle nach dem EntgTranspG das Einverständnis des Betroffenen voraus. Der Betriebsrat ist Hüter der Lohngerechtigkeit und der diesbezüglichen Transparenz im Betrieb.²⁵ Stellt der Betriebsrat Ungleichbehandlungen fest, so kann er die davon betroffenen Arbeitnehmer darüber informieren.²⁶ Für die Personalvertretung gilt die gleiche Befugnis, wenngleich auch eine ausdrückliche Regelung fehlt. Das BVerwG²⁷ hat dem Personalrat ein Recht zur Einsichtnahme zugesprochen.

Ein allgemeines Einsichtsrecht in Personalakten steht der Mitarbeitervertretung dagegen – jedenfalls ohne Zustimmung des Beschäftigten – nicht zu.

Schließlich ist zu beachten, dass Datenschutzverstöße zur Auflösung des Betriebsrats wegen grober Pflichtverletzung führen können,²⁸ da als grobe Pflichtverletzungen insbesondere die grundsätzliche Missachtung der Gebote des § 2 Abs. 1 BetrVG im Hinblick auf die vertrauensvolle Zusammenarbeit²⁹ und die Weitergabe vertraulicher Vorgänge und Daten an Dritte³⁰ von Relevanz sind.

c) Der Datenschutzbeauftragte

Für die Einsichts- und Auskunftsrechte des Datenschutzbeauftragten bei der Kontrolle der Personaldatenverarbeitungen enthält die DS-GVO keine speziellen Aussagen, d.h. es gilt die allgemein gehaltene und damit umfassende Formulierung des Art. 39 Abs. 1 Nr. 2 DS-GVO, nach dem die Überwachung der Einhaltung der Datenschutzvorschriften dem DSB obliegt und ihm dazu Zugang zu allen personenbezogenen Datenverarbeitungen zu gewähren ist (Art. 38 Abs. 2 DS-GVO). Insofern wird er im Rahmen seiner Weisungsfreiheit einerseits quasi „von Amts wegen“ tätig, andererseits kann bzw. muss er einem berechtigtem individuellen Wunsch eines Betroffenen auf Kontrolle und Einschreiten nachkommen.

Einschränkungen seines Kontrollrechts – wie sie das BetrVG für den Betriebsrat vorsieht – kennt die DS-GVO nicht.

Eine besondere Regelung enthält das Landesdatenschutzgesetz von Sachsen-Anhalt.³¹ So gestattet § 14a Abs. 3 Satz 1 DSG-LSA dem Beauftragten für den Datenschutz, zur Auf-

gabenerfüllung Einsicht in personenbezogene Datenverarbeitungsvorgänge zu nehmen. Nach Satz 2 gilt dies jedoch nicht, soweit Berufs- oder besondere Amtsgeheimnisse bestehen, also die Schweigepflicht des Arztes oder das Personalaktengeheimnis des § 90 Abs. 1 Satz 1, Satz 3 und Abs. 3 BG LSA greift. Auch wenn damit der Schutz der Personaldaten Vorrang hat, bleibt die Aufgabenerfüllung des behördlichen Datenschutzbeauftragten gesichert. Er kann jederzeit die Einwilligung des Betroffenen einholen, falls die Einsicht in eine konkrete Personalakte erforderlich sein sollte.

II. Der gemeinsame Schutzauftrag

1. Der Schutzauftrag der Mitarbeitervertretung

a) Der allgemeine Schutzauftrag des § 80 Abs. 1 Nr. 1 BetrVG/§ 68 Abs. 1 Nr. 2 BPersVG

Das BAG³² und des BVerwG³³ haben bereits Anfang der 80er Jahre festgehalten, dass die Kontrolle der Einhaltung von Datenschutznormen, soweit sie die Verarbeitung von Beschäftigtendaten betreffen, zu den Aufgaben der Mitarbeitervertretung gehört. Gemäß § 80 Abs. 1 Nr. 1 BetrVG obliegt es dem Betriebsrat, die Einhaltung der zu Gunsten der Arbeitnehmer geltenden Gesetze durch den Arbeitgeber zu überwachen. § 62 Nr. 2 BPersVG und die Personalvertretungsgesetze der Länder enthalten gleiche Regelungen für die Personalvertretungen. Die dort enthaltene Verpflichtung der Mitarbeitervertretungen, auf die Einhaltung von dem Schutz der Mitarbeiter dienenden Gesetze zu achten, umfasst gewichtig auch alle Regelungen des Beschäftigtendatenschutzes.

Damit ist die Rolle der Mitarbeitervertretungen als Wächter des Datenschutzes der Beschäftigten³⁴ klargestellt. Die Kontrollaufgabe wird durch Mitbestimmung bei unterschiedlichen Phasen der Verarbeitung von Beschäftigtendaten komplettiert.³⁵

Zuständig für die Wahrnehmung der Überwachungsaufgabe ist nicht der Gesamt-, sondern der Einzelbetriebsrat.³⁶ Die Überwachungsbefugnis des Betriebsrats wird auch nicht dadurch tangiert, dass der Gesamtbetriebsrat im Rahmen

22 BAG, Beschl. v. 11.03.1982 – 1 ABR 59/85.

23 Vgl. BVerwG, Beschl. v. 26.03.1985 – 6 P 31.82 und 08.11.1989 – 6 P 7/87.

24 Zuletzt LAG Niedersachsen, Beschl. v. 22.10.2018 -12 TaBV 23/18.

25 Vgl. BAG, Beschl. v. 28.04.1998 – 1 ABR 50/97; zuletzt BAG Beschl. v. 29.11.2020 – 1 ABR 32/19.

26 Vgl. Fitting, BetrVG, 31. Aufl., 2022, § 80 Rn. 70, 20.

27 BVerwG, Beschl. v. 16.05.2012 – 6 PB 2.12.

28 ArbG Iserlohn, Beschl. v. 14.01.2020 – 2 BV 5/19.

29 ArbG Krefeld, Beschl. v. 06.02.1995 – 4 BV 34/94.

30 ErfK/Koch, 20. Aufl. 2020, BetrVG § 23 Rn. 5.

31 II. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt vom 01.04.2003 – 31.03.2005, Ziff. 12.6.

32 BAG, Beschl. v. 11.03.1982 – 1 ABR 59/85.

33 Vgl. BVerwG, Beschl. v. 26.03.1985 – 6 P 31.82 und 08.11.1989 – 6 P 7/87.

34 Althoff, Die Rolle des Betriebsrats im Zusammenhang mit der EU-35, DS-GVO, ArbRAktuell, 2018, 414.

35 Vgl. umfassend: Flink, Beschäftigtendatenschutz als Aufgabe des Betriebsrats – 2021, S. 113; Möhle, Die datenschutzrechtliche Verantwortlichkeit des Betriebsrats, 2021, S. 183.

36 BAG, Beschl. v. 16.08.2011 – 1 ABR 22/10.

seiner Zuständigkeit eine Betriebsvereinbarung zur Personaldatenverarbeitung abschließt.

Auch ein Tarifvertrag kann die gesetzliche Aufgabe des Betriebsrats aus § 80 Abs. 1 Nr. 1 BetrVG, die Durchführung getroffener Regelungen zu überwachen, nicht aufheben oder einschränken.³⁷

Letztendlich ist festzuhalten, dass die Mitarbeitervertretung – ebenso wie alle Beschäftigten – die Pflicht zur Einhaltung der geltenden Gesetze und damit auch der DS-GVO und sonstiger besonderer datenschutzrechtlicher Rechtsvorschriften hat,³⁸ was in der Praxis unter anderem beinhaltet, dass sie

- die in Artikel 5 Absatz 1 DS-GVO genannten Grundsätze für die Verarbeitung personenbezogener Daten, auch wenn für deren Einhaltung der Verantwortliche zuständig ist, im Rahmen ihrer Tätigkeit zu beachten hat. Hierzu zählen die Beachtung des Grundsatzes der Datenminimierung (Datensparsamkeit) sowie des Vertraulichkeitsgrundsatzes,
- dem Verantwortlichen die für die Durchführung von Datenschutz-Folgenabschätzungen erforderlichen Informationen zu liefern muss,
- die geeigneten technisch-organisatorischen Maßnahmen wie die zur Wahrung der Datensicherheit und zur Löschung von Betriebsratsunterlagen umzusetzen hat und
- dem Verantwortlichen unverzüglich Datenpannen nach Artikel 33 DS-GVO aus seinem Geschäftsbereich zu melden hat.³⁹

b) Der einzelfallbezogene Schutzauftrag

Die Kontrollfunktion der Mitarbeitervertretung greift aber nicht nur zur Wahrung der Rechtspositionen der Mitarbeiter als Kollektiv, sondern auch im Einzelfall, wenn sich ein Beschäftigter an den Betriebs-/Personalrat mit einem Datenschutzproblem wendet. Es gehört zu den allgemeinen Aufgaben der Mitarbeitervertretung, Anregungen von Arbeitnehmern entgegenzunehmen und, falls sie berechtigt erscheinen, darauf hinzuwirken, dass der Arbeitgeber ihnen nachkommt (§ 80 Abs. 1 Nr. 3 BetrVG; § 68 Abs. 1 Nr. 3 BPersVG). Für die Mitarbeitervertretung besteht eine Handlungspflicht.

Die „Anregung“ kann auch die Einstellung einer bestimmten Verarbeitung der Daten des Beschäftigten zum Inhalt haben. Das Verlangen um Unterstützung kann einmal begründet sein, weil die beanstandete Datenverarbeitung wegen Datenschutzverstößes rechtswidrig ist; des weiteren hat eine nach Art. 6 Abs. 1 lit. e oder f DS-GVO erfolgende Verarbeitung nach Art. 21 Abs. 1 DS-GVO zu unterbleiben, wenn sich aus der besonderen Situation des Beschäftigten Gründe ergeben, jederzeit gegen die an sich rechtmäßige Verarbeitung seiner Daten beim Arbeitgeber Widerspruch einzulegen. Zur Unterstützung in einem solchen Fall können sich Beschäftigte natürlich auch an die Mitarbeitervertretung wenden.

Bleibt die Mitarbeitervertretung bei ihren Verhandlungen mit dem Arbeitgeber erfolglos, verbleibt es primär beim Betroffenen selbst, weitere Schritte zu ergreifen. Eine Ausnahme bildet der Fall, dass die gerügte Datenverarbeitung

deshalb rechtswidrig erfolgt, weil sie ohne die erforderliche Mitbestimmung stattfindet. Hier hat der Betriebsrat einen nachfolgend dargestellten Unterlassungsanspruch.

c) Handlungsmöglichkeit der Mitarbeitervertretung gegenüber Datenschutzverstößen

aa) Allgemeines

Will die Mitarbeitervertretung gegen Datenschutzverstöße des Arbeitgebers vorgehen, kann dies mit gerichtlich festgestellten Unterlassungsansprüchen geschehen oder einer Einschaltung der Aufsichtsbehörde.

bb) Unterlassungsansprüche

Ein Unterlassungsanspruch besteht dann, wenn Rechte der Mitarbeitervertretung verletzt sind, weil mitbestimmungspflichtige Personaldatenverarbeitung, ohne Einschaltung der Mitarbeitervertretung oder entgegen einer mit ihr vereinbarten Regelung erfolgen. Gestützt werden kann der Anspruch jedoch nicht unmittelbar auf § 80 Abs. 1 Nr. 1 BetrVG/§ 68 Abs. 1 Nr. 2 BPersVG,⁴⁰ da die Bestimmung reine Überwachungs- und „Mahnfunktion“ hat.⁴¹ Das gilt auch bei Verstößen gegen eine Betriebsvereinbarung.⁴² Ebenfalls nicht als Rechtsgrundlage zur Abwehr von persönlichkeitsrechtsverletzenden Maßnahmen kann § 75 Abs. 2 S. 1 BetrVG herangezogen werden.⁴³

Gestützt werden kann der Unterlassungsanspruch jedoch auf § 23 Abs. 3 S. 1 BetrVG i.V.m. § 75 Abs. 2 S. 1 BetrVG. Vorausgesetzt ist: Es handelt sich um einen den dort geforderten „groben“ Verstoß des Arbeitgebers gegen seine betriebsverfassungsrechtlichen Pflichten zur Achtung der Persönlichkeitsrechte der Beschäftigten.⁴⁴

Anders sieht es für die Personalvertretung aus: Der Personalvertretung steht bei Verletzung ihrer Mitbestimmungsrechte über die Feststellung dieser Rechte hinaus ein Anspruch auf Unterlassung der mitbestimmungspflichtigen Maßnahme nicht zu.⁴⁵ Sie kann jedoch, sofern die Maßnahme tatsächlich und rechtlich rücknehmbar oder abänderbar ist, vom Dienststellenleiter die nachträgliche Einleitung

37 BAG, Beschl. v. 21.10.2003 – 1 ABR 39/02 zum Auskunftsanspruch des Betriebsrats zu Zielvereinbarungen; vgl. auch LAG Frankfurt vom 24.11.2015 – 16 TaBV 106/15 – zur Kontrolle von in einer Gesamtbetriebsvereinbarung getroffenen Regelungen zu Zielvereinbarungen durch den Einzelbetriebsrat.

38 Zum Datenschutzkonzept des Betriebsrats: Kiesche, Kooperieren beim Datenschutz, AiB extra 8/2022, 24 (26).

39 LfDI Niedersachsen, <https://lfd.niedersachsen.de> > ... > faq-fur-betriebsrate-194163.

40 Fitting, BetrVG; 31 Aufl. 2022, Rn. 14, detailliert bei Flink, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, S. 119 f.

41 BAG, Beschl. v. 22.08.2017 – 1 ABR 24/16; Lücke, Die Betriebsverfassung in Zeiten der DS-GVO. „Bermuda-Dreieck“ zwischen Arbeitgeber, Betriebsräten und Datenschutzbeauftragten 1, NZA 2019, 658 (667).

42 BAG, Beschl. v. 17.10.1989 – 1 ABR 75/88.

43 BAG, Beschl. v. 28.05.2002 – 1 ABR 32/01; Gola, Der neue Beschäftigtendatenschutz nach § 26 BDSG n.F., BB 2017, 1462 (1469).

44 BAG; Beschl. v. 28.05.2002 – 1 ABR 32/01; Kort, Betriebsrat und Arbeitnehmerdatenschutz, Rechte der Interessenvertretung bei datenschutzrechtlich relevanten Maßnahmen des Arbeitgebers, ZD 2026, 3 (9).

45 VGH Baden-Württemberg, Beschl. v. 02.07.2002 – PL 15 S 2497/01; Fortführung Beschl. v. 24.06.1997 – PL 15 S 419/97.

des Mitbestimmungsverfahrens und eine vollständige Unterrichtung verlangen und den Anspruch verfahrensrechtlich im Beschlussverfahren mit einem Feststellungsantrag verfolgen.⁴⁶

Verstößt der Arbeitgeber zugleich gegen datenschutzrechtliche Regelungen einer Betriebsvereinbarung, kann ferner ein Unterlassungsanspruch aus § 77 Abs. 1 S. 1 BetrVG folgen, sofern der Arbeitgeber Rechte des Betriebsrats verletzt, die diesem gerade durch die Betriebsvereinbarung eingeräumt wurden.

cc) Einschaltung der Aufsichtsbehörde

Jedenfalls dann, wenn die Mitarbeitervertretung mit der Beanstandung datenschutzwidriger Beschäftigtendatenverarbeitung beim Arbeitgeber kein Gehör findet,⁴⁷ wird sie die Datenschutzaufsichtsbehörde quasi als „Whistleblower“ informieren können, ohne gegen ihre in § 2 Abs. 1 BetrVG vorgegebene Pflicht zur vertrauensvollen Zusammenarbeit oder zur Verschwiegenheit nach § 79 Abs. 1 BetrVG zu verstoßen.⁴⁸ § 89 Abs. 1 S. 2 BetrVG legt dem Betriebsrat im Bereich des Arbeitsschutzes die Pflicht zur Unterstützung der Aufsichtsbehörde auf, was aber nicht auf den Fall beschränkt ist, dass diese sich an ihn wendet. Gleiches gilt für die im BetrVG bzw. dem BDSG nicht geregelte Kooperation der Mitarbeitervertretung mit den für den Beschäftigtendatenschutz zuständigen Behörden.⁴⁹ Keinesfalls kann aus der Tatsache, dass die DS-GVO einzig dem Betroffenen ein Beschwerderecht bei der Aufsichtsbehörde einräumt, dem Betriebsrat das Recht zur Information der Aufsichtsbehörden versagt werden; zu achten hat er jedoch darauf, dass er keine Geschäfts- oder Betriebsgeheimnisse gemäß § 79 Abs. 1 BetrVG offenlegt.

In diese Richtung tendiert auch das BAG in seiner Entscheidung zu § 89 BetrVG, in der ausgeführt wird, dass einiges dafür spricht, „dass der Betriebsrat wegen des Grundsatzes der vertrauensvollen Zusammenarbeit der Betriebsparteien jedenfalls vor der unaufgeforderten Unterrichtung einer Überwachungsbehörde erfolglos den Versuch unternommen haben muss, den Arbeitgeber zur Abhilfe der Mängel zu bewegen“.⁵⁰

Die Beratung des Betriebsrats im Zusammenhang mit seinen Aufgaben zum Beschäftigtendatenschutz durch die Aufsichtsbehörde kann zudem im Rahmen von § 80 Abs. 3 BetrVG liegen, da man die Aufsichtsbehörde als Sachverständigen sehen kann. Zur Einschaltung der Aufsichtsbehörde bedarf es auch keiner „näherer Vereinbarung mit dem Arbeitgeber“ nach § 80 Abs. 3 BetrVG, da hier keine Kosten entstehen.⁵¹ § 80 Abs. 3 BetrVG ist nicht einschlägig, wenn die Auskunftsperson unentgeltlich informiert,⁵² was Art. 57 Abs. 1 lit. c i.V.m. Abs. 3 DS-GVO ausdrücklich vorsieht.

Sinn der Norm ist, dass die genannten „anderen Einrichtungen oder Gremien“ vom Expertenwissen der Aufsichtsbehörden profitieren sollen.⁵³ Daher fällt auch der Betriebsrat darunter und kann die unentgeltliche Expertise der Aufsichtsbehörden jederzeit in Anspruch nehmen.⁵⁴

dd) Einschaltung des Datenschutzbeauftragten

An erster Stelle der einzuschaltenden Stellen steht jedoch nach § 79a BetrVG der DSB als Kooperationspartner.⁵⁵ Eine Rahmenbetriebsvereinbarung⁵⁶ kann die Basis der Unterstützung und Zusammenarbeit sein.⁵⁷ Sie muss sowohl dem Beschäftigtendatenschutz als auch der Verschwiegenheitspflicht des Betriebsrats sowie der informationellen Selbstbestimmung der Beschäftigten gerecht werden.⁵⁸

2. Der Schutzauftrag des Datenschutzbeauftragten

a) Allgemeines

Die dem Schutzauftrag der Mitarbeitervertretung parallele Funktion des Datenschutzbeauftragten gibt in allgemein gehaltener Formulierung Art. 39 Abs. 1 DS-GVO vor, nach dem u.a. die Überwachung der Einhaltung dieser Verordnung, sowie anderer Datenschutzvorschriften dem DSB obliegt. Insofern wird er im Rahmen seiner Weisungsfreiheit „von Amts wegen“ tätig. Einbezogen in die Kontrolle sind die Datenverarbeitungen der Mitarbeitervertretung.⁵⁹

b) Der einzelfallbezogene Schutzauftrag

Ebenso wie gegenüber der Mitarbeitervertretung haben auch die Betroffenen das Recht, den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate zu ziehen. Wendet sich ein Betroffener an den Datenschutzbeauftragten, so ist dieser ausdrücklich zum Stillschweigen über die Identität des beschwerdeführenden Betroffenen berechtigt und verpflichtet (Art. 38 Abs. 5 DS-GVO).

Der Bundesgesetzgeber hat somit in Art. 38 Abs. 5 DS-GVO einen Handlungsauftrag erteilt⁶⁰ und in § 6 Abs. 5 S. 2 BDSG⁶¹ für Bundesbehörden nebst der Erstreckung dieser

46 BVerwG, Beschl. v. 15.03.1995 – 6 P 31.93, vgl. aber auch BVerwG v. 08.11.2011 – 6 P 23.10.

47 BAG, Beschl. v. 03.06.2003 – 1 ABR19/02; Fitting, BetrVG, 31. Aufl., § 89 Rn. 18.

48 Flink, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, S. 128 m.N.w.

49 Kort, Das Dreiecksverhältnis von Betriebsrat, betrieblichen Datenschutzbeauftragten und Aufsichtsbehörde beim Arbeitnehmer-Datenschutz, NZA 2015, 1345 (1352); Däubler, Gläserne Belegschaften, 8. Aufl. Rn 65; a.A. Dzida, Der neue Beschäftigtendatenschutz, BB 2018, 2677.

50 BAG, Beschl. v. 03.06.2003 – 1 ABR 19/02.

51 Vgl. BAG, Beschl. v. 19.04.1989 – 7 ABR 87/87.

52 Kania, in: ErfK, 2018, 18. Aufl. § 80 BetrVG, Rn. 33.

53 Boehm, in: Kühling/Buchner, DS-GVO, 2. Aufl., Art. 38, Rn. 15.

54 Körner, Der Betriebsrat als datenschutzrechtlich verantwortliche Stelle, S. 14.

55 Kiesche, Kooperieren beim Datenschutz, AiB extra 8/2022, 24.

56 Vgl. das Beispiel bei Gola, RDV 2021, 183 das von Kiesche (Fn. 55) als zu arbeitgeberfreundlich kritisiert wird.

57 Kiesche, 24 (26).

58 Fitting, BetrVG, 31. Aufl., § 79a Rn. 42.

59 Aßmus, Kontrolle des Betriebsrats durch den betrieblichen Datenschutzbeauftragten, ZD 2011, 27.

60 Vgl. bei Kühling/Martini u.a., Die Datenschutz-Grundverordnung und das nationale Recht, S. 99.

61 Gola, in: Gola/Heckmann, BDSG § 6 Rn. 29 ff.

Regelung auf nichtöffentliche Stellen in § 38 Abs. 2 BDSG verfügt, dass der Datenschutzbeauftragte „zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen,“ verpflichtet ist, soweit die betroffene Person keine „Sprecherlaubnis“ erteilt.

Damit ist gesetzlich sichergestellt, dass sich eine betroffene Person an den DSB wenden kann, ohne Nachteile durch Indiskretionen befürchten zu müssen, was insbesondere nicht fern liegt, wenn der Verantwortliche, gegen den die Beanstandung gerichtet ist, der Arbeitgeber, Dienstherr oder Auftraggeber des Anzeigenden ist.⁶² Somit darf der DSB in Nachforschungen und Berichten die um seine Unterstützung in eigener Sache nachsuchende Person ohne deren Einwilligung nicht kenntlich machen.

Der datenschutzrechtliche Vertraulichkeitsschutz des Art. 38 Abs. 5 DS-GVO bzw. des § 6 Abs. 5 S. 2 BDSG und der entsprechenden Landesregelungen umfasst nicht den Schutz sonstiger sich an den Datenschutzbeauftragten wendender Informanten. Das heißt aber nicht, dass insoweit unbeschränkte Offenbarungsrechte oder gar -pflichten für den DSB bestehen. Ein Recht zur Verschwiegenheit ergibt sich unter Beachtung der Weisungsunabhängigkeit des DSB auch dann, wenn sich ein Nicht-Betroffener in Art eines internen oder externen „Whistleblowers“ an den DSB wendet. Dem Datenschutzbeauftragten muss das Recht zustehen, z.B. um Informationen zu erhalten, die sonst nicht mitgeteilt würden, dem Informanten die vertrauliche Behandlung seiner Person zusichern zu können.

Das BayDSG trägt dem ausdrücklich Rechnung, indem es in Art. 12 Abs. 2 in einer erweiterten Schweigepflicht die behördlichen Datenschutzbeauftragten verpflichtet „Tatsachen, die ihnen in Ausübung ihrer Funktion anvertraut wurden, und die Identität der mitteilenden Personen nicht ohne deren Einverständnis zu offenbaren.“

c) Handlungsmöglichkeiten gegenüber Datenschutzverstößen

aa) Information des Verantwortlichen

Stellt der Datenschutzbeauftragte im Rahmen seiner Kontrolltätigkeit mit Datenschutzvorgaben nicht konformes Verhalten fest, ist der erste Ansprechpartner der Verantwortliche. Es besteht ein unmittelbarer Berichtsweg ohne Zwischenschaltung anderer Personen (§ 38 Abs. 3 S. 3 DS-GVO). Seine Aufgabe ist, festgestellte Mängel zu melden und Vorschläge zur Beseitigung machen.

bb) Einschaltung der Aufsichtsbehörden

Bei nach seiner Ansicht nach problematischen Datenverarbeitungen kann der DSB den Rat der Datenschutz Kontrollinstanz kostenlos einholen (Art. 57 Abs. 3 DS-GVO).

Eine solche ratsuchende Einschaltung bedarf nicht zwingend der vorherigen Einschaltung des Verantwortlichen.

Kritischer sieht es jedoch aus, wenn der DSB sich im Konfliktfall an die Aufsichtsbehörde wendet und seiner Ansicht nach datenschutzwidriges Verhalten des Verantwortlichen, d.h. idR seines Arbeitgebers „anzeigt“.

Ob seine Pflicht zur Meldung von ihm nicht zu beseitigenden Datenschutzverstößen nach der DS-GVO weiter reicht als zuvor nach dem BDSG aber auch den Fall mit einem Aktenvermerk „abheften“ kann, ist zumindest offen.⁶³

cc) Einschaltung der Mitarbeitervertretung

So wie bei der Aufsichtsbehörde, deren Einschaltung erst nach dem vergeblichen Versuch die Datenschutzverstöße intern abzustellen, zulässig ist, kann und darf die Mitarbeitervertretung über Datenschutzverstöße im Betrieb erst informiert werden, wenn keine unmittelbare Lösung erreichbar ist. Über diese ist dann die Mitarbeitervertretung aber auch zu informieren.

III. Die gegenseitige Kontrolle und Kooperation von Mitarbeitervertretung und DSB

1. Kontrolle der Datenverarbeitung der Mitarbeitervertretung durch den DSB

a) Allgemeines

Der Datenschutzbeauftragte kann bzw. muss – entgegen früher bestehender Ansicht⁶⁴ – ggf. auch die bei der Mitarbeitervertretung stattfindenden Datenverarbeitungen auf ihre datenschutzrechtliche Rechtmäßigkeit überprüfen.⁶⁵ Obwohl der Betriebsrat über seine Datenverarbeitungsverfahren und die Organisation der hierbei erforderlichen Datensicherheit selbst entscheidet, ist der Arbeitgeber von Gesetzes wegen – entgegen nicht sofort von der Hand zu weisender anderweitiger Überlegungen⁶⁶ – hierfür der Verantwortliche.⁶⁷ Die dem Betriebs- bzw. Personalrat durch das BetrVG bzw. BPersVG gewährte Unabhängigkeit steht dem nicht entgegen.⁶⁸

Bereits Art. 39 Abs. 1 lit b DS-GVO überträgt dem Datenschutzbeauftragten eine umfassende Überwachungsaufgabe, von der durch nationales Recht keine Ausnahmen gemacht werden können.⁶⁹ Art. 38 Abs. 2 DS-GVO macht das mit dem

62 Raum, in: Auerhammer, BDSG, 5. Aufl. § 4f Rn. 88.

63 Vgl. Gola/Schomerus, BDSG, § 4g, Rn 16; Bergt, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 39, Rn 19.

64 BAG, Beschl. v. 11.11.1997 – 1 ABR 21/97, Fitting, BetrVG, 22. Aufl. 2004, Rn. 216; offen gelassen hatte das BAG die Frage im Ur. v. 23.03.2011 – 10 AZR 562/09.

65 Vgl. bereits Gola, Eigenständigkeit des Betriebsrats und Kontrolle durch den Datenschutzbeauftragten – ein ungelöster Konflikt, ZBVR online 2017, Nr 7/8, 31; Aßmus, Kontrolle des Betriebsrats durch den betrieblichen Datenschutzbeauftragten, ZD 2011, 27.

66 Bonnani/Niklas, Ist der Betriebsrat Verantwortlicher im Sinne der DS-GVO?, ArbRB 2018, 371; Brams/Möhle, Die Stellung des Betriebsrats unter der DS-GVO, ZD 2018, 570; Brink/Joos, Datenschutzrechtliche Verantwortlichkeit der betrieblichen und behördlichen Datenschutzbeauftragten, NZA 2019, 1395.

67 Maschmann, Der Arbeitgeber als Verantwortlicher für den Datenschutz im Betriebsratsbüro, NZA 2021, 834; Kleinebrink, Arbeitgeber und Betriebsrat als „Verantwortliche“ im neuen Datenschutzrecht, DB 2018, 2566.

68 Auf anders lautende gewerkschaftsnahe Stimmen sei aber hingewiesen: DGB-Information zu Betriebsrätemodernisierungsgesetz; <https://datenschutzfrankfurt.de> > datenschutz-Betriebsrat.

69 Vgl. bei Flink, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, 2021, S. 291.

dem DSB uneingeschränkt eingeräumten Zugangsrecht zu allen vom Verantwortlichen verarbeiteten personenbezogenen Daten deutlich.⁷⁰ Datenverarbeitungen der Mitarbeitervertretung, die nach nunmehriger gesetzlicher Regelung ihre Datenverarbeitung nicht als eigenständig Verantwortlicher⁷¹ betreibt, unterliegen seiner Kontrolle. § 79a BetrVG bzw. § 68 BPersVG gehen von diesem Recht aus und präzisieren es durch – auch wohl auch schon zuvor bestehende⁷² – spezielle Schweigepflichten.

b) Verschwiegenheitspflicht

In Satz 4 des § 79a BetrVG findet sich eine spezielle Regelung zur Verschwiegenheitsverpflichtung des Datenschutzbeauftragten: „Die oder der Datenschutzbeauftragte ist gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen“, wobei es zunächst schwierig sein wird, zwischen Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen, und anderen Informationen abzugrenzen.

Anzweifeln mag man die Wirksamkeit dieser Klausel, weil dem Datenschutzbeauftragten bei einer Verletzung seiner Verschwiegenheitsverpflichtung so gut wie keine Sanktionen drohen.⁷³ Allenfalls der Arbeitgeber könnte den Datenschutzbeauftragten aus wichtigem Grund in entsprechender Anwendung des § 626 BGB abberufen (vgl. §§ 38 Abs. 2, 6 Abs. 4 BDSG).⁷⁴ Ob der Arbeitgeber von der Möglichkeit der Abberufung Gebrauch macht, ist in Anbetracht der Tatsache, dass er in diesem Fall von der Verletzung der Verschwiegenheitsverpflichtung profitiert, zweifelhaft. Dem ist jedoch entgegenzuhalten, dass der Betriebsrat Informationen gegenüber dem die Vertraulichkeit nicht beachtenden DSB verweigern könnte.

Weitere Geheimhaltungspflichten ergeben sich für den DSB, wenn er Kontrolltätigkeiten bei der Verarbeitung von Daten ausübt, die besonderen, ggf. strafrechtlich abgesicherten Vertraulichkeitsregelungen unterliegen. Das gilt für die Wahrung von Privatgeheimnissen, die bei den in § 203 StGB genannten als Berufsheimnisträgern tätigen DSB bekannt werden.

Das Zeugnisverweigerungsrecht in § 6 Abs. 6 BDSG n.F. sichert die Verschwiegenheitspflicht ab.

2. Kontrolle der Tätigkeit des DSB durch die Mitarbeitervertretung

a) Allgemeines

Parallel stellt sich die Frage, inwieweit die Mitarbeitervertretung bei der Installation eines DSB mitwirken und ihn bei den von ihm z.B. in einem Beschwerdefall durchgeführten Verarbeitungen von Beschäftigtendaten überwachen darf. Ein unmittelbares Kontrollrecht hat die Mitarbeitervertretung nicht. Ihr Adressat ist der Arbeitgeber, der aber den DSB anweisen kann, unmittelbar Auskunft zu geben. Diese Auskunftspflicht hat aber sowohl gegenüber dem Arbeitgeber als auch dem Betriebsrat wiederum datenschutzrechtliche Grenzen. Im Rahmen der ihm gesetzlich gewährten „völligen Unabhängigkeit“⁷⁵ hat der DSB gegenüber dem

Arbeitgeber und damit auch der Revision einen unantastbaren „Schutzbereich“.⁷⁶ Ein Einsichtsrecht in die Unterlagen oder in den E-Mail-Verkehr von Datenschutzbeauftragten besteht für die Revision eines Unternehmens nicht. Gemäß Art. 38 Abs. 5 DS-GVO sind Datenschutzbeauftragte an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden. Besondere Rechtsvorschriften, die eine Offenlegung der Akten des DSB gegenüber der Revision erlauben (Einsichtsrecht) oder einschränkende Regelungen zur Geheimhaltungspflicht von DSB enthalten, sind nicht bekannt. Ein DSB sollte nach Ansicht der LfDI Niedersachsen der Revision auch schon deshalb kein Einsichtsrecht gewähren, um nicht bei unbefugter Offenlegung von Daten gegen § 203 Abs. 4 StGB (Verletzung von Privatgeheimnissen) zu verstoßen. Andererseits kann die für den Verantwortlichen tätige Revision von dem DSB Nachweise für die Erfüllung seiner Aufgaben fordern; wie z.B. die Vorlage eines „Tätigkeitsberichts“ oder von Arbeitszeitrachweisen.

b) Keine Mitbestimmung bei der Bestellung

Als inkonsequent festzustellen ist, dass trotz der gesetzlich vorausgesetzten Pflicht zur kooperativen Zusammenarbeit der Gesetzgeber dem Betriebsrat kein spezielles Recht zur Mitwirkung bei der Bestellung eines Datenschutzbeauftragten im Rahmen der betriebsverfassungsrechtlichen Zusammenarbeitsklausel zugestanden hat, wie es im HessPersVG in § 74 Abs: 1 Nr. 3 verankert ist.⁷⁷

Zwar greift, wenn der DSB als Beschäftigter neu eingestellt oder auf die Position versetzt wird, Mitbestimmung nach § 99 BetrVG, der ggf. eine betriebsinterne Ausschreiben vorausgehen hat (§ 93 BetrVG). Ihre Zustimmung versagen kann die Mitarbeitervertretung nur, wenn sie Belege hat, dass der vorgesehene DSB nicht den gesetzlichen Anforderungen entspricht.

Diese Rechte greifen zudem nur, wenn die Position des Datenschutzbeauftragten zu einer Eingliederung des DSB in die Organisation des Unternehmens führt, was regelmäßig nicht gegeben ist, wenn der Datenschutzbeauftragte als externer Dienstleister auf Basis eines Dienstleistungsvertrages gem. § 611 BGB seine Tätigkeit im Unternehmen wahrnehmen soll, worüber nur der Arbeitgeber entscheidet..

70 Gola, Der neue Beschäftigtendatenschutz nach §26 BDSG n.F., BB 2017, 1462 (1470); Kurzböck/Weinbeck, Die datenschutzrechtliche Verantwortlichkeit des Betriebsrats, BB 2018, 1652.

71 Möllenkamp, Das Betriebsrätemodernisierungsgesetz 2021 – Regelungsinhalte und Praxisauswirkungen, DB 2021,1198 (1201).

72 Bergt, in: Kühling/Buchner, DS-GVO Art. 38 Rn. 38; Pötter/Hansen, Datenschutzanforderungen an die Betriebsratsarbeit, ArbRAktuell,2020, 193; Stück, Betriebsrat oder Geheimrat? Beschäftigtendatenschutz beim Betriebsrat, ZD 2019, 256, (259), a.A. Klebe/Wankel, in: DKW, BetrVG, 17. Aufl., 2020, § 94 Rn. 15.

73 Schiefer/Worzalla, Das Betriebsrätemodernisierungsgesetz – eine Moglepackung? NZA 2021, 817.

74 Ehmann, Abberufung eines DSB wegen Pflichtverletzung, datenschutzpraxis 8/20, S. 1.

75 Erwägungsgrund (EG) 97.

76 LfDI Niedersachsen, Datenschutzbeauftragte – keine Kontrolle durch die Revision, https://lfdi.niedersachsen.de/startseite/infothek/faqs_zur_ds_gvo/datenschutzbeauftragte-inunternehmen-197585.html.

77 VGH Hessen, Beschl. v. 22.07.2014 – 22 A 2226/13.PV.

IV. Zur Inkompatibilität der Funktionen von Betriebs-/Personalrat und Datenschutzbeauftragten

1. Allgemeines/Rückblick

Ob Datenschutzbeauftragte Mitglied der Mitarbeitervertretung sein können oder ob aufgrund einer Interessenkollision Art. 38 Abs. 6 S. 2 DS-GVO insoweit eine Inkompatibilität besteht, wird möglicherweise demnächst abschließend vom EuGH beantwortet worden sein. Das BAG hat eine entsprechende Anfrage gestellt,⁷⁸ obwohl es zuvor diesbezüglich keine Bedenken hatte.

Nach der Rechtsprechung des BAG wurde der Betriebsrat vor In-Kraft-Treten der DS-GVO nicht als Verantwortlicher, sondern nur als (institutionell unselbstständiger) Teil des primär verantwortlichen Arbeitgebers gesehen.⁷⁹ Nach In-Kraft-Treten der DS-GVO ist das LAG Hessen⁸⁰ der bisherigen Rechtsauffassung des BAG gefolgt.

2. Aktuelle Situation

Von einem Interessenkonflikt ist auszugehen, wenn der Datenschutzbeauftragte durch seine anderen Aufgaben derart beeinflusst wird, dass eine objektive Wahrnehmung seiner Aufgaben nicht mehr gewährleistet ist.

Im Fall der Mitarbeiterbeschwerde gegen Datenverarbeitungen des Arbeitgebers ist jedenfalls nicht zu erkennen, dass gleichgültig, ob sich ein Beschäftigter an den Betriebsrat oder an den DSB oder an beide wendet, Gründe für eine unterschiedliche Entscheidung vorliegen könnten. Andererseits sehen vier Augen mehr als zwei. Problematisch ist die Situation auch bei eigener Datenverarbeitung des Betriebsrats oder des DSB. Die Problematik liegt somit in der vom Gesetz gewollten doppelten und beiderseitigen Kontrolle, die jedenfalls eindeutig entfällt, wenn die Funktionen des DSB und jedenfalls des Vorsitzenden der Mitarbeitervertretung in einer Hand liegen.⁸¹

Die Aufsichtsbehörden⁸² haben in der Vergangenheit gegenüber der Kombination der Funktionen DSB und Mitglied im Betriebsrat durchweg Bedenken geäußert und jedenfalls bei der Wahl zum Vorsitzenden die Notwendigkeit der Beendigung der DSB-Funktion gesehen. Als BR-Vorsitzender sei ein DSB maßgeblich für die Einhaltung des Datenschutzes in der Mitarbeitervertretung verantwortlich und müsste in seiner Rolle als Datenschutzbeauftragter die Einhaltung des Datenschutzes bei sich selbst kontrollieren. Aber auch bei einem einfachen Mitglied des Personalrats rät der BfDI⁸³ eher von einer Benennung zum Datenschutzbeauftragten ab. Auf der anderen Seite erscheint ihm jedoch eine Abberufung nicht zwingend geboten, wenn der Datenschutzbeauftragte erst zu einem späteren Zeitpunkt in den Personalrat gewählt wird.

Wichtig und unabdingbar sei bei jeder Doppelfunktion stets die strikte Trennung der Aufgaben.

Soweit erkennbar, liegt jedoch bisher kein Fall vor, in dem Aufsichtsbehörden in einem angenommenen Inkompatibilitätsfall die DSB-Abberufung mit Zwangsmitteln durchgesetzt haben.

Wie aufgezeigt, wird infolge einer Vorlage des BAG⁸⁴ an den EuGH dieser demnächst über diese Streitfrage entscheiden. Auf Grund der mit der DS-GVO geschaffenen neuen Rechtslage hat das BAG Bedenken, ob es an seiner im Jahre 2011⁸⁵ gefällten Entscheidung, dass beide Ämter von ein und derselben Person bekleidet werden können, festhalten kann.

V. Die Haftung von DSB und Mitarbeitervertretung gegenüber den Beschäftigten bei „Schlechtbetreuung“

1. Die gleiche Problemstellung

Kommen der DSB oder die Mitarbeitervertretung dem Ersuchen eines Beschäftigten um Beratung und Unterstützung nicht nach oder fällt ihre Beurteilung der Rechtslage falsch aus, stellt sich die Frage nach ihrer Haftbarkeit. Die DS-GVO äußert sich hierzu nicht. Speziell geregelt ist dort nur die Haftung der verantwortlichen Stelle (Art. 82 DS-GVO).⁸⁶

Zwar mag die Frage, ob der DSB bzw. der Betriebsrat für eine Fehl- bzw. Nichtentscheidung zum einen von dem Unternehmen oder zum anderen von einem geschädigten Betroffenen in Anspruch genommen werden kann, insofern wenig Bedeutung haben, als derartige Fälle bislang so gut wie nicht evident geworden sind bzw. die Rechtsprechung beschäftigt haben.

Eine Ausnahme bildet die Entscheidung des OLG München,⁸⁷ das eine Schadensersatzverpflichtung eines externen DSB wegen vermeintlich unbefugter Offenlegung von Daten einer Wohnungseigentümergeinschaft mit knapp einem Satz deshalb ablehnte, weil dieser nicht „Verantwortlicher“ im Sinne von Art. 4 Nr. 7 DS-GVO sei. Auf eventuelle Ansprüche außerhalb des Art. 82 DS-GVO ging das Gericht nicht ein.

2. Haftung des Arbeitgebers als Verantwortlicher

Bejaht man die Stellung des Arbeitgebers als „Verantwortlicher“ für die „unter seiner Verantwortung“ agierenden DSB bzw. BR, so ist Adressat eines vom DSB bzw. dem BR beim Beschäftigten durch Unterlassen oder falsche Beurteilung verursachten Schadens, ist grundsätzlich das Unternehmen als Verantwortlicher nach Art. 82 DS-GVO (sofern es sich nicht ausnahmsweise um einen „Mitarbeiterexzess“ oder „Kollektivexzess“ des Betriebsrates bzw. DSB handelt. Für

78 BAG, Beschl. v. 27.04.2021 – 9 AZR 383/19 (A).

79 BAG, Beschl. v. 03.06.2003 – 1 ABR 19/02, und BAG, Beschl. v. 14. 1. 2014 – 1 ABR 54/12

80 Beschl. v. 10.12.2018 – TaBV 130/18); a.A. LAG Sachsen-Anhalt, Beschl. v. 18.12.2018 – 4 TaBV 19/17[1] sowie LAG Mecklenburg-Vorpommern, Beschl. v. 15.05.2019 – 3 TaBV 10/18[2].

81 Vgl. bereits Dzida/Kröpelin, Kann ein Betriebsrat zugleich Datenschutzbeauftragter sein, NZA 2019, 1018.

82 Vgl. jüngst HessLfDI, 30. TB vom 27.05.2022, S. 140.

83 BfDI – Info 4 17.

84 BAG, Beschl. v. 27.04.2021 – 9 AZR 383/19 (A).

85 BAG, Beschl. v. 23.03.2011 – 10 AZR 562/09.

86 Zu Sanktionen gegen Betriebsrat und Betriebsratsmitglieder nach der DS-GVO vgl. Bott/Vogel, BB 2019, 2100.

87 Endurteil v. 27.10.2021 – 20 U 7051/20.

derartige „Grenzüberschreitungen“ gelten jedoch hohe Anforderungen.⁸⁸

Entlasten gemäß Art. 82 Abs. 3 DS GVO kann sich der Arbeitgeber nicht, auch wenn die Verstöße gegen die Verordnung allein auf Beschlüssen der Mitarbeitervertretung oder Handlungen einzelner Betriebsratsmitglieder bzw. des DSB beruhen.

3. Haftung von DSB und BR

Da aber die Mitarbeitervertretung und der im Beschäftigtenverhältnis tätige betriebliche und behördliche DSB nach Willen des Gesetzgebers⁸⁹ und trotz ihrer Sonderstellung wohl „Teil der verantwortlichen Stelle“ sein sollen, stellt sich die Frage, ob der Verantwortliche, d.h. der Arbeitgeber, für sie einstehen muss. Die Meinungen in der Literatur weisen fast alle denkbaren Haftungsmöglichkeiten auf.⁹⁰

So wird die Haftung des Datenschutzbeauftragten im Verhältnis zu der ihn benennenden Stelle entgegen verbreiteter Auffassung⁹¹ sogar regelmäßig schon dem Grunde nach abgelehnt, da sein Schutzauftrag primär gegenüber dem Betroffenen, nicht dem Verantwortlichen bestehe.⁹² Eine mögliche Haftung gegenüber Beschäftigten nach § 823 Abs. 1 und 2 BGB u.a. wegen Verletzung des Art. 39 DS-GVO als Schutznorm ist jedoch nicht auszuschließen.⁹³

Ähnlich sieht es bei der Beurteilung der Haftung der Mitarbeitervertretung bzw. einzelner Mitglieder des Gremiums aus, sofern sie Fehlentscheidungen zum Nachteil des Beschäftigten in Ausübung ihrer Funktion treffen.

Auch hier können nur der Arbeitgeber und einzelne Betriebsratsmitglieder beim Datenschutzexzess nach § 823 Abs. 1 und 2 BGB (so. z.B. bei der Vermarktung von Mitarbeiterdaten), nicht aber der Betriebsrat selbst für Datenschutzverstöße des Betriebsrats haften.⁹⁴ Für derartige „Grenzüberschreitungen“ gelten jedoch hohe Anforderungen.⁹⁵

4. Sanktionen gegen BR oder DSB

Da die Mitarbeitervertretung und ebenfalls der DSB keine „Verantwortliche“ sind, scheidet die Möglichkeit der Aufsichtsbehörde zur Verhängung von Sanktion bei Nichtbeachtung der gemeinsamen Kontrollpflichten aus.

Adressaten des ein Bußgeld nach Abs. 4, 5 und 6 des Art. 83 DS GVO verhängenden Verwaltungsakts sind ausschließlich Verantwortliche und Auftragsdatenverarbeiter. Die tatsächlichen handelnden Personen sind irrelevant, wenn sie einer der genannten Stellen zuzurechnen sind.⁹⁶

VI. Zusammenfassendes Ergebnis

Mitarbeitervertretungen und Datenschutzbeauftragte haben im Bereich des Beschäftigtendatenschutzes den gleichen Kontroll- und Schutzauftrag gegenüber dem

Verantwortlichen in seiner Funktion als Arbeitgeber, der sich jeweils auch auf die Datenverarbeitungen der „anderen“ Seite erstreckt, d.h. dem DSB steht auch ein Kontrollrecht hinsichtlich der personenbezogenen Datenverarbeitungen der Mitarbeitervertretung zu, wie diese im Rahmen ihrer Pflicht zur Überwachung der ordnungsgemäßen Umsetzung der DS-GVO darauf zu achten hat, dass der DSB seinen Schutzpflichten im Bereich des Beschäftigtendatenschutzes nachkommt.

Diese Überwachungsbefugnis darf nicht die daneben bestehende Pflicht zur Kooperation und gegenseitigen Unterstützung überlagern. Die Pflicht ist nunmehr eigenständig geregelt.

Der Beauftragte kann die Beratung des Betriebsrats auch außerhalb der Funktion als sachverständiger Arbeitnehmer im Rahmen seines Sicherstellungsauftrags und als „Anwalt der Betroffenen“ auch ohne Weisung oder Genehmigung des Arbeitgebers wahrnehmen.

Verarbeitet die Mitarbeitervertretung sensible Daten, hat sie besondere Schutzmaßnahmen zu ergreifen. Hierbei ist im Rahmen der gebotenen Zusammenarbeit der Datenschutzbeauftragte beratend hinzuzuziehen. Der Arbeitgeber muss die Übermittlung sensibler Daten bei fehlendem – also vom DSB nicht gebilligtem – Sicherheitskonzept verweigern.



Prof. Peter Gola

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

88 Niedersachsen, load FAQ für Betriebsräte (Juni 20; <https://lfd.niedersachsen.de> > ... > faq-fur-betriebsrate-194163.

89 Vgl. vorstehend S. 311

90 Vgl. die ausführliche Zusammenstellung des Meinungsstands zur Betriebsratshaftung bei Möhle, Die datenschutzrechtliche Verantwortlichkeit des Betriebsrats, S. 162, f.

91 Bergt, in: Kühling/Buchner, DS-GVO Art. 37, Rn. 53; Pauly, in: Paal/Pauly, DS-GVO Art. 39, Rn. 12.

92 Jaspers/Reif, Heidelberger Kommentar, DS-GVO Art. 39, Rn. 25.

93 Jaspers/Reif, Heidelberger Kommentar, DS-GVO Art. 39, Rn. 26

94 Vgl. ausführlich bei Flink, Beschäftigtendatenschutz aus Aufgabe des Betriebsrats, S. 224 ff., S.238; Brahm/Möhle, Die Stellung des Betriebsrats unter das DS-GVO, ZD 2028, 570.

95 LfDI Niedersachsen, load FAQ für Betriebsräte (Juni 20; <https://lfd.niedersachsen.de> >...< fag-fur-betriebsrate-194163.

96 Berg, in: Kühling/Buchner, DS GVO, Art. 83, Rn 21.

Kurzbeiträge

DS-GVO: Wer trägt die Kosten einer anlasslosen Inspektion bei einem Auftragsdatenverarbeiter?

Die Sichtweise des BayLfd auf wirtschaftliche Fragen hat sich geändert

Thomas Söbbing*

War der Bayerische Landesbeauftragte für den Datenschutz (BayLfd) in der Vergangenheit noch der Auffassung, dass der Auftragnehmer einer Auftragsdatenverarbeitung nach Art. 28 DS-GVO die Kosten für ein anlassloses Audit tragen muss, so vertritt er die Sichtweise in dieser Form nicht mehr. Grundsätzlich hat er sich nun der Sichtweise des Europäischen Datenschutzausschusses angeschlossen, wonach die wirtschaftliche Gestaltung der Austauschbeziehung zwischen dem Verantwortlichen und dem Auftragsverarbeiter durch den Markt und nicht durch die Datenschutz-Grundverordnung reguliert wird.

In der Vergangenheit wurde der BayLfd gerne von Verantwortlichen zitiert, wenn es um die Kosten für anlassloses Audit beim Auftragsdatenverarbeiter ging entfällt zukünftig diese Argumentationsgrundlage.

Früher vertrat der BayLfd die Ansicht,¹ wonach keine gesonderte Entgeltspflicht für die Wahrnehmung von Kontrollrechten beim Auftragsverarbeiter vereinbart werden darf. Denn die Wahrnehmung der Kontrollrechte des Auftraggebers aus datenschutzrechtlicher Sicht soll nicht von einem besonderen Entgelt abhängig gemacht werden. Dies gilt gerade auch für Vor-Ort-Kontrollen beim Auftragsverarbeiter. Ein gesondertes Entgelt würde einer Ausübung der Kontrollrechte entgegenwirken. Die Vereinbarung eines Entgelts, einer Aufwandsentschädigung oder eines sonstigen Kostenbeitrags – auch die Vereinbarung, hierzu im Bedarfsfall nachträglich eine die Auftragsverarbeitungsvereinbarung ergänzende Regelung zu treffen – führt dazu, dass eine Inspektion beim Auftragsverarbeiter als etwas „Außergewöhnliches“ wahrgenommen wird, das dem Auftraggeber „eigentlich“ nicht zusteht und gerade deshalb außerhalb der wechselseitigen Austauschbeziehung zu vergüten ist. Davon abgesehen, kann ein solches Entgelt entweder auf Grund seiner bereits erkennbaren (absoluten) Höhe oder der vertraglich angelegten Unklarheit seiner Berechnung abschreckende Wirkung entfalten. Diese Sichtweise wurde in der Literatur erheblich wegen der Verletzung der Vertragsfreiheit kritisiert² und stand auch im Gegensatz zur Sichtweise des Bayerischen Landesamts für Datenschutzaufsicht: Auf die Frage „Darf ein Auftragsverarbeiter für Kontrollmaßnahmen des Auftraggebers Extrakosten verlangen?“ antwortete die Behörde: „Die Preisgestaltung für DV-Dienstleistungen nach Art. 28 DS-GVO ist eine primär zivilrechtliche Frage des Vertragsverhältnisses und, solange kein Rechtsmissbrauch vorliegt, Sache der Vertragspartner.“³

Nun hat der BayLfd seine Ansicht erfreulicherweise geändert⁴ und schließt sich der Auffassung des Europäischen Datenschutzausschusses an. So hat der Europäische Datenschutzausschuss bereits im Juli 2021 nach öffentlicher Konsultation die überarbeiteten Leitlinien 7/2020 zu den Begriffen des Verantwortlichen und des Auftragsverarbeiters in der DS-GVO veröffentlicht, in denen zur Frage einer Entgeltspflicht für Kontrollen bei der Auftragsverarbeitung die folgenden Erwägungen neu aufgenommen wurden.⁵

„Die Frage der Kostenverteilung zwischen einem Verantwortlichen und einem Auftragsverarbeiter im Zusammenhang mit Überprüfungen fällt nicht unter die DS-GVO und unterliegt wirtschaftlichen Erwägungen. Artikel 28 Absatz 3 Buchstabe h sieht jedoch vor, dass der Vertrag den Auftragsverarbeiter verpflichtet, dem Verantwortlichen alle erforderlichen Informationen zur Verfügung zu stellen, und dass er verpflichtet ist, Überprüfungen einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen vom Verantwortlichen beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen. In der Praxis bedeutet dies, dass die Vertragsparteien keine Klauseln vereinbaren sollten, die die Zahlung eindeutig unangemessen oder unverhältnismäßig hoher Kosten und Gebühren zum Gegenstand haben und dadurch eine abschreckende Wirkung auf eine der Parteien ausüben würden. Solche Klauseln würden in der Tat bedeuten, dass die in Artikel 28 Absatz 3 Buchstabe h festgelegten Rechte und Pflichten in der Praxis nie ausgeübt würden und rein theoretisch wären, obwohl sie integraler Bestandteil der Datenschutzgarantien nach Artikel 28 DS-GVO sind.“

Der Europäische Datenschutzausschuss weist auch neuerdings nach der Ansicht des BayLfd zutreffend darauf hin,

* Prof. Dr. Thomas Söbbing, LL.M. lehrt Zivilrecht mit dem Recht der Digitalen Wirtschaft an der Hochschule Kaiserslautern.

1 Aktuelle Kurz-Information 6 in der Fassung vom 01.08.2018: Keine gesonderte Entgeltspflicht für Kontrollen bei der Auftragsverarbeitung“, <https://www.datenschutz-bayern.de/datenschutzreform2018/aki06.html>, abgerufen am 15.07.2021.

2 Söbbing, DB 2021, DSB 2021, 308.

3 <https://www.lda.bayern.de/de/faq.html>, abgerufen am 16.07.2021.

4 Aktuelle Kurz-Information 6 des BayLfd: Entgeltspflicht für Kontrollen bei der Auftragsverarbeitung?, Stand: 15.11.2021.

5 European Data Protection Board, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, Version 2.0, angenommen am 07.07.2021, Nr. 145, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de, abgerufen am 16.08.2022.

dass die wirtschaftliche Gestaltung der Austauschbeziehung zwischen dem Verantwortlichen und dem Auftragsverarbeiter durch den Markt und nicht durch die DS-GVO reguliert wird.⁶ Dies bedeutet jedoch nach der Ansicht des BayLFD auch, dass es dem Verantwortlichen unbenommen ist, ihm unterbreitete Angebote von Auftragsverarbeitern auf ihre Datenschutzfreundlichkeit zu prüfen und diesen Gesichtspunkt bei der Auswahl des Vertragspartners zu berücksichtigen.⁷ Der Verantwortliche wird zudem entsprechende Vorgaben in einen Ausschreibungstext aufnehmen können, wenn die benötigte Leistung in einem Vergabeverfahren beschafft wird.⁸ Dies ändert aber nichts daran, dass die Hoheit über die kommerziellen Aspekte einer Auftragsverarbeitungsvereinbarung (AVV) in den Händen der Vertragsparteien liegen und hierzu maximal Rahmenbedingungen als Empfehlungen genannt werden dürfen. Denn nach der ständigen Rechtsprechung des Bundesverfassungsgerichts ist die Vertragsfreiheit die Ausprägung des Grundsatzes der Privatautonomie im deutschen Zivilrecht, die es jedermann gestattet, Verträge abzuschließen, die sowohl hinsichtlich des Vertragspartners als auch des Vertragsgegenstandes frei bestimmt werden können. Dies gilt, sofern sie nicht gegen zwingende Vorschriften des geltenden Rechts, gesetzliche Verbote oder die guten Sitten verstoßen,⁹ und solche zwingenden Vorschriften sieht die DS-GVO nicht vor.¹⁰

Die Bedenken des Europäischen Datenschutzausschusses, dass die Kosten oder Gebühren Maßnahmen des Verantwortlichen nach Art. 28 Abs. 3 Satz 2 Buchst. h DS-GVO behindern können,¹¹ sind dabei auf jeden Fall ernst zu nehmen, ändern aber nichts an der grundsätzlichen Vertragshoheit der Parteien.

Die Bedenken des BayLFD, dass ein gesondertes Entgelt einer Ausübung der Kontrollrechte entgegenwirken würde, ändert ebenfalls nichts an der grundsätzlichen Vertragsfreiheit.¹² Allerdings ist auch hier die Sichtweise des BayLFD zu beachten, dass die Vereinbarung eines Entgelts, einer Aufwandsentschädigung oder eines sonstigen Kostenbeitrags für eine Inspektion den Eindruck erweckt, als sei ein solches Audit etwas, das über die vereinbarte Geschäftsbeziehung hinausgeht und gerade deshalb außerhalb der wechselseitigen Austauschbeziehung zu vergüten ist.¹³ Dabei sollte es nicht dazu kommen, dass ein solches Entgelt entweder auf Grund seiner bereits erkennbaren (absoluten) Höhe oder der vertraglich angelegten Unklarheit seiner Berechnung abschreckende Wirkung entfalten.¹⁴

Der BayLFD äußert sich auch zur Unverhältnismäßigkeit der Kosten für ein anlassloses Audit. Ob nach der Ansicht des BayLFD eine Klausel für Maßnahmen nach Art. 28 Abs. 3 Satz 2 Buchst. h DS-GVO ein eindeutig unverhältnismäßiges oder überhöhtes Entgelt vorsieht, das auf den Verantwortlichen eine abschreckende Wirkung hat, ist stets in Anbetracht der Umstände des Einzelfalls zu würdigen.¹⁵ Eine abschreckende Wirkung sollte aber nicht vorliegen, wenn der Auftragsverarbeiter eine angemessene Taxe verlangt, wie sie z.B. das Gesetz in § 612 Abs. 2 BGB oder § 632 Abs. 2 BGB vorsieht. So sieht es in gewisser Weise auch der BayLFD, da er zu Recht sagt, dass ein eindeutig überhöhtes Entgelt insbesondere dadurch erkennbar ist, dass der tat-

sächliche Aufwand beim Auftragsverarbeiter zu den vereinbarten Kosten oder Gebühren in einem grob unangemessenen Verhältnis steht (so etwa bei „Fantasiepreisen“ für den Einsatz personeller oder sachlicher Ressourcen oder bei der Erhebung von Kontrollgebühren, denen der Auftragsverarbeiter einen Aufwand nicht plausibel zuordnen kann).¹⁶ Diese Fantasiepreise würden sicherlich nicht den zitierten gesetzlichen Regelungen entsprechen, und ein pauschales Verlangen von Kontrollgebühren würden auch nicht dem zivilrechtlichen Modell eines synallagmatischen Vertrages entsprechen.¹⁷

Auch ist der Auftragsverarbeiter immer noch ein Wirtschaftsunternehmen und keine Non-Profit-Organisation; deshalb kann er für seine Leistungen eine angemessene Vergütung verlangen. Wird eine angemessene Vergütung schon als unverhältnismäßig angesehen, so scheint dem Verantwortlichen nicht klar zu sein, dass es die Maßnahmen zum Datenschutz nicht umsonst gibt.

Auch führt der Gedanke an eine Pauschale für alle anlasslosen Audits nicht zum gewünschten Ziel, denn der Auftragsverarbeiter kann, wie bei allen pauschal vereinbarten Beträgen, nur sehr schwer abschätzen, wie hoch der Aufwand und die Kosten für den jeweiligen Kunden im Vorfeld sein könnten.¹⁸

Nach der Ansicht des BayLFD kann ein Fall eindeutiger Unverhältnismäßigkeit insbesondere vorliegen, wenn die während der Vertragsdauer für Maßnahmen nach Art. 28 Abs. 3 Satz 2 Buchst. h DS-GVO erwartbaren Kosten oder Gebühren die Gestalt der vom Verantwortlichen zu erbringenden Hauptleistung wesentlich verändern.¹⁹ Hierbei ist sicherlich über den Begriff „wesentlich“ zu diskutieren. Aber die grundsätzliche Sichtweise des BayLFD ist dabei absolut richtig, insbesondere für den Fall, dass die Vorgabe aus Art. 28 Abs. 3 Satz 2 Buchst. h DS-GVO dadurch nicht mehr erfüllt wird.

Im weiteren Verlauf der Kurz-Information weist der BayLFD zu Recht darauf hin, dass seine Empfehlung nur für bayerische öffentliche Stellen gelten.²⁰ Oft wurde in der Praxis die Sichtweise des BayLFD auch für private Unterneh-

6 Aktuelle Kurz-Information 6 des BayLFD: Entgeltspflicht für Kontrollen bei der Auftragsverarbeitung?, Stand: 15.11.2021.

7 Aktuelle Kurz-Information 6 des BayLFD: Entgeltspflicht für Kontrollen bei der Auftragsverarbeitung?, Stand: 15.11.2021.

8 Aktuelle Kurz-Information 6 des BayLFD: Entgeltspflicht für Kontrollen bei der Auftragsverarbeitung?, Stand: 15.11.2021.

9 BVerfGE 8, 274 – Rn. 212, BVerfGE 95, 267 – Rn. 142.

10 Söbbling, DB 2021, DSB 2021, 308.

11 European Data Protection Board Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, Version 2.0, angenommen am 07.07.2021.

12 Söbbling, DB 2021, DSB 2021, 308.

13 Aktuelle Kurz-Information 6 des BayLFD in der Fassung vom 01.08.2018.

14 Aktuelle Kurz-Information 6 des BayLFD in der Fassung vom 01.08.2018.

15 Aktuelle Kurz-Information 6 des BayLFD in der Fassung vom 01.08.2018.

16 Aktuelle Kurz-Information 6 des BayLFD in der Fassung vom 01.08.2018.

17 BGH, NJW 2000, 3046.

18 Söbbling, DB 2021, DSB 2021, 308.

19 Aktuelle Kurz-Information 6 des BayLFD in der Fassung vom 01.08.2018.

20 Aktuelle Kurz-Information 6 des BayLFD in der Fassung vom 01.08.2018.

men und auch außerhalb von Bayern als verbindlich angesehen. Dies hat der BayLfD in seiner Information nun noch einmal richtiggestellt, obwohl sich dies bereits aus seiner Aufgabenstellung ergibt.²¹

Fraglich sollte dagegen sein, ob die Vertragsparteien bereits im Vorfeld eine Aufwandsprognose erstellen können, wie sie der BayLfD empfiehlt. Gegebenenfalls wäre denkbar, dass man generell eine konkrete Zahl anlassloser Audits im Jahr im AVV vereinbart und dafür eine feste Vergütung vorsieht. Richtig ist auch, dass dafür entsprechende Mittel im Haushalt der jeweiligen Behörde zu berücksichtigen sind.

III. Resümee

Sehr zu begrüßen ist, dass der BayLfD – wie schon immer das Bayerische Landesamts für Datenschutzaufsicht –, nun

auch der Auffassung ist, dass die Vergütung für anlasslose Audits von den Vertragsparteien unter den Aspekt der Vertragsfreiheit zu vereinbaren sind.

Die Empfehlung, eine angemessene Vergütung zu vereinbaren, ist richtig und Fantasiepreise für die Vergütung von Audits zu verlangen, würde nicht den Rechtsgedanken der § 612 Abs. 2 BGB oder § 632 Abs. 2 BGB entsprechen. Eine generelle Kontrollgebühr zu verlangen ohne dass eine konkrete Gegenleistung damit verbunden ist, würde ebenfalls nicht dem zivilrechtlichen Modell eines synallagmatischen Vertrages entsprechen. Auch sind die weiteren Empfehlungen des BayLfD durchaus als vernünftig und richtig anzusehen, wenn auch nicht immer im Absolutum.

²¹ <https://www.datenschutz-bayern.de/ODSP.htm>, abgerufen am 16.08.2022.

Aus den Berichten und Informationen der Aufsichtsbehörden (63): GPS-Ortung von Beschäftigten (27. Tätigkeitsbericht der LfDI Niedersachsen (2021) vom 03.09.2022

Zusammengestellt von Prof. Peter Gola*

Unter Ziffer 6.5 ihres Berichts für das Jahr 2021 beurteilt die LfDI Niedersachsen die GPS-Ortung von Beschäftigten als häufig rechtswidrig, weil sie für die verfolgten Ziele nicht erforderlich ist.

Dazu stellt sie zunächst fest: „Im Rahmen eines bestehenden Arbeitsvertrages dürfen Arbeitgeberinnen und Arbeitgeber Beschäftigtendaten nach § 26 Absatz 1 Satz 1 des Bundesdatenschutzgesetzes (BDSG) unter zwei Voraussetzungen verarbeiten:

1. Die Verarbeitung der Beschäftigtendaten muss grundsätzlich für den Zweck „Durchführung des Beschäftigungsverhältnisses“ erfolgen, mit anderen Worten für die „Erfüllung des jeweiligen Arbeitsvertrages“.

2. Darüber hinaus muss die Verarbeitung der konkreten Beschäftigtendaten für diesen Zweck erforderlich sein.

Unter den Begriff „verarbeiten“ fallen laut der Definition in Artikel 4 Nummer 2 der Datenschutz-Grundverordnung (DS-GVO) unter anderem die Erhebung und Nutzung von Beschäftigtendaten. Hierzu zählt auch die Erhebung und Nutzung mittels GPS erhobener Positionsdaten von Beschäftigten.“

Sodann geht die LfDI auf die für die Datenerfassung benötigte Erlaubnisnorm ein: „Die unternehmerische Freiheit erlaubt es Arbeitgeberinnen und Arbeitgebern im Rahmen ihres Weisungsrechts, gegenüber den Beschäftigten die Art und Weise der Erbringung der jeweiligen Arbeitsleistung, also Arbeitsabläufe, zu bestimmen. Folglich dürfen sie

grundsätzlich die für die Gestaltung von Arbeitsabläufen erforderlichen Beschäftigtendaten erheben und nutzen.“

Damit ist im konkreten Fall die im Rahmen einer Interessenabwägung festzustellende Erforderlichkeit zu statuieren.

Arbeitgeber geben häufig an, mittels der GPS-Ortung ihrer Beschäftigten Arbeitsabläufe bestimmen zu wollen oder aber berechnete Interessen zu verfolgen, unter anderem: Tourenplanung, Mitarbeiterinsatz, präventiver Diebstahlschutz für die eingesetzten Firmenfahrzeuge oder zum Nachweis für geleistete Tätigkeiten gegenüber Vertragspartnern.

Jedoch soll die GPS-Ortung von Beschäftigten in der Regel nach Auffassung der LfDI hierfür nicht erforderlich sein. Die LfDI verweist dazu auf das Urteil des VG Lüneburg vom 19. März 2019 (Az. 4 A 12/19), das mit Beschluss des OVG Lüneburg vom 3. April 2020 (Az. 11 LA 154/19) rechtskräftig wurde.

Demnach gilt: In der Regel ist eine GPS-Ortung von Beschäftigten nicht aufgrund von berechtigten Interessen von Arbeitgebern möglich. Auch wenn Diebstahlschutz sowie eine Beweisführung gegenüber Vertragspartnern berechnete Interessen darstellen, ist eine fortlaufende GPS-Ortung der Beschäftigten nicht geeignet, Diebstähle zu verhindern. Die in der Vergangenheit erhobenen Positionsdaten der Beschäftigten können nicht dazu führen, die aktuelle Position

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

des Täters zu bestimmen. Daher würde es ausreichen, die GPS-Ortung erst nach einem Diebstahl zu aktivieren. Weiter würde durch die GPS-Ortung der Beschäftigten gegenüber Vertragspartnern nicht nachgewiesen, dass eine Leistung tatsächlich erbracht worden ist, sondern allenfalls, dass ein Beschäftigter sich möglicherweise am Leistungsort befand.

Sodann erörtert die LfDI, wann eine Ortung mit Einwilligung der Beschäftigten stattfinden kann. Um rechtswirksam zu sein, muss diese Einwilligung aber freiwillig erteilt worden sein. Tatsächlich freiwillig soll eine Einwilligung aber selten sein, weil hier ein Über- und Unterordnungsverhältnis herrsche. Beschäftigte willigen häufig nicht freiwillig ein, sondern weil sie andernfalls Nachteile befürchten. Andererseits könne von einer Freiwilligkeit der Einwilligung eines Beschäftigten ausgegangen werden, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person

gleichgelagerte Interessen verfolgen (§ 26 Absatz 2 Satz 2 BDSG). Diese Indizien seien jedoch häufig nicht gegeben.

Die Freiwilligkeit und damit Rechtswirksamkeit einer Einwilligung von Beschäftigten in die Verarbeitung ihrer Positionsdaten nimmt die LfDI zum Beispiel dann an, wenn den Beschäftigten hierfür ein Vorteil, wie die private Nutzung der Firmenfahrzeuge, gewährt worden ist und weitere Indizien für die Freiwilligkeit der Einwilligung in die Datenverarbeitung vorlagen, zum Beispiel wenn die Beschäftigten die Möglichkeit hatten, das am Firmenfahrzeug angebrachte GPS-Ortungsgerät selbständig auszuschalten. Können Arbeitgeber nicht belegen, dass eine Einwilligung freiwillig erteilt wurde, bleibt die Verarbeitung der Beschäftigtendaten rechtswidrig. Zudem müssen Einwilligungen im Beschäftigtenverhältnis schriftlich erteilt werden und formellen Ansprüchen genügen (§ 26 Abs. 2 S. 3 und 4 BDSG).

Praxisfälle zum Datenschutzrecht XIX: Sonderkonditionen für Auszubildende bei Versicherungsunternehmen aus dem Konzernverbund

RAin Yvette Reif, LL.M.*

I. Sachverhalt

Die mit der X-Bank konzernverbundene Y-Versicherung schlägt der Bank vor, dass diese ihr künftig jährlich Namen und Anschriften der neu eingestellten Auszubildenden mitteilen solle, damit die Versicherung die Auszubildenden von X per Briefpost anschreiben, diese über relevante Produkte informieren und ihnen den für eigene Mitarbeiter der Versicherung üblichen Rabatt i.H.v. 25 % anbieten kann. Kann die Bank dem Wunsch der Versicherung nachkommen?

Abwandlung:

Der Betriebsrat hat keine Bedenken, dass alle Auszubildenden das im Ausgangsfall geschilderte Angebot direkt von der Versicherung erhalten. Daher stimmt der Betriebsrat der Weitergabe der Anschriften aller Auszubildenden in einer Betriebsvereinbarung zu. Ändert sich hierdurch die Beurteilung des Sachverhalts?

II. Musterlösung des Ausgangsfall

1. Kein Konzernprivileg

Nach Erwägungsgrund 40 DS-GVO brauchen personenbezogene Datenverarbeitungen, wozu nach der Legaldefinition der Verarbeitung in Art. 4 Nr. 2 DS-GVO auch die Weitergabe

personenbezogener Daten zählt, um zulässig zu sein, einer entsprechenden Rechtsgrundlage (sog. Verbot mit Erlaubnisvorbehalt). Ein „Konzernprivileg“ kennt die DS-GVO insoweit nicht. Selbstständige juristische Einheiten innerhalb eines Konzerns sind datenschutzrechtlich grundsätzlich als eigenständige verantwortliche Stellen i.S.v. Art. 4 Nr. 7 DS-GVO anzusehen, und Datenflüsse zwischen diesen bedürfen der Legitimation durch eine Rechtsgrundlage.

2. Durchführung des Beschäftigungsverhältnisses als mögliche Rechtsgrundlage

Als Rechtsgrundlage der Weitergabe der Auszubildendendaten ist zunächst § 26 Abs. 1 S. 1 BDSG zu prüfen. Nach der genannten Bestimmung personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die

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

1 Gola, Handbuch Beschäftigtendatenschutz, 8. Aufl., Rn. 752 ff.; LfDI BW, Ratgeber Beschäftigtendatenschutz, Stand: April 2020 (4. Aufl.), S. 59 f.

Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Festzustellen ist insofern zunächst, dass nach dem weiten Beschäftigtenbegriff des § 26 Abs. 8 BDSG auch „zu ihrer Berufsbildung Beschäftigte“ Beschäftigte i.S.d. BDSG darstellen, § 26 Abs. 8 Nr. 2 BDSG. Mangels konkreten Bezugs der Datenweitergabe zum Ausbildungsverhältnis sind allerdings die Voraussetzungen des § 26 Abs. 1 S. 1 BDSG nicht gegeben. Die Vermittlung vergünstigter Versicherungen gehört nicht zu den Pflichten oder Rechten des Arbeitgebers aus dem Ausbildungsvertrag. Die Datenweitergabe an die Y-Versicherung ist damit nicht i.S.v. § 26 Abs. 1 S. 1 BDSG zur Durchführung des Beschäftigungsverhältnisses erforderlich.

3. Interessenabwägung

Es entspricht herrschender Meinung, dass Verantwortliche im Hinblick auf die Verarbeitung von Beschäftigtendaten für sog. „beschäftigungsfremde Zwecke“, wie sie vorliegend mit der Datenweitergabe an die Y-Versicherung verfolgt werden, potenziell auf Art. 6 Abs. 1 lit. f DS-GVO als Rechtsgrundlage zurückgreifen dürfen.¹ Die genannte Bestimmung gestattet die Verarbeitung personenbezogener Daten, sofern diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (sog. Interessenabwägung).

Als berechtigtes Interesse kommt hier einerseits das werbliche Interesse der Y-Versicherung, andererseits aber auch das Interesse der X-Bank in Betracht, ihren Auszubildenden als Maßnahme der Mitarbeiterbindung die Möglichkeit zu bieten, innerhalb des Konzerns Versicherungen zu vergünstigten Konditionen abzuschließen. Diese Interessen stellen unzweifelhaft berechnete Interessen i.S.v. Art. 6 Abs. 1 lit. f DS-GVO dar. Den Umstand, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann, statuiert Erwägungsgrund 47 S. 7 DS-GVO sogar explizit. Dies gilt – jedenfalls im Grundsatz – auch für personenbezogene Datenverarbeitungen für Werbezwecke Dritter, denn nach Art. 6 Abs. 1 lit. f DS-GVO sind neben berechtigten Interessen des Verantwortlichen auch entsprechende Interessen Dritter berücksichtigungsfähig.

Keine Hilfe bietet im vorliegenden Fall hingegen Erwägungsgrund 48 DS-GVO. Zwar nennt Erwägungsgrund 48 DS-GVO Konzerninteressen explizit als potenzielle berechnete Interessen i.S.v. Art. 6 Abs. 1 lit. f DS-GVO, beschränkt dies aber auf Verarbeitungen im Zusammenhang mit sog. „internen Verwaltungszwecken“. Eine Privilegierung der Interessen anderer Konzernunternehmen oder der Unternehmensgruppe insgesamt – als Konzerninteresse – ist folglich nicht

bezweckt.² Der Erwägungsgrund hat primär die Zentralisierung bestimmter Funktionen innerhalb großer Organisationen vor Auge,³ wie z.B. eine zentrale Kreditoren-/Debitorenstammdatenverwaltung. Datenverarbeitungen im Zusammenhang mit der Werbung für Produkte anderer Konzernunternehmen lassen sich nicht auf Erwägungsgrund 48 DS-GVO stützen.⁴

Im Hinblick auf die festgestellten berechtigten Interessen an der Werbung (Y-Versicherung) bzw. an der Mitarbeiterbindung (X-Bank) bleibt zu prüfen, ob nicht ggf. die Interessen der betroffenen Auszubildenden an einem Unterbleiben der Datenweitergabe an Y überwiegen. Hierfür spricht, dass Auszubildende grundsätzlich erwarten dürfen, nicht mithilfe ihres Arbeitgebers zum Werbeobjekt Dritter zu werden. Das schutzwürdige Interesse der Auszubildenden, dass der Arbeitgeber ihre Daten regelmäßig nur für Zwecke des Beschäftigungsverhältnisses verwendet und nicht Dritten für deren kommerzielle Interessen zur Verfügung stellt, dürfte die dargestellten berechtigten Interessen von Arbeitgeber und Versicherung an einer Datenweitergabe überwiegen.

Hiergegen kann auch nicht wirksam eingewandt werden, dass es durchaus dem Interesse eines Teils des Auszubildenden entsprechen mag, über die Angebote der Y-Versicherung und die Sonderkonditionen informiert zu werden. Dies mag zwar zutreffen, eine entsprechende Information der Auszubildenden kann aber auch ohne Weitergabe der Adressdaten an Y erreicht werden, so dass es insofern an einer Erforderlichkeit i.S.v. Art. 6 Abs. 1 lit. f DS-GVO fehlt. Denkbar ist etwa ein Auslegen bzw. Aushängen entsprechender Printinformationen im Ausbildungsbetrieb, was sogar gänzlich ohne Datenverarbeitung möglich ist, oder eine Information über das Intranet der X-Bank.

Denkbar erscheint auch, dass die X-Bank sich bereit erklärt, die Informationen zu den vergünstigten Versicherungen selbst per Brief an ihre Auszubildenden zu senden. Dies könnte etwa in der Form geschehen, dass Informationsmaterial der Versicherung etwaiger dienstlicher Post, z.B. der Lohn- und Gehaltsabrechnung, beige packt wird. Soweit insofern eine Verarbeitung personenbezogener Daten erfolgt,⁵ ist diese einfacher zu legitimieren als eine Datenweitergabe an die Versicherung. Bei der Möglichkeit, Sonderkonditionen in Anspruch nehmen zu können, handelt es sich, wie bereits ausgeführt, um eine Information, die Teile der Auszubildenden sicher gern erhalten wollen, und im Verhältnis zu der angedachten Datenweitergabe wäre eine rein interne Nutzung der Adressdaten durch X zur Versendung von Information der Versicherung deutlich weniger eingriffsinvasiv.

2 Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 1. Aufl. 2019, DS-GVO Art. 6 Abs. 1 Rn. 117.

3 Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 1. Aufl. 2019, DS-GVO Art. 6 Abs. 1 Rn. 117.

4 Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 1. Aufl. 2019, DS-GVO Art. 6 Abs. 1 Rn. 117.

5 Vgl. Gola/Heckmann/Schulz, DS-GVO/BDSG, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 81: „Ist die Beipack- oder Empfehlungswerbung an individuell ausgewählte Adressaten gerichtet, ist der Anwendungsbereich der DS-GVO eröffnet.“ Erfolgt das Beipacken über eine komplette Versandaktion ohne Rücksicht auf konkrete Empfänger, wird es an einer Verarbeitung personenbezogener Daten fehlen.

Der Belästigungseffekt der Beipackwerbung für nicht interessierte Auszubildende ist schließlich überschaubar.

Ergebnis: Eine Weitergabe der Auszubildendendaten an die Y-Versicherung kommt ohne Einwilligung der Auszubildenden nicht in Betracht, da weniger eingriffsinvasive Methoden zur Verfügung stehen, diese zu informieren.

4. Ergänzende Informationen zur Einwilligung

Aufgrund des typischerweise bestehenden Abhängigkeitsverhältnisses im Verhältnis zum Arbeitgeber bedürfen Einwilligungen im Zusammenhang mit Beschäftigungsverhältnissen einer besonderen Prüfung im Hinblick auf die Freiwilligkeit der Erklärung, vgl. § 26 Abs. 2 S. 1 und 2 BDSG. Dies gilt insbesondere im Hinblick auf Auszubildende, die häufig noch minderjährig, jedenfalls aber geschäftlich unerfahren und insoweit besonders schutzbedürftig sind. Dennoch kann auch einem/einer Beschäftigten nicht generell, vor allem nicht außerhalb der Bewerbungssituation, abgesprochen werden, eine freiwillige Entscheidung treffen zu können. Entscheidend ist stets der konkrete Einzelfall. Solange der Arbeitgeber keinen entsprechenden Druck aufbaut und eine Datenweitergabe ohne zu befürchtende negative Konsequenzen abgelehnt werden kann, ergäben sich etwa im vorliegenden Fall keine Bedenken bezüglich der Freiwilligkeit.

Sofern Beschäftigtendatenverarbeitungen auf eine Einwilligung gestützt werden sollen, sind die besonderen nationalen Formanforderungen an Einwilligungen von Beschäftigten zu beachten. Während die DS-GVO keine bestimmte Form für die Einwilligung vorsieht, sondern sogar ein konkludentes Handeln für ausreichend ansieht,⁶ verlangt § 26 Abs. 2 S. 3 BDSG, dass die Einwilligung durch Beschäftigte schriftlich oder elektronisch zu erfolgen hat, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Gemäß § 26 Abs. 2 S. 4 BDSG hat der Arbeitgeber die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 DS-GVO in Textform aufzuklären. Fraglich ist, ob mit „schriftlich“ und „elektronisch“ die Schriftform gemäß § 126 BGB bzw. die elektronische Form gemäß § 126a BGB gemeint ist.⁷ Zum Teil wird vertreten, dass § 26 Abs. 2 S. 3 BDSG von einem eigenen Schriftlichkeitsbegriff ausgeht, der die Nachweispflicht des Verantwortlichen bezweckt.⁸

III. Abwandlung: Betriebsvereinbarung als Grundlage der Datenweitergabe

Gemäß § 26 Abs. 4 BDSG können Betriebsvereinbarungen grundsätzlich einen datenschutzrechtlichen Erlaubnistatbestand darstellen: „Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig.“ Eine Betriebsvereinbarung ist eine Kollektivvereinbarung i.S.v. § 26 Abs. 4 BDSG.

Vorliegend stellt sich allerdings die Frage nach der Wirksamkeit der Betriebsvereinbarung. Dies gilt zum einen hin-

sichtlich der Zuständigkeit des Betriebsrats zur Regelung des fraglichen Sachverhalts. Denn die Weitergabe der Anschriften der Auszubildenden für die beschriebenen Zwecke liegt außerhalb der betrieblichen Sphäre. Der Abschluss von Versicherungen sowie vorhergehende diesbezügliche Kontakte und Angebote betreffen die private Sphäre der Auszubildenden.

Fraglich ist zum anderen, ob die Betriebsparteien wirksam eine Datenverarbeitung gestatten können, die nach den Regelungen von DS-GVO bzw. BDSG – wie zuvor festgestellt – nicht erlaubt wäre. Inwiefern per Betriebsvereinbarung vom Schutzstandard der DS-GVO abgewichen werden kann, ist im Detail umstritten.⁹ Für unzulässig erachtet es die herrschende Meinung jedenfalls, wenn die innerbetriebliche Regelung den Schutzstandard der DS-GVO unterschreitet.¹⁰ Möglich sind hingegen innerbetriebliche Regelungen, welche die geltenden Datenschutzvorgaben unter Beachtung des Verhältnismäßigkeitsprinzips für die betrieblichen Gegebenheiten konkretisieren.

Die hier zu beurteilende Betriebsvereinbarung nimmt den Auszubildenden die durch DS-GVO bzw. BDSG an sich vorgesehene Möglichkeit, selbst darüber bestimmen zu können, ob sie betreffende personenbezogene Daten an die Versicherung weitergegeben werden. Insofern kann von einer Konkretisierung bestehender Datenschutzvorgaben keine Rede sein. Vielmehr wird den betroffenen Auszubildenden im konkreten Fall ihr Recht auf informationelle Selbstbestimmung genommen.

Ergebnis: Die Betriebsvereinbarung ist unwirksam (§ 134 BGB) und kommt nicht als Rechtsgrundlage der konzerninternen Weitergabe der Auszubildendendaten in Betracht.

IV. Ergänzende Informationen zum Thema Betriebsvereinbarungen und Datenschutz

Betriebsvereinbarungen spielen in der Praxis eine zentrale Rolle zur Legitimation von Datenverarbeitungen im Beschäftigtenkontext. Dies liegt an den strukturellen Schwächen anderweitiger Instrumente zur Rechtfertigung von Beschäftigtendatenverarbeitungen, z.B. der freiwilligen und jederzeit widerruflichen Einwilligung, vor allem aber an der Doppelfunktion von Betriebsvereinbarungen zur Verarbeitung von Beschäftigtendaten: Denn der Abschluss von Betriebsvereinbarungen ist aufgrund der Mitbestimmungsrechte des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG oftmals unumgänglich, gleichzeitig liefern diese infolgedessen aber auch eine verlässliche datenschutzrechtliche Rechtfertigungsgrundlage für die Verarbeitung von Beschäftigtendaten.¹¹

6 Vgl. Art. 4 Nr. 11 DS-GVO: „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung“.

7 Hitzelberger-Kijima, öAT 2020, 133 (135).

8 Thüsing/Rombey, NZA 2019, 1399.

9 Vgl. hierzu auch Praxisfall XVIII: Videoüberwachung im Pausenraum, RDV 2022, 269 (271).

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

11 Klösel/Manhold, NZW 2017, 1425 (1428).



©BillionPhotos.com - stockadobe.com

GDD-BASIS-SCHULUNG TEIL 1

Einführung in den Datenschutz für die Privatwirtschaft

27.02.-03.03.2023 | Köln

Referenten: RA Andreas Jaspers, Thomas Mütthlein,
Prof. Dr. Rolf Schwartzmann

Schwerpunkte:

- ✓ Einführung in das Datenschutzrecht
- ✓ Arbeitnehmerdatenschutz
- ✓ Kundendatenschutz und Fallübungen
- ✓ Umsetzung des Datenschutzes in der Praxis

Jetzt anmelden: www.datakontext.com

Rechtsprechung

EuGH zu Bekanntmachungen nach der Geldwäscherichtlinie

(Europäischer Gerichtshof, Urteil vom 22. November 2022 – C-37/20 und C-601/20 –)

Die Bestimmung, dass die Angaben über die wirtschaftlichen Eigentümer von im Hoheitsgebiet der Mitgliedstaaten eingetragenen Gesellschaften in allen Fällen für alle Mitglieder der Öffentlichkeit zugänglich sein müssen, ist ungültig. Der mit dieser Maßnahme verbundene Eingriff in die durch die Charta gewährleisteten Rechte ist weder auf das absolut Erforderliche beschränkt noch steht er in einem angemessenen Verhältnis zum verfolgten Ziel

Aus der Pressemitteilung

Gemäß der Geldwäscherichtlinie¹ wurde durch ein im Jahr 2019 erlassenes luxemburgisches Gesetz² ein Register des *bénéficiaires effectifs* (Register der wirtschaftlichen Eigentümer) geschaffen. Dieses Gesetz sieht vor, dass eine Reihe von Informationen über die wirtschaftlichen Eigentümer der eingetragenen Einrichtungen in dieses Register aufgenommen und gespeichert werden. Zu einem Teil dieser Informationen hat die breite Öffentlichkeit Zugang, u. a. über das Internet. Ferner hat ein wirtschaftlicher Eigentümer nach diesem Gesetz die Möglichkeit, bei Luxembourg Business Registers (LBR), dem Verwalter des Registers, zu beantragen, den Zugang zu solchen Informationen in bestimmten Fällen zu beschränken.

In diesem Zusammenhang wurden beim Bezirksgericht Luxemburg Klagen von einer luxemburgischen Gesellschaft und dem wirtschaftlichen Eigentümer einer solchen Gesellschaft eingereicht, die erfolglos bei LBR beantragt hatten, den Zugang der breiten Öffentlichkeit zu den sie betreffenden Informationen zu beschränken. Dieses Gericht vertrat die Ansicht, dass die Verbreitung solcher Informationen ein unverhältnismäßiges Risiko einer Beeinträchtigung der Grundrechte der betroffenen wirtschaftlichen Eigentümer mit sich bringen könne, und stellte daher dem Gerichtshof eine Reihe von Vorlagefragen nach der Auslegung gewisser Bestimmungen der Geldwäscherichtlinie und zu deren Gültigkeit im Licht der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

Hierzu stellt der Gerichtshof (Große Kammer) die im Licht der Charta bestehende Ungültigkeit derjenigen Bestimmung der Geldwäscherichtlinie fest, nach der die Mitgliedstaaten in allen Fällen den Zugang aller Mitglieder der Öffentlichkeit zu den Informationen über die wirtschaftlichen Eigentümer der in ihrem Gebiet eingetragenen Gesellschaften oder anderen juristischen Personen sicherzustellen haben.

Nach Ansicht des Gerichtshofs stellt der Zugang aller Mitglieder der Öffentlichkeit zu den Informationen über die wirtschaftlichen Eigentümer einen schwerwiegenden Eingriff

in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten dar, die in den Art. 7 bzw. 8 der Charta verankert sind. Die verbreiteten Angaben ermöglichen es nämlich einer potenziell unbegrenzten Zahl von Personen, sich über die materielle und finanzielle Situation eines wirtschaftlichen Eigentümers Kenntnis zu verschaffen. Außerdem werden die möglichen Folgen einer etwaigen missbräuchlichen Verwendung ihrer personenbezogenen Daten für die betroffenen Personen dadurch verschärft, dass diese Daten, sobald sie der Öffentlichkeit zur Verfügung gestellt worden sind, nicht nur frei abgerufen, sondern auch auf Vorrat gespeichert und verbreitet werden können.

Allerdings möchte der Unionsgesetzgeber mit der fraglichen Maßnahme Geldwäsche und Terrorismusfinanzierung verhindern, indem er mittels erhöhter Transparenz ein Umfeld schafft, das weniger leicht für diese Zwecke genutzt werden kann. Nach Auffassung des Gerichtshofs verfolgt der Gesetzgeber somit eine dem Gemeinwohl dienende Zielsetzung, die selbst schwerwiegende Eingriffe in die in den Art. 7 und 8 der Charta verankerten Grundrechte zu rechtfertigen vermag; auch ist der Zugang aller Mitglieder der Öffentlichkeit zu den Informationen über die wirtschaftlichen Eigentümer zur Verwirklichung dieser Zielsetzung geeignet.

Der Gerichtshof stellt jedoch fest, dass der Eingriff, den diese Maßnahme mit sich bringt, weder auf das absolut Erforderliche beschränkt ist noch in einem angemessenen Verhältnis zur verfolgten Zielsetzung steht. Neben der Tatsache, dass die fraglichen Bestimmungen die öffentliche Zugänglichmachung von Daten gestatten, die weder hinreichend bestimmt noch identifizierbar sind, stellt die mit der Geldwäscherichtlinie eingeführte Regelung einen erheblich schwereren Eingriff in die in den Art. 7 und 8 der Charta verbürgten Grundrechte dar als die Vorgängerregelung (die neben dem Zugang der zuständigen Behörden und bestimmter Einrichtungen den Zugang aller Personen oder Organisationen vorsah, die ein berechtigtes Interesse nachweisen konnten), ohne dass diese zusätzliche Schwere durch etwaige Vorteile kompensiert würde, die sich aus der neuen Regelung im Vergleich zur früheren hinsichtlich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung ergeben könnten.

Insbesondere das von der Kommission geltend gemachte etwaige Vorliegen von Schwierigkeiten bei der genauen Bestimmung der Fälle und Bedingungen, in bzw. unter denen ein solch berechtigtes Interesse besteht, kann nicht rechtfertigen, dass der Unionsgesetzgeber den Zugang aller Mitglieder der Öffentlichkeit zu den fraglichen Informationen vorsieht.

Zudem hält der Gerichtshof die fakultativen Bestimmungen, die es den Mitgliedstaaten erlauben, die Bereitstellung der Informationen über die wirtschaftlichen Eigentümer von einer Online-Registrierung abhängig zu machen und für au-

Bergewöhnliche Umstände Ausnahmen vom Zugang aller Mitglieder der Öffentlichkeit zu diesen Informationen vorzusehen, als solche für weder geeignet, zu belegen, dass eine ausgewogene Gewichtung der dem Gemeinwohl dienenden Zielsetzung und der in den Art. 7 und 8 der Charta verankerten Grundrechte vorgenommen wurde, noch, dass hinreichende Garantien bestehen, die es den betroffenen Personen ermöglichen, ihre personenbezogenen Daten wirksam wahrzunehmen.

Zur Regelung einer allgemeinen und unterschiedslosen Speicherung der Verkehrsdaten durch die Anbieter von Diensten der elektronischen Kommunikation (Ls)

(Europäischer Gerichtshof (Große Kammer), Urteil vom 20. September 2022 – C-339/20 und C-397/20 –)

1. **Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003 über Insider-Geschäfte und Marktmanipulation (Marktmissbrauch) und Art. 23 Abs. 2 Buchst. g und h der Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission in Verbindung mit Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung und im Licht der Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union sind dahin auszulegen, dass sie einer gesetzlichen Regelung, die zur Bekämpfung von Straftaten des Marktmissbrauchs, u. a. von Insidergeschäften, präventiv eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrsdaten für ein Jahr ab dem Zeitpunkt der Speicherung vorsieht, entgegenstehen.**
2. **Das Unionsrecht ist dahin auszulegen, dass es dem entgegensteht, dass ein nationales Gericht die nach nationalem Recht zu treffende Feststellung, dass innerstaatliche Rechtsvorschriften, mit denen die Anbieter von Diensten der elektronischen Kommunikation zur allgemeinen und unterschiedslosen Vorratsspeicherung der Verkehrsdaten verpflichtet werden und nach denen solche Daten ohne vorherige Genehmigung durch ein Ge-**

richt oder eine unabhängige Behörde an die zuständige Finanzaufsichtsbehörde übermittelt werden können, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung im Licht der Charta der Grundrechte der Europäischen Union ungültig sind, in ihren zeitlichen Wirkungen beschränkt. Die Verwertbarkeit von Beweismitteln, die gemäß innerstaatlichen Rechtsvorschriften erlangt wurden, die unionsrechtswidrig sind, unterliegt nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten – vorbehaltlich der Beachtung u.a. der Grundsätze der Äquivalenz und der Effektivität – dem nationalen Recht.

BGH legt EuGH erneut Frage zur Klagebefugnis von Verbraucherschutzverbänden bei Datenschutzverstößen durch Facebook vor

(Bundesgerichtshof, Beschluss vom 10. November 2022 – I ZR 186/17 –)

Der Bundesgerichtshof ersucht den Europäischen Gerichtshof um die Vorabentscheidung, ob eine Rechtsverletzung „infolge einer Verarbeitung“ im Sinne von Art. 80 Abs. 2 DSGVO geltend gemacht wird, wenn ein Verband zur Wahrung von Verbraucherinteressen seine Klage darauf stützt, die Rechte einer betroffenen Person seien verletzt, weil die Informationspflichten gemäß Art. 12 Abs. 1 Satz 1 DSGVO in Verbindung mit Art. 13 Abs. 1 Buchst. c und e DSGVO über den Zweck der Datenverarbeitung und den Empfänger der personenbezogenen Daten nicht erfüllt worden seien.

Sachverhalt:

Der unter anderem für Wettbewerbsrecht zuständige I. Zivilsenat des Bundesgerichtshofs hat darüber zu entscheiden, ob ein Verstoß des Betreibers eines sozialen Netzwerks gegen die datenschutzrechtliche Verpflichtung, die Nutzer dieses Netzwerks über Umfang und Zweck der Erhebung und Verwendung ihrer Daten zu unterrichten, wettbewerbsrechtliche Unterlassungsansprüche begründet und von Verbraucherschutzverbänden verfolgt werden kann.

Die in Irland ansässige Beklagte, die Meta Plattform Ireland Limited (ehemals Facebook Ireland Limited), betreibt das soziale Netzwerk „Facebook“. Auf der Internetplattform dieses Netzwerks befindet sich ein „App-Zentrum“, in dem die Beklagte den Nutzern ihrer Plattform kostenlos Online-Spiele anderer Anbieter zugänglich macht. Im November 2012 wurden in diesem App-Zentrum mehrere Spiele angeboten, bei denen unter dem Button „Sofort spielen“ folgende Hinweise zu lesen waren: „Durch das Anklicken von ‚Spiel spielen, oben erhält diese Anwendung: Deine allgemeinen Informationen, Deine-Mail-Adresse, Über Dich, Deine Statusmeldungen. Diese Anwendung darf in deinem Namen posten, einschließlich dein Punktestand und mehr.“ Bei einem Spiel endeten die Hinweise

mit dem Satz: „Diese Anwendung darf Statusmeldungen, Fotos und mehr in deinem Namen posten.“

Der Kläger ist der in der Liste qualifizierter Einrichtungen nach § 4 UKlaG eingetragene Dachverband der Verbraucherzentralen der Bundesländer. Er beanstandet die Präsentation der unter dem Button „Sofort spielen“ gegebenen Hinweise im App-Zentrum als unlauter unter anderem unter dem Gesichtspunkt des Rechtsbruchs wegen Verstoßes gegen gesetzliche Anforderungen an die Einholung einer wirksamen datenschutzrechtlichen Einwilligung des Nutzers. Ferner sieht er in dem abschließenden Hinweis bei einem Spiel eine den Nutzer unangemessen benachteiligende Allgemeine Geschäftsbedingung. Er hält sich zur Geltendmachung von Unterlassungsansprüchen im Wege der Klage vor den Zivilgerichten gemäß § 8 Abs. 3 Nr. 3 UWG und § 3 Abs. 1 Satz 1 Nr. 1 UKlaG für befugt.

Bisheriger Prozessverlauf:

Der Bundesgerichtshof hat das Verfahren mit Beschluss vom 28. Mai 2020 (I ZR 86/17, GRUR 2020, 896 = WRP 2020, 1182 – App-Zentrum I) ausgesetzt und dem Gerichtshof der Europäischen Union die Frage zur Vorabentscheidung vorgelegt, ob die in Kapitel VIII, insbesondere in Art. 80 Abs. 1 und 2 sowie Art. 84 Abs. 1 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) getroffenen Bestimmungen nationalen Regelungen entgegenstehen, die – neben den Eingriffsbefugnissen der zur Überwachung und Durchsetzung der Verordnung zuständigen Aufsichtsbehörden und den Rechtsschutzmöglichkeiten der betroffenen Personen – einerseits Mitbewerbern und andererseits nach dem nationalen Recht berechtigten Verbänden, Einrichtungen und Kammern die Befugnis einräumen, wegen Verstößen gegen die Datenschutz-Grundverordnung unabhängig von der Verletzung konkreter Rechte einzelner betroffener Personen und ohne Auftrag einer betroffenen Person gegen den Verletzer im Wege einer Klage vor den Zivilgerichten vorzugehen.

Der Gerichtshof der Europäischen Union hat dazu mit Urteil vom 28. April 2022

C-319/20, GRUR 2022, 920 = WRP 2022, 684 – Meta Platforms Ireland) entschieden, dass Art. 80 Abs. 2 der VO (EU) 2016/679 einer nationalen Regelung, nach der ein Verband zur Wahrung von Verbraucherinteressen gegen den mutmaßlichen Verletzer des Schutzes personenbezogener Daten ohne entsprechenden Auftrag und unabhängig von der Verletzung konkreter Rechte betroffener Personen Klage mit der Begründung erheben kann, dass gegen das Verbot der Vornahme unlauterer Geschäftspraktiken, ein Verbraucherschutzgesetz oder das Verbot der Verwendung unwirksamer Allgemeiner Geschäftsbedingungen verstoßen worden sei, nicht entgegensteht, sofern die betreffende Datenverarbeitung die Rechte identifizierter oder identifizierbarer natürlicher Personen aus dieser Verordnung beeinträchtigen kann.

Die Entscheidung des Bundesgerichtshofs:

Der Bundesgerichtshof hat nach mündlicher Verhandlung vom 29. September 2022 das Verfahren erneut ausgesetzt und dem Gerichtshof der Europäischen Union die Frage zur Vorabentscheidung vorgelegt, ob eine Rechtsverletzung „infolge einer Verarbeitung“ im Sinne von Art. 80 Abs. 2 DSGVO geltend gemacht wird, wenn ein Verband zur Wahrung von Verbraucherinteressen seine Klage darauf stützt, die Rechte einer betroffenen Person seien verletzt, weil die Informationspflichten gemäß Art. 12 Abs. 1 Satz 1 DSGVO in Verbindung mit Art. 13 Abs. 1 Buchst. c und e DSGVO über den Zweck der Datenverarbeitung und den Empfänger der personenbezogenen Daten nicht erfüllt worden seien.

Die Notwendigkeit einer erneuten Vorlage ergibt sich aus folgenden Umständen: Der Senat ist in seinem ersten Vorlagebeschluss vom 28. Mai 2020 davon ausgegangen, dass sich eine nach deutschem Recht gemäß § 8 Abs. 3 Nr. 3 UWG und § 3 Abs. 1 Satz 1 Nr. 1 UKlaG bestehende Klagebefugnis des Klägers wegen seines im Streitfall allein auf die objektiv-rechtliche Durchsetzung des Datenschutzrechts gerichteten Klagebegehrens nicht den die Rechtsbehelfe, die Haftung und Sanktionen regelnden Bestimmungen des Kapitels VIII der Datenschutz-Grundverordnung und insbesondere nicht den Art. 80 Abs. 1 und 2 DSGVO oder Art. 84 Abs. 1 DSGVO entnehmen lässt. Er hat daher dem Gerichtshof der Europäischen Union mit seinem ersten Vorabentscheidungsersuchen die Frage vorgelegt, ob die Datenschutz-Grundverordnung in Bezug auf die Klagebefugnis eine abschließende Regelung trifft, die der Anwendbarkeit der § 8 Abs. 3 Nr. 3 UWG und § 3 Abs. 1 Satz 1 Nr. 1 UKlaG entgegensteht.

Der Gerichtshof der Europäischen Union hat – abweichend von der vom Senat im Vorlagebeschluss vertretenen Ansicht – entschieden, dass sich die Klagebefugnis des Klägers aus Art. 80 Abs. 2 DSGVO ergeben kann. Die in Art. 80 Abs. 2 DSGVO den Mitgliedstaaten eröffnete Möglichkeit, ein Verfahren einer Verbandsklage gegen den mutmaßlichen Verletzer des Schutzes personenbezogener Daten vorzusehen, besteht allerdings nur für den Fall, dass der klagende Verband geltend macht, die Rechte einer betroffenen Person gemäß der Datenschutz-Grundverordnung seien „infolge einer Verarbeitung“ verletzt worden. Es ist fraglich, ob diese Voraussetzung erfüllt ist, wenn – wie im Streitfall – die sich aus Art. 12 Abs. 1 Satz 1, Art. 13 Abs. 1 Buchst. c und e DSGVO ergebenden Informationspflichten verletzt worden sind. Die erneute Vorlage an den Gerichtshof der Europäischen Union dient der Klärung dieser Frage.

(Pressemitteilung des EuGH vom 10. 11. 2022)-

Prüfpflichten eines Bewertungsportals (Ls)

(Bundesgerichtshof, Urteil vom 9. August 2022 – VI ZR 1244/20 –)

Bei einem Bewertungsportal (hier: Hotelbewertungsportal) reicht die Rüge des Bewerteten, einer Bewertung liege kein Gästekontakt zugrunde, grundsätzlich aus, um Prüfpflichten des Bewertungsportals auszulösen. Zu weiteren Darlegungen, insbesondere einer näheren Begründung seiner Behauptung des fehlenden Gästekontakts, ist der Bewertete gegenüber dem Bewertungsportal grundsätzlich nicht verpflichtet. Dies gilt nicht nur in dem Fall, dass die Bewertung keinerlei tatsächliche, die konkrete Inanspruchnahme der Leistung beschreibende Angaben enthält und dem Bewerteten daher eine weitere Begründung schon gar nicht möglich ist, sondern auch dann, wenn für einen Gästekontakt sprechende Angaben vorliegen (Klarstellung zu Senatsurteil vom 1. März 2016 – VI ZR 34/15, BGHZ 209, 139 Rn. 26). Denn der Bewertete kann diese Angaben regelmäßig nicht überprüfen und damit den behaupteten Gästekontakt nicht sicher feststellen. Einer näheren Begründung der Behauptung des fehlenden

Gästekontakts bedarf es nur, wenn sich die Identität des Bewertenden für den Bewerteten ohne Weiteres aus der Bewertung ergibt. Im Übrigen gilt die Grenze des Rechtsmissbrauchs.

BAG-EuGH-Anfrage zu immateriellen Schadensersatz wegen der Übermittlung personenbezogener Daten an die vormalige Konzernmutter der Arbeitgeberin in den USA auf Grund einer Betriebsvereinbarung (Ls)

(Bundesarbeitsgericht, Beschluss vom 22. September 2022 – 8 AZR 209/21 (A) –)

Das BAG ersucht den EuGH gemäß Art. 267 AEUV um Vorabentscheidung über folgende Fragen:

1. Ist eine nach Art. 88 Abs. 1 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung; im Folgenden DS-GVO) erlassene nationale Rechtsvorschrift – wie etwa § 26 Abs. 4 Bundesdatenschutzgesetz, im Folgenden BDSG – in der bestimmt ist, dass die Verarbeitung personenbezogener Daten – einschließlich besonderer Kategorien personenbezogener Daten – von Beschäftigten für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen unter Beachtung von Art. 88 Abs. 2 DS-GVO zulässig ist, dahin auszulegen, dass stets auch die sonstigen Vorgaben der DS-GVO – wie etwa Art. 5, Art. 6 Abs. 1 und Art. 9 Abs. 1 und Abs. 2 DS-GVO – einzuhalten sind?
2. Sofern die Frage zu 1. bejaht wird:
Darf eine nach Art. 88 Abs. 1 DS-GVO erlassene nationale Rechtsvorschrift – wie § 26 Abs. 4 BDSG – dahin ausgelegt werden, dass den Parteien einer Kollektivvereinbarung (hier den Parteien einer Betriebsvereinbarung) bei der Beurteilung der Erforderlichkeit der Datenverarbeitung im Sinne der Art. 5, Art. 6 Abs. 1 und Art. 9 Abs. 1 und Abs. 2 DS-GVO ein Spielraum zusteht, der gerichtlich nur eingeschränkt überprüfbar ist?
3. Sofern die Frage zu 2. bejaht wird:
Worauf darf in einem solchen Fall die gerichtliche Kontrolle beschränkt werden?
4. Ist Art. 82 Abs. 1 DS-GVO dahin auszulegen, dass Personen ein Recht auf Ersatz des immateriellen Schadens bereits dann haben, wenn ihre personenbezogenen Daten entgegen den Vorgaben der DS-GVO verarbeitet wurden oder setzt der Anspruch auf Ersatz des immateriellen Schadens darüber hinaus voraus, dass die betroffene Person einen von ihr erlittenen immateriellen Schaden – von einigem Gewicht – darlegt?

5. 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?

6. 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?

II. Das Revisionsverfahren des Urteils LAG Baden-Württemberg vom 25.02.2021 – 17 SA 37/20 wird bis zur Entscheidung des Gerichtshofs der Europäischen Union über das Vorabentscheidungsersuchen ausgesetzt.

Kein Initiativrecht des Betriebsrats zur Einführung eines Systems der Arbeitszeiterfassung (Ls)

(Bundesarbeitsgericht, Beschluss vom 13. September 2022 – 1 ABR 22/21 –)

Der Arbeitgeber ist nach § 3 Abs. 2 Nr. 1 ArbSchG verpflichtet, ein System einzuführen, mit dem die von den Arbeitnehmern geleistete Arbeitszeit erfasst werden kann. Aufgrund dieser gesetzlichen Pflicht kann der Betriebsrat die Einführung eines Systems der (elektronischen) Arbeitszeiterfassung im Betrieb nicht mithilfe der Einigungsstelle erzwingen. Ein entsprechendes Mitbestimmungsrecht nach § 87 BetrVG besteht nur, wenn und soweit die betriebliche Angelegenheit nicht schon gesetzlich geregelt ist.

BAG-Vorabanfrage an den EuGH nach ordentlicher Kündigung durch kirchliche Einrichtung wegen Kirchenaustritt vor Beginn des Arbeitsverhältnisses (Ls)

(Bundesarbeitsgericht, Beschluss vom 21.07.2022 – 2 AZR 130/21 (A) –)

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

1. Ist es mit Unionsrecht, insbesondere der Richtlinie 2000/78/EG des Rates vom 27. November 2000 zur

Festlegung eines allgemeinen Rahmens für die Verwirklichung der Gleichbehandlung in Beschäftigung und Beruf (RL 2000/78/EG) im Licht von Art. 21 der Charta der Grundrechte der Europäischen Union (Charta), vereinbar, wenn eine nationale Regelung vorsieht, dass eine private Organisation, deren Ethos auf religiösen Grundsätzen beruht,

- a) Personen als ungeeignet für eine Beschäftigung in ihren Diensten erachten darf, die vor Begründung des Arbeitsverhältnisses aus einer bestimmten Religionsgemeinschaft ausgetreten sind, oder
 - b) von den für sie arbeitenden Personen verlangen darf, dass sie nicht vor Begründung des Arbeitsverhältnisses aus einer bestimmten Religionsgemeinschaft ausgetreten sind, oder
 - c) den Fortbestand des Arbeitsverhältnisses davon abhängig machen darf, dass eine für sie arbeitende Person, die vor Begründung des Arbeitsverhältnisses aus einer bestimmten Religionsgemeinschaft ausgetreten ist, dieser wieder beitrifft, wenn sie von den für sie arbeitenden Personen im Übrigen nicht verlangt, dieser Religionsgemeinschaft anzugehören?
2. Sofern die erste Frage bejaht wird: Welche gegebenenfalls weiteren Anforderungen gelten gemäß der RL 2000/78/EG im Licht von Art. 21 der Charta an die Rechtfertigung einer solchen Ungleichbehandlung wegen der Religion?

Anordnung von Coronatests durch den Arbeitgeber

(Bundesarbeitsgericht Urteil vom 1. Juni 2022 – 5 AZR 28/22 –)

Der Arbeitgeber kann in Umsetzung der ihn treffenden arbeitsschutzrechtlichen Verpflichtungen nach § 618 Abs. 1 BGB i.V.m. § 106 Satz 2 GewO berechtigt sein, auf Grundlage eines betrieblichen Schutz- und Hygienekonzepts Corona-Tests einseitig anzuordnen

Aus den Gründen:

- a) Berufte sich der Arbeitgeber gegenüber einem Anspruch des Arbeitnehmers aus Annahmeverzug auf dessen Leistungsunfähigkeit oder -unwilligkeit i.S.d. § 297 BGB, erhebt er eine Einwendung, für deren Voraussetzungen er als Gläubiger der Arbeitsleistung die Darlegungs- und Beweislast trägt (BAG v. 21. Juli 2021 – 5 AZR 543/20 – Rn. 11).
- b) Die Klägerin war nicht leistungswillig, weil sie sich geweigert hat, der Anordnung des beklagten Freistaats – handelnd durch die Bayerische Staatsoper – Folge zu leisten, vor Dienstantritt, d.h. der Teilnahme an Proben und Aufführungen, einen PCR-Test auf eine Infektion mit SARS-CoV-2 durchzuführen. Anders als beispielsweise bei Fällen eines von Kunden erteilten Hausverbots oder beim Entzug einer hoheitli-

chen Einsatzgenehmigung (vgl. dazu BAG 28. September 2016 – 5 AZR 224/16 – Rn. 25, BAGE 157, 34; 21. Oktober 2015 – 5 AZR 843/14 – Rn. 23, BAGE 153, 85; 23. September 2015 – 5 AZR 146/14 – Rn. 18, BAGE 152, 327) handelte es sich nicht um einen Fall der Leistungsunfähigkeit, weil die Klägerin es selbst in der Hand hatte, den Hinderungsgrund zu beseitigen.

Darlegungslast bei Überstundenvergütung (Ls)

(Bundesarbeitsgericht, Urteil vom 4. Mai 2022 – 5 AZR 359/21 –)

Verlangt der Arbeitnehmer Überstundenvergütung, hat er im Prozess die Leistung solcher und deren Veranlassung durch den Arbeitgeber darzulegen. Vom Erfordernis der arbeitgeberseitigen Veranlassung ist nicht wegen der Entscheidung des Gerichtshofs der Europäischen Union zur Pflicht des Arbeitgebers zur Einrichtung eines Systems zur Erfassung der täglichen effektiven Arbeitszeit (EuGH, Urt. v. 14.05.2019 – Rs. C-55/18 –) abzurücken.

Beweislast bei Geltendmachung eines Berichtigungsanspruchs (Ls)

(Bundesverwaltungsgericht, Urteil vom 2. März 2022 – 6 C 7/20 –)

1. Statthafte Klageart für die Geltendmachung eines Anspruchs auf Berichtigung des Melderegisters ist die Verpflichtungsklage.
2. Rechtsgrundlage für einen solchen Anspruch ist Art. 16 Satz 1 DS-GVO.
3. Bei Geltendmachung dieses Berichtigungsanspruchs trägt der Betroffene die Beweislast für die Richtigkeit des von ihm angegebenen Datums.
4. Die Zulässigkeit der Verpflichtungsklage als auch der allgemeinen Leistungsklage setzt grundsätzlich einen vorherigen Antrag bei der Behörde voraus.

Anspruch auf Berichtigung des Geburtsdatums im Melderegister (verneint) (Ls)

(Bundesverwaltungsgericht, Urteil vom 2. März 2022 – 6 C 7/209 –)

1. Statthafte Klageart für die Geltendmachung eines Anspruchs auf Berichtigung des Melderegisters ist die Verpflichtungsklage.

2. Rechtsgrundlage für einen solchen Anspruch ist Art. 16 Satz 1 DS-GVO.
3. Bei Geltendmachung eines Berichtigungsanspruchs nach Art. 16 Satz 1 DS-GVO trägt der Betroffene die Beweislast für die Richtigkeit des von ihm angegebenen Datums.
4. Die Zulässigkeit sowohl der Verpflichtungsklage als auch der allgemeinen Leistungsklage setzt grundsätzlich einen vorherigen Antrag bei der Behörde voraus.

Zur Anwendung der Datenschutzgesetze der Kirchen bei von ihnen als GmbH betriebenen Kliniken

(Oberlandesgericht Hamm, Beschluss vom 23. September 2022 – I-26 w 6/22 –)

1. Die Trägerin diakonischer Krankenhäuser fällt aufgrund ihres Bezuges zur Evangelischen Kirche auch dann unter das Merkmal „Kirche“ i.S.v. Art. 91 DS-GVO, wenn es sich bei ihr um eine selbstständige, privatrechtlich (als GmbH) organisierte Einrichtung der Kirche handelt.
2. Aus dem weit gezogenen Anwendungsbereich des Art. 91 DS-GVO folgt, dass die Tätigkeit einer diakonischen Klinik datenschutzrechtlich dem Kernbereich der Kirche zuzuordnen ist, weswegen der karitative Betrieb eines kirchlichen Krankenhauses nicht dem Anwendungsbereich der DS-GVO unterfällt.
3. Dies 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 dem Menschen dienende Aufgabe erfüllt werden soll.
4. Der datenschutzrechtliche Kernbereich einer Kirche ist nicht nur dann betroffen, wenn es um Seelsorge geht. Entscheidend ist, ob die Kirche mit der Einrichtung ihrer Aufgaben gerecht werden will, wozu nach dem Selbstbild der Kirche auch karitative und fürsorgliche Aufgaben gehören. Diese umfassen nicht nur ehrenamtliche bzw. unentgeltliche Betreuungsaufgaben, sondern auch der notwendige wirtschaftliche Betrieb von Betreuungsangeboten für hilfsbedürftige Menschen, wie z.B. Kindergärten, Alten- und Pflegeheime und Krankenhäuser.

(Leitsätze des Einsenders)

Sachverhalt:

Die Klägerin begehrt die Bewilligung von weiterer Prozesskostenhilfe für einen behaupteten Auskunfts- und Schmerzensgeldanspruch gegen die Beklagte aus der Europäischen Datenschutz-Grundverordnung.

Die Parteien streiten über ärztliche Behandlungsfehler im Rahmen einer Wirbelsäulenoperation und deren Vor- und Nachsorge im Hause der Beklagten, dem Krankenhaus in x, in den Jahren 2017 und 2018. Über diesen Sachverhalt ist bereits ein selbständiges Beweisverfahren vor dem Landgericht geführt worden, in dessen Zuge die Beklagte die Behandlungsunterlagen der Klägerin zur Akte gereicht hat.

Des Weiteren begehrt die Klägerin eine vollständige Datenauskunft nach Art. 15 DS-GVO, welche sie erstmals am 18.01.2019 von der Beklagten eingefordert hat, sowie wegen bislang nicht erteilter Auskunft ein Schmerzensgeld auf Basis von Art. 83 Abs. 5b) DS-GVO.

Die Klägerin 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 („DSG-EKD“) anwendbar, da sie gem. Art. 91 DS-GVO als kirchliche Einrichtung deren Anwendbarkeit nicht unterliege.

Das Landgericht hat mit Beschluss vom 26.11.2021 der Klägerin Prozesskostenhilfe für den Antrag zu 1 a) betreffend die behaupteten Behandlungsfehler bewilligt und den weitergehenden Antrag bezüglich der geltend gemachten Ansprüche aus der DS-GVO zurückgewiesen. Gegen diese Teilversagung wendet sich die Klägerin mit ihrer sofortigen Beschwerde vom 29.11.2021. Das Landgericht hat der sofortigen Beschwerde mit Beschluss vom 30.11.2021 nicht abgeholfen und die Sache dem Senat zur Entscheidung vorgelegt.

Aus den Gründen:

Zu Recht hat das Landgericht die Anträge zu Ziffer 1 b) und c) auf Bewilligung von Prozesskostenhilfe zurückgewiesen. Die beabsichtigte Klage hat auch nach Auffassung des Senats insoweit keine hinreichende Aussicht auf Erfolg.

In der Sache selbst hat das Landgericht mit zutreffender und ausführlicher Begründung – welcher sich der Senat anschließt – dargelegt, dass der Klägerin gegen die Beklagte keine Ansprüche gem. Art. 82 DS-GVO zugestehen, da die DS-GVO vorliegend nicht anwendbar ist. Auf die entsprechenden Ausführungen wird insoweit vorab Bezug genommen.

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.

Wie das Landgericht zu Recht ausgeführt hat, folgt hieraus, 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 (vgl. BeckoK DatenschutzR/Mundil, 41. Ed. 01.11.2021, DS-GVO Art. 91 Rn. 18a; Gola DS-GVO/Gola, 2. Aufl. 2018, DS-GVO Art. 91 Rn. 11). Die Beklagte als Trägerin von diakonischen Krankenhäusern fällt 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.

Der Senat schließt sich hierbei der Ansicht des Landgerichts an, dass von den zahlreichen vertretenen Auffassungen (vgl. nur: Preuß ZD 2015, 217, 222) vorliegend mit der differenzierenden Ansicht darauf abzustellen ist, ob es sich bei der Tätig-

keit der Beklagten, um eine solche aus dem Kernbereich der Kirche handelt, was vorliegend zu bejahen ist. Hierfür spricht, dass sich zunächst aus Art. 91 DS-GVO selbst keine Einschränkung ableiten lässt. Der Anwendungsbereich ist entsprechend weit auszulegen (BeckOK DatenschutzR/Mundil, 41. Ed. 01.11.2021, DS-GVO Art. 91 Rn. 15). Dementsprechend wird vertreten, dass auch Tätigkeiten von Religionsgemeinschaften von Art. 17 Abs. 1 AEUV umfasst sind, wenn auch nur in sehr restriktivem Maße. Eine typische Tätigkeit von Religionsgemeinschaften ist bspw. der Betrieb von karitativen Krankenhäusern. Träger dieser kirchlichen Krankenhäuser ist jedoch zu meist eine GmbH. Folglich handelt es sich um privatrechtliche Einrichtungen einer Religionsgemeinschaft. Es lässt sich demnach vertreten, dass auch privatrechtliche Einrichtungen von Religionsgemeinschaften in den Schutzbereich des Art. 17 AEUV fallen und damit auch nach Art. 91 vom Anwendungsbereich der DS-GVO ausgenommen und dem kirchlichen Datenschutz unterstellt sind (vgl. Paal/Pauly/Pauly, 3. Aufl. 2021, DS-GVO Art. 91 Rn. 10).

Der vorliegende karitative Betrieb des Krankenhauses der Beklagten unterliegt nicht dem Anwendungsbereich der DS-GVO. Wie das Landgericht zutreffend ausgeführt hat, ist hierbei zu berücksichtigen, 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 nicht nur dann der Kernbereich kirchlicher Aufgaben betroffen, wenn es um direkte Seelsorge geht. Entscheidend ist, ob die Kirche mit der Einrichtung ihren Aufgaben gerecht werden will. Hierzu gehören nach dem Selbstbild der Kirche insbesondere auch karitative und fürsorgliche Aufgaben, wozu nicht nur ehrenamtliche bzw. unentgeltliche Betreuungsaufgaben zählen, sondern auch der notwendigerweise wirtschaftliche Betrieb von Betreuungsangeboten für hilfsbedürftige Menschen, wie z.B. von Kindergärten, Alten- und Pflegeheimen und Krankenhäusern. Dies ist vorliegend der Fall. Zutreffend hat das Landgericht insoweit auch darauf verwiesen, dass sich der karitative Aspekt der kirchlichen Trägerschaft auch aus den eigenen Ausführungen der Beklagten auf ihrer Krankenhaus-Homepage ergibt. Dort wird unter der Rubrik „über uns“ die persönliche Zuwendung als eine ihrer besonderen Stärken bezeichnet, wobei sich aus dem grundlegenden christlichen Selbstverständnis – dem Dienst am Menschen – die hohe Qualität von Pflege und Medizin ableite. Als evangelische Einrichtung sei das Unternehmen fest in einem christlichen Weltbild verankert. Soweit die Klägerin unter Hinweis auf die Entscheidung des Bundesverfassungsgerichts (Beschluss von 14.01.2021 1 BvR 2853/19, NJW 2021, 1005) der Ansicht ist, die vorliegende Rechtsfrage sei von grundsätzlicher Bedeutung für das vollvereinheitliche europäische Datenschutzrecht und bedürfe damit letztlich einer Klärung durch den Europäischen Gerichtshof, hält der Senat eine Vorabentscheidung nach Ad. 267 Abs. 3 AEUV nicht für geboten. Im dortigen Fall ging es um die Auslegung des Schadensbegriffs aus Art. 82 I DS-GVO. Vorliegend ist die DS-GVO jedoch bereits aufgrund tatsächlicher Umstände nicht anwendbar.

Entsprechend war der Klägerin mangels Erfolgsaussicht die begehrte weitere Prozesskostenhilfe zu verweigern.

(Eingesandt von RA Riemer, Brühl)

Kein Ausschluss aus Vergabeverfahren wegen Einbindung der luxemburgischen Tochtergesellschaft eines US-amerikanischen Unternehmens

(Oberlandesgericht Karlsruhe, Beschluss vom 7. September 2022 – 15 Verg 8/22 –)

Auftraggeber dürfen sich auf bindende Zusagen US-amerikanischer Cloudanbieter verlassen – auch zum Datenschutz.

Aus den Gründen:

Die Anbieterin eines digitalen Entlassmanagements für Patienten ist nicht allein deswegen aus einem Vergabeverfahren zweier kommunaler Krankenhausgesellschaften auszuschließen, weil sie die luxemburgische Tochtergesellschaft eines US-amerikanischen Unternehmens als Hosting-Dienstleisterin einbinden will. Die öffentlichen Auftraggeber dürfen sich vielmehr auf die bindenden Zusagen der Anbieterin verlassen, dass die Daten ausschließlich in Deutschland verarbeitet und in kein Drittland übermittelt werden.

Zur Berechtigung einer Abmahnung bei Datenschutzvernachlässigung

(Sächsisches Landesarbeitsgericht, Urteil vom 7. April 2022 – 9 Sa 250/21 –)

- Auch Abmahnungen im Arbeitsverhältnis unterliegen mit Blick auf das Übermaßverbot einer Verhältnismäßigkeitsprüfung (wie BAG, Urteil vom 7. November 1979 – 5 AZR 962/77, juris). Der Entscheidung des Landesarbeitsgerichts Schleswig-Holstein im Urteil vom 29.11.2005 (Az. 2 Sa 350/05, juris) lässt sich Gegenteiliges nicht entnehmen.**
- Eine Abmahnung ist aber nicht grundsätzlich deshalb unverhältnismäßig, weil nur ein leichter Pflichtverstoß vorliegt (hier Verstoß gegen Clean Desk Regelung) und zuvor keine einschlägige Ermahnung oder Rüge als milderer Mittel erteilt wurde.**
- Häufen sich die Verstöße gegen eine Clean-Desk-Regelung trotz wiederholter Abmahnungen, kann eine verhaltensbedingte Kündigung des Arbeitsverhältnisses gerechtfertigt sein.**

Tatbestand:

Die Parteien streiten um die Wirksamkeit einer verhaltensbedingten ordentlichen Kündigung.

Die zum Kündigungszeitpunkt 51 Jahre alte, 3 Kindern zum Unterhalt verpflichtete Klägerin ist seit dem 01.03.2016 bei der Beklagten bzw. deren Rechtsvorgängern zuletzt in Teilzeit mit 30 Wochenstunden als Kreditsachbearbeiterin Baufinanzierung Schwerpunkt Bewertung zu einem durchschnittlichen monatlichen Bruttogehalt i.H.v. 3.573,50 € beschäftigt.

Bei der Beklagten, die regelmäßig mehr als 10 Vollzeitmitarbeiter beschäftigt, besteht ein Betriebsrat. Weiterhin besteht eine Arbeitsanweisung „Procedure zur Informationssicherheit am Arbeitsplatz und Clean Desk Policy“ auszugsweise wie folgt:

„Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren (Clean Desk Policy-Anhang A 11.2.9)

Es ist dafür Sorge zu tragen, dass schützenswerte oder geheime Informationen – egal ob in papierhafter Form oder auf dem Bildschirm – nicht durch Dritte eingesehen werden können.

Wenn der Arbeitsplatz verlassen wird oder unbeaufsichtigt ist:

- Sind schützenswerte Akten, Datenträger oder Hardware mit Informationen ordnungsgemäß wegzuschließen oder ordnungsgemäß zu entsorgen. Für Notebooks gilt der nächste Punkt.
- Muss darauf geachtet werden, dass das jeweilige Arbeitsgerät immer gesperrt wird, also mindestens der Bildschirmschoner aktiv ist.
- Dürfen Ausdrucke mit vertraulichem Inhalt und Datenträger nicht offen liegen gelassen werden, sondern müssen in eine Schublade, einen Schrank oder dergleichen gesperrt werden.
- Dürfen der Schlüssel für Rollcontainer oder Schränke mit vertraulichem Inhalt nicht am Arbeitsplatz oder an den Schlössern verbleiben.
- Dürfen Passwörter auf keinen Fall sichtbar (als Klebezettel am Monitor oder an einem leicht erratenden Ort wie z.B. unter der Schreibtischauflage z.B. in der unverschlossenen Schreibtischschublade oder unter der Tastatur bzw. Mousepad) aufbewahrt werden.
- Sind am Ende des Arbeitstages die IT-Systeme abzumelden und herunterzufahren. Ausnahmen bilden Systeme, die aus technischen oder organisatorischen Gründen nicht neu gebootet werden dürfen.
- Sind gekippte bzw. offenen Fenster am Ende des Arbeitstages zu verschließen.“ Auf die Kopie der „Procedure zur Informationssicherheit am Arbeitsplatz und Clean Desk Policy“, vorgelegt als Anlage B 2 wird Bezug genommen (hier insbesondere Bl. 45 d. Ausgangsakte, im Folgenden: AA.).

Unter anderem am 28.05.2020 wurden die Klägerin und weitere Mitarbeiter noch einmal an die Einhaltung der Clean Desk Policy erinnert. Dies wurde, für die Mitarbeiter und auch die Klägerin einsehbar, in das sogenannte Endlosprotokoll aufgenommen.

Unter dem 02.12.2019 wurde der Klägerin eine schriftliche Ermahnung (Anlage B6, Bl. 57 d.AA.) auszugsweise wie folgt erteilt:

„Am Mittwoch, den 27.11.2019 haben Sie den Fall 5050234000 (fertiggestelltes LORA Gutachten) an VDV zurückgegeben, obwohl der Fall einen unzureichenden Markt- und Beileihungswert ergeben hatte.

Wie bereits in 2017 festgelegt, werden diese Fälle nur auf ausdrücklichen Wunsch von VDV durch BFI abschließend bearbeitet.

Mithin sind Sie nicht den Weisungen Ihres Vorgesetzten, der Ihnen gegenüber weisungsberechtigt ist, gefolgt. Damit haben Sie gegen Ihre arbeitsvertraglichen Pflichten verstoßen.

Wir sind nicht bereit, weitere Verstöße gegen arbeitsvertragliche Pflichten zu akzeptieren und fordern Sie hiermit auf, sich in Zukunft vertragsgemäß zu verhalten.“

Mit Schreiben vom 27.04.2020 (Anlage B5, Bl. 51/52 d.AA.) wurde der Klägerin eine weitere Ermahnung auszugsweise wie folgt ausgesprochen:

Zu Ihren Aufgaben gehört u.a. die Wertermittlung von Immobilien.

Am Dienstag, den 21.04.2020 haben Sie die Wertermittlung – Fall 5086895006 – abgeschlossen, jedoch den dazugehörigen „Auftrag Wertermittlung“ nicht im Cockpit als erledigt gekennzeichnet (zdA).

Aufgrund dessen ist die durch den Gruppenleiter Herrn F. anschließend zu tätige Kapazitätenmeldung erheblich im Betriebsablauf gestört.

Herr F. hat Sie mehrfach mündlich als auch per Email darauf hingewiesen: Am 20. Dezember 2019, am 29. November 2019 sowie am 19.07.2019.

Zusätzlich ist die Arbeitsanweisung vom 17.03.2016 im laufenden Protokoll festgehalten.

In oben genannten Fällen haben Sie gegen Ihre arbeitsvertraglichen Verpflichtungen verstoßen. Bisher konnten Sie die Verstöße nicht begründen. Für dieses Verhalten sprechen wir Ihnen eine Ermahnung aus.

Wir fordern Sie auf, Ihre Arbeitsverpflichtungen künftig mit größerer Genauigkeit zu erfüllen und insbesondere auch die Anweisungen aus dem Benutzerhandbuch Elektronische Kreditakte „Cockpit“ zu beachten.

Sollte es wider Erwarten zu erneuten Pflichtverstößen kommen, sehen wir uns gezwungen, entsprechende weitere arbeitsrechtliche Maßnahmen zu ergreifen.“

Mit Schreiben vom 03.06.2020 (Anlage B5, Bl. 53/54 d.AA.) wurde der Klägerin eine Abmahnung auszugsweise wie folgt erteilt:

„Im Rahmen Ihrer Tätigkeit legen wir Ihnen Folgendes zur Last: Sie haben sich an den unten genannten Tagen nicht ordnungsgemäß von den von Ihnen genutzten IT-Systemen abgemeldet. Im Einzelnen war dies an folgenden Tagen der Fall:

Am 18.05.2020 haben Sie die Erfassungsliste bei Beendigung Ihrer Arbeit nicht geschlossen, sodass die anderen Nutzer dieser Datei keine neuen Fälle eintragen konnten.

Am 19.05.2020 haben Sie die Datei des Teamprotokolls (Endlosprotokoll) nicht geschlossen, somit konnten durch die anderen Nutzer keine weiteren notwendigen Eintragungen, u.a. zum Gruppendialog gemacht werden.

Am 25.05.2020 haben Sie vor Antritt Ihres Urlaubs die Anwendung LORA nicht geschlossen, sodass die anderen Mitarbeiter während Ihres 1-wöchigen Urlaubs in ihrer Arbeitsleistung erheblich beeinträchtigt wurden, da sie den Dummy-Fall für die Berechnung von Voranfragen ohne HD-Nr. nicht nutzen konnten.

Trotz mehrfacher Hinweise und Mails sowie persönlichen Gesprächen über den korrekten Abmeldeprozess, haben Sie in den genannten Fällen Dokumente und Anwendungen des Teamlaufwerks nach Beendigung Ihrer Arbeit nicht korrekt geschlossen und so die Arbeit der anderen Teammitglieder behindert.

Für dieses Verhalten sprechen wir Ihnen eine Abmahnung aus.

Wir fordern Sie auf, Ihre Arbeitsverpflichtungen künftig mit größerer Genauigkeit zu erfüllen und insbesondere die Regelungen zum Abmeldeprozess an den IT-Systemen bei Beendigung der Arbeit an Dateien und Anwendungen einzuhalten.

Sollte es wider Erwarten zu erneuten Pflichtverstößen kommen, sehen wir uns gezwungen, entsprechende weitere arbeitsrechtliche Maßnahmen, bis hin zur Kündigung, zu ergreifen.

Unter dem 22.07.2020 erteilte die Beklagte der Klägerin drei Abmahnungen in jeweils getrennten Schreiben. Das erste Schreiben vom 22.07.2020 (Anlage B4, Bl. 31 d.AA.) lautet auszugsweise wie folgt:

„Im Rahmen Ihrer Tätigkeit legen wir Ihnen Folgendes zur Last:

Sie haben an mehreren Tagen im Monat Juni (03.06., 09.06. und 19.06.2020) die Regelungen der Clean-Desk-Policy nicht eingehalten. Nach dieser Policy dürfen schützenswerte oder geheime Informationen – ob auf dem Bildschirm oder papierhaft – nicht durch Dritte einsehbar sein (5.4. der Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren-Clean-Desk-Policy-Anhang A 11.2.9.)

Am 03.06.2020 haben Sie gegen die Clean-Desk-Policy verstoßen, indem Sie sensible Unterlagen auf Ihrem Schreibtisch liegen gelassen haben. Auf Ihrem Schreibtisch lagen papierhafte Kreditakten und ausgedruckte Emails.

Am 09.06.2020 hat Sie die stellvertretende Gruppenleiterin, Frau B. per Email auf die Notwendigkeit der Einhaltung der Clean-Desk-Policy hingewiesen, da diese auch an diesem Tag von Ihnen nicht eingehalten wurde. Auf Ihrer Schreibtischunterlage waren Haupt-

darlehensnummern der Kunden vermerkt, der Datenmüll war nicht ordnungsgemäß entsorgt.

Am 19.06.2020 hat Frau B., die in Ihrer krankheitsbedingten Abwesenheit Ihren Schreibtisch, der wegen der Corona-Pandemie desinfiziert werden musste, abgeräumt und in diesem Zusammenhang festgestellt, dass — trotz der mehrfach erfolgten Anweisungen — mehrere Klebezettel mit verschiedenen Darlehensnummern auf Ihrem Schreibtisch gelegen haben.

Darlehensnummern unterliegen, wie u.a. am 28.05.2020 im Gruppendialog besprochen und als Arbeitsanweisung in das Endlosprotokoll aufgenommen, dem besonderen Schutz und damit den Anforderungen der o.g. Policy. Das Endlosprotokoll dient Ihnen und Ihren Kollegen zum Nachlesen der besprochenen Sachverhalte, insbesondere nach krankheits- oder urlaubsbedingten Abwesenheiten und ist damit ein Teil Ihrer Arbeitsmittel.“

Für das o.g. Verhalten sprechen wir Ihnen eine Abmahnung aus.

Wir fordern Sie auf, Ihre Arbeitsverpflichtungen künftig mit größerer Genauigkeit zu erfüllen und insbesondere die Clean-Desk-Policy einzuhalten.

Sollte es wider Erwarten zu erneuten Pflichtverstößen kommen, sehen wir uns gezwungen, entsprechende weitere arbeitsrechtliche Maßnahmen, bis hin zur Kündigung, zu ergreifen.“

Das zweite Schreiben vom 22.07.2020 (Anlage B5, Bl. 55/56 d.AA.) lautet auszugsweise wie folgt:

„Im Rahmen Ihrer Tätigkeit legen wir Ihnen Folgendes zur Last:

Sie haben sich am Freitag, den 17.07.2020 nicht ordnungsgemäß an den von Ihnen genutzten IT-Systemen abgemeldet. Konkret haben Sie im Programm CVM II den Fall 5114894005 nicht geschlossen, bevor Sie mittags Ihren Arbeitstag beendet haben. Sie haben durch Ihr Verhalten die Arbeit der anderen mit dem Fall beauftragten Kollegen behindert. Der Fall konnte deshalb nicht zeitnah weiterbearbeitet werden, so dass es zu Verzögerungen in der Rückmeldung an den Vermittler gekommen ist.

Sie wurden am 03.06.2020 wegen eines gleichgelagerten Fehlverhaltens abgemahnt.

Für den erneuten Verstoß gegen die Anweisung, sich am Ende des Arbeitstages von allen genutzten IT-Systemen abzumelden, s. auch die Clean-Desk-Policy, sprechen wir Ihnen eine zweite Abmahnung aus.

Wir fordern Sie auf, Ihre Arbeitsverpflichtungen künftig mit größerer Genauigkeit zu erfüllen und insbesondere die Regelungen zum Abmeldeprozess an den IT-Systemen bei Beendigung der Arbeit an IT-Systemen und damit an Dateien und Anwendungen einzuhalten.

Sollte es wider Erwarten zu erneuten Pflichtverstößen kommen, sehen wir uns gezwungen, entsprechende weitere arbeitsrechtliche Maßnahmen, bis hin zur Kündigung, zu ergreifen.

Wenige Tage später, am 28.07.2020 ist einem Kollegen der Klägerin der gleiche Fehler passiert. Der Gruppenleiter der Klägerin hat in einer E-Mail (Anlage K12, Bl. 101 d.AA.) hierauf wie folgt reagiert: „warum bin ich hier in cc? Bitte solche Prozessthemen in Eigenregie bearbeiten /steuern.“

Bei einem so trivialen Prozesssthema wie dem Abschließen einer Checkliste in CVM II ist die Einbindung eines Vorgesetzten entbehrlich.“

Das dritte Schreiben vom 22.07.2020 (Anlage B6, Bl. 59 d.AA.) lautet auszugsweise wie folgt:

„Im Rahmen Ihrer Tätigkeit legen wir Ihnen Folgendes zur Last:

Am Freitag, den 10.07.2020 haben Sie den Fall 5113168009 (fertiggestelltes LORA Gutachten) an VDV zurückgegeben, obwohl der Fall einen unzureichenden Marktwert ergeben hatte. Bereits in 2017 wurde festgelegt, dass diese Fälle nur nach Rücksprache und auf ausdrücklichen Wunsch von VDV durch die Abteilung Immobilienbewertung zu finalisieren sind. Diese Regelung ist Ihnen bekannt. Bereits am 02.12.2019 wurde Ihnen wegen des gleichen Fehlers (Fall 5050234000) eine schriftliche Ermahnung ausgesprochen. Trotz die-

ser Ermahnung, die die Aufforderung beinhaltete, sich zukünftig an die geltenden Regeln zu halten, haben Sie im o.g. Fall erneut gegen die Vorgaben verstoßen.

Für dieses Verhalten sprechen wir Ihnen eine Abmahnung aus.

Wir fordern Sie auf, Ihre Arbeitsverpflichtungen künftig mit größerer Genauigkeit zu erfüllen und insbesondere die Regelungen zur Bearbeitung von Gutachten zu beachten.

Sollte es wider Erwarten zu erneuten Pflichtverstößen kommen, sehen wir uns gezwungen, entsprechende weitere arbeitsrechtliche Maßnahmen, bis hin zur Kündigung, zu ergreifen.“

Bei der Beklagten besteht ein Zielerreichungstool. Dieses ist Grundlage für die Ermittlung der Arbeitsmengen für den Individualbonus der Mitarbeiter. Mit E-Mail vom 13.03.2019 wies der Vorgesetzte der Klägerin diese darauf hin, dass es hier zu einer Doppelerfassung von Fällen kam, die nur einmal finalisiert wurden. Dies wurde in einem Feedbackgespräch am 13.03.2019 mit der Klägerin besprochen. Hierbei mussten 15 Fälle von Doppelerfassungen festgestellt werden. Mit E-Mail vom 26.09.2019 wies der Vorgesetzte die Klägerin erneut auf doppelte, teilweise dreifach oder falsch erfasste Arbeitsfälle hin. Am 09.03.2020 informierte der Vorgesetzte die Klägerin darüber, dass es erneut zu erheblichen Fehlerfassungen, hier 6 Fälle, gekommen ist.

Mit Schreiben vom 25.08.2020 (Anlage B6, Bl. 71 d.AA.) wurde der Klägerin eine Abmahnung auszugsweise wie folgt erteilt:

„Im Rahmen Ihrer Tätigkeit legen wir Ihnen Folgendes zur Last:

Am Mittwoch, den 05.08.2020 haben Sie Ihrem Gruppenleiter Herrn F. die monatliche Übersicht aus dem Zielerreichungstool BFI IB mit Ihren eigenen Aufzeichnungen der erledigten Fälle übersandt.

Nach stichprobenartiger Prüfung wurde festgestellt, dass Sie zwei Fälle eingetragen haben, die nicht vorhanden waren:

06.07.2020 HDNR. 5102210

23.07.2020 HDNR. 5114297

Wie zu Beginn des Jahres im Zusammenhang mit der Zielvereinbarung festgelegt wurde, sind nur tatsächlich bearbeitete Fälle im Tool zu erfassen. Gegen diese Vorgabe haben Sie verstoßen. Für dieses Verhalten sprechen wir Ihnen eine Abmahnung aus.

Wir fordern Sie auf, Ihre Arbeitsverpflichtungen künftig mit größerer Genauigkeit zu erfüllen und insbesondere die Regelungen zur Erfassung der erledigten Fälle im Zielerreichungstool zu beachten.

Sollte es wider Erwarten zu erneuten Pflichtverstößen kommen, sehen wir uns gezwungen, entsprechende weitere arbeitsrechtliche Maßnahmen, bis hin zur Kündigung, zu ergreifen.

Bei der Beklagten fand im November 2020 ein Umzug in neue Räumlichkeiten statt. Daher mussten sämtliche Möbel, Akten, etc. gepackt und in die neuen Räumlichkeiten verbracht werden. Die Klägerin war zu diesem Zeitpunkt erkrankt. Auf Anfrage stimmte die Klägerin zu, dass ihr Gruppenleiter im Beisein eines Betriebsratsmitglieds die Beräumung ihres Schreibtisches durchführen könne, was am 02.11.2020 auch geschah. Dabei wurde festgestellt, dass in dem unverschlossenen Schreibtisch der Klägerin mehrere Markt- und Beleihungswertermittlungen und Prüfbögen der Qualitätssicherung mit den jeweiligen Kundendaten abgelegt waren. Auf den Unterlagen waren Daten – auch Kundendaten – vermerkt, die nach dem 22.09.2020 dort eingetragen wurden.

Jedenfalls vor dem Umzug bestand in der Abteilung, in welcher die Klägerin eingesetzt war, kein Kundenbesuchsverkehr. Die gesamte Etage wurde ausschließlich von der Beklagten bzw. deren Angestellten genutzt. Die einzelnen Arbeitsräume wurden grundsätzlich abgeschlossen, wenn niemand mehr am Arbeitsplatz war. Wer in das Gebäude wollte, musste sich an der Pforte im Eingangsbereich melden und gelangte dann über Treppe oder Lift auf die 5. Etage. Die Etagentür war stets verschlossen und elektronisch gesichert. Man musste entweder als Mitarbeiter einen Schlüssel/Zugangscodes haben oder als Gast klingeln, damit jemand öffnet.

Am 08.12.2020 wurde dem Vorsitzenden des Betriebsrates eine schriftliche Anhörung gem. § 102 Abs. 1 BetrVG übersandt. Auf die

vorgelegte Kopie des Schreibens wird wegen des Inhalts Bezug genommen (Anlage B7, Bl. 63-65 d.AA.). Der Vorsitzende des Betriebsrates, Herr C., hat mit Schreiben vom 10.12.2020 (Anlage B8, Bl. 66 d.AA.) der Beklagten mitgeteilt, dass in der Sitzung vom 10.12.2020 der Betriebsrat einstimmig beschlossen hätte, zur beabsichtigten Kündigung keine Stellungnahme abzugeben.

Nach Erhalt dieser Mitteilung wurde der Klägerin mit Schreiben vom 11.12.2020 die streitgegenständliche ordentliche Kündigung zum 28.02.2021 ausgesprochen. Das Schreiben ist der Klägerin durch Einwurf in den Briefkasten am Mittwoch, 16.12.2020, zugegangen. Mit der am 30.12.2020 beim Arbeitsgericht eingegangenen und der Beklagten am 14.01.2021 zugestellten Klage macht die Klägerin die Unwirksamkeit der Kündigung geltend.

Sie hat erstinstanzlich bestritten, dass der Betriebsrat ordnungsgemäß zur Kündigung angehört worden sei. Der hinsichtlich der Tatsachen unstreitige Kündigungsvorwurf verfange nicht, denn was in der Schreibtischschublade aufbewahrt werde, sei nicht „frei zugänglich“. Aufgrund der unstreitigen Zugangsbeschränkungen sei es Dritten nicht möglich gewesen, unberechtigt die Räume zu betreten und dort Kenntnis von Daten zu erlangen. Auch die Reinigungskräfte würden die Arbeitsräume nie unbeaufsichtigt betreten. Außerdem würden sie nicht das Schreibtischinnere reinigen, sondern nur frei zugängliche Flächen. Es sei daher kein Verstoß gegen die Clean Desk Policy gegeben. Diese diene dazu, dass schützenswerte oder geheime Informationen nicht durch „Dritte“ eingesehen werden könnten. Dies meine ersichtlich betriebsfremde Personen als Dritte, denn alle anderen Mitarbeiter inkl. der Gruppenleiter sind – insoweit unstreitig – ebenso wie die Klägerin den Grundsätzen der Vertraulichkeit und Verschwiegenheit unterworfen und seien also in diesem Zusammenhang nicht „Dritte“. Die Klägerin vermutet, dass die Beklagte versuche, sie aus dem Arbeitsverhältnis zu drängen, weil sie nicht in das Team passe. Auf die Ausführungen zur Begründung dieser Vermutung im Schriftsatz vom 17.03.2021, dort S. 3 bis 7 (Bl. 70-74 d.AA.) wird Bezug genommen. Hinsichtlich der mit den Ab- und Ermahnungen erhobenen Vorwürfe verteidigt sich die Klägerin im Wesentlichen mit Flüchtigkeitsfehlern, Unachtsamkeit und Vergesslichkeit. Bezüglich der nicht geschlossenen Anwendungen sei es bedauerlich, dass – unstreitig – systemseitig nicht vorgesehen ist, dass alle Anwendungen automatisch geschlossen werden, wenn man sich vom System abmeldet. Es sei von der Klägerin nicht intendiert gewesen, dass die Kolleginnen und Kollegen dadurch die Probedatei (den Dummy-Fall) für die Berechnung von Voranfragen ohne HD-Nr. – unstreitig – nicht nutzen könnten. Die Klägerin habe hier einen Fehler gemacht, der nicht vorkommen dürfe, sich aber im laufenden Geschäft als menschlich herausstelle und dem Grunde nach durch technische Vorrichtungen habe vermieden werden können. Eine Abmahnung rechtfertige das vergessene Schließen des Dokuments nicht.

Am Freitag, dem 10.07.2020 (Abmahnung vom 22.07.2020) habe die Klägerin nach Feststellung des unzureichenden Marktwerts Rücksprache gehalten. Dazu sei sie extra zu Frau A. von VDV gegangen und habe nachgefragt. Frau A. sei sehr beschäftigt gewesen und habe gesagt (sinngemäß): „mach’s erst mal fertig, ich gucke es mir dann an“. Diesem Wunsch sei die Klägerin nachgekommen und habe das Wertermittlungsgutachten fertiggestellt. Sie habe daher nicht gegen die Arbeitsanweisung der Beklagten verstoßen.

Am 05.08.2020 habe sie nicht die monatliche Übersicht aus dem Zielerreichungstool mit zwei gar nicht vorhandenen Fällen befüllt. Sie trage keine Fantasiefälle als erreichtes Ziel in die Liste ein, es müsse sich daher um einen Zahlendreher handeln.

Es sei zwar in der Vergangenheit zu fehlerhaften Eintragungen gekommen, die Eintragung im Zielerreichungstool betreffe aber nicht die Arbeitsabläufe, sondern diene der Kontrolle, welche Aufgaben am Tag erledigt worden seien und ob die Zielvorgaben für

die Erreichung der individuellen zielgebundenen jährlichen Bonuszahlung erreicht werden.

Die Klägerin hat erstinstanzlich beantragt:

Es wird festgestellt, dass das Arbeitsverhältnis der Parteien durch die Kündigung der Beklagten vom 11.12.2020, der Klägerin zugegangen am 16.12.2020, nicht aufgelöst ist.

Die Beklagte hat erstinstanzlich

Klageabweisung beantragt.

Sie hat erstinstanzlich geltend gemacht, dass die Unterlagen im Schreibtisch nicht gegen Zugriff durch Dritte geschützt gewesen seien. Hierdurch sei es Dritten möglich gewesen, Einsicht in die ausgelegten Unterlagen zu nehmen und also schützenswerte Daten von Kunden zu erlangen. Zwar erfolge die Reinigung grundsätzlich während der Dienstzeit. Hiervon gebe es jedoch Ausnahmen z.B. wenn Mitarbeiter erkrankt seien, werde die Reinigung dennoch durchgeführt. Insofern erfolge eine Öffnung der jeweiligen Tür durch den Hausmeister. Die Mitarbeiter der Reinigungsfirma würden sich dann ins Büro begeben und dort reinigen. Dabei könne nicht ausgeschlossen werden, dass der Schreibtisch geöffnet werde. Es bestehe keine Berechtigung der Klägerin, gegen die Clean Desk Policy zu verstoßen nach dem Motto „es kann ja nur ein Mitarbeiter die Unterlagen sehen“. Vor dem Hintergrund der einschlägigen Abmahnung sei eine störungsfreie Durchführung des Arbeitsverhältnisses für die Zukunft nicht zu erwarten. Die Abmahnungen seien wirksam erteilt, die vorgeworfenen Pflichtverletzungen im Wesentlichen unstreitig. Die Klägerin versuche lediglich, deren Bedeutung herunterzuspielen.

Mit der Replik habe die Klägerin wiederum verdeutlicht, dass sie nicht gewillt sei, die datenschutzrechtlichen Auflagen bei der Beklagten einzuhalten. Entgegen der Darstellung der Klägerin sei diese kein „Opfer“ von Querelen und Auseinandersetzungen innerhalb der Abteilung, sondern sie habe sämtliche Ermahnungen und Abmahnungen und auch den der Kündigung zugrundeliegenden Sachverhalt selbst verursacht.

Das Arbeitsgericht hat der Klage stattgegeben und führt zur Begründung aus, die bei der verhaltensbedingten Kündigung zu beachtende Prognose sei nicht negativ zu bewerten, die Pflichtverletzung sei nicht erheblich und die Beklagte habe nicht davon ausgehen dürfen, dass eine Kündigungsandrohung nicht zu einer Änderung des Verhaltens geführt haben würde. Die Abmahnung vom 22.07.2020 sei zwar einschlägig, sie habe aber bei der Klägerin zur Änderung des Verhaltens bezgl. des Aufräumens des Schreibtisches geführt. Verstoßen habe sie nunmehr gegen die Pflicht, den Schreibtisch abzuschließen. Eine weitere Abmahnung hätte bei der Klägerin zu einer entsprechenden Verhaltensänderung führen können, weshalb die fehlende Abmahnung die Kündigung unverhältnismäßig und damit rechtsunwirksam mache.

Gegen das dort am 03.06.2021 zugestellte Urteil des Arbeitsgerichts Leipzig vom 24.03.2021 hat die Beklagte mit Schriftsatz vom 24.06.2021, beim Sächsischen Landesarbeitsgericht am selben Tag eingegangen, Berufung eingelegt. Die Beklagte wurde mit gerichtlicher Verfügung vom 28.06.2021 darauf hingewiesen, dass das eingereichte elektronische Dokument für das Gericht zur Bearbeitung nicht geeignet und damit der Eingang unwirksam war. Daraufhin wurde der Schriftsatz mit Datum 29.06.2021 am selben Tag erneut eingereicht, diesmal in ordnungsgemäßer elektronischer Form. Gleichzeitig hat der Prozessbevollmächtigte der Beklagten anwaltlich und an Eides statt versichert, dass das nunmehr nachgereichte Dokument mit dem am 24.06.2021 eingereichten Dokument übereinstimme. Die Berufung wurde mit am 02.08.2021 eingegangener Begründung ausgeführt. Die Berufungsbegründung wurde der Klägerin am 03.08.2021 zugestellt. Gemäß Antrag vom 12.08.2021 wurde die Frist zur Erwidern verlängert bis zum 24.09.2021. Am 23.09.2021 ging die Erwidern verbunden mit einer Anschlussberufung beim Sächsischen Landesarbeitsgericht ein.

Die beklagte Partei führt zur Begründung der Berufung aus, das Arbeitsgericht habe zu Unrecht sowohl den unstreitigen Pflichtverstoß als nicht erheblich angesehen sowie die Abmahnungen als nicht einschlägig. Fehlerhaft habe das Arbeitsgericht die Auffassung vertreten, dass die Klägerin „lediglich mit leichter Fahrlässigkeit“ gehandelt habe und daher eine Erheblichkeit nicht vorliegen würde.

Bei der Beklagten bestehe eine erhöhte Verpflichtung zur Wahrung des Datenschutzes und des Bankgeheimnisses. Wie das Arbeitsgericht Leipzig zu der Auffassung komme, dass „leichte“ Fahrlässigkeit vorliege, könne nicht erkannt werden. Fehlerhaft gehe das Arbeitsgericht zudem davon aus, dass die Abmahnung vom 22.07.2020 zwar einschlägig sei, aber dennoch eine weitere Abmahnung der Kündigung habe vorausgehen müssen, weil ein nicht direkt vergleichbarer Pflichtverstoß gegeben sei. Denn die Abmahnungen stammten aus demselben Bereich, die Pflichtverstöße seien gleichartig. Es mache keinen Unterschied, ob Unterlagen auf dem Schreibtisch liegen oder in der offenen Schreibtischschublade. In soweit sei die Arbeitsanweisung der Beklagten auch eindeutig, dass Akten ordnungsgemäß wegzuschließen seien. Ihren erstinstanzlichen Vortrag ergänzend trägt die Beklagte vor, bereits am 18.05.2020 habe es einen Verstoß gegen die Clean Desk Policy durch die Klägerin gegeben. Der Vorgesetzte, Herr F., habe an diesem Tag festgestellt, dass die Klägerin zum Feierabend ihren Schreibtisch ohne Beachtung der Clean Desk Policy verlassen habe. Auf dem Schreibtisch hätten z.B. noch zwei Kreditakten mit vertraulichen Inhalten und weitere ebenfalls vertrauliche Unterlagen gelegen.

Aufgrund dessen habe der Vorgesetzte ein Gespräch am 19.05.2020 mit der Klägerin geführt. Hierbei habe er erneut auf die Clean Desk Policy hingewiesen. Zudem sei auch darauf hingewiesen worden, dass Verstöße arbeitsrechtliche Konsequenzen haben können.

Die Beklagte beantragt zweitinstanzlich, das Urteil des Arbeitsgerichts Leipzig vom 24.03.2021, Az. 11 Ca 3518/20, abzuändern und die Klage abzuweisen.

Die Klägerin beantragt

1. die Berufung zurückzuweisen,

2. die Beklagte zu verurteilen, die Klägerin bis zum rechtskräftigen Abschluss des vorliegenden Rechtsstreits zu den bisherigen Bedingungen als Kreditsachbearbeiterin in Leipzig mit 30 Wochenarbeitsstunden und gemäß Tarifgruppe 7, Stufe 3 des Entgelttarifvertrages Postbank AG weiterzubeschäftigen.

Die Beklagte beantragt,

die Anschlussberufung zurückzuweisen.

Die Klägerin hat sich den Ausführungen des Erstgerichts im Urteil angeschlossen und Letzteres verteidigt. Sie führt ergänzend aus „in einen Schrank oder dergleichen gesperrt“ bedeute nicht zwingend, dass Schublade oder Schrank auch verschlossen sein müssten. „Wegsperrn“ meine den Schutz vor unbefugten Blicken und unbefugtem Gebrauch. Was im Schreibtisch liege, sei nicht durch Dritte einsehbar, sondern „weggesperrt“. Der behauptete Verstoß gegen die Clean Desk Policy wegen des nicht abgeschlossenen Schreibtisches sei dem Bereich der Nebenpflichtverletzungen zuzuordnen und wiege nicht schwer. Das Argument, es könnten Dritte unberechtigt Schreibtische durchsuchen, überzeuge nicht. Wenn sich Dritte rechtswidrig verhalten, dürfe das nicht der Klägerin angelastet werden. Die Klägerin bestreitet, dass das Foto vom 18.05.2020 nach Verlassen des Arbeitsplatzes aufgenommen worden sei.

Es handele sich nicht um ein „Feierabendfoto“, sondern um ein Foto vom Schreibtisch der Klägerin während der Arbeitszeit. Dies sei klar zu erkennen am Umstand, dass die Brille der Klägerin ebenso auf dem Tisch liege wie das persönliche (geblümete) Notizbuch. Die Klägerin verlasse den Arbeitsplatz nie ohne Brille, nie ohne ihr persönliches Notizbuch, nie ohne die Stifte in den Stifthalter zu stecken und nie ohne den Stuhl heranzustellen und nie

ohne ihren Trinkbecher abzuräumen. Der Schreibtisch sei während der Arbeitszeit „hinter dem Rücken“ der Klägerin fotografiert. Ein Abmahnungsgespräch am 19.05.2020 unter Hinweis darauf, dass Verstöße auch arbeitsrechtliche Konsequenzen nach sich ziehen können, habe es nicht gegeben.

Hinzu komme, dass sowohl die betriebliche als auch die private Situation der Klägerin seit Ende 2019 stark angespannt gewesen sei. Die Beklagte habe der Klägerin vorgeworfen, aufgrund „hoher Fehlzeiten“ sei sie eine „hohe Belastung für das Team“ (siehe Anlage K 5, Bl. 80 d.AA.) und ihre Eingruppierung in Tarifgruppe 7 würde eine deutlich über dem Teamschnitt liegende Arbeitsleistung erwarten lassen, die die Klägerin nicht erbringe.

Mit ihrer Anschlussberufung macht sie klageerweiternd den allgemeinen Weiterbeschäftigungsantrag geltend. Überwiegende Interessen der Beklagtenseite an der Nichtbeschäftigung bis zum rechtskräftigen Abschluss dieses Rechtsstreits würden nicht vorliegen.

Die Beklagte tritt der Anschlussberufung entgegen und meint, der Weiterbeschäftigungsantrag sei bereits unbestimmt. Die von der Klägerin angestrebte Tätigkeit, die von ihr genau umschrieben werden müsse, finde sich nicht in dem Klageantrag. Darüber hinaus fehle es an jeglichem Sachvortrag seitens der Klägerin, welches Interesse sie an einer Weiterbeschäftigung bis zum rechtskräftigen Abschluss des Verfahrens überhaupt haben wolle. Jedenfalls überwiegen die Interessen der Beklagten an der Nichtbeschäftigung diejenigen der Klägerin, denn sie habe auch im Prozess gezeigt, dass sie nicht gewillt sei, die datenschutzrechtlichen Bestimmungen der Beklagten einzuhalten. Das Foto sei am 18.05.2021 aufgenommen worden, nachdem die Klägerin um 13:55 Uhr ihre Arbeit beendet habe. Letzteres ergebe sich aus dem Zeitkontennachweis der Klägerin für die Woche vom 18.05. – 24.05.2020. Das Foto sei von dem Vorgesetzten am 18.05.2020 um 14:25 Uhr gefertigt worden, was sich aus der Kopie des Screenshots (Anlage BK 3, Bl. d.BA) ersehen lasse. Die Klägerin sei offensichtlich der Auffassung, dass die gerügten Verstöße wegen „Unerheblichkeit“ nicht zu berücksichtigen wären oder max. eine Ermahnung rechtfertigen würden. Bei dieser Einschätzung verkenne die Klägerin insbesondere, dass auf eine Abmahnung und dem hierin dargelegten objektiv gegebenen Pflichtverstoß das Verhältnismäßigkeitsprinzip keine Anwendung finde. Auch der erste Verstoß berechtige den Arbeitgeber, eine Abmahnung auszusprechen.

Wegen des weiteren Vorbringens der Parteien in der Berufungsinstanz wird Bezug genommen auf die wechselseitigen Schriftsätze nebst Anlagen sowie auf das Protokoll der mündlichen Verhandlung am 07.04.2022.

Aus den Gründen:

Die gemäß § 64 Abs. 1 und 2 ArbGG statthafte und gemäß den §§ 66 Abs. 1, 64 Abs. 6 Satz 1 ArbGG i. V. m. §§ 519, 520 ZPO form- und fristgerecht eingelegte und begründete, damit zulässige Berufung hat in der Sache Erfolg. Das Arbeitsgericht hat der zulässigen Klage zu Unrecht stattgegeben, denn sie ist unbegründet. Die der Klägerin ausgesprochene Kündigung ist aus verhaltensbedingten Gründen sozial gerechtfertigt.

I. Die Berufung ist zulässig. Sie ist insbesondere fristgerecht beim Sächsischen Landesarbeitsgericht eingegangen. Das Urteil des Arbeitsgerichts vom 24.03.2021 wurde der Beklagten am 03.06.2021 zugestellt. Die Frist des § 66 Abs. 1 Satz 1 ArbGG begann gemäß § 64 Abs. 6 ArbGG i.V.m. § 222 Abs. 1 ZPO, § 187 Abs. 1 BGB am 04.06.2021 und endete gemäß § 188 Abs. 2 BGB am 03.07.2021. Am 29.06.2021 ging beim Sächsischen Landesarbeitsgericht der Berufungsschriftsatz vom 29.06.2021 in ordnungsgemäßer elektronischer Form ein. Auf die – hier vorsorglich abgegebene – anwaltliche Versicherung der Übereinstimmung

mit dem Schriftsatz vom 24.06.2021 (die hinsichtlich des Datums allerdings nicht gegeben ist), kommt es somit nicht an.

Die in der ebenfalls zulässig erhobenen Anschlussberufung enthaltene Klageerweiterung ist gemäß § 264 Nr. 2 ZPO zulässig (Koch, in: Erfurter Kommentar, 21. Aufl. 2021, ArbGG § 64 Rn. 14).

II. Gründe, die zur Unzulässigkeit der Klage führen könnten, sind nicht erkennbar und nicht geltend gemacht. Die Bedenken der Beklagten gegen die Zulässigkeit des erweiterten Klageantrages werden nicht geteilt. Die Klägerin ist laut Arbeitsvertrag als „Kreditsachbearbeiterin Baufinanzierung Schwerpunkt Bewertung in Leipzig“ eingestellt worden. Ebenso wie die Angabe des Arbeitsortes dürfte auch die Konkretisierung der Arbeitsaufgabe lediglich erste Ausübung des Weisungsrechts und nicht verbindliche Festlegung sein, welche das Weisungsrecht einschränken würde. Die Kammer geht daher davon aus, dass die Klägerin auch mit anderen Aufgaben als in der Baufinanzierung vertragsgemäß als Kreditsachbearbeiterin beschäftigt werden kann.

Selbst wenn dies unzutreffend sein sollte, ist für die Beklagte hinreichend erkennbar, welche Art der Beschäftigung von ihr gewollt ist.

Das gemäß § 256 Abs. 1 ZPO erforderliche Feststellungsinteresse für den Bestandsschutzantrag ergibt sich hier bereits aus der sonst drohenden Präklusion nach §§ 13, 4, 7 KSchG.

III. Die Klage ist hinsichtlich des Kündigungsschutzantrages aber unbegründet, denn die Kündigung der Beklagten vom 11.12.2020 ist als verhaltensbedingte Kündigung wirksam und hat das Arbeitsverhältnis mit Ablauf des 28.02.2021 beendet.

1. Das ergibt sich nicht bereits aus §§ 4, 7 KSchG, denn die Klägerin ist mit der Geltendmachung der Unwirksamkeit nicht präkludiert. Sie hat nach Erhalt der schriftlichen Kündigung am 16.12.2020 mit Eingang der Klage beim Arbeitsgericht am 30.12.2020 und Zustellung am 14.01.2020 binnen der Frist von 3 Wochen rechtzeitig Klage erhoben, § 253 Abs. 1 ZPO, §§ 187 Abs. 1, 188 Abs. 2 BGB hier i.V.m. § 167 ZPO. Die Verzögerung der Zustellung stammt aus der Sphäre des Gerichts, sie erfolgte damit demnächst im Sinne des § 167 ZPO.

2. Die Kündigung ist gemäß § 1 Abs. 2 KSchG sozial gerechtfertigt, weil ein im Verhalten der Klägerin liegender Grund vorliegt, der eine negative Zukunftsprognose rechtfertigt und die Interessenabwägung hier zugunsten der Beklagten ausfällt.

2.1. Die Voraussetzungen des allgemeinen Kündigungsschutzes liegen vor. Die Beklagte beschäftigt regelmäßig deutlich mehr als 10 vollzeitbeschäftigte Arbeitnehmer, § 23 Abs. 1 KSchG. Die Klägerin ist seit 01.03.2016 beschäftigt, also zum Kündigungszeitpunkt offensichtlich länger als 6 Monate, § 1 Abs. 1 KSchG.

2.2. Für eine verhaltensbedingte Kündigung genügen im Verhalten des Arbeitnehmers liegenden Umstände, die bei verständiger Würdigung in Abwägung der Interessen der Vertragsparteien die Kündigung als billigenswert und angemessen erscheinen lassen. Als verhaltensbedingter Grund ist insbesondere eine schuldhaft, vorwerfbare und rechts- oder vertragswidrige Verletzung von Haupt- und/oder Nebenpflichten aus dem Arbeitsverhältnis geeignet. Entsprechende Pflichten bestehen im Leistungs- und im Vertrauensbereich. Vertragsstörungen im Leistungsbereich sind z.B. dann gegeben, wenn der Arbeitnehmer eine Schlechtleistung erbringt, wobei grundsätzlich eine Arbeitsleistung „mittlerer Art und Güte“ geschuldet ist. Es genügen Umstände, die aus Sicht eines ruhig und verständig urteilenden Arbeitgebers eine Kündigung als angemessene Reaktion auf das Fehlverhalten des Arbeitnehmers erscheinen lassen (BAG, Urteil vom 17.01.2008, Az. 2 AZR 536/06, juris, m.w.N.). Die Berechtigung einer verhaltensbedingten Kündi-

gung ist allerdings nicht daran zu messen, ob sie als Sanktion für den in Rede stehenden Vertragsverstoß angemessen ist. Im Kündigungsrecht gilt nicht das Sanktionsprinzip, sondern das Prognoseprinzip. Eine verhaltensbedingte Kündigung ist gerechtfertigt, wenn eine störungsfreie Vertragserfüllung in Zukunft nicht mehr zu erwarten ist und künftigen Pflichtverstößen nur durch die Beendigung der Vertragsbeziehung begegnet werden kann (BAG, Urteil vom 10.06.2010, Az. 2 AZR 541/09, juris, m.w.N.). Das ist nicht gegeben, wenn mildere Mittel und Reaktionen, z.B. eine Abmahnung, geeignet sind, beim Arbeitnehmer eine Verhaltensänderung zu bewirken. Beruht die Vertragspflichtverletzung auf steuerbarem Verhalten des Arbeitnehmers, ist grundsätzlich davon auszugehen, dass sein künftiges Verhalten schon durch die Androhung von Folgen für den Bestand des Arbeitsverhältnisses positiv beeinflusst werden kann. Einer Abmahnung bedarf es nach Maßgabe des Verhältnismäßigkeitsgrundsatzes u.a. dann nicht, wenn bereits ex ante erkennbar ist, dass eine Verhaltensänderung in Zukunft auch nach Abmahnung nicht zu erwarten steht (BAG, Urteil vom 11.07.2013, Az. 2 AZR 994/12, juris, m.w.N.). Schlussendlich bedarf es einer Interessenabwägung. Abzustellen ist auf einen objektiven Beurteilungsstandpunkt. Dabei sind u.a. zu berücksichtigen

– auf Arbeitgeberseite: evtl. angerichteter Schaden, Gefährdung von Kollegen, verursachte Betriebsablaufstörungen, Auswirkungen auf das Verhalten der Kollegen, Wiederholungsgefahr sowie Imageverlust gegenüber Kunden und Mitbewerbern

– auf Arbeitnehmerseite: eine langjährige Betriebszugehörigkeit, evtl. Mitverschulden des Arbeitgebers, früheres beanstandungsloses Verhalten des Arbeitnehmers, Häufigkeit des kritisierten Fehlverhaltens, Schwere des Pflichtverstoßes, das Lebensalter bzw. die Möglichkeit, noch einen vergleichbaren Arbeitsplatz zu finden, sowie etwaige Unterhaltsverpflichtungen.

Gemäß § 1 Abs. 2 Satz 4 KSchG hat die Beklagte die Tatsachen darzulegen und zu beweisen, die die Kündigung rechtfertigen. Sie ist dabei auch für den Ausschluss von seitens der Klägerin vorgebrachten Rechtfertigungs- und Entschuldigungsgründen darlegungs- und beweispflichtig.

2.3. Ausgehend von diesen Grundsätzen gilt hier Folgendes:

2.3.1. Eine Pflichtverletzung liegt in Form der Nichteinhaltung der Arbeitsanweisung „Clean desk policy“ unstrittig vor. Die Klägerin hat entgegen der Anweisung Unterlagen mit sensiblen Daten unverschlossen zu einem Zeitpunkt im Schreibtisch aufbewahrt, zu dem sie selbst nicht im Büro anwesend war. Unstrittig war ihr diese Anweisung hinreichend bekannt.

Die Argumentation in der Berufungserwiderung dahingehend, die Klägerin habe den behaupteten Verstoß nicht unstrittig gestellt und er werde „auch nicht unstrittig dadurch, dass das Arbeitsgericht – insoweit unzutreffend – einen Pflichtenverstoß angenommen“ habe, ist unzutreffend, weil undifferenziert. Die allein dem Bestreiten zugänglichen Tatsachen sind hier tatsächlich unstrittig, die Klägerin führt in der Berufungserwiderung selbst aus, dass die fraglichen Unterlagen im unverschlossenen Schreibtisch lagen. Soweit die Klägerin meint, hierin liege kein Pflichtverstoß, ist dies eine dem Bestreiten nicht zugängliche Frage der rechtlichen Bewertung durch das Gericht. Die Kammer sieht einen Verstoß als gegeben an. Der Wortlaut der Arbeitsanweisung geht im ersten Punkt dahin, dass „schützenswerte Akten, Datenträger oder Hardware mit Informationen ordnungsgemäß wegzuschließen oder ordnungsgemäß zu entsorgen“ sind, „wenn der Arbeitsplatz verlassen wird oder unbeaufsichtigt ist“. Nach der Regelung im dritten Punkt dürfen „Ausdrucke mit vertraulichem Inhalt und Datenträger

nicht offen liegen gelassen werden, sondern müssen in eine Schublade, einen Schrank oder dergleichen gesperrt werden“.

Soweit die Klägerin meint, „in einen Schrank oder dergleichen gesperrt“ bedeute nicht zwingend, dass Schublade oder Schrank auch verschlossen sein müssten, ist dies mit der Bedeutung des Wortes „Wegsperrn“ nicht vereinbar. Denn es bezeichnet ausweislich der Internetseite <https://www.duden.de/rechtschreibung/wegsperrn> mit der ersten Bedeutung dasselbe wie „wegschließen“. Dieses Wort wiederum hat ausweislich der Internetseite <https://www.duden.de/rechtschreibung/wegschliessen> die Bedeutung: „einschließen (1a), damit jemand anderes nicht darankommen kann“.

Das auch von der Klägerin in dem Wort „Wegsperrn“ erkannte Ziel, nämlich den Schutz vor unbefugten Blicken und unbefugtem Gebrauch, kann durch eine Ablage im unverschlossenen Schreibtisch offensichtlich nicht erreicht werden. Unbehelflich ist in diesem Zusammenhang die Ansicht, wonach es nicht der Klägerin angelastet werden könne, wenn Dritte unberechtigt und rechtswidrig Schreibtische durchsuchen. Mit diesem Argument könnte man sich Datenschutz insgesamt sparen. Er dient nämlich gerade und ausschließlich dazu, vor unberechtigtem Zugriff zu schützen.

Der Annahme eines Pflichtverstoßes steht nicht entgegen, dass die Clean Desk Policy „ersichtlich betriebsfremde Personen als Dritte“ meine, weil alle anderen Mitarbeiter inkl. der Gruppenleiter ebenso wie die Klägerin den Grundsätzen der Vertraulichkeit und Verschwiegenheit unterworfen sind. Entgegen der Ansicht der Klägerin sind auch diese solange als „Dritte“ anzusehen, wie sie nicht selbst im Rahmen ihrer Arbeitstätigkeit Zugriff auf genau die hier fraglichen Daten hatten. Denn auch ihrerseits dem Datenschutz verpflichtete Mitarbeiter dürfen über Kunden nichts erfahren, was sie nicht ihrer eigenen Arbeitsaufgabe wegen angeht, selbst wenn sie es nicht weitersagen dürfen. Mit dieser Argumentation zeigt die Klägerin – wie von der Beklagten auch ausgeführt – dass sie tatsächlich bis heute die hohe Bedeutung des Datenschutzes nicht wirklich verstanden hat. Der Pflichtverstoß als solcher ist auch nicht abhängig davon, ob ein Schaden bereits eingetreten ist oder zumindest drohte. Die Arbeitsanweisung ist klar und deutlich sowie angesichts der bei der Beklagten zu verarbeitenden sensiblen Daten auch nicht unverhältnismäßig. Es ist nicht Sache der Klägerin, zu entscheiden, ob eine Einhaltung erforderlich war oder nicht, weil Dritte keinen unbeaufsichtigten Zugang zu Büro oder Etage hatten. Wie ausgeführt, genügt hier auch bereits der ungehinderte Zugang anderer, mit den Daten nicht befasster Mitarbeiter.

Unzutreffend ist auch die Ansicht der Klägerin, der behauptete Verstoß gegen die Clean Desk Policy wegen des nicht abgeschlossenen Schreibtischs sei dem Bereich der Nebenpflichtverletzungen zuzuordnen. Die Erbringung der Arbeitsleistung im Rahmen des rechtmäßig ausgeübten Direktionsrechts – zu dem auch Arbeitsanweisungen zum Datenschutz gehören – ist Hauptleistungspflicht. Soweit die Klägerin hierzu darüber hinaus geltend macht, der Verstoß wiege nicht schwer, mag dies für den einzelnen Verstoß noch gelten. Es liegen aber wiederholte Verstöße trotz einschlägiger Er- und Abmahnungen vor, siehe dazu unten. Die Beklagte durfte diesen weiteren Verstoß daher zum Anlass für die Kündigung nehmen.

2.3.2. Die Kündigung ist verhältnismäßig. Steuerbares Verhalten eines Arbeitnehmers rechtfertigt in aller Regel nur nach erfolgloser einschlägiger Abmahnung eine Kündigung (st. Rspr., vgl. z.B. BAG, Urteil vom 20.11.2014, Az. 2 AZR 651/13, juris). Hier liegen einschlägige wirksame Abmahnungen vor, die eine

negative Prognose bzgl. der weiteren störungsfreien Durchführung des Arbeitsverhältnisses rechtfertigen.

2.3.2.1. Mit einer Abmahnung übt ein Arbeitgeber seine arbeitsvertraglichen Gläubigerrechte in doppelter Hinsicht aus. Zum einen weist er den Arbeitnehmer als seinen Schuldner auf dessen vertragliche Pflichten hin und macht ihn auf die Verletzung dieser Pflichten aufmerksam (Rüge- und Dokumentationsfunktion). Zum anderen fordert er ihn für die Zukunft zu einem vertragstreuen Verhalten auf und kündigt, sofern ihm dies angebracht erscheint, individualrechtliche Konsequenzen für den Fall einer erneuten Pflichtverletzung an (Warnfunktion; BAG, Urteil vom 19.07.2012, Az. 2 AZR 782/11, juris, m.w.N.).

2.3.2.2. Diesen Anforderungen wird insbesondere die Abmahnung vom 22.07.2020 bezüglich der Verstöße gegen die Clean Desk Policy gerecht. Sie enthält den erforderlichen Warnhinweis dergestalt, dass die Klägerin bei weiteren Verstößen mit arbeitsvertraglichen Maßnahmen bis hin zur Kündigung rechnen müsse.

Die Abmahnung wird auch der Rügefunktion gerecht, denn es wird für den 03.06.2020 ausgeführt, dass die Klägerin gegen die Clean Desk Policy verstoßen habe, weil sie auf ihrem Schreibtisch papierhafte Kreditakten und ausgedruckte E-Mails trotz ihrer Abwesenheit liegen gelassen hat. Gleiches gilt für den Vorwurf bzgl. des 09.06.2020, wo auf der Schreibtischunterlage Hauptdarlehensnummern von Kunden vermerkt sowie der Datenmüll nicht ordnungsgemäß entsorgt waren.

Ebenso verhält es sich für den Vorwurf, es sei am 19.06.2020 bei einer aufgrund der Corona-Pandemie notwendigen Desinfektion und der diesbezüglich vorherigen Beräumung der Schreibtische festgestellt worden, dass durch die Klägerin mehrere Klebezettel mit verschiedenen Darlehensnummern auf dem Schreibtisch angebracht waren. Die Klägerin tritt den Abmahnungen unter den Gesichtspunkten Rüge- und Warnfunktion auch nicht entgegen.

Die der Abmahnung zugrundeliegenden Tatsachen hat die Klägerin nicht bestritten. Entgegen ihrer Ansicht rechtfertigen diese den Ausspruch einer Abmahnung.

Zwar schließt sich die Kammer der auf die Entscheidung des Landesarbeitsgerichts Schleswig-Holstein (Urteil vom 29.11.2005, Az. 2 Sa 350/05, juris) gestützten Ansicht der Beklagten nicht an, wonach das Verhältnismäßigkeitsprinzip auf Abmahnungen keine Anwendung finde. Zum einen lässt sich dies der genannten Entscheidung so schon nicht entnehmen. Das Landesarbeitsgericht Schleswig-Holstein führt vielmehr aus wie folgt:

„Der Verhältnismäßigkeitsgrundsatz ist im Rahmen der gerichtlichen Abmahnungskontrolle nur insoweit von Bedeutung, als Form und Umstände der Abmahnung gemeint sind, nicht die Frage, ob die Abmahnung als solche eine Überreaktion darstellt (LAG Köln, Urt. v. 12.05.1995 – 13 Sa 137/95 – NZA-RR 1996 – 204). Ebenso ist für den Gleichbehandlungsgrundsatz im Abmahnungsrecht nicht Raum (LAG Köln a.a.O.).“

Das Landesarbeitsgericht Schleswig-Holstein stützt seine Entscheidung dabei auf das Urteil des Bundesarbeitsgerichts vom 31. August 1994 (Az. 7 AZR 893/93, juris). Dort heißt es:

„Bei Abmahnungen im Arbeitsverhältnis ist der Grundsatz der Verhältnismäßigkeit zu beachten (BAG Urteil vom 7. November 1979 – 5 AZR 962/77 – AP Nr. 3 zu § 87 BetrVG 1972 Betriebsbuße, zu II 2 c der Gründe; BAG Urteil vom 13. November 1991 – 5 AZR 74/91 – AP Nr. 7 zu § 611 BGB Abmahnung). Danach ist die Ausübung eines einseitigen Bestimmungsrechts unzulässig, wenn sie der Gegenseite unverhältnismäßig große Nachteile zufügt und andere weniger schwerwiegende Maßnahmen möglich gewesen wären, die den Interessen des Berechtigten

ebensogut Rechnung getragen hätten oder ihm zumindest zumutbar gewesen wären. Der Grundsatz der Verhältnismäßigkeit wird als Übermaßverbot zur Vermeidung schwerwiegender Rechtsfolgen bei nur geringfügigen Rechtsverstößen verstanden (BGH Urteil vom 19. Dezember 1979 – VIII ZR 46/79 – WM 1980, 215, 216). Bei der Verletzung arbeitsvertraglicher Pflichten durch den Arbeitnehmer hat der Arbeitgeber als Gläubiger der Arbeitsleistung zunächst selbst zu entscheiden, ob er ein Fehlverhalten des Arbeitnehmers mißbilligen will und ob er deswegen eine mündliche oder schriftliche Abmahnung erteilen will (BAG Urteil vom 23. April 1986 – 5 AZR 340/85 –, n. v.; Herschel, Anm. zum BAG Urteil vom 22. Februar 1978 – 5 AZR 801/76 – AR-Blattei Betriebsbußen Nr. 9). Eine Abmahnung ist aber nicht allein deswegen unzulässig, weil der Arbeitgeber auch über den erhobenen Vorwurf hinwegsehen könnte (BAG Urteil vom 13. November 1991 – 5 AZR 74/91 – AP Nr. 7 zu § 611 BGB Abmahnung, zu II 2 der Gründe), weil etwa dem Arbeitnehmer ein bewußter Verstoß gegen arbeitsvertragliche Pflichten fern lag.“

Danach ist davon auszugehen, dass der Verhältnismäßigkeitsgrundsatz zu beachten ist und nur nicht dazu führt, dass z.B. – ohne weitere Anhaltspunkte – einer Abmahnung grundsätzlich immer eine Ermahnung vorauszugehen habe. Auch bei erstmaligem und nur leichtem Pflichtverstoß kann eine Abmahnung verhältnismäßig sein.

Soweit bei Pflichtverletzungen mehrere Reaktionen möglich sind, kann § 242 BGB vor allem bei Dauerschuldverhältnissen aber dazu verpflichten, die mildere Reaktion zu wählen (Grüneberg, in: Palandt, 80. Aufl. 2021, § 242 BGB Rn. 54). Als mildere Reaktion zur Abmahnung kommt grds. eine Ermahnung/Verwarnung/Verweis/Rüge in Betracht, also ein unterhalb der Schwelle der Abmahnung liegender Hinweis darauf, dass nach Auffassung des Arbeitgebers eine Pflichtverletzung vorliege, welcher aber nicht mit einer Warnung für die Zukunft hinsichtlich der Bestandsgefährdung verbunden wird. Im Unterschied zur Abmahnung dient die Ermahnung nicht der Vorbereitung einer Kündigung, da die erforderliche Warnfunktion fehlt. Der Arbeitgeber kann gehalten sein, den Arbeitnehmer auf sein Fehlverhalten hinzuweisen, ohne ihm sofort Konsequenzen für das Arbeitsverhältnis im Wiederholungsfall anzudrohen.

Unverhältnismäßig ist eine Maßnahme dann, wenn in einem Konflikt von Interessen und Freiheiten diese auf einer Seite mehr als nötig geschmälert werden, als es für den anzustrebenden Ausgleich notwendig ist (vgl. dazu das Urteil des Sächsischen Landesarbeitsgericht vom 24. Februar 2022 – 2 Sa 453/20 –, Rn. 47, juris).

Vorliegend ist das Übermaßverbot nicht verletzt. Die Klägerin macht geltend, dass es sich bei Darlehensnummern zwar um datenschutzrelevante Informationen handele, der Verstoß aber nicht schwer wiege, weil aus der bloßen Ziffernabfolge der Informationsgewinn für Dritte gleich Null sein dürfte. Dem kann wohl zugestimmt werden, ohne dass die Abmahnung in ihrer Gesamtheit dadurch unverhältnismäßig würde. Denn mit ihr wird auch das Liegenlassen von papierhaften Akten und ausgedruckten Emails auf dem Schreibtisch gerügt und ebenso die nicht ordnungsgemäße Entsorgung des Datenmülls. Die Klägerin verkennt, dass hier die Erheblichkeit auch bzgl. der Darlehensnummern aus der Anzahl der Verstöße resultiert und die Beklagte der Sache nach gerade die unstreitig aufgetretenen Flüchtigkeitsfehler und Nachlässigkeiten als bestandsgefährdend ansieht. Darüber hinaus sind sowohl das Liegenlassen der Akten als auch die fehlende Entsorgung des Datenmülls für sich

genommen als erheblich anzusehen. Die Beklagte war daher nicht gehalten, nur eine Rüge oder Ermahnung auszusprechen.

Dabei sind auch die weiteren der Klägerin ausgesprochenen und im Tatbestand dargestellten Ermahnungen und Abmahnungen zu berücksichtigen, mit Ausnahme derjenigen im weiteren Schreiben vom 22.07.2020 bzgl. der Weitergabe eines Falls trotz Feststellung des unzureichenden Marktwerts. Der Sachvortrag der Klägerin bzgl. einer hierzu erfolgten Rücksprache ist streitig. Wie dargestellt, ist die Beklagte für den Ausschluss dieser Rechtfertigung beweispflichtig. Die Beklagte hat entsprechenden Beweis auch angetreten (Schriftsatz vom 22.03.2021, dort Seite 5, Bl. 94 d.AA.). Es kommt für die Entscheidung über die Kündigung aber auf diese möglicherweise gegebene weitere Pflichtverletzung nicht an, so dass eine Einvernahme der benannten Zeugin unterbleiben konnte. Die unstreitigen Pflichtverletzungen genügen, um die Kündigung unter dem Gesichtspunkt vorheriger Abmahnung nicht als unverhältnismäßig erscheinen zu lassen.

2.3.2.3. Die Ermahnung vom 02.12.2019 bzgl. der Rückgabe eines Falls an VDV greift die Klägerin nicht an. Die Kammer legt diese daher der Beurteilung der Kündigung mit zu Grunde.

2.3.2.4. Gegen die Ermahnung vom 27.04.2020 (Auftrag Wertermittlung nicht im Cockpit als erledigt gekennzeichnet) wendet die Klägerin ein, es handele sich um einen Flüchtigkeitsfehler, siehe dazu noch unten.

2.3.2.5. Die Abmahnungen vom 03.06.2020 und vom 22.07.2020 (jeweils fehlende Abmeldung von IT-Systemen) entsprechen sowohl den Anforderungen an die Rüge- als auch an die Warnfunktion. Die von der Beklagten vorgetragene Tatsache sind unstreitig. Die Klägerin wendet ein, es sei bedauerlich, dass – unstreitig – systemseitig nicht vorgesehen ist, dass alle Anwendungen automatisch geschlossen werden, wenn man sich vom System abmeldet. Es sei von der Klägerin nicht intendiert gewesen, dass die Kolleginnen und Kollegen dadurch die Probedatei (den Dummy-Fall) für die Berechnung von Voranfragen ohne HD-Nr. – unstreitig – nicht nutzen konnten. Die Klägerin habe hier einen Fehler gemacht, der nicht vorkommen dürfe, sich aber im laufenden Geschäft als menschlich herausstelle und dem Grunde nach durch technische Vorrichtungen habe vermieden werden können. Eine Abmahnung rechtfertige das vergessene Schließen des Dokuments nicht.

Damit verkennt die Klägerin, dass es auf eine Absicht bzgl. der Pflichtverletzung nicht ankommt. Auch eine fahrlässige Handlungsweise ist schuldhaft, § 276 BGB. Die Klägerin verkennt weiter, dass die von ihr eingestandenen Flüchtigkeitsfehler, Nachlässigkeiten und Versehen gerade die Schlechtleistung darstellen, die die Beklagte rügt. Es ist zwar grundsätzlich eine Arbeitsleistung „mittlerer Art und Güte“ geschuldet. Dabei kann es also auch vorkommen, dass entsprechende Fehler mal passieren, wie dies im von der Klägerin angeführten Fall des Kollegen gewesen sein dürfte, auf den der Vorgesetzte per E-Mail am 28.07.2020 reagiert hat mit der Bewertung des vergessenen Abschließens einer Checkliste in CVM II als „trivialem Prozessthema“. Eine – hier feststellbare – Vielzahl an solchen Fehlern ist aber nicht mehr als „mittlerer Art und Güte“ anzusehen. Es genügen insoweit Umstände, die aus Sicht eines ruhig und verständlich urteilenden Arbeitgebers eine Kündigung als angemessene Reaktion auf das Fehlverhalten des Arbeitnehmers erscheinen lassen (BAG, Urteil vom 17.01.2008, Az. 2 AZR 536/06, juris, m.w.N.). Gleiches gilt für die Erteilung einer Abmahnung. Dass der Arbeitsprozess evtl. verbessert werden

könnte, wenn eine Abmeldung vom System automatisch zur Schließung aller Anwendungen führen würde, entbindet die Klägerin nicht davon, sorgfältig zu arbeiten, solange dies nicht der Fall ist.

2.3.2.6. Die vorgenannten Abmahnungen sind auch einschlägig. Das gilt insbesondere, aber nicht nur für die Abmahnung vom 22.07.2020 bzgl. der Einhaltung der Vorgaben der Clean desk policy.

Nach der Rechtsprechung des Bundesarbeitsgerichtes ist es für eine negative Prognose ausreichend, wenn die jeweiligen Pflichtwidrigkeiten aus demselben Bereich stammen und somit Abmahnungs- und Kündigungsgründe in einem inneren Zusammenhang stehen (BAG, Urteil vom 13.12.2007, Az. 2 AZR 818/06, juris, unter Hinweis auf BAG, Urteil vom 16. Januar 1992, Az. 2 AZR 412/91, ebenfalls juris). Wie oben schon ausgeführt, handelt es sich um Pflichtverstöße aus Nachlässigkeit bzw. Flüchtigkeit, verstoßen wird gegen ausdrückliche mündliche und schriftliche Arbeitsanweisungen. Die Ansicht, das Liegenlassen von Akten auf dem Schreibtisch sei ein anderer Verstoß gegen die Clean desk policy, als das fehlende Abschließen des Schreibtisches, ist zu streng. Mit diesem Maßstab dürften Kündigungen nur noch ausgesprochen werden, wenn wirklich exakt derselbe Verstoß gegeben wäre. So verhält es sich aber nicht, siehe die zitierte und zutreffende Rechtsprechung des Bundesarbeitsgerichts, der sich die Kammer aus eigenen Erwägungen anschließt. Ob auch die Abmahnung vom 25.08.2020 bzgl. der Eintragungen in die Übersicht für das Zielerreichungstool rechtmäßig erteilt wurde und einschlägig ist, kann angesichts der vorstehenden Ausführungen offenbleiben. Auch hier rechtfertigt sich die Klägerin wieder mit „Zahldreihern“, also mit Flüchtigkeitsfehlern. Eben diese möchte und muss die Beklagte aber nicht weiter hinnehmen.

Das Bundesarbeitsgericht führt hierzu in der o.g. Entscheidung vom 13.12.2007 dazu aus, was folgt:

„Selbst wenn kein gravierender Verstoß gegen arbeitsvertragliche Verpflichtungen vorliegt, (ist) eine negative Prognose dann gegeben ..., wenn der Arbeitnehmer nach einer Abmahnung den Vertrag in gleicher oder ähnlicher Art erneut verletzt (vgl. hierzu BAG, NZA 2008, 589, Rn. 38). Es kann insofern ein Schluss auf eine negative Entwicklung des Arbeitsverhältnisses gezogen werden, wenn wiederholte Vertragsverletzungen vorliegen.“

2.3.3. Die vorzunehmende Interessenabwägung führt ebenfalls nicht zur Unwirksamkeit der Kündigung.

Wie vorstehend dargestellt, handelt es sich in der Summe um erhebliche Pflichtverletzungen, die auch zu Ablaufstörungen bei der Beklagten geführt haben. Der die Kündigung letztlich auslösende Verstoß gegen die Datenschutzvorgaben ist für sich gesehen ebenfalls erheblich, auch wenn die Klägerin dies nicht einsehen will, siehe dazu schon oben. Zugunsten der Klägerin sind ihre Unterhaltsverpflichtungen gegenüber 3 Kindern zu berücksichtigen sowie eine Betriebszugehörigkeit von rund vier-einhalb Jahren. Die Kammer verkennt hier nicht, dass insbesondere die Unterhaltsverpflichtungen dazu führen, dass die Klägerin von der Kündigung erheblich betroffen ist. Sie hatte aber genügend Zeit und Gelegenheit, ihre Arbeitsleistung „mittlerer Art und Güte“ zu erbringen. Es ist der Beklagten nicht zuzumuten, weitere Abmahnungen auszusprechen, die keine Verbesserungen zeitigen. Sie muss im Gegenteil aufpassen, dass aufgrund der Vielzahl die Warnfunktion nicht verloren geht. Die 51 Jahre alte Klägerin hat durchaus noch Aussicht, auf dem Arbeitsmarkt eine vergleichbare Stelle zu finden. Die Betriebszugehörigkeit ist vergleichsweise kurz.

3. Die Kündigung ist auch nicht gemäß § 102 Abs. 1 Satz 3 BetrVG unwirksam, denn die Beklagte hat die erforderliche Betriebsratsanhörung ordnungsgemäß durchgeführt.

3.1. Gemäß § 102 Abs. 1 S. 3 BetrVG ist die ohne Beteiligung des Betriebs- oder Personalrats erfolgte Kündigung unwirksam (vgl. BAG 16.03.2000 EzA § 108 BPersVG Nr. 2). Das gilt aufgrund einer ausdehnenden Auslegung dieser Vorschrift auch dann, wenn das Anhörungsverfahren nicht wirksam eingeleitet oder durchgeführt oder abgeschlossen worden ist (BAG 04.06.2003 EzA § 209 InsO Nr. 1; 06.10.2005 EzA § 102 BetrVG 2001 Nr. 16; Landesarbeitsgericht BW 11.08.2006 LAGE § 102 BetrVG 2001 Nr. V; vgl. Dörner/Luczak/Wildschütz/Baeck/Hoß, Handbuch des Fachanwalts Arbeitsrecht; DLW/Dörner, 15. Aufl. 2020, Kap. 4 Rz. 354 ff.).

Das Anhörungsverfahren ist dann abgeschlossen, wenn die Äußerungsfrist gemäß § 102 Abs. 2 BetrVG (eine Woche für die ordentliche Kündigung) abgelaufen ist oder der Betriebsrat bereits vorher eine abschließende Stellungnahme abgegeben hat.

Einer Äußerung des Betriebsrats während des Anhörungsverfahrens kommt nur fristverkürzende Wirkung zu, wenn ihr der Arbeitgeber unzweifelhaft entnehmen kann, dass es sich um eine abschließende Stellungnahme handelt. Dies ist beispielsweise dann der Fall, wenn es sich um ein Formular des Arbeitgebers handelt, aufgrund dessen der Betriebsrat eine „abschließende“ Stellungnahme durch Ankreuzen des entsprechenden Kästchens abgibt. Erklärt der Betriebsrat dies – wie im vorliegenden Fall – nicht ausdrücklich, ist der Inhalt seiner Mitteilung durch Auslegung entsprechend den §§ 133, 157 BGB zu ermitteln. Diese Auslegung muss eindeutig ergeben, dass der Betriebsrat sich bis zum Ablauf der Anhörungsfrist nicht noch einmal – und sei es „nur“ zur Ergänzung der Begründung seiner bereits eröffneten Entschließung – äußern möchte. Der Arbeitgeber muss aufgrund der bisherigen Äußerungen des Betriebsrats davon ausgehen können, dieser werde unter keinen Umständen mehr tun als bereits geschehen (vgl. zum Vorstehenden die Entscheidung des BAG vom 25.05.2016 – 2 AZR 345/15, Rdn. 24 mit weiteren Zitaten der ständigen Rechtsprechung des Senats). Die Annahme einer vorfristig abgegebenen verfahrensbeendenden Äußerung bedarf nach diesen Ausführungen „besonderer Anhaltspunkte“. Solche liegen regelmäßig vor, wenn der Betriebsrat dem Arbeitgeber mitteilt, er stimme der beabsichtigten Kündigung ausdrücklich und vorbehaltlos zu oder erklärt, von einer Äußerung zur Kündigungsabsicht abzusehen (BAG, Urteil vom 25. Mai 2016, Az. 2 AZR 345/15, BAGE 155, 181-190, juris).

3.2. Hier wurde am 08.12.2020 dem Vorsitzenden des Betriebsrates zur Anhörung das in Kopie als Anlage B7 vorgelegte Schreiben zugeleitet. Das Schreiben enthält alle erforderlichen Angaben, Fehler sind weder erkennbar noch von der Klägerin gerügt. Unter dem 10.12.2020 teilte der Betriebsrat darauf Folgendes mit:

„In der Sitzung vom 10.12.2020 hat der Betriebsrat einstimmig beschlossen, zur beabsichtigten Kündigung keine Stellungnahme abzugeben.“

(vgl. Anlage B8, Bl. 66 d.AA.)

Die Wochenfrist war somit bei Ausspruch der Kündigung am 16.12.2020, § 130 Abs. 1 BGB, bereits abgelaufen, darüber hinaus liegt eine abschließende Stellungnahme vor.

4. Die somit wirksame Kündigung wurde unter Einhaltung der Frist aus § 622 Abs. 2 Nr. 1 BGB ausgesprochen, zu anderen Fristen haben die Parteien nicht vorgetragen.

Aus Nr. 8.1. des Arbeitsvertrages ergibt sich, dass für das Arbeitsverhältnis die einschlägigen Tarifverträge der Deutsche Post-

bank AG in ihrer jeweils gültigen Fassung anzuwenden sind, soweit in diesem Arbeitsvertrag nicht ausdrücklich etwas anderes vereinbart ist. Laut Nr. 10.3. des Arbeitsvertrages gelten die im einschlägigen Tarifvertrag vorgesehenen Kündigungsfristen. Dass diese nicht eingehalten sei, hat die Klägerin nicht geltend gemacht.

IV. Da das Arbeitsverhältnis beendet ist, steht der Klägerin die Weiterbeschäftigung nicht zu. Die Anschlussberufung war daher zurückzuweisen.

V. Die Entscheidung über die Kosten folgt aus § 91 Abs. 1 ZPO, die Klägerin unterliegt in erster wie in zweiter Instanz vollständig.

Gründe für die Zulassung der Revision im Sinne des § 72 Abs. 2 ArbGG sind weder erkennbar noch vorgebracht. Es liegt insbesondere keine entscheidungserhebliche Rechtsfrage grundsätzlicher Bedeutung vor, die Kammer hat vielmehr einen Einzelfall unter Berücksichtigung der höchstgerichtlichen Rechtsprechung entschieden.

Auf die Möglichkeit einer Nichtzulassungsbeschwerde nach § 72 a ArbGG wird hingewiesen.

Datenzugangsrechte von Betriebsrats-Wahlinitiatoren fehlen (Ls)

(Arbeitsgericht Berlin, Beschluss vom 26. August 2022 – 41 BVGa 7430/22 –)

1. In einem betriebsratslosen Betrieb besteht mangels gesetzlicher Regelung kein Anspruch der Wahlinitiatoren gegen den Arbeitgeber auf Herausgabe von Arbeitnehmerlisten für die Durchführung einer Betriebsversammlung zur Wahl eines Wahlvorstandes.
2. Der Gesetzgeber hat in § 2 Abs. 2 WO Auskunfts- und Herausgabeansprüche zur Erstellung der Wählerlisten nur für den Wahlvorstand vorgesehen. Diese gesetzliche Regelung kann nicht entsprechend auf die vorliegende Fallgestaltung angewendet werden. Es fehlt insoweit an einer unbewussten Gesetzeslücke.

Selbstbestimmung Minderjähriger gegenüber Auskunftserteilung an den Vater (Ls)

(Interdiözesanes Datenschutzgericht (römisch-katholische Kirche), Beschluss vom 25. Februar 2022 – IDSG 23/2020 –)

Der Auskunftsanspruch des Vaters nach § 17 Abs. 1 KDG gegen einen kirchlichen Heimträger mit dem Ziel, Kenntnis von nach Unterbringung der 16-jährigen Tochter erstellten Dokumente zur familiären Situation zu erlangen, ist bei einem entgegenstehenden Willen der Tochter nach § 17 Abs. 4 KDG abzulehnen.

Verpflichtung zur Aufbewahrung von Beistandsakten (Ls)

(Interdiözesanes Datenschutzgericht (römisch-katholische Kirche), Beschluss vom 25. April 2022 – IDSG 10/2021 –)

1. Eine für die Verfahrensbeistandschaft nach § 158 FamFG einschlägige gesetzliche Aufbewahrungsfrist findet sich weder im Zivilrecht noch im öffentlichen Recht, etwa im Sozialgesetzbuch Achtes Buch (SGB VIII).
2. Die Vernichtung der Akte des Verfahrensbeistandes nach erstinstanzlicher Entscheidung des Familiengerichts ist unzulässig und verletzt den von der Datenverarbeitung Betroffenen in seinen Rechten. Auch nach Eintritt der Rechtskraft einer familiengerichtlichen Entscheidung ist eine weitere Aufbewahrung der Beistandsakte geboten.
3. Für Schadenersatzbegehren ist der Rechtsweg zu den kirchlichen Datenschutzgerichten nicht eröffnet. Hierfür sind die staatlichen Zivilgerichte zuständig (vgl. § 47 Abs. 2 KDG).

(Eingesandt und Leitsätze von G. Walther, Frankfurt)

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



Berichte, Informationen, Sonstiges

Bitkom-Umfrage: Nur 22 Prozent der Unternehmen setzen DS-GVO vollständig um

Seit Mai 2018 gilt innerhalb der Europäischen Union die DS-GVO. Laut einer Bitkom-Umfrage haben lediglich 22 Prozent der Unternehmen die Regelungen vollständig umgesetzt. Sie bemängeln, dass der strenge Datenschutz die Digitalisierung erschwert.

Die Europäische Datenschutz-Grundverordnung (DS-GVO) stößt in der deutschen Wirtschaft weiterhin auf Kritik. Das geht aus einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom unter Unternehmen ab 20 Beschäftigten in Deutschland hervor, die am Dienstag in Berlin veröffentlicht wurde. Auch im fünften Jahr seit dem Inkrafttreten der Datenschutzaufgaben bestehe eine erhebliche Rechtsunsicherheit zu den genauen Vorgaben der DS-GVO, erklärten 78 Prozent der befragten Unternehmen. Die Umsetzung der Verordnung sei etwa wegen neuer Richtlinien dazu nie vollständig abgeschlossen, bemängelten 88 Prozent.

Nur 22 Prozent setzten DS-GVO vollständig um

Gut zwei Drittel (68 Prozent) der Unternehmen sind der Auffassung, dass der strenge Datenschutz die Digitalisierung erschwere, sagte Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung. 61 Prozent meinen, in Deutschland übertreibe man es mit dem Datenschutz. Trotzdem hat die Mehrheit der Unternehmen die DS-GVO umgesetzt. 22 Prozent reklamieren für sich, die DS-GVO vollständig umgesetzt zu haben, 40 Prozent „größtenteils“. Ein Drittel räumt ein, sich nur „teilweise“ an die Verordnung angepasst zu haben.

Die Defizite bei der Umsetzung sind nicht mehr so häufig auf fehlendes Fachpersonal zurückzuführen. Vor

einem Jahr beklagte ein Drittel der Unternehmen einen Mangel an qualifizierten Beschäftigten. Dieser Wert sank in der aktuellen Umfrage auf 24 Prozent. Und auch bei den benötigten Finanzmitteln zeichnet sich eine leichte Entspannung ab: 2021 nannten 37 Prozent „fehlende finanzielle Ressourcen“ als eine der größten Herausforderungen bei der DS-GVO-Umsetzung, in der aktuellen Umfrage sank der Wert auf 32 Prozent.

Globale Lösung notwendig

In der Umfrage machten die Unternehmen weiterhin deutlich, wie wichtig eine Rechtsgrundlage für internationale Datentransfers ist. 60 Prozent praktizieren eine Übertragung von personenbezogenen Daten in Länder außerhalb der EU. Ein Verzicht dieser Datentransfers habe gravierende Folgen. 60 Prozent der Unternehmen sagen, sie könnten dann einen globalen Sicherheits-Support nicht mehr aufrechterhalten, 57 Prozent geben an, dass sie bei einem Aus für Datentransfers bestimmte Produkte und Dienstleistungen nicht mehr anbieten könnten. 55 Prozent befürchten in diesem Fall Wettbewerbsnachteile gegenüber Unternehmen aus Nicht-EU-Ländern.

Die Datentransfers in Länder außerhalb der EU stehen rechtlich auf wackeligen Beinen, weil der Europäische Gerichtshof in zwei Entscheidungen Absprachen für die Übermittlung von Daten aus Europa über den Atlantik für ungültig erklärt hat. Im Juni 2020 hatte der EuGH den „Privacy Shield“ mit der Begründung gekippt, dass das Datenschutzniveau in den USA nicht den Standards der EU entspreche. Die Richter bemängelten vor allem die weitreichenden Zugriffsmöglichkeiten von US-Geheimdiensten auf Daten von Europäern. Mit einer ähnlichen Begründung hatte der EuGH im Oktober 2015 bereit das transatlantische Datenschutz-Abkommen „Safe Harbor“ eingekassiert.

Rekordstrafe von 405 Millionen Euro für Instagram

In Irland waren auf Instagram vorübergehend die persönlichen Daten von Teenagern öffentlich zugänglich. Foto: prima91 – stock.adobe.com

Weil zeitweise neben den Social-Media-Inhalten auch die Telefonnummern und E-Mail-Adressen von Teenagern öffentlich waren, hat die irische Datenschutzbehörde gegen Instagram eine Geldstrafe von 405 Millionen Euro verhängt.

Wegen schwerer Verstöße gegen Datenschutzregeln für Kinder muss das soziale Netzwerk Instagram in Irland 405 Millionen Euro Strafe zahlen. „Wir haben unsere endgültige Entscheidung am vergangenen Freitag getroffen, und sie enthält eine Geldstrafe in Höhe von 405 Millionen Euro“, sagte der Sprecher des irischen Datenschutzbeauftragten der Nachrichtenagentur Reuters zufolge. Die vollständigen Details der Entscheidung werden demnach in der kommenden Woche veröffentlicht. Es ist die höchste Geldbuße, die die irische Datenschutzbehörde (DPC) bisher verhängt hat, wie der Sender RTÉ am Dienstag berichtete.

Die Tochter des Internetriesen Meta hatte Jugendlichen im Alter von 13 bis 17 Jahren erlaubt, „Business-Accounts“ auf der Plattform zu betreiben. Dadurch waren Telefonnummern und E-Mail-Adressen der Teenager teils vorübergehend öffentlich. Zudem seien die Konten von Kindern standardmäßig auf „öffentlich“ gesetzt worden und mussten eigenständig auf „privat“ geschaltet werden. Dadurch waren ihre Social-Media-Inhalte von allen Nutzern einsehbar.

Die DPC hatte bereits 2021 wegen Verstößen gegen Datenschutzregeln eine Geldstrafe von 225 Millionen Euro gegen die Meta-Tochter WhatsApp verhängt sowie im März 2022 eine weitere Strafe von 17 Millionen Euro

gegen den Mutterkonzern ebenfalls wegen Datenschutzverstößen.

Zum Konzern Meta Platforms gehört auch die Internet-Plattform Facebook.

Meta betonte in einer Stellungnahme, es habe sich um veraltete Einstellungen gehandelt, die der Konzern längst überarbeitet habe. Die Konten von

unter 18-Jährigen seien beim Beitritt nun standardmäßig auf „privat“ gesetzt. Der Konzern kündigte an, die Entscheidung anzufechten.

Literaturhinweise

*Carla-Charlotte Schmidt, **Regelungsoptionen des deutschen Gesetzgebers zum Whistleblower-Schutz in Umsetzung der EU-Richtlinie 2019/1937***, Abhandlungen zum deutschen und internationalen Arbeits- und Sozialrecht (ADIA), Band 9, Duncker & Humblot, Berlin 2022, 359 S., 109,90 €

Der Schutz von Whistleblowern ist seit Jahren Gegenstand juristischer und auch politischer Diskussionen. In Deutschland gibt es bisher jedoch keinen umfassenden gesetzlichen Schutz von Whistleblowern. Dies wird sich künftig jedoch ändern: Der deutsche Gesetzgeber ist zur Umsetzung der mindest-harmonisierenden EU-Richtlinie 2019/1937 zum Schutz von Personen verpflichtet, die Verstöße gegen das Unionsrecht melden (sog. Whistleblowing-Richtlinie). Die Arbeit zeigt die Regelungsoptionen des nationalen Gesetzgebers bei diesem gesetzgeberischen Vorhaben auf: Der Gesetzgeber muss im Rahmen der unionsrechtlich bestehenden Regelungsspielräume eine verfassungskonforme Rechtslage schaffen und hierbei Widersprüche zum geltenden Recht – insbesondere zum Völkerrecht, Datenschutzrecht und zu den Bestimmungen des Geschäftsgeheimnisgesetzes – vermeiden. Die Arbeit schließt mit der Darstellung eines Entwurfs eines Hinweisgeberschutzgesetzes.

(Redaktion)

*Jonas Michael Schnell, **Auskunft im Familienrecht zwischen Anspruch und Informationspflicht – Ein Beitrag zum extensiven Verständnis der Pflicht zur ungefragten Information***, Schriften zum Bürgerlichen Recht (BR), Band 543, Duncker & Humblot, Berlin 2022, 292 S., 89,90 €

Die Arbeit untersucht die Auskunft im Familienrecht in einem Gesamtzusammenhang. Somit erfolgt zum einen eine dogmatische Bestandsaufnahme der vier verschiedenen Quellen familienrechtlicher Auskunft: der normierten Anspruchsgrundlagen im BGB, der beiden familienrechtlichen Generalklauseln, eine auf Treu und Glauben basierende Auskunft im Kontext des Familienrechts sowie schließlich die Pflicht zur ungefragten Informationspreisgabe. Hierzu werden die verfolgten Normzwecke herausgearbeitet und diese als das verbindende Element familienrechtlicher Auskunft ermittelt. Darüber hinaus wird diese Verbindung daran verdeutlicht, dass auf ihrer Grundlage die bislang dem Bereich des Unterhaltsrechts vorbehaltene Pflicht zur ungefragten Information einer Erweiterung zugeführt wird und die hierfür erforderlichen dogmatischen Grundlagen herausgearbeitet werden. Im Einzelnen werden erörtert die allgemeinen Grundlagen zivilrechtlicher Auskunft, die Funktion und Systematik zivilrechtlicher Auskunftsansprüche, Familienrechtliche Auskunftsansprüche:

Der Auskunftsanspruch aus Treu und Glauben im Familienrecht: Die Pflicht zur ungefragten Information im Familienrecht.

(Redaktion)

*Peter Gola/Dirk Heckmann, **Datenschutz-Grundverordnung, BDSG: DS-GVO***, Kommentar, C.H. Beck Verlag, München 2022, 1864 S., 99,00 €

Die Beachtung des Datenschutzes ist eine existenzielle Vorgabe in fast allen Bereichen von Wirtschaft und Verwaltung. Informationsverarbeitung ist einerseits unverzichtbar, andererseits gilt es die Freiheitsrechte des „Betroffenen“ insbesondere angesichts stetig fortschreitender technischer Entwicklungen weiterhin zu gewährleisten. Aufgabe der Kommentierung bleibt es, das diesen Konflikt lösende Recht praxisnah darzustellen. Die Regelungen, die sich speziell der digitalen Lebenswelt der Bürgerin und des Bürgers annehmen, bedürfen dabei besonderer Betrachtung.

Die bislang getrennt erschienenen Kommentierungen der DS-GVO und des BDSG werden in dieser Neuauflage zusammengefasst. Erreicht wurde damit zum einen eine bessere Übersichtlichkeit, zum anderen die Straffung der Kommentierungen durch Verweisungen insbesondere dort, wo DS-GVO und BDSG inhaltsgleiche Regelungen enthalten. Dadurch wurde auch Platz für

die erforderliche Darstellung neuer gesetzlicher Regelungen und die Berücksichtigung aktueller Rechtsprechung, Literatur und Stellungnahmen der Aufsichtsbehörden gewonnen.

(Redaktion)

Peter Gola, Recht bei der Personalgewinnung – Datenschutz-, Wettbewerbs- und Arbeitsrecht in der Praxis, 1. Aufl., DATAKONTEXT Facherlag, Frechen 2022, 252 S., 69,99 €

Der mit der fortschreitenden Digitalisierung verbundene Fachkräftemangel macht in vielen Branchen neben der klassischen, auf die Bewerbung von unbekanntem Interessenten abstellende „Stellenausschreibung“ ein aktives Suchen und Rekrutieren von Beschäftigten seitens des Arbeitgebers nötig.

Unabhängig des für die Anwerbung von Beschäftigten gewählten Weges muss das Vorgehen mit den Vorgaben des Datenschutz-, des Wettbewerbs-, des Verbraucher- und des Gleichbehandlungsrechts vereinbar sein. Ferner sind Konkurrenzverbote, Geschäftsgeheimnisse und besonderen Vertraulichkeitspflichten ins Kalkül zu ziehen. Dies gilt insbesondere, wenn Arbeitnehmer im Rahmen eines „active sourcing“ bzw. „active recruitment“ aus einem bestehenden Arbeitsverhältnis abgeworben werden sollen.

Das Buch stellt die ineinandergreifenden Regelungsbereiche des Datenschutzes, Wettbewerbs-, des Gleichbehandlungs- und allgemeinen Arbeitsrechts mit folgenden Themenschwerpunkten dar:

- Gewinnung und Auswahl von Bewerbern – Grundsatz- und Verfahrensfragen gemäß DS-GVO und BDSG
- Unlautere wettbewerbliche Handlungen bei der Personalgewinnung nach dem UWG
- Gesetzliche und vertragliche Verbote von Konkurrenzaktivitäten nach HGB und BGB
- Das Geschäftsgeheimnis bei der An- / Abwerbung von Geheimnisträgern

- Der für die Verarbeitung von Bewerberdaten unter Vorgabe von DS-GVO, BDSG, AGG, BetrVG und GeschGehG geltende Zulässigkeitskatalog

(Redaktion)

Detlef Grimm/Jonas Singraven (Hrsg.), Digitalisierung und Arbeitsrecht, Verlag Dr. Otto Schmidt, Köln 2022, 506 S., 99,00 €

Das Werk behandelt in 29 Kapiteln alle wichtigen Trends, die sich im Zuge der digitalen Transformation für den Personalbereich ergeben. Ausgangspunkt ist dabei jeweils ein Sachproblem, in der Regel eine Umsetzungs Herausforderung der Personalabteilung, und keine Rechtsfrage. Beigetragen zu dem Werk hat ein Team folgender Autoren: Farzan Daneshian, Stefan Freh, Arne Gehrke, Malte Göbel, Detlef Grimm, Simon Kohm, Sebastian Pelzer, Patrick Pommerening und Jonas Singraven

Die Kapitel beantworten jeweils drei Fragen:

- Worum geht es?
- Welche rechtlichen Probleme und Herausforderungen können sich ergeben?
- Wie können diese rechtlichen Probleme (im Sinne einer Best Practice) gelöst werden?

Jedes Kapitel ist als in sich geschlossener Beitrag konzipiert. Dies soll es dem fachlich vorgebildeten Leser ermöglichen, sich mit dem behandelten Thema in kurzer Zeit vertraut zu machen.

Für Lösungsvorschläge im Rahmen der Best Practices werden insgesamt über 60 Formulare und Muster zur Verfügung gestellt (u.a. zu Betriebsvereinbarungen, Dienstanweisungen, speziellen Vertragsklauseln und viele mehr).

Besonders hilfreich: Sie nutzen das gesamte Werk und alle Muster komfortabel online.

In sieben Teilen werden folgende Themenbereiche abgedeckt:

- Flexibilisierung der Arbeit
- Unternehmensübergreifende Zusammenarbeit und Freelancer
- Digitale Prozesse und Datenschutz
- Schutz von Knowhow
- Arbeitsschutz 4.0
- Recruitment und Personalentwicklung
- Social Media und Web 2.0

Dabei vereinfacht das Werk die rechtlichen Probleme nicht, sondern behandelt sie erschöpfend. Die Beiträge stellen den Meinungsstand zu den einschlägigen Rechtsfragen in Rechtsprechung und Literatur eingehend dar und ergreifen im Rahmen der aktuellen rechtswissenschaftlichen Diskussionen Position.

(Schriftleitung)

Josef Haverkamp, Datenschutz – Grundlagen, Empfehlungen und Arbeitshilfen für Betriebs- und Personalräte, 3. Aufl., Bund-Verlag, Frankfurt 2022, 420 S., 32,00 €

Gut vier Jahre nach Inkrafttreten der Datenschutz-Grundverordnung und des neuen Bundesdatenschutzgesetzes gibt es noch immer viele Baustellen im Datenschutz. Aber so langsam werden die Anforderungen an Arbeitgeber und Interessenvertretungen klarer. Die Schonzeit ist vorbei..

Was müssen Interessenvertretungen beim Datenschutz beachten? Der umfassend aktualisierte Ratgeber gibt Antwort, liefert Tipps und Hilfen ? mit Blick auf die Pflichten, die Mitbestimmungs- und Kontrollrechte von Betriebs- und Personalräten. Inhalt und Schwerpunkte der Neuauflage: sind u.a. ein Datenschutzkonzept der gesetzlichen Interessenvertretung, Muster-Verfahrensverzeichnisse für Betriebs- und Personalräte, Datenschutz in der Schwerbehindertenvertretung

(Redaktion)



Wie Handydaten Menschenleben verlängern können

Nach dem Ergebnis einer Untersuchung von Forschenden der Universität von Illinois in den USA können per Handy erhobene Daten sehr aufschlussreich sein. Die Informationen eines sechsminütigen Spaziergangs reichen danach aus, um das Sterberisiko eines Smartphone-Nutzers innerhalb der nächsten fünf Jahre vorzusagen. Basis dafür sind Daten von gut 100.000 Menschen aus der „UK Biobank“. Sie enthält Gesundheitsdaten von Erwachsenen aus dem Vereinigten Königreich. Mit Hilfe künstlicher Intelligenz entwickelte man unter Berücksichtigung der Bewegungsdaten und der Sterbefälle einen Algorithmus. Auf dessen Basis

lässt sich anhand von Bewegungsdaten eines sechsminütigen Spaziergangs das Sterberisiko innerhalb der nächsten fünf Jahre vorhersagen. Dabei macht sich die Technik die Aussagekraft typischer Muster zunutze. Parameter ist bei Herz- oder Lungenerkrankungen etwa, ob eine Person beim Spaziergang langsamer wird, wenn sie außer Atem ist und dann in kurzen Abständen wieder schneller. Weil Smartphones bei kurzen Spaziergängen dieselben Bewegungsdaten erfassen wie die im Rahmen der Studie genutzten Bewegungssensoren, planen die Forscher nun eine Studie mit reinen Handydaten. Bei Menschen, die ihre Smartphones mit

sich führen, kann man – so die Forscher – wöchentliche oder monatliche Vorhersagen errechnen. Rückt das Ende wegen mangelnder Bewegung näher, kann man gegensteuern. Für Menschen, die so etwas wollen, kann das ein sinnvolles Angebot sein, denn schließlich wird das Sterberisiko errechnet und nicht mehr gefühlt.





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 349 €.



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

Fachkräfte rechtssicher rekrutieren

NEU!



Recht bei der Personalgewinnung
Datenschutz-, Wettbewerbs- und Arbeitsrecht in der Praxis
Prof. Peter Gola

1. Auflage 2023, 248 Seiten, Hardcover 17 cm x 24 cm
ISBN: 978-3-89577-939-8

69,99 € mit E-Book zum Download (PDF)

Jetzt bestellen: datakontext.com/personalgewinnung