ISSN 0178-8930
HZ208364

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

4/2021

Recht der Datenverarbeitung

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

Aufsätze

GOLA, Das Betriebsrätemodernisierungsgesetz und die parallele Neufassung des BPersVG

CONRAD/SEITER, Inhaltliche Herausforderungen bei der Auftragsverarbeitung nach Art. 28 DS-GVO

EICHMANN/NOWAK, Zum Rechtsrahmen für den transatlantischen Datenverkehr

ZIELBAUER, Personenfotografie im nicht-journalistischen Bereich

Kurzbeiträge

BLECKAT, Abdingbarkeit des Art. 32 DS-GVO durch Einwilligung

GOLA, Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (54): Aspekte des Beschäftigtendatenschutzes im 30. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

CLAUS/REIF, Praxisfälle zum Datenschutzrecht XI: Die Kundenbefragung

LEPPERHOFF, Rechtsgrundlagen zur Verarbeitung von Kopf- und Körpermaßen

Rechtsprechung

Aus dem Inhalt

EUGH, Voraussetzungen für Ausübung der Befugnisse der nationalen Aufsichtsbehörden bei grenzüberschreitender Datenverarbeitung (Ls)

EUGH, Unmittelbare Wirkung des unionsrechtlich verankerten Grundsatzes des gleichen Entgelts (Ls)

EUGH, Feststellung einer Diskriminierung muss auch bei Anerkenntnis einer Schadensersatzforderung möglich sein (Ls)

EUGH, Unzulässigkeit der vollkommen anlasslosen Vorratsdatenspeicherung (Ls)

37. Jahrgang
August 2021
Seiten 179–240

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Datenschutz-Wissen aus erster Hand

GDD-Datenschutz Akademie Praxis-Reihe

Online-Kompaktkurse zum operativen Datenschutz

- ✓ 90 Minuten
- ✓ von Grundlagen- bis Spezialwissen
- ✓ für Ihren Expertenalltag

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

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht

37. Jahrgang 2021
Heft 4
Seiten 179–240

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 179

Veranstaltungen 180

Aufsätze

Prof. Peter GOLA
Das Betriebsrätemodernisierungsgesetz und die parallele Neufassung des BPersVG 181

Conrad Sebastian CONRAD/Stefan R. SEITER
Inhaltliche Herausforderungen bei der Auftragsverarbeitung nach Art. 28 DS-GVO 186

Nadine Eichmann/Jaroslaw Norbert NOWAK, LL.M.
Zum Rechtsrahmen für den transatlantischen Datenverkehr 194

RA Jochen ZIELBAUER, LL.M.
Personenfotografie im nicht-journalistischen Bereich 200

Kurzbeiträge

Alexander BLECKAT
Abdingbarkeit des Art. 32 DS-GVO durch Einwilligung 206

Prof. Peter GOLA
Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (54): Aspekte des Beschäftigtendatenschutzes im 30. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz 209

Miriam CLAUS, LL.M./Yvette REIF, LL.M.
Praxisfälle zum Datenschutzrecht XI: Die Kundenbefragung 212

Dr. Niels LEPPERHOFF
Rechtsgrundlagen zur Verarbeitung von Kopf- und Körpermaßen 215

Rechtsprechung

Voraussetzungen für Ausübung der Befugnisse der nationalen Aufsichtsbehörden bei grenzüberschreitender Datenverarbeitung (Ls)
(EuGH, Urteil vom 15.06.2021) 220

Unmittelbare Wirkung des unionsrechtlich verankerten Grundsatzes des gleichen Entgelts (Ls)
(EuGH, Urteil vom 03.06.2021) 221

Feststellung einer Diskriminierung muss auch bei Anerkenntnis einer Schadensersatzforderung möglich sein (Ls)
(EuGH, Urteil vom 15.04.2021) 221

Unzulässigkeit der vollkommen anlasslosen Vorratsdatenspeicherung (Ls)
(EuGH, Urteil vom 02.03.2021) 221

Zum Recht auf eigenständige Überprüfung des Messergebnisses und eines standardisierte Geschwindigkeits-Messverfahrens
(BVerfG, Beschluss vom 04.05.2021) 221

Vorlagepflicht zum EuGH bei Schadensersatz gem. Art. 82 DS-GVO
(BVerfG, Beschluss vom 14.01.2021) 222

Zur Reichweite des Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO
(BGH, Urteil vom 15.06.2021) 224

Elektronische Kommunikation der Bundesrechtsanwaltskammer (Ls)
(BGH, Urteil vom 22.03.2021) 227

Abmahnung eines Redakteurs wegen Nicht-Anzeige einer Nebentätigkeit (Ls)
(BAG, Urteil vom 15.06.2021) 227

Vorlage an den EuGH zum Abberufungsschutz eines Beauftragten für Datenschutz
(BAG, Beschluss vom 27.04.2021) 228

Zum Beseitigungsanspruch des Betriebsrats
(BAG, Beschluss vom 23.03.2021) 228

Rechtsweg im Konkurrentenstreit um ein öffentliches Amt (Ls)
(BVerwG, Beschluss vom 17.03.2021) 231

Anspruch eines fristlos gekündigten Personalratsmitglieds auf Erlass einer einstweiligen Verfügung zwecks Gestattung bzw. Duldung der weiteren Amtsausübung (Ls)
(BVerwG, Beschluss vom 04.02.2021) 231

Zur Ausrüstung des Betriebsrats mit Videokonferenztechnik (Ls)
(LAG Berlin-Brandenburg, Urteil vom 14.04.2021) 231

Zur Zulässigkeit videobeochteter Klauren wegen Corona (I) (Ls)
(OVG Nordrhein-Westfalen, Beschluss vom 04.03.2021) 231

Eignung einer audio-visuelle Übertragung (Videoaufsicht) zur Vermeidung von Täuschungsversuchen bei Prüfungen (Ls)
(OVG Schleswig-Holstein, Beschluss vom 03.03.2021)
Mit Anmerkung von Dr. Felix Neumann, M.A. 231

Gezieltes Fotografieren fremder Personen in der Öffentlichkeit ist unzulässig (Ls)
(AG Hamburg, Beschluss vom 03.07.2020) 233

Tätigkeit des DSB nach Art. 39 DS-GVO mit RDG vereinbar (Ls)
(AGH Nordrhein-Westfalen, Beschluss vom 12.03.2021) 233

Berichte, Informationen, Sonstiges

Verliebt am Arbeitsplatz – Aus dem aktuellen TB des BdgLfDI 235

Forum Privatheit: EU-Kommission hat aus den Schwächen der DS-GVO gelernt: Entwurf der KI-Verordnung regelt Gefahren für Grundrechte deutlich konkreter 235

BDSG feiert 45-jähriges Jubiläum 236

22. Euroforum Datenschutzkongress 236

Literaturhinweise

Buchbesprechungen

Flemming Moos/Jens Schuftig/Marian Alexander Arning (Hrsg.), Praxishandbuch DS-GVO
(SCHRIFTLEITUNG) 237

Dennis-Kenji Kipker,/Friederike Voskamp (Hrsg.), Sozialdatenschutz in der Praxis
(SCHRIFTLEITUNG) 237

Lukas Zeyher, Strafprozessuale Beweisverwertung von privatem Videomaterial am aktuellen Beispiel der Dashcam
(SCHRIFTLEITUNG) 238

Maike Flink, Beschäftigtendatenschutz als Aufgabe des Betriebsrats
(SCHRIFTLEITUNG) 238

Flemming Moos (Hrsg.), Datenschutz und Datennutzung – Verträge – Datenschutzklauseln – Datenschutzerklärungen
(SCHRIFTLEITUNG) 238

Neuerscheinungen

Aufsätze 239

Nachgefasst 240

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

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

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

in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

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

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

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

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

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

Prof. Dr. Karl LINNENKOHL, Universität Kassel

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

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

Prof. Dr. Michael RONELLENFITSCH, Hessischer Datenschutzbeauftragter

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

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

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

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

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 4/2021

Manuskripte:
Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an die Schriftleitung erbeten. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Beiträge werden grundsätzlich nur angenommen, wenn sie nicht einer anderen Zeitschrift zur Veröffentlichung angeboten wurden. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Autor alle Rechte, insbesondere das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken mit Hilfe fotomechanischer oder anderer Verfahren.

Urheber- und Verlagsrechte:
Sie sind einschließlich der Veröffentlichung als PDF im Online-Archiv vorbehalten. Sie erstrecken sich auch auf die veröffentlichten Gerichtsentscheidungen und deren Leitsätze; diese sind geschützt, soweit sie vom Einsender oder von der Schriftleitung erstellt oder bearbeitet sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen: Diese bedürfen zur Auswertung einer Genehmigung des Verlages.
Der Verlag gestattet in der Regel die Herstellung von Fotokopien zu innerbetrieblichen Zwecken, wenn dafür eine Gebühr an die VG Wort, Abteilung Wissenschaft, Goethestraße 49, 80336 München, entrichtet wird, von der die Zahlungsweise zu erfragen ist.

Schriftleitung
Prof. Peter Gola (federführend)
RA Dr. Georg Wronka
RA Andreas Jaspers
RDV-Schriftleitung@gdd.de

Redaktionsanschrift
Birgit Koppitsch
Heinrich-Böll-Ring 10, 53119 Bonn
Telefon: (02 28) 96 96 75-00
Telefax: (02 28) 96 96 75-25
RDV-Redaktion@gdd.de

Erscheinungsweise
6 x jährlich

Bezugspreis

Jahresabonnement	€ 155,–
Einzelheft	€ 25,–

MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Vertrieb
Dieter Schulz
Tel.: 02234/98949-99
dieter.schulz@datakontext.com

Abo-Service
Telefon: 089-2183-7110
Telefax: 089-2183-32
aboservice@hjr-verlag.de

Abbestellungen
Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Verlag
DATAKONTEXT GmbH, Frechen
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-30
Telefax: (0 22 34) 9 89 49-32
www.datakontext.com
Geschäftsführung: Dr. Karl Ulrich;
Hans-Günter Böse
HRB 337678

Satz
alka mediengestaltung gmbh
Willmuthstraße 30, 53332 Bornheim-Sechtem

Druck
Grafisches Centrum Cuno GmbH & Co. KG
Gewerbering West 27, 39240 Calbe (Saale)

Anzeigenverwaltung
DATAKONTEXT GmbH, Frechen
Wolfgang Scharf
Telefon: (0 22 34) 9 89 49-60
wolfgang.scharf@datakontext.com
www.datakontext.com

Zeitschrift für
Datenschutz–, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
37. Jahrgang 2021 Heft 4
Seiten 179–240

RDV
Recht der Datenverarbeitung

37. Jahrgang · August 2021 · Seiten 179–240

Editorial

45 Jahre BDSG

Die Datenschutzgesetzgebung verzeichnete zwei – wenn auch nicht ganz runde – Jubiläen. Das BDSG wurde 45 Jahre alt, und sein von ihm mitbestimmter Nachkömmling DS-GVO ist seit drei Jahren die maßgebende Datenschutznorm. Beides ist Anlass, eine (Zwischen-)Bilanz zu ziehen: Für das BDSG tut das zunächst der BfDI: Die Bilanz fällt positiv aus https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2021/11_BDSG-45-jähriges-Jubiläum.html: Schon als der Bundestag am 10. Juni 1976 das Bundesdatenschutzgesetz beschlossen hatte, ging es darum, die Menschen vor dem damals mehr erahnten Missbrauch ihrer personenbezogenen Daten zu schützen. An die rasante technische Entwicklung dachte niemand, und Orwell war ja erst für 1984 terminiert. Deutlich wurde jedoch, dass nicht mehr vorrangig der Staat als der „große Bruder" sondern Wirtschaftsinteressen und die Wirtschaftsmacht neuer weltweit tätiger Internetriesen mit ihrem Datenhunger die Datenverarbeitungen bestimmen würden. Daneben nimmt die weltweit tätige Computerkriminalität neue Ausmaße an. An beides und an soziale Netzwerke, Staatstrojaner und biometrische Videoüberwachung oder Facebook und andere hatte 1976 vermutlich keiner der Abgeordneten gedacht. Sie kannten keine PC, Laptops, Mobiltelefone. Am 03.08.1984 wurde die erste E-Mail in Deutschland empfangen.

Die Herausforderungen für das BDSG wuchsen jedes Jahr, und stetige Anpassungen des Gesetzes wurden notwendig, ohne dass an seiner Struktur und seinen Prinzipien etwas geändert werden musste. 2017 wurde bereits die dritte Fassung des BDSG beschlossen. Dies wurde notwendig, um das Gesetz mit der seit 2018 wirksamen europäischen Datenschutz-Grundverordnung (DS-GVO) zu harmonisieren. Dass mit der DS-GVO das Schutzziel, der Weg, um diesen Schutz zu erreichen, und die maßgebenden Prinzipien des BDSG nicht geändert wurden, ist auch ein deutscher Verdienst. Das BDSG hat insbesondere weiter dort Bedeutung, wo die DS-GVO nationale Regelungen den EU-Staaten überlässt bzw. aufgibt. Dazu zählt zum Beispiel die Verarbeitung von Beschäftigtendaten, mit deren umfassender zeitgemäßer Regelung der deutsche Gesetzgeber sich bisher als überfordert erwiesen hat.

Aktuell findet eine planmäßige Evaluierung der Gesetze statt, um weitere Anpassungen vorzunehmen; Zweifeln an der Europarechtskonformitäte einiger Bestimmungen des BDSG ist nachzugehen. Die eigentliche Fortschreibung des Datenschutzrechts muss sich aber auf europäischer Ebene vollziehen. Dazu äußert der BfDI den Wunsch, dass bei den kommenden Anpassungen ähnlich viel Weitsicht bewiesen wird, wie es der Bundestag 1976 getan hat. Weiterhin gilt es, die im wahrsten Sinne des Wortes Betroffenen vor denen zu schützen, die ihre Daten missbrauchen und damit ihr Verhalten manipulieren wollen.

Prof. Peter Gola

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

Termine	Thema	Ort	Kontakt
28.09.2021	Die Aufgaben und der Tätigkeitsbericht des betrieblichen DSB praxisnah im Unternehmen	Köln	GDD e.V. und DATAKONTEXT
28.09.2021	Datenschutz-Leit- und Richtlinien	Online	GDD e.V. und DATAKONTEXT
29.09.2021	Planung und Umsetzung der Überwachungsaufgaben des DSB	Düsseldorf	GDD e.V. und DATAKONTEXT
30.09.2021	Datenschutz und Betriebsrat unter der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
05.-07.10.2021	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Berlin	GDD e.V. und DATAKONTEXT
06.10.2021	Datenschutz-Management light	Köln	GDD e.V. und DATAKONTEXT
06.10.2021	Strategischer Umgang mit Bußgeldbescheiden bei Datenschutzverstößen	Stuttgart	GDD e.V. und DATAKONTEXT
12.10.2021	Der neue Kundendatenschutz: Kunden datenschutzkonform gewinnen und binden	Köln	GDD e.V. und DATAKONTEXT
13.10.2021	Verzeichnis von Verarbeitungstätigkeiten	Köln	GDD e.V. und DATAKONTEXT
19.10.2021	Videoüberwachung nach BDSG und DS-GVO	Köln	GDD e.V. und DATAKONTEXT
20.10.2021	Datenschutz-Folgenabschätzung	Köln	GDD e.V. und DATAKONTEXT
25.-26.10.2021	Datenschutzrecht Kompakt	Frankfurt/M.	GDD e.V. und DATAKONTEXT
25.10.2021	Hilfe, an AV-Vertrag	Online	GDD e.V. und DATAKONTEXT
26.10.2021	Den Umgang mit Betroffenenrechten organisieren	Online	GDD e.V. und DATAKONTEXT
27.10.2021	Strafverfolgung, Whistleblowing, Internal Investigations – Datenschutz und Strafrecht	Köln	GDD e.V. und DATAKONTEXT
28.10.2021	Onlinedatenschutz auf dem Weg zur ePrivacy-Verordnung	Köln	GDD e.V. und DATAKONTEXT
02.11.2021	Hacker-Tools für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
03.11.2021	Konzerndatenschutz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
04.11.2021	Teleworking unter Beachtung von Datenschutz und Sicherheit	Köln	GDD e.V. und DATAKONTEXT
04.11.2021	Hilfe, eine Betroffenenanfrage	Online	GDD e.V. und DATAKONTEXT
09.11.2021	Beschäftigtendatenverarbeitung nach DS-GVO und BDSG	Köln	GDD e.V. und DATAKONTEXT
09.-10.11.2021	Datenschutz-Management nach der DS-GVO – Teil 3	Berlin	GDD e.V. und DATAKONTEXT
10.11.2021	Den Umgang mit Datenschutz-Pannen organisieren	Online	GDD e.V. und DATAKONTEXT
10.11.2021	IT-Sicherheitsmanagement aus Sicht der DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
17.11.2021	40. RDV-Forum	Köln	GDD e.V. und DATAKONTEXT
18.-19.11.2021	45. Datenschutz-Fachtagung (DAFTA)	Köln	GDD e.V. und DATAKONTEXT

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

Aufsätze

Prof. Peter Gola

Das Betriebsrätemodernisierungsgesetz und die parallele Neufassung des BPersVG

Die Beteiligung des Betriebsrats bei neuen Arbeitsformen und das Verhältnis zum betrieblichen DSB

Am 18.06.2021 ist das vom Bundestag am 21.05.2021 verabschiedete und am 28.05.2021 vom Bundesrat gebilligten Betriebsrätemodernisierungsgesetz in Kraft getreten[1]. Mit den neuen Regelungen sollen zunächst die Wahl von Betriebsräten vereinfacht und zudem die Rechte des Betriebsrats bei der Weiterbildung, dem Einsatz von künstlicher Intelligenz und bei mobiler Arbeit gestärkt werden. Digitale Arbeitsabläufe werden für die Betriebsratsarbeit dauerhaft ermöglicht. Der neue§ 79a BetrVG soll klarstellen, dass auch bei Datenverarbeitungen des Betriebsrats der Arbeitgeber Verantwortlicher – und damit der betriebliche DSB Kontrollorgan – im Sinne der datenschutzrechtlichen Vorschriften ist. In gleiche Richtung gehen verschiedene Vorschriften des am 15.06.2021 in Kraft getretenen[2], grundlegend novellierten[3] Personalvertretungsgesetzes des Bundes.

I. Die Neuregelungen im Überblick

1. Allgemeines

Mit dem neuen Betriebsrätemodernisierungsgesetz soll zunächst dem stetigen Rückgang der Anzahl von betrieblichen Mitarbeitervertretungen entgegengewirkt werden.[4] Hierzu sollen die Gründung und Wahl von Betriebsräten erleichtert und zugleich die Möglichkeiten von Arbeitgebern zur Behinderung von Betriebsratswahlen reduziert werden. Dazu wird der Kündigungsschutz von Betriebsratsmitgliedern auf die Initiatoren einer Betriebsratswahl ausgedehnt (§ 15 Abs. 3b KSchG). In Unternehmen mit mehr als 20 Beschäftigten genügen bereits zwei Unterschriften für Wahlvorschläge. In Firmen mit weniger Beschäftigten sind keine Unterstützungsunterschriften mehr erforderlich. Zudem wird das Mindestalter für die Wahlberechtigung auf 16 Jahre abgesenkt. (vgl. § 14a BetrVG).

Des Weiteren wird eine Reihe von insbesondere im Zusammenhang mit der Digitalisierung der Arbeit zusammenhängende Beteiligungsrechten neu eingeführt bzw. präzisiert. Gleiches geschieht in einer Neufassung des Bundespersonalvertretungsgesetzes.

2. Virtuelle Betriebsratssitzung

Die im Zuge der Coronakrise befristet eingeführte Möglichkeit, Betriebsratssitzungen ganz oder teilweise virtuell abhalten zu können[5], wird fester Bestandteil des Betriebsverfassungsgesetzes. Die Regelungen zur Durchführung von Betriebsratssitzungen mittels Video- und Telefonkonferenzen finden sich in Ergänzungen der §§ 30 bis 34 BetrVG. Bei Beibehaltung des Vorrangs von Präsenzsitzungen kann die Teilnahme an einer Betriebsratssitzung mittels Video- und Telefonkonferenz erfolgen, wenn die Voraussetzungen für eine solche Teilnahme in der Geschäftsordnung festgelegt sind, nicht mindestens ein Viertel der Mitglieder des Betriebsrats binnen einer von dem Vorsitzenden zu bestimmenden Frist diesem gegenüber widerspricht und der Datenschutz gewahrt ist. Auch Hybrid-Formate sollen zulässig werden – mit der Maßgabe, dass "auch eine Teilnahme vor Ort als erforderlich" gilt, der Arbeitgeber Gremien also nicht auf Video-Calls beschränken darf.[6] Dabei muss u.a. durch technische Sicherungsmaßnahmen (§ 40 Abs. 2 BetrVG) sichergestellt sein, dass der Datenschutz gewahrt wird und Dritte vom Inhalt der Sitzung keine Kenntnis nehmen können.[7] Die technische Aufzeichnung einer Betriebsratssitzung, an der mittels Video- und Telefonkonferenz teilgenommen wird, ist nach § 30 Abs. 2 Satz 2 BetrVG nicht zulässig.

Entsprechendes bestimmt nunmehr § 38 Abs. 3 BPersVG. Es bleibt bei dem Grundsatz, dass Personalratssitzungen in Präsenz stattfinden. Ausnahmen sind möglich, wenn die

1 BGBl. I vom 17.06.2021, S. 17.

2 Gesetz zur Novellierung des Bundespersonalvertretungsgesetzes vom 09.06.2021 (BGBl. I S. 1614).

3 Beschlüsse des BT vom 22.04.2021; des Bundesrats am 28.05.2021, auf der Basis von Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat, BT-Drs 19/28839, 19. Wahlperiode, 21.04.2021, Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat (4. Ausschuss).

4 Derzeit haben nur etwa 10% der betriebsratsfähigen Betriebe eine Mitarbeitervertretung.

5 Vgl. Gola, HR Performance 4/2020, 11.

6 Vgl. dazu bereits zur früheren Rechtslage: Landesarbeitsgericht Berlin-Brandenburg am 24.08.2020 – 12 TaBVGa 1015/20.

technischen Voraussetzungen gegeben sind, sich im Gremium eine Mehrheit dafür findet und Dritte keine Kenntnis vom Ablauf der Sitzung erhalten (§ 38 Abs. 3 BPersVG). Es wird die Möglichkeit eingeräumt, dass in der Geschäftsordnung die Beschlussfassung im elektronischen Verfahren vorgenommen wird (§ 39 Abs. 4 BPersVG). Personalversammlungen und Sitzungen der Einigungsstelle können als Video-Konferenzen durchgeführt werden (§§ 58 Abs. 1; 74 Abs. 5 BPersVG).

3. Schutz bei mobiler Arbeit

a) Mitbestimmung bei der Ausgestaltung

Die Tatbestände der zwingenden Mitbestimmung werden erweitert um den Bereich der „Ausgestaltung von mittels Informations- und Kommunikationstechnik regelmäßig oder vorübergehend erbrachter mobiler Arbeit" (§ 87 Abs. 1 Nr. 14 BetrVG). Die Beteiligung betrifft das „wie"; das „ob" verbleibt weiterhin in der alleinigen Entscheidungsbefugnis des Arbeitgebers. Der Mitbestimmung unterliegen somit zum Beispiel Regelungen über den zeitlichen Umfang mobiler Arbeit, über Beginn und Ende der täglichen Arbeitszeit in Bezug auf mobile Arbeit oder über den Ort, von welchem aus mobil gearbeitet werden kann und darf. Das neue Mitbestimmungsrecht des § 87 Abs. 1 Nr. 14 BetrVG bildet einen Auffangtatbestand für alle Regelungen, mit denen mobile Arbeit ausgestaltet werden kann; es ermöglicht keine Regelungen zu diesbezüglich arbeitsvertraglich geschuldeten Tätigkeiten.

b) Unfallversicherung bei mobiler Arbeit

Tätigkeiten im Homeoffice erhalten in § 8 SGB VII einen erweiterten Unfallversicherungsschutz. Einbezogen ist der Weg im eigenen Haushalt zur Nahrungsaufnahme oder zu Toilette und zur Betreuung von Kindern außer Haus. Somit sind Wege zwischen Home-Office und Schule und Kita fortan abgesichert, wenn Kinder dorthin gebracht oder abgeholt werden.

4. Klarstellung der Beteiligung beim Einsatz künstlicher Intelligenz (KI)

§ 95 BetrVG ermöglicht dem Betriebsrat bei Auswahlrichtlinien für Einstellungen, Versetzungen, Umgruppierungen und Kündigungen mitzuentscheiden, wobei Abs. 2a nunmehr klarstellt, dass das Beteiligungsrecht auch greift, wenn KI zum Einsatz kommt. Der Begriff KI wird nicht definiert und ist in der Abgrenzung wohl nicht strittig, wenn „künstliche Intelligenz Methoden meint, die es einem Computer ermöglichen, Aufgaben zu lösen, die, wenn sie vom Menschen gelöst würden, „Intelligenz", d.h. Lernen, Beurteilen, Bewerten, erfordern."[8]

Zur Beurteilung des zulässigen Einsatzes von KI steht dem Betriebsrat ohne weitere Prüfung der Erforderlichkeit ein vereinfachter Zugriff auf besonderen Sachverstand zu.

II. Die „klarstellende" Regelung der Stellung von BR und DSB in § 79a BetrVG

1. Allgemeines

Hinsichtlich der datenschutzrechtlichen Verantwortlichkeit des Arbeitgebers bei der Verarbeitung personenbezogener Daten durch den Betriebsrat, soll mit der Einfügung eines neuen § 79a BetrVG eine weitere klarstellende gesetzliche Regelung geschaffen werden. Dies gelingt jedoch nur teilweise, da viele Fragen zur Umsetzung der Norm vom Gesetzgeber unbeantwortet bleiben.[9]

> „§ 79a BetrVG „Datenschutz"
> Bei der Verarbeitung personenbezogener Daten hat der Betriebsrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften. Arbeitgeber und Betriebsrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften. Die oder der Datenschutzbeauftragte ist gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. Die §§ 6 Abs. 5 Satz 2, 38 Abs. 2 des Bundesdatenschutzgesetzes gelten auch im Hinblick auf das Verhältnis der oder des Datenschutzbeauftragten zum Arbeitgeber."

Festgeschrieben wird unter Nutzung der Regelungsbefugnis des Art. 4 Nr. 7 Hs. 2 DS-DVO nunmehr, dass für Datenverarbeitungen des Betriebsrats der Arbeitgeber der für die Verarbeitung Verantwortliche – und damit der betriebliche DSB auch insoweit Kontrollorgan – im Sinne der datenschutzrechtlichen Vorschriften – ist[10]. Die vormals vom BAG verneinte[11] bzw. offen gelassene[12] Kontrollbefugnis des betrieblichen Datenschutzbeauftragten[13] gegenüber dem Betriebsrat ist damit – wenn auch mit Einschränkungen – zwar positiv entschieden (§ 79a S. 2 BetrVG); andererseits steht die datenschutzrechtliche Verantwortlichkeit des Arbeitgebers im Konflikt mit der innerorganisatorischen Selbständigkeit und Weisungsfreiheit des Betriebsrats. So entscheidet der Betriebsrat innerhalb seines Zuständigkeitsbereichs eigenverantwortlich die Umsetzung techni-

7 Vgl. Gesetzesbegründung BT-Drs. 19/28899, 20.

8 Künstliche Intelligenz (KI): Definition: Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/kuenstliche-intelligenz-ki-40285.

9 Vgl. Brink/Joos, Betriebsrätestärkungsgesetz und Datenschutz – voll eigenverantwortlich „ohne" Verantwortlichkeit: https://www.juris.de/jportal/portal/page/homerl.psml?nid=jpr-NLAR; siehe auch RDV 2/2021, S. 116.

10 Gesetzesbegründung, BT-Drs. 19/29819, 19. Wahlperiode S. 17.

11 BAG vom 11.11.1997 – 1 ABR 21.97.

12 BAG vom 09.04.2019 – 1 ABR 51/17.

13 BAG vom 11.11.1997 – 1 ABR 21/97.

scher und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit im Sinne der Artikel 24 und 32 der DS-GVO. Der Arbeitgeber hat den Betriebsrat mit den hierfür erforderlichen Sachmitteln auszustatten (§ 40 Abs. 2 BetrVG). Erfüllt der Betriebsrat die gebotenen Sicherheitsregeln nicht und kommen ggf. deshalb personenbezogene Daten in die Hände Unbefugter, stellt sich Frage, wer Ansprechpartner der Beschäftigten für Entschädigungsansprüche nach Art. 82 DS-GVO ist. § 79a BetrVG regelt dazu nichts. Wird dem Arbeitgeber bekannt, dass die Datensicherheit beim Betriebsrat nicht gewährleistet ist, kann bzw. muss er jedenfalls die Weiterleitung von personenbezogenen Daten unterlassen.[14]

2. Die beiderseitige Unterstützungspflicht

Dieser Konflikt kann nur gelöst werden, wenn beide Parteien der in § 79a S. 2 BetrVG vorgegebenen Pflicht zur gegenseitigen Unterstützung bei der Einhaltung der datenschutzrechtlichen Vorschriften kooperativ nachkommen. Fakt ist, dass den Arbeitgeber als verantwortlichen Verpflichtungen obliegen, die faktisch aber nur vom Betriebsrat erfüllt werden können. U.a. hat der Betriebsrat keine Pflicht, ein eigenes Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) zu führen, Der Arbeitgebers, dem diese Aufgabe als auch insoweit „Verantwortlicher" obliegt, kann ihr nur nachkommen, wenn er entsprechende Informationen der Mitarbeitervertretung erhält, zu denen sie jedenfalls nicht konkret verpflichtet ist. Gleiches gilt bei der Erfüllung datenschutzrechtlicher Auskunftspflichten hinsichtlich der personenbezogenen Datenverarbeitungen des Betriebsrats. Hier kann nur darauf vertraut werden, dass Arbeitgeber und Betriebsrat der in § 79a S. 3 BetrVG verankerten beiderseitigen Unterstützungspflicht kooperativ nachkommen. So kann beispielsweises im Einzelfall oder generell festgelegt werden, ob zur Wahrung der Vertraulichkeits- und Verschwiegenheitspflichten Auskunftspflichten unmittelbar vom Betriebsrat erfüllt werden, wobei das diesbezügliche gesetzeskonforme Vorgehen der Kontrolle des DSB unterliegt. Zur Klarstellung der diesbezüglichen innerbetrieblichen Arbeitsabläufe empfiehlt sich der Abschluss einer Betriebsvereinbarung.

Betriebsvereinbarung zur Kooperation zwischen Arbeitgeber und Betriebsrat im Rahmen des § 79a BetrVG, Präambel:

Unter der Vorgabe des § 79a BetrVG, nach der der Betriebsrat kein Verantwortlicher iSd Art. 4 Nr. 7 DS-GVO ist er andererseits aber weitgehend eigenständig über ggf. gegenüber dem Arbeitgeber vertraulich zu behandelnde Verarbeitungen von Beschäftigtendaten bestimmt, wird zur Gewährleistung des Datenschutzes der Beschäftigten in Befolgung des Kooperationsgebots des § 79a S. 3 BetrVG nachfolgende Betriebsvereinbarung geschlossen:

§ 1 Interne Eigenverantwortlichkeit des Betriebsrats

1. Über die Gewährleistug des Datenschutzes bei der von ihm im Rahmen der betriebsverfassungsrechtlichen Erforderlichkeit durchgeführten Verarbeitungen von Beschäftgtendaten entscheidet der Betriebsrat gemäß seiner institionellen Unabhängigkeit eigenständig.
2. Der Betriebsrat hat innerhalb seines Zuständigkeitsbereichs eigenverantwortlich die Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit im Sinne der Artikel 24 und 32 der DS-GVO sicherzustellen.
3. Der Arbeitgeber stellt die hierfür notwendige Hard- und Software zur Verfügung (§ 40 BetrVG).

§ 2 Äußere Verantwortung des Arbeitgebers

Der Arbeitgeber ist für die Verarbeitungen gleichwohl als Verantwortlicher iSd § 4 Abs. DS-GVO u.a. verpflichtet, die Dokumentations- und Rechenschaftspflichten nach der DS-GVO zu erfüllen, wobei er in dieser Vereinbarung Teile der sich hieraus ergebenden Aufgaben an den Betriebsrat delegiert.

§ 3 Zuständigkeiten und Pflichten des betrieblichen Datenschutzbeauftragten

1. Der betriebliche Datenschutzbeuftragte nimmt die ihm nach Art. 39 DS-GVO übertragenen Beratungs- und Kontrollaufgaben nach eigener Entscheidung bzw. auf Nachfrage auch gegenüber dem Betriebsrat wahr.
2. Erhält er dabei Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen, ist er gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet.
3. Die Verschwiegenheitsverpflichtung des Datenschutzbeauftragten nach den §§ 6 Abs. 5 Satz 2, 38 Abs. 2 des Bundesdatenschutzgesetzes hinsichtlich der vom Betriebsrat verarbeiteten personenbezogenen Daten gilt auch gegenüber dem Arbeitgeber.
4. Stellt der Datenschutzbeauftragte hinsichtlich bestimmter Datenverarbeitungen des Betriebsrats fest, dass diese nicht gesetzeskonform sind, ist er nach fehlgeschlagener Beanstandung beim Betriebsrat befugt, den Arbeitgeber oder die Aufsichtsbehörde zu informieren. Betrifft der Fall einen konkreten Beschäftigten, so bedarf es hierfür dessen Einwilligung.
5. Will der Betriebsrat Anträgen eines Beschäftigten auf Auskunft, Korrektur etc. nicht entsprechen, ist der Datenschutzbeauftragte zu informieren.

§ 4 Führung des Verzeichnisses der Verarbeitungstätigkeiten

1. Gemäß betriebsinterner Rgelung ist die organisatorosche Führung des Verfahrensverzeichnisses nach Art. 30 DS-GVO dem betrieblichen Datenschutzbeauftragten übertragen.
2. Der Betriebsrat meldet die von ihm geführten Verfahren zur Aufnahme in dieses Register dem Datenschutzbeauftragten.

14 BAG vom 09.04.2019 – 1 ABR 51/17.

§ 5 Erfüllung der Transparenzpflichten bezüglich der Datenverarbeitung des Betriebsrats

1. Die bezüglich der Datenverarbeitungen des Betriebsrats gegenüber den Betroffenen nach der DS-GVO zu erfüllenden Transparenzpflichten (Benachrichtigung, Auskunft, Korrektur) nimmt der Betriebsrat unmittelbar wahr.
2. Werden Auskunfts- oder Korrekturwünsche gegenüber dem Arbeitgeber geltend gemacht, gibt dieser, – sofern – ggf. auf Nachfrage – festgestellt wurde, dass sie sich auch auf Verarbeitungen des Betriebsrats beziehen, diese an den Betriebsrat zur selbstständigen und unmittelbaren Bearbeitung weiter.
3. Dem Betriebsrat obliegt es, bei sensiblen Beschäftigtendaten (Art. 9 Abs. 1 DS-GVO) das Vorhandensein von „angemessenen und spezifischen Maßnahmen zur Wahrung der Interessen der betroffenen Person" darzulegen (§ 26 Abs. 3 S. 3 BDSG in Verbindung mit § 22 Abs. 2).

§ 6 Schlussbestimmung

Gleichfalls sollte der Arbeitgeber sollte das Thema Datensicherung gemeinsam mit dem Betriebsrat angehen und konkrete Festlegungen für das Schutzniveau im Rahmen der betriebsverfassungsrechtlichen Zusammenarbeit treffen. Dies macht schon deshalb Sinn, weil andernfalls arbeitgeberseitige Maßnahmen, die einer Beteiligung des Betriebsrats mit unvermeidbarer Weitergabe von Beschäftigtendaten unterliegen (z.B. Anhörungen zu geplanten Versetzungen und Kündigungen, §§ 99, 102 BetrVG) verzögert würden.

3. Außerhalb der gesetzlichen Aufgabenzuweisung liegende Verarbeitungen

Die „rechtliche Zuordnung" der Beschäftigtendatenverarbeitungen des Betriebsrats in die Verantwortungssphäre des Arbeitgebers betrifft – nur – solche, bei denen der Betriebsrat „zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben" handelt (§ 79a S. 2 BetrVG). Erhebt der Betriebsrat außerhalb seiner gesetzlich zugewiesenen Aufgaben Beschäftigtendaten, kann eine solche Datenverarbeitung nicht dem Arbeitgeber „zugeordnet" werden. Vielmehr disponiert der Betriebsrat dann vollständig selbst über die Zwecke der Verarbeitung. Die offene Folgefrage ist, ob hier noch die Zuständigkeit des betrieblichen DSB besteht und ob im Fall von Datenschutzverstößen eine eigene Haftung der Mitglieder des Betriebsrats in Betracht kommen kann. Jedenfalls besteht bei kompetenzwidriger Datenverarbeitung durch den Betriebsrat außerhalb seiner gesetzlichen Pflichten keine datenschutzrechtliche Verantwortlichkeit des Arbeitgebers, und er kann nicht Adressat von Bußgeldern sein.

4. Einschränkungen der Kontrollbefugnis des DSB

Die Aufgaben und Befugnisse des Datenschutzbeauftragten gegenüber dem „Betriebsteil" Mitarbeitervertretung richten sich nach der Datenschutz-Grundverordnung (Art. 38 und 39). Wie aufgezeigt, muss die konkrete Ausgestaltung der Kontroll- und Beratungsaufgabe der Unabhängigkeit und Eigenständigkeit des Betriebsrats Rechnung tragen. Dies bringt der Gesetzgeber in § 76a S. 4 und 5 BetrVG zum Ausdruck. Vertraulichkeitspflichten gelten speziell für alle Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats ermöglichen und deren Kenntnis eine frei von Beobachtung durch den Arbeitgeber stattfindende Meinungsbildung im Betriebsrat gefährden würden (§ 79a S. 4 BetrVG). Dabei kommt es nicht darauf an, ob es sich um personenbezogene Daten handelt. Auf welche Informationen sich dies erstreckt, kann nur durch eine Einzelfallbewertung ermittelt werden.

§ 79a Satz 5 BetrVG stellt klar, dass die Verschwiegenheitsverpflichtung von Datenschutzbeauftragten nach den §§ 6 Abs. 5 S. 2, 38 Abs. 2 des BDSG hinsichtlich der vom Betriebsrat verarbeiteten personenbezogenen Daten auch gegenüber dem Arbeitgeber gilt. In Bezug auf personenbezogene Daten, welche Datenschutzbeauftragte im Rahmen ihrer Aufgaben aus der Sphäre des Betriebsrats zur Kenntnis erhalten, ist – sofern die betroffene Person nicht einwilligt – gegenüber dem Arbeitgeber Verschwiegenheit zu wahren.

5. Die diesbezüglichen Regelungen im Personalvertretungsrecht

a) Die Neuregelung im BPersVG

Die aktuell beschlossene grundlegende Neufassung des BPersVG enthält eine der Regelung des § 79a BetrVG in etwa entsprechende, jedoch im Detail noch weniger aussagekräftige Bestimmung in § 69 BPersVG. Geregelt wird zunächst die Selbstverständlichkeit, dass der Personalrat bei der Verarbeitung personenbezogener Daten die Vorschriften über den Datenschutz einzuhalten hat. Soweit der Personalrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, wird sodann die Dienststelle als der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften festgelegt, was aber nichts daran ändert, dass die „Datenverabeitungshoheit" bei der Mitarbeitervertretung liegt. Abgeschlossen wird die Norm durch ein gegenseitiges Unterstützungsgebot bei der Einhaltung der datenschutzrechtlichen Vorschriften.

§ 69 BPersVG Datenschutz

Bei der Verarbeitung personenbezogener Daten hat der Personalrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Personalrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist die Dienststelle der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften. Die Dienststelle und der Personalrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften.

Die Gesetzesbegründung[15] bezeichnet die datenschutzrechtliche Verantwortlichkeit der Dienststelle für die Verarbeitung

15 Vgl. zur Übersicht: Baden, Der Personalrat, 6/2021, S. 16.

personenbezogener Daten durch den Personalrat (§ 69 BPersVG) als sachgerecht, weil der Personalrat lediglich eine organisationsinterne Einrichtung, jedoch keine nach außen rechtlich verselbständigte Institution sei. Die Regelung führe die bislang bestehende, seit dem Inkrafttreten der Datenschutz-Grundverordnung jedoch umstrittene Rechtslage fort und diene der Schaffung von Rechtsklarheit.[16]

Die beiderseitige Unterstützungspflicht bei der Einhaltung der datenschutzrechtlichen Vorschriften (Satz 3) ist die Grundlage, dass die datenschutzrechtlichen Verantwortlichkeit der Dienststelle einerseits und der innerorganisatorischen Selbständigkeit und Weisungsfreiheit des Personalrats andererseits zusammenfinden So hat der Personalrat keine Pflicht, ein eigenes Verzeichnis von Verarbeitungstätigkeiten (Art. 30 der Datenschutz-Grundverordnung) zu führen, allerdings muss das Verarbeitungsverzeichnis der Dienststelle auch die Verarbeitungstätigkeiten des Personalrats enthalten. Auch bei den datenschutzrechtlichen Auskunftsrechten (Art. 15 DS-GVO) ist die Dienststelle, wenn der Auskunftsanspruch sich auf die durch den Personalrat verarbeiteten Daten bezieht, auf die Unterstützung durch den Personalrat angewiesen. Schließlich hat der Personalrat innerhalb seines Zuständigkeitsbereichs eigenverantwortlich die Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit im Sinne der Art. 24 und 32 DS-GVO sicherzustellen. Zu der Stellung und den Aufgaben des behördlichen Datenschutzbeauftragten in diesem Bereich äußert sich das Gesetz nicht. Die Gesetzesbegrünung verweist lapidar darauf, dass die Datenschutz-Grundverordnung (Artikel 38 und 39) auch gegenüber dem Personalrat als Teil der verantwortlichen Stelle gilt. Auf die bei der Tätigkeit des DSB zu beachtende Vertraulichkeitsaspekte wird nicht speziell hingewiesen.

Durch die Schaffung neuer und Präzisierung bestehender Mitbestimmungstatbestände wird auf die Einführung flexibler Arbeitsformen und -zeiten reagiert. Konkretisiert werden die Voraussetzungen zur Abhaltung von Sitzungen als Video- oder Telefonkonferenz und die Möglichkeit zur Beschlussfassung im elektronischen Verfahren. Nicht im BetrVG findet sich die Regelung, dass die Dienststelle auf Verlangen einer Gewerkschaft oder einer Vereinigung der Arbeitgeber ihr Intranet mit dem Internetauftritt der Gewerkschaft oder der Arbeitgebervereinigung verlinken muss. (§ 9 Abs.3 BPersVG).

b) Regelungen im Landesrecht

Entsprechend der Bundesregelung hatte bereits Bayern die datenschutzrechtliche Rechtsstellung der Personalvertretungen in Gebrauchmachung der Ermächtigung in Art. 4 Nr. 7 Hs. 2 DS-GVO in seinem Landesdatenschutzgesetz – indirekt – geregelt, indem in Art. 3 Abs. 2 BayDSG die Verarbeitung personenbezogener Daten einheitlich – d.h. ohne weitere Untergliederungen vorzunehmen – der zuständigen öffentliche Stelle zugewiesen. Damit werde nach Ansicht des BayLfD[17] eine Zersplitterung der datenschutzrechtlichen Verantwortlichkeit im Bereich der Verwaltung vermieden.

Anders sieht das im Land Thüringen aus. In § 80 Abs. 1 ThürPersVG wird der Personalvertretung zunächst aufgegeben, die Vorschriften über den Datenschutz einzuhalten und sich für deren Wahrung in der Dienststelle einzusetzen (S. 1). Sie hat dazu einen Datenschutzbeauftragten zu bestellen (S. 2), wobei der Gesetzgeber der Personalvertretung und Dienststelle quasi empfiehlt, im Einvernehmen einen gemeinsamen Datenschutzbeauftragten zu bestellen (S. 3). Ferner wird der Mitarbeitervertretung aufgegeben, ein eigenes Verarbeitungsverzeichnis zu führen.[18]

III. Zusammenfassung

Geht man davon aus, dass es in der Regelungskompetenz des Gesetzgebers liegt, die „Unselbstständigkeit" von Mitarbeitervertretungen – trotz durchaus gewichtiger entgegenstehender Argumente – festzuschreiben, so gilt es nun für die Praxis, sachgerechte Lösungen zu finden, die den reibungslosen Ablauf der täglich zwischen Arbeitgeber/Dienstelle und Mitarbeitervertretung anfallenden Arbeitsvorgänge unter Wahrung der beiderseitigen Verantwortung sicherstellen.

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

16 Gesetzesbegründung BT-Drucksache 19/18696, 19, vom 21.04.2020, S. 75.

17 Vgl. Handreichung des BayLfD, Aktuelle Kurzinformation 23 vom 08.07.2019.

18 Zu dieser – bei voller Geltung der DS-GVO an sich obsoleten – Regelung siehe bei Brink/Joos, NZA 2019, 1395.

Conrad Sebastian Conrad/Stefan R. Seiter

Inhaltliche Herausforderungen bei der Auftragsverarbeitung nach Art. 28 DS-GVO

Für die Praxis bedeutsame Vertragsgestaltung und deren mögliche Grenzen

Eine elementare Rolle im Datenschutzrecht nehmen Verträge über die Auftragsverarbeitung nach Art. 28 DS-GVO ein. Deren Ausgestaltung ist selbst zwischen zwei Unternehmen jedoch nicht grenzenlos. Sowohl die Vorgaben aus der DS-GVO als auch die AGB-Kontrolle aus §§ 307 ff. BGB legen den Beteiligten rechtliche Bandagen an.

I. Einleitung

Verträge zur Auftragsverarbeitung (AV-Verträge) treten in der unternehmerischen Praxis in verschiedenen Formen in Erscheinung. So fällt die Nutzung von Software „aus der Cloud“[1] ebenso darunter wie die Auslagerung zum Versenden eines Newsletters oder die Aktenvernichtung.[2] Für all diese Dienste ist der Verantwortliche gehalten, einen datenschutzrechtlichen Vertrag nach Art. 28 Abs. 3 DS-GVO mit dem externen Dienstleister abzuschließen. Die Praxis zeigt, dass auch noch Jahre nach Inkrafttreten der DS-GVO Unklarheit über die Ausgestaltung der gesetzlichen Vorgaben besteht und dies bisweilen zu schwierigen Vertragsverhandlungen führen kann.

1. Auswahl des Vertragspartners

Dabei gilt es zu bedenken, dass der Verantwortliche bei seiner Auswahlentscheidung über den Einsatz eines Auftragsverarbeiters nicht (rechts)frei ist, sondern „er auch bei seiner Auswahl von Dienstleistern seine Verantwortlichkeit wahrzunehmen und zu prüfen [hat], ob bei der Inanspruchnahme des Auftragsverarbeiters eine rechtmäßige und sichere Verarbeitung gewährleistet ist.“[3] Somit sind solche Erwägungen einzubeziehen, die nach objektiven Kriterien einer Überprüfung standhalten.[4] Gleichwohl trifft nunmehr nach dem Verständnis der DS-GVO beide Parteien die Verpflichtung zum Abschluss eines entsprechenden Vertrages.[5]

2. Form des Vertragsschlusses

Der Abschluss des Vertrages in formeller Hinsicht kann dabei in vielfältiger Weise geschehen. Denn nach der Abkehr vom (strengen) Schriftformerfordernis unter der alten Rechtslage[6] ist nach Art. 28 Abs. 9 DS-GVO nun auch ein „elektronisches Format“ zulässig.[7] Was darunter genau zu verstehen ist, ließ der Verordnungsgeber offen; so finden sich weder im Gesetzestext selber noch in den Erwägungsgründen ergänzende Hinweise oder Konkretisierungen hierzu. Nach Art. 28 Abs. 3 S. 1 DS-GVO wird lediglich ein Vertrag „nach dem Unionsrecht oder dem Recht der Mitgliedstaaten“ erfordert.

Soweit ersichtlich, findet sich auch in anderen einschlägigen EU-Verordnungen keine Definition des elektronischen Formats. Der Klärung dieser Frage am nächsten kommt wohl eine Norm aus dem Vergaberecht, namentlich die Durchführungs-Verordnung 2016/7/EU,[8] die darauf schließen lässt, dass weder ein bestimmtes Dateiformat noch eine spezifische Verschlüsselung oder Signatur dafür erforderlich ist. So ließ auch die Europäische Kommission auf Anfrage verlautbaren, dass ein wirksamer Vertragsschluss nach Art. 28 DS-GVO es nicht zwingend voraussetze, dem Vertragsdokument eine elektronische Signatur beizufügen; dies sei lediglich eine unter mehreren Möglichkeiten.[9]

In der Praxis am häufigsten anzutreffen sind bisher die folgenden Methoden:

- die Nutzung von Signatur-Diensten wie z.B. DocuSign;
- das Anklicken einer Checkbox auf einer Webseite mit Protokollierung im Hintergrund und Download des Vertragstextes oder ggf. Zugang zum Vertrag im Benutzeraccount;
- eigenhändiges Unterschreiben und Einscannen von Unterlagen, um sie dann per (zu protokollierender) E-Mail zu verschicken.[10]

Für den Vertragsschluss via Webseite und den Versand per E-Mail ist ergänzend zu beachten, dass diese nur dann taugliche Kommunikationskanäle darstellen, wenn auch geeignete Maßnahmen zur klaren Identifizierbarkeit der Parteien gewährleistet sind, also insbesondere eine Verschlüsselung nach dem aktuellen Stand der Technik zum Einsatz kommt. Als Orientierung können dafür die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der entsprechenden Richtlinie TR-02102[11] herangezogen werden. Zum jetzigen Zeitpunkt wird diesbezüglich zumin-

1 Mehr zum technischen und rechtlichen Hintergrund Conrad/Licht/Strittmatter, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, Teil C, § 22 Cloud Computing, Rn. 185 ff.

2 DSK, Kurzpapier Nr. 13 zur Auftragsverarbeitung, S. 4.

3 Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 28 DS-GVO Rn. 35.

4 S. hierzu den Erwägungsgrund 81 der DS-GVO.

5 Hartung, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 28 DS-GVO Rn. 64.

6 Vgl. § 11 Abs. 2 S. 2 BDSG-alt.

7 Hartung (o. Fn. 5), Art. 28 Rn. 95; Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 28 DS-GVO Rn. 75.

8 S. Amtsbl. EU L3/19 f. (dort Rn. 9, 15), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0007&from=DE?uri=CELEX:32016R0007&from=DE.

9 S. https://www.europarl.europa.eu/doceo/document/E-8-2018-003163-ASW_EN.html; vgl. dazu Hartung (o. Fn. 5), Art. 28 DS-GVO Rn. 96.

10 So auch die Empfehlung des BayLDA, https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_ADV_Formerfordernis.pdf.

11 S. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html.

dest eine Transportverschlüsselung nach TLS 1.2 und 1.3 empfohlen. Was insgesamt den Beweiswert der auf diesen Wegen ausgetauschten Willenserklärungen zum Vertragsschluss angeht, sind sie als untereinander gleichwertig anzusehen und erfüllen damit die oben aufgestellten Anforderungen in jedem Fall.

3. Inhaltliche Anforderungen des Datenschutzrechts

Ebenso vielfältig wie ihre Erscheinungsformen sind aber die Herausforderungen bei der Auslegung und Prüfung dieser Verträge. Denn es existieren zwar verschiedene Muster,[12] die teils von Verbänden und auch von den Aufsichtsbehörden zur Verfügung gestellt werden. Doch genießen diese Vorlagen keinen allgemeinverbindlichen Charakter, solange es sich nicht um solche handelt, die gemäß Art. 28 Abs. 7 oder 8 DS-GVO durch die Kommission oder die Aufsichtsbehörden festgelegt wurden.[13] Nachdem von dieser Möglichkeit bislang noch kein Gebrauch gemacht worden ist, obliegt es also dem Anwender in jedem Einzelfall, die Prüfung der Vertragsinhalte am Katalog des Art. 28 Abs. 3 S. 2 DS-GVO auszurichten.

Zum einen sind aber die dort aufgestellten Kriterien nicht in der Weise abschließend, dass ein festgelegter Rahmen von Inhalten und Vertragsklauseln vorgeschrieben wäre.[14] Zum anderen beinhalten die im Folgenden aufgelisteten Regelungen auch selbst unbestimmte Rechtsbegriffe, die folglich durch eigene gestalterische Maßnahmen im Vertrag ausgefüllt werden müssen. Dies wiederum bedeutet, dass die fachgerechte Prüfung eines solchen Vertrages mitunter weitaus mehr erfordert als das bloße Abgleichen des jeweiligen Dokuments mit einer vorgefertigten „Ja/Nein"-Checkliste. Es erscheint vielmehr angebracht und erforderlich, die einzelnen verwendeten Formulierungen inhaltlich zu bewerten. In Anlehnung an die bereits oben zu den Formvorschriften angestellten Überlegungen ist zunächst zu konstatieren, dass die Verordnung in diesem Zusammenhang nur abstrakt-generelle Kriterien aufstellt, die wiederum im Einzelnen umstritten sind. Es sollten daher die Vorschriften aus dem nationalen Recht als Maßstab heranzuziehen sein.

4. Berücksichtigung des AGB-Rechts

Für eine Inhaltskontrolle von vertraglichen Bestandteilen kennt das deutsche Zivilrecht die Regelungen über die Gestaltung von Allgemeinen Geschäftsbedingungen (AGB). Der Übersichtlichkeit wegen soll hier davon ausgegangen werden, dass die beteiligten Vertragspartner ihren Sitz in Deutschland haben oder jedenfalls deutsches Recht zur Anwendung kommt. Eine Überprüfung wäre daher nach den §§ 305 ff. BGB vorzunehmen, sofern diese auf AV-Verträge anwendbar sind.

a) Einbeziehen in den Vertrag

Nach § 305 Abs. 1 S. 1 BGB gelten als AGB alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen. Gerade in Anbetracht der zahlreichen als Muster zur Verfügung stehenden Unterlagen dürfte das Merkmal des Vorformulierten unstreitig erfüllt sein.[15] Auch sind diese Vertragsbedingungen stets für eine Vielzahl von Verträgen vorgesehen – entweder auf Seiten des Verantwortlichen, um sie (nach Möglichkeit) für alle seine Auftragsverarbeiter zum Einsatz zu bringen, oder umgekehrt auf dessen Seiten, um sie gegenüber all seinen Kunden zu verwenden. Ob dies tatsächlich auch so erzielt werden wird, ist dabei unerheblich. Es kommt einzig darauf an, ob die Vertragsbedingungen dazu angedacht sind, also ob – übertragen auf das Szenario der Datenverarbeitung – die AV-Verträge in der gewünschten Art und Weise Verwendung finden sollen.[16] Trotz allem können Zweifel aufkommen, ob diese Folgerung (noch) dem Sinn und Zweck des Gesetzes entspricht. Immerhin verfolgen die AGB-Vorschriften das Ziel, dort einen Ausgleich zu schaffen, wo im Zuge der Privatautonomie ein Vertragspartner durch den anderen eine mögliche Benachteiligung erfährt. Wenn aber der Inhalt eines Vertrages bereits im Wesentlichen per Gesetz vorgeschrieben ist (wie hier im Falle des Art. 28 Abs. 3 S. 2 DS-GVO), so stellt sich die Frage, ob diese zusätzliche Kontrolle gerechtfertigt ist oder ob es nicht sinnvoll wäre, die Auftragsverarbeitung davon auszunehmen. So hat etwa das BayLDA in der Formulierungshilfe für einen AV-Vertrag nach Art. 28 DS-GVO eine Prüfung nach dem AGB-Recht gem. §§ 307 ff. BGB zwar nicht vorgenommen, dies jedoch den Parteien überlassen;[17] eine ähnliche Position vertritt auch die Landesbeauftragte für Datenschutz und Informationsfreiheit im Saarland.[18]

Die Rechtsnatur eines Vertrages ist zunächst einmal unerheblich für die Beurteilung der Frage, ob und in welchem Umfang eine Inhaltskontrolle stattzufinden hat. Das Gesetz hat stattdessen in § 310 BGB Bereichsausnahmen definiert, nach denen bestimmte Vorschriften in Bezug auf einzelne Vertragsarten keine Anwendung finden. In diesem „Ausnahmekatalog" sind aber AV-Verträge nicht enthalten. Das Institut der Auftragsverarbeitung war bereits unter Geltung der alten Datenschutz-Richtlinie 95/46/EG bekannt – wenngleich auf nationaler Ebene unter geringfügig anderer Bezeichnung. Deswegen ist davon auszugehen, dass der BGB-Gesetzgeber den Aspekt der Kontrollfähigkeit von AV-Verträgen bewusst außen vor gelassen und es nicht etwa übersehen hat, dies zu regeln. Der Umstand, dass diese Verträge im Zuge der zahlreichen Änderungen, welche das BGB im Allgemeinen und die schuldrechtlichen Bestimmungen im Speziellen über die Jahre erfahren haben, nicht vom Anwendungsbereich ausgenommen wurden, spricht vielmehr dafür, dass dies eine gewollte Lücke darstellt. Folglich sind AV-Verträge unter die (allgemeinen) Regelungen des § 305 Abs. 1 S. 1 BGB zu fassen. Es steht dabei nicht zu befürchten, dass eine doppelte Kontrolle bzw.

12 S. Abschnitt II. 2. c).

13 Dieser Artikel entstand vor der Veröffentlichung des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021.

14 Nähere Einzelheiten unter Abschnitt II. 1. a).

15 Grüneberg, in: Palandt, Bürgerliches Gesetzbuch, 80. Aufl. 2021, § 305 BGB Rn. 8.

16 Ulmer/Habersack, in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016,§ 305 BGB Rn. 23f.

17 S. https://www.lda.bayern.de/media/muster/formulierungshilfe_av.pdf.

18 S. https://www.datenschutz.saarland.de/themen/auftragsverarbeitung unter dem Menüpunkt „Gibt es eine Formulierungshilfe zum Vertrag über die Auftragsverarbeitung"?; vgl. auch Hartung (o. Fn. 5), Art. 28 DS-GVO Rn. 24.

ein gewissermaßen doppelter Maßstab – einerseits durch den Katalog in Art. 28 Abs. 3 S. 2 DS-GVO und andererseits durch die Klauselverbote nach den §§ 307 ff. BGB – die Vertragsfreiheit der Parteien über Gebühr einschränkt. Dass überdies eine solche doppelte Kontrolle verhältnismäßig und sachlich geboten sein kann, wird an den einzelnen Beispielen von verwendeten Klauseln noch zu zeigen sein.

b) Verwender

Denjenigen Vertragspartner, welcher die AGB einbringt, nennt das Gesetz den Verwender. Diese Einordnung ist wiederum maßgeblich für die Frage, wem der beiden Vertragsparteien die Schutzwirkung der AGB-Normen zugutekommen soll. Hingegen ist datenschutzrechtlich nicht festgelegt, ob entweder der Verantwortliche oder der Auftragsverarbeiter für den Abschluss des Vertrages zu sorgen hat. Rein vom Wortsinn her sollte es primär der Verantwortliche sein, der für die Einhaltung des Datenschutzes Sorge trägt; zumal dieser auch berechtigt ist, dem Auftragsverarbeiter bestimmte Weisungen zu erteilen. Dieser Umstand legt wohl die Vermutung nahe, dass er deswegen auch als Verwender im AGB-rechtlichen Sinne gelten sollte. In der Praxis jedoch macht dies kaum einen Unterschied. Weder für die eine noch für die andere Seite sind datenschutzrechtliche Vor- oder Nachteile damit verbunden, selbst einen Vertragsentwurf einzubringen. Zudem kommt es relativ häufig vor, dass bereits der Dienstleister einen eigens für seine angebotenen Leistungen angepassten Mustervertrag vorschlägt. Vor allem aus Sicht von Anbietern, für die solche Vorgänge Massengeschäfte darstellen, kann das sehr effektiv sein.

Glücklicherweise ist eine Entscheidung, wer von beiden letztlich als Verwender gilt, jedenfalls nicht für die Einordnung eines AV-Vertrages als AGB ausschlaggebend. Zum einen muss ein Vertragswerk nicht im Ganzen als AGB angesehen werden. So ist es denkbar, dass einzelne in einem Vertrag enthaltene Bestimmungen individuell ausgehandelt werden und demzufolge von der Inhaltskontrolle ausgenommen sind, wohingegen die übrigen Klauseln einer solchen weiterhin unterliegen. Zum anderen gestatten die gesetzlichen Regelungen ihrerseits eine flexible Handhabung des Verwender-Begriffes. Denn es ist durchaus möglich, dass eine Vertragspartei ausschließlich in Bezug auf einzelne Klauseln, auf die sie sich beruft bzw. die sie eingebracht hat, als Verwender gilt. Es spielt auch keine Rolle, ob Vertragsbedingungen, die von einem Dritten erstellt wurden, gar im Interesse beider Parteien einbezogen werden.[19] Es ist also genauso gut möglich, dass die Vertragspartner den Mustervertrag eines Interessenverbandes oder einer Aufsichtsbehörde heranziehen und damit das Dokument im Ganzen oder auch nur einzelne Bestandteile davon zum Inhalt des konkret abzuschließenden AV-Vertrages machen. In diesem Fall jedoch kann der AV-Vertrag weder dem Verantwortlichen noch dem Auftragsverarbeiter eindeutig als Verwender „zugeordnet" werden.

c) Anwendungsbereich

Praktische Probleme sind aus dieser Folgerung indes nicht zu erwarten. Zwar ist damit ein direkter Rückgriff auf die §§ 305 ff. BGB verwehrt. Es spricht aber viel dafür, trotzdem eine Anwendung von denjenigen Vorschriften (analog) zuzulassen, welche losgelöst davon dem Schutz der einen wie der anderen Partei zugutekommen können; dies gilt insbesondere für die §§ 305b, 305c und 306 BGB.[20] Ohnehin sind die Klauselverbote der §§ 308, 309 BGB (mit Ausnahme zweier für das hiesige Szenario in AV-Verträgen irrelevanten) von der direkten Anwendung ebenfalls ausgeschlossen, wie § 310 Abs. 1 S. 1 BGB festlegt. Jedoch fließen die Rechtsgedanken aus eben diesen Vorschriften in die Bewertung § 307 BGB ein, und überdies sind auch die im Handelsverkehr zwischen Unternehmern geltenden Gewohnheiten und Gebräuche angemessen zu berücksichtigen (vgl. hierzu § 310 Abs. 1 S. 2 BGB). Der Rahmen der vorzunehmenden Inhaltskontrolle ist damit bereits ein Stück weit flexibilisiert, sodass die oben genannten Vorschriften letztlich in einer deren Schutzzweck unterstreichenden Art und Weise daran anknüpfen.

Von besonderer Bedeutung dürfte dabei regelmäßig § 307 Abs. 2 BGB sein – wenn es also zu thematisieren sein wird, ob gegen wesentlichen Grundgedanken der gesetzlichen Regelung in Art. 28 DS-GVO verstoßen wird oder wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrags ergeben, so eingeschränkt werden, dass die Erreichung des Vertragszwecks gefährdet ist. Unangemessen ist danach eine Benachteiligung, wenn der Verwender durch einseitige Vertragsgestaltung missbräuchlich eigene Interessen auf Kosten eines Vertragspartners durchzusetzen versucht, ohne von vornherein auch dessen Belange hinreichend zu berücksichtigen und ihm einen angemessenen Ausgleich zuzugestehen.[21] Dies in den jeweils passenden Kontext der einzelnen zur Diskussion stehenden Vertragsklausel zu rücken, soll im Folgenden versucht werden.

II. Umstrittene Klauseln aus der Praxis

Bei der Ausgestaltung von AV-Verträgen ergeben sich ob der relativ allgemein gefassten gesetzlichen Vorgaben nicht selten Diskrepanzen im Detailgrad einzelner Formulierungen. Im Folgenden sollen einige der häufig umstrittenen Klauseln vorgestellt und besprochen werden.

1. Laufzeit und Verbindung mit etwaigem Hauptleistungsvertrag

Oftmals wird hinsichtlich der Vertragslaufzeit sowie des Gegenstandes der konkreten Verarbeitung auf einen Hauptleistungsvertrag Bezug genommen. Trotz der Parallelität zweier Verträge mit unterschiedlichen Rechtsfolgen soll diese Koppelung zur Einheitlichkeit bzw. zu vermeintlich mehr Rechtssicherheit beitragen. Dabei stellt sich die Frage, inwiefern der separat abgeschlossene AV-Vertrag auch nach Beendigung oder Anfechtung des Hauptleistungsvertrages oder bei Formmängeln des selbigen wirksam bliebe – und ob deswegen die wesentlichen Inhalte vielmehr und besser direkt im AV-Vertrag zu regeln seien.

19 Grüneberg (o. Fn. 14),§ 305 Rn. 13; Ulmer/Habersack (o. Fn. 15), § 305 BGB Rn. 29.

20 Ulmer/Habersack (o. Fn. 15), § 305 BGB Rn. 30.

21 BGH NJW 2005, 1774.

a) Keine Detail-Regelung der DS-GVO

Aus Art. 28 DS-GVO ergeben sich hier keine unmittelbaren Vorgaben. Es wird lediglich in Art. 28 Abs. 3 S. 1 DS-GVO normiert, dass in einem solchen Vertrag (oder anderen Rechtsinstrument) unter anderem Gegenstand und Dauer der Verarbeitung „festzulegen sind", was auch begrifflich durch die gewählte Formulierung deutlich wird, dass diese Parameter nicht noch erst (nach)verhandelt oder später ausgelegt werden dürfen, sondern eindeutiger und präziser Bestandteil dieses Vertrages bei Vertragsschluss (im Sinne der essentialia negotii) zu sein haben.[22] Im Gegensatz zu den in Abs. 3 S. 2 aufgeführten Vorgaben (eingeleitet durch die Formulierung „sieht insbesondere vor"), sind die zuvor genannten Kriterien – schon wegen des Wortlauts und der Systematik dieser Vorschrift – zwingend und abschließend in den Vertrag aufzunehmen. Sie müssen den Vertragsinhalt eindeutig regeln und geben damit gewissermaßen den Rahmen vor, den die weiteren Modalitäten nach S. 2 dann ausfüllen.

b) Vertraglicher Spielraum

Diese Deutung könnte gegen die häufig beobachtete, rein praktisch herausgebildete Erscheinung sprechen, dass hierzu auf einen Hauptleistungsvertrag Bezug genommen wird. Im Falle von dessen Unwirksamkeit (etwa auf Grund Formfehlers oder Anfechtung) würde nämlich dann der Verweis aus dem AV-Vertrag ins Leere laufen und dieser somit keine Festlegungen (mehr) bezüglich dieser zwingenden Vorgaben aufweisen. Dann läge vor dem Hintergrund des Art. 28 Abs. 1 S. 1 DS-GVO zumindest eine unvollständige Vereinbarung vor, oder sie wäre gar zur Gänze unwirksam. Schließlich lässt sich argumentieren, der AV-Vertrag selbst müsse bereits den wesentlichen Inhalt der Verarbeitung fixieren[23] bzw. verbindlich festhalten.[24] Es empfiehlt sich daher, diese Regelungen bereits im AV-Vertrag festzuhalten.

Auch hinsichtlich der Frage, ob eine (eigenständige) Laufzeit des AV-Vertrages zu treffen oder diese aus den oben genannten Erwägungen vom Hauptvertrag abhängig zu machen ist, bietet die DS-GVO keine eindeutigen Antworten. Für die Festlegung einer eigenständigen Laufzeit könnte argumentiert werden, dass das Gesetz eine „Dauer" (Art. 28 Abs. 3 S. 1 DS-GVO) bzw. eine Beendigung nach „Abschluss der Erbringung der Verarbeitungsleistungen" vorsehe (Art. 28 Abs. 3 S. 2 lit. g) DS-GVO). Derartige Zeitpunkte dürften freilich in der Praxis mit der Durchführung einer zu vergütenden Hauptleistung bzw. der beauftragten Leistung zusammenfallen. Nach Beendigung steht dem Verantwortlichen zwar ein Anspruch auf Löschung oder Rückgabe (Art. 28 Abs. 3 S. 2 lit. g) DS-GVO) der betroffenen Daten zu. Die Rechte, Kontrollen durchzuführen und Weisungen zu erteilen, gelten jedoch nur für die Dauer des Vertragsverhältnisses. So würde der Verantwortliche aber nach Beendigung des AV-Vertrages keine Kontrollrechte mehr ausüben können. Umgekehrt müsste der Auftragsverarbeiter bei Fortbestand der AV-Vertragspflichten noch Jahre nach dem Ende des Auftrages mit dieser für ihn belastenden Situation (z.B. einem Audit) rechnen.

Dem lässt sich entgegnen, dass vielfältige Szenarien denkbar sind, in denen deutlich nach Beendigung einer Auftragsverarbeitung weiterhin personenbezogene Daten in der Sphäre des Auftragsverarbeiters vorzufinden sind oder dort unerwartet auftauchen. Ein unbefristeter AV-Vertrag würde dem Verantwortlichen dauerhaft Kontrollrechte einräumen, die zeitlich weit über den eigentlichen Auftrag hinausgehen. Dies könnte beiden Parteien zugutekommen, indem es ihr Bewusstsein um Ihre rechtliche Rolle und die ihnen obliegenden Pflichten im Hinblick auf die Verarbeitung personenbezogener Daten nachhaltig schärfen würde. Eine unbefristete Laufzeit wäre daher zulässig, müsste jedoch eine Möglichkeit zur Beendigung durch ordentliche Kündigung vorsehen.[25]

Andere knüpfen demgegenüber die (befristete) Laufzeit des AV-Vertrages streng an die Dauer des Hauptleistungsverhältnisses, um mehr Einheitlichkeit zu erzielen. Schließlich sei auf diese Weise ein besser praktikables Vertragsmanagement mit einheitlichen Kündigungsfristen gewährleistet. Damit könnte jedoch nach Beendigung des AV-Vertrages ggf. auch nicht mehr die Rückgabe von Daten gefordert werden, wenn diese beispielsweise nach Wahl des Verantwortlichen etwa in archivierter Form dort verblieben. Mithin stellt auch die Löschung bzw. Vernichtung von Daten eine eigenständige Verarbeitung im Sinne von Art. 4 Nr. 2 DS-GVO dar. Dies zu veranlassen, würde also eine neue/eigenständige Auftragsverarbeitung begründen, weshalb ein auf unbestimmte Zeit geschlossener AV-Vertrag mit Möglichkeit zur ordentlichen Kündigung vorzugswürdig erscheint, anstatt (in dieser Fiktion) immer wieder einen neuen AV-Vertrag schließen zu müssen. Auch eine Terminierung des Endes wäre aus diesem Grund nicht sinnvoll.

Eine solche Klausel zur unbefristeten Laufzeit mit ordentlicher Kündigung nach § 314 BGB dürfte in jedem Fall einer AGB-Prüfung gem. §§ 307 ff. BGB standhalten, ist sie doch transparent und als Ausgestaltung eines Dauerschuldverhältnisses zu verstehen.[26]

2. Kontrollrechte des Verantwortlichen

Zu den meistdiskutierten Regelungen zählen die Kontrollrechte des Verantwortlichen, die in Art. 28 Abs. 3 S. 2 lit. h) DS-GVO explizit zur Mitwirkungspflicht ausgestaltet sind. Sie bergen ein enormes Konfliktpotential, da sich in der Realität zumeist Unternehmen mit unterschiedlichen Interessen gegenüberstehen. Daraus kann sich rasch Uneinigkeit hinsichtlich der Reichweite dieser Rechte und Pflichten ergeben, wenn womöglich gar die Befürchtung im Raum steht, dass ganze Geschäftsmodelle beeinträchtigt würden.

a) Regelungen der DS-GVO

Zwar spricht die DS-GVO in Art. 28 Abs. 3 S. 2 lit. h) unter anderem von aktiven Maßnahmen wie „Überprüfungen"

22 Vgl. EDSA DSA, Guidelines 7/2020, Version 2.0, Rn. 111 ff.; Spoerr, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Ed. 2021, Art. 28 DS-GVO Rn. 51 ff.

23 Martini (o. Fn. 7), Art. 28 DS-GVO Rn. 29.

24 Gabel/Lutz, in: Taeger/Gabel, DS-GVO BDSG, 3. Aufl. 2019, Art. 28 DS-GVO Rn. 35.

25 Spoerr (o. Fn. 22), Art. 28 DS-GVO Rn. 52.

26 Heydn, CR 2018, 621, 623.

bzw. „Inspektionen", „die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden", weist im Übrigen aber einen relativ abstrakten Wortlaut auf. Der Verordnung sind zum Leidwesen der Vertragsparteien keine spezifischen Vorgaben in Bezug auf Art und Umfang solcher Überprüfungen und die damit verbundenen Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters zu entnehmen.[27]

b) Vertraglicher Spielraum

Den Vertragsparteien wird also vom Gesetzgeber ein weitreichender Gestaltungsspielraum eingeräumt. Diese Regelung hat auch durchaus ihre Berechtigung und ist – wie in vielen anderen Bereichen der DS-GVO auch – gewissermaßen technologieoffen[28] formuliert. Schließlich fordert auch Art. 32 Abs. 1 lit. d) DS-GVO einen Mechanismus zur regelmäßigen Bewertung und Überprüfung von einmal eingerichteten Maßnahmen lediglich (aber immerhin) in Abhängigkeit vom konkreten Schutzbedarf, wobei sogar wirtschaftliche Erwägungen (die Implementierungskosten) berücksichtigt werden dürfen.[29] Deshalb wäre es unverhältnismäßig, vor dem Hintergrund der äußerst vielfältigen Erscheinungsformen von AV-Verhältnissen, gerade in diesem speziellen Punkt, was die Ausübung von Kontrollen angeht, starre Fristen und Vorgaben zu fordern.

Unterm Strich und zuvorderst ist festzuhalten, dass der Verantwortliche in die Lage zu versetzen ist, jederzeit alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zu erhalten und deren Umsetzung zu überprüfen bzw. überprüfen zu lassen. Das ergibt sich ohnehin aus dem Sinn und Zweck der Norm: Der Verantwortliche hat die Aufgabe, den Auftragsverarbeiter auszuwählen und zu überwachen.[30] Dabei wird eine zeitliche Spanne von vor der Beauftragung über die fortlaufende Kontrolle[31] während der teilweise jahrelang dauernden Auftragsverarbeitung bis hin zur Beendigung abgebildet und eine Art „Dauerüberwachung" formiert.

Allerdings ist unklar, wie weit diese „Überprüfungen" und „Inspektionen" reichen können, beispielsweise ob sie auch die Einsichtnahme in allgemeine Prozesse und interne Unterlagen erlauben, die nicht im Zusammenhang mit der konkreten Datenverarbeitung im Auftrag stehen; wie oft diese Informationen zur Verfügung zu stellen sind (z.B. im jährlichen Turnus oder aber beliebig oft) und ob die Kontrollen (rechtzeitig) anzukündigen sind.

c) Vorschläge in Musterverträgen

Nach dem Mustervertrag des bitkom e.V.[32] sollten deshalb Inspektionen durch den Verantwortlichen „zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt" werden. Eine derartige Klausel würde dem Auftragsverarbeiter hinreichend Zeit zur Vorbereitung und Planung geben und insgesamt einen solchen Termin effizienter gestalten.

Gemäß des Mustervertrags des LDA Bayern[33] könnte dies wie folgt ausgestaltet sein: „Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO)." Dieser Vorschlag dürfte unterstreichen, dass unter Berücksichtigung der Interessen beider Parteien ein angemessener Ausgleich zu schaffen ist, um Benachteiligungen eines Vertragspartners zu verhindern und eine vertrauensvolle Zusammenarbeit zu gewährleisten.[34]

In diesem Kontext können Überlegungen vorgenommen werden, anstelle eines umfassenden „Vor-Ort"-Audits lediglich entsprechende Nachweise und Berichte auf Seiten des Auftragsverarbeiters zu führen bzw. dem Verantwortlichen textlich oder fernmündlich[35] vorzulegen. Dabei dürfen jedoch keine Geschäftsgeheimnisse oder die gesetzliche Schweigepflicht verletzt werden. So hat es der Verordnungsgeber offenbar nicht als zwingend erforderlich angesehen, dass sich der Verantwortliche ausschließlich vor Ort beim Auftragsverarbeiter durch eigene Inaugenscheinnahme von der Einhaltung der Maßnahmen überzeugt, obgleich er sich diese Möglichkeit vertraglich einräumen lassen kann.[36] In der Vergangenheit vor Geltung der DS-GVO wurde mitunter kritisiert, dass es ausschließlich der Verantwortliche selbst sei, der (seine) Kontrollmaßnahmen durchführen könne.[37] Dass diese Aufgabe nun auch ausdrücklich an Dritte übertragen werden kann, stellt eine wesentliche praktische Erleichterung dar[38] und kann die Wirksamkeit der Kontrolle steigern, indem spezialisierte Experten mit entsprechender Fachkunde diese Kontrolle zielgerichtet vornehmen.

d) Kontrolle von Unterauftragnehmern

Zusätzlich herrschen in der Beratungspraxis oftmals Meinungsverschiedenheiten darüber, ob der Verantwortliche auch Einsicht nehmen kann in datenschutzrechtliche Vereinbarungen zwischen dem Auftragsverarbeiter und weiteren von ihm eingeschalteten Auftragsverarbeitern ("Unterauftragnehmern"), und ob er beispielsweise auch deren technische und organisatorische Maßnahmen einsehen kann, obwohl er (in der Regel) keine direkte Vertragsbeziehung zu diesen hat.[39]

27 Gabel/Lutz (o. Fn. 24), Art. 28 DS-GVO Rn. 57.

28 Erwägungsgrund 15, S. 1 der DS-GVO.

29 Jandt (o. Fn. 5), Art. 28 DS-GVO Rn. 7 ff.

30 Sog. „Auswahlverantwortung" des Verantwortlichen, Martini (o. Fn. 7), Art. 28 Rn. 19 f.

31 Martini (o. Fn. 7), Art. 28 DS-GVO Rn. 20.

32 Vgl. https://www.bitkom.org/sites/default/files/file/import/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf.

33 S. https://www.lda.bayern.de/media/muster_adv.pdf.

34 Vgl. EDSA, Guidelines 07/2020, Version 2.0, Rn. 144.

35 Zu denken wäre an eine Videokonferenz während der derzeitigen Corona-Pandemie.

36 Klug, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 28 DS-GVO Rn. 11.

37 Mehr zur Gegenüberstellung der alten und aktuellen Rechtslage Gürtler, ZD 2019, 51, 51f.

38 Petri (o. Fn. 3), Art. 28 DS-GVO Rn. 81.

39 Dies Problem kann auch innerhalb eines Konzerns bestehen, vgl. Nickel, ZD 2021, 143, 144.

aa) Vorgehen in der Datenverarbeitungskette

Gegen eine derart weitreichende Überprüfung lässt sich anführen, dass aus dem Haftungskonstrukt des Art. 82 DS-GVO bzw. der Vorgaben nach Art. 28 Abs. 3 Abs. 4 S. 2 DS-GVO ohnehin nur auf Grundlage der direkten Vertragsbeziehung eine Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen besteht. Da der Auftragsverarbeiter seinerseits für die Wahrung und Einhaltung dieser Bestimmungen hinsichtlich der „Unterauftragnehmer" einzustehen hat,[40] dürfte es für den Verantwortlichen möglicherweise gar nicht auf die Verträge zwischen den Auftragsverarbeitern untereinander ankommen. Schließlich soll haftungsrechtlich immer das vorherige Glied in der Kette (Verantwortlicher – Auftragsverarbeiter – Unterauftragnehmer) heranzuziehen sein, was der einheitlichen Rechtsanwendung und damit der Rechtssicherheit für die Beteiligten dient.[41]

Dieses Konstrukt von Art. 28 DS-GVO könnte als zusätzliche „Privilegierung" des Verantwortlichen verstanden werden, der bereits dann seinen Pflichten nachgekommen wäre, wenn er den direkten Vertragspartner, d.h. den unmittelbaren weisungsgebundenen Auftragsverarbeiter geprüft und für datenschutzkonform bewertet hat, ohne weitere einbezogene Auftragsverarbeiter kontrollieren, respektive überwachen zu müssen. So sieht es der Vertrag in der Regel auch vor. Eine darüber hinaus gehende Überwachung aller involvierten Unterauftragnehmer wäre freilich aufwändig und würde zunächst voraussetzen, dass ihm die Unterauftragnehmer auf dritter Ebene (oder gar darunter) überhaupt bekannt gemacht würden und er vertragliche Regelungen mit diesen getroffen hat, die eine solche Kontrolle überhaupt erlaubten bzw. ausgestalteten. Darüber hinaus müssten aber auch noch praktikable Mechanismen entwickelt werden, um solche Kontrollen zielgerichtet und ohne größere Störungen im Betriebsablauf tatsächlich vornehmen zu können.

bb) „Durchgriffsrecht" des Verantwortlichen

Andere Rechtspositionen[42] räumen dem Verantwortlichen hingegen ein solches „Durchgriffsrecht" ein, auch wenn sich dieses wohl nur mittelbar aus Art. 28 Abs. 3 S. 2 lit. h) DS-GVO ergeben dürfte. Hierfür könnte sprechen, dass der Verantwortliche seine Kontrollrechte effektiv ausüben können muss. Der Verantwortliche muss sich sowohl das Handeln seiner Mitarbeiter wie auch des Auftragsverarbeiters zurechnen lassen.[43] Demzufolge kann er ein großes Interesse daran haben, sich auch hinsichtlich der Unterauftragnehmer möglichst umfassend selbst von der Rechtmäßigkeit der Verarbeitung zu überzeugen. Immerhin sieht es die DS-GVO in der „Grundkonstellation" vor, dass er selbst die AV-Kontrollen vornimmt;[44] er muss sich daher nicht darauf verweisen lassen, sich diese von dem nächsten Glied in der AV-Kette gewissermaßen abnehmen zu lassen. Es hätten folglich auch alle weiteren „Unterauftragnehmer", die sich eine Ebene weiter unter dem ersten Auftragsverarbeiter befinden, ebenso eine Prüfung durch ihn (den Verantwortlichen) hinzunehmen.

Diese Folge wäre zumindest vom Wortlaut her auch konsequent, kennt die Vorschrift doch lediglich den „weiteren Auftragsverarbeiter" und jedenfalls sprachlich keinen sog. Unter-(Unter-)Auftragsverarbeiter. Mithin wird jeder weitere Auftragsverarbeiter in der Kette der Verantwortung gleichrangig zum jeweils ersten behandelt. Als Argument pro „Durchgriffsrecht" kann daher insbesondere die Regelung Art. 28 Abs. 3 S. 2 lit. h) i.V.m. Abs. 4 DS-GVO herangezogen werden.[45] So kann der „erste" Auftragsverarbeiter selbst ein Interesse daran haben, die eigene Kontrolltätigkeit in Bezug auf den „zweiten" an den Verantwortlichen abzugeben, weil er auf diese Weise weniger Gefahr liefe, gegen diesbezügliche Vorgaben und Weisungen zu verstoßen; vielmehr wäre der Verantwortliche frei, die Kontrollen unmittelbar nach seinem Gusto abzuhalten. Ferner ist hier die Rede davon, dass dem weiteren Auftragsverarbeiter „dieselben Datenschutzpflichten" wie dem ersten in der Reihe auferlegt werden müssen.[46] Wiederum streng am Wortlaut orientiert wären die Pflichten tatsächlich deckungsgleich in der Weise auszurichten, dass es nicht der vorige Auftragsverarbeiter, sondern eben der Verantwortliche zu sein hat, dem der weitere Auftragsverarbeiter in Sachen Kontrollen unterworfen ist. Doch dann müsste dieser hiervon auch effektiv Gebrauch machen, was ihn zusätzlich belasten würde und in der Praxis eher für einen „Rechenzentrums-Tourismus" sorgen dürfte.[47]

cc) Zwischenergebnis

Vieles spricht gegen letztere Ansicht, da es kaum zu mehr Rechtssicherheit führen würde, wenn sich Dienstleister und Kunden/Verantwortliche auch ohne direkte Vertragsbeziehung Kontrollen ausgesetzt sehen, die in der Realität wenig erfolgversprechend sein dürften. Der Auftragsverarbeiter wäre nahezu schutzlos, sähe er sich einer unbestimmten ihm unbekannten Vielzahl an Verantwortlichen und derartigen Anfragen ausgesetzt. Zu denken wäre beispielsweise daran, dass vermutlich ein Großteil der internationalen Dienstleister auch auf bekannte Cloud-Infrastrukturen[48] aus den USA setzen, die sodann faktisch als ein weiterer Auftragsverarbeiter in der IT-Landschaft zu benennen sind.

Die denkbare Umsetzung dieser Kontrollrechte liegt im Handlungsspielraum beider Vertragsparteien und sollte von den konkreten Gegebenheiten, wie beispielsweise auch der Art der Datenverarbeitung und der Rechtslage abhängig sein.[49] Zur Vermeidung von Missverständnissen und Rechtsunsicherheiten sollte die Handhabung der Kontrollmöglichkeiten in jedem Fall vorab im AV-Vertrag eindeutig festge-

40 Gabel/Lutz (o. Fn. 24), Art. 28 DS-GVO Rn. 67; vgl. Klug (o. Fn. 36), Art. 28 DS-GVO Rn. 14.

41 Petri (o. Fn. 5), Art. 28 DS-GVO Rn. 85; Hartung (o. Fn. 5), Art. 28 DS-GVO Rn. 86.

42 Müthlein, RDV 2016, 74, 82; Gabel/Lutz (o. Fn. 23), Art. 28 DS-GVO Rn. 67.

43 Bergt (o. Fn. 5), Art. 82 DS-GVO Rn. 55.

44 S. oben II. 2. c).

45 Hartung (o. Fn. 5), Art. 28 DS-GVO Rn. 85.

46 Spoerr (o. Fn. 21), Art. 28 DS-GVO Rn. 43.

47 Müthlein, RDV 2016, 74, 82.

48 Petri (o. Fn. 5), Art. 28 DS-GVO Rn. 19.

49 So auch Petri (o. Fn. 5), Art. 28 DS-GVO Rn. 81.

legt werden.[50] In Ansehung einer AGB-Kontrolle erscheint es überdies empfehlenswert, nur dem direkten Vertragspartner eine solche Pflicht aufzuerlegen, da diese nicht zu Lasten Dritter gehen kann. Andernfalls würden solche Klauseln, die ein direktes Durchgriffsrecht festlegen, zur unangemessenen einseitigen Belastung einer Vertragspartei führen, wenn der Verantwortliche eine weit über den Wortlaut hinausgehende Kontrollbefugnis besäße und – spiegelbildlich – sich der Auftragsverarbeiter einer unbestimmten Vielzahl an solchen Kontrollen ausgesetzt sähe. Eine derartige Klausel könnte also im Wege der Inhaltskontrolle nach § 307 BGB beanstandet werden.

3. Vergütung für Unterstützungsleistung

Die Frage, ob und welche Vergütung der Auftragsverarbeiter für seine Unterstützungsleistung bei der Umsetzung der Betroffenenrechte vom Verantwortlichen verlangen kann, sorgt regelmäßig für Diskussion.

a) Regelungen der DS-GVO

Die DS-GVO sieht weder in Art. 28 noch an anderer Stelle konkrete Anhaltspunkte hierzu vor, und überlässt es den Vertragsparteien, über Vergütungsregelungen bzw. das Tragen von Kosten zu entscheiden.[51] Offenbar war eine solche Kostenbeteiligung nicht vom Verordnungsgeber gewünscht, andernfalls hätte er diese zugelassen oder zumindest angesprochen bzw. ausdrücklich den Parteien angeboten.

b) Deutung und vertraglicher Spielraum

Vertretbar ist die Ansicht, dass in Ermangelung an Vorgaben aus der DS-GVO und zur Verhinderung von Beschränkungen der dem Verantwortlichen zustehenden Kontrollrechte eine ihn treffende Kostenbeteiligung oder gar das komplette Auferlegen von Kosten unzulässig wäre. Allerdings könnte eine solche Kostenbeteiligung in speziellen Konstellationen (z.B. auf Seiten eines Aktenvernichters als Auftragsverarbeiter) angezeigt sein, wenn die Inspektion vor Ort einen erheblichen Aufwand für den externen Dienstleister bedeuten, und dadurch vorübergehend Geschäftsprozesse behindert würden. Vor allem kleinere Unternehmen könnten benachteiligt sein, wenn sie sich unentgeltlich an dieser Unterstützung beteiligen müssten oder dafür sogar auf eigene Rechnung rechtliche Beratung/Unterstützung benötigen. Eine derartige Mitwirkung dürfte bei sog. Freelancern und kleineren Einzelbetrieben regelrecht zur Abschreckung führen und möglicherweise das gesamte Geschäftsmodell gefährden.

c) Regelungsvorschläge…

So spricht sich der bitkom e.V. in der Stellungnahme[52] zum Bundesmuster zur Auftragsvertrag nach dem BMWi[53] für eine gesonderte Klausel zur Vergütung von Unterstützungsleistungen aus, in der solche Tätigkeiten klar zu definieren sind – am besten nach konkretem Aufwand ohne Obergrenze. Dieser Vorschlag ist insofern zu begrüßen, als er für beide Vertragsparteien eindeutige Regelungen und Kostenvorgaben etabliert, ohne dabei den Auftragsverarbeiter unangemessen zu benachteiligen. Gleichwohl könnte eine solche Bestimmung wiederum den Verantwortlichen benachteiligen, wenn dieser bei einer geringwertigen Dienstleistung (für wenige Euro pro Monat) mit hohen Kosten dafür zu rechnen hat, dass der Auftragsverarbeiter seiner ihm ohnehin vom Verordnungsgeber zugesprochenen Pflicht zur Mitwirkung nachkommt. Dabei befindet sich der Verantwortliche gleichsam in einer Zwangslage, da er auf diese Unterstützung angesichts fehlender technischer Zugriffe bzw. Kenntnisse angewiesen ist. Es könnte sogar die Option im Raume stehen, ein Dienstleister im Massengeschäft könnte sich durch diese „Hintertür" eine zusätzliche Vergütung einräumen, um damit sein Geschäftsmodell kostensparend zu gestalten.

Der aktuelle Mustervertrag der GDD e.V.[54] weist hingegen keine Kostenregelungen auf. Gleichwohl sei es nach deren Praxishilfe-Muster den Vertragsparteien unbenommen, „eine Vergütung des Auftragnehmers allgemein für Unterstützungshandlungen zugunsten des Auftraggebers zu regeln."[55] Eine Eingrenzung auf eine „angemessene Höhe" ist nicht zu erkennen, was den Parteien je nach Kräfteverhältnis unter Umständen unbillige Ausgestaltungen ermöglicht.

d) …und deren Umsetzung

Im Ergebnis obliegt es sicherlich dem konkreten Einzelfall der Auftragsverarbeitung und wohl auch der Macht der Vertragsparteien, eine Vergütungsklausel zu verhandeln oder von dieser abzusehen. Hier bietet sich ggf. eine transparente Auflistung der Kosten an. Vor allem große internationale IT-Dienstleister werden aber in der Regel mit einer Marktmacht auftreten, infolge derer der datenschutzrechtlich so gewichtig daherkommende Verantwortliche als die kleinere bzw. schwächere Vertragspartei dasteht. Grenzen einer unangemessenen Benachteiligung ergeben sich vor allem aus der AGB-Kontrolle nach §§ 307 ff. BGB. Mithin darf die Kostenfrage nicht dazu führen, dass der Verantwortliche zur Kostenvermeidung von der Geltendmachung seiner Kontrollrechte absieht bzw. in seiner Rolle nicht den Anforderungen aus der DS-GVO gerecht werden kann. Spätestens dies dürfte bei einer gerichtlichen Überprüfung zur Unzulässigkeit solcher Klauseln führen.

III. Fazit

Da es sich bei Verträgen zur Auftragsverarbeitung um AGB handelt, unterfallen sie der zivilrechtlichen Inhaltskontrolle nach den §§ 307 ff. BGB – wohl aber vor dem Hintergrund, dass es sich nahezu immer um Verträge zwi-

50 Spoerr (o. Fn. 22), Art. 28 DS-GVO Rn. 83; vgl. Völkel, PinG 2018, 189, 194.

51 So auch im Hinblick auf die Kosten eines Audits durch einen Verantwortlichen, vgl. EDSA, Guidelines 07/2020, Version 2.0, Rn. 145.

52 S. https://www.bitkom.org/sites/default/files/2020-07/190925_position-zum-bundesmuster-zur-auftragsverarbeitung.pdf.

53 S. https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/Muster_Auftragsverarbeitung.html.

54 S. https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-mustervertrag-zur-auftragsverarbeitung-gemaess-art-28-ds-gvo, Stand Dezember 2020.

55 GDD e.V., Mustervertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO, S. 16; https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-mustervertrag-zur-auftragsverarbeitung-gemaess-art-28-ds-gvo.

schen Unternehmern (B2B) handeln dürfte und deshalb die Kataloge der zu prüfenden Klauselverbote entsprechend restriktiv anzuwenden sind.

Es sollte dabei der Verarbeitungsgegenstand abschließend im AV-Vertrag selbst benannt sein; die gesetzliche Systematik[56] gebietet es, dass – wie in der Beratungspraxis häufig anzutreffen – nicht ausschließlich auf einen separaten Hauptleistungsvertrag verwiesen wird. Diese gedankliche Trennung des zivilrechtlichen Charakters vom datenschutzrechtlichen ist ebenfalls geboten hinsichtlich der Laufzeit des AV-Vertrages. Sie sollte auf unbegrenzte Dauer festgelegt sein – was regelmäßig mit dem Hauptvertrag kollidiert –, weil auf diese Weise die Umsetzung der datenschutzrechtlichen Pflichten am effektivsten gewährleistet ist. Besonderheiten innerhalb einer länger andauernden und sich gewissermaßen immer wieder erneuernden Datenverarbeitung können ebenso einen Anlass dafür bieten, die Vertragslaufzeit(en) separat zu regeln, wie das Risiko, dass der Hauptvertrag z.B. wegen Formmangels oder Anfechtung nichtig ist.

Beim Durchführen von Kontrollen oder sog. Inspektionen sind hingegen vielfältige Regelungen denkbar. So steht es dem Verantwortlichen frei, nicht nur den „ersten", sondern auch alle „weiteren" Auftragsverarbeiter eigenständig zu kontrollieren, wenn er dies tatsächlich und effektiv umzusetzen in der Lage ist. Im Vergleich zur alten Rechtslage (BDSG-alt) bietet aber die DS-GVO auch ausdrücklich die Möglichkeit, diese Pflichten entweder an Dritte oder an den jeweils in der „Datenverarbeitungskette" nachfolgenden Auftragsverarbeiter zu delegieren. Da dies auch dem gesetzlichen Haftungskonstrukt entspricht, ist es vorzugswürdig, die Kontrollen innerhalb des jeweiligen konkreten Vertragsverhältnisses stattfinden zu lassen und auf ein solches Durchgriffsrecht des Verantwortlichen zu verzichten.

Das leidige Thema der „Kosten" würde der gemeine Datenschützer wahrscheinlich am liebsten aus seiner rechtlichen Bewertung ausklammern, und diesbezüglich lieber auf die Vertragsverhandlung der Parteien verweisen. Diese romantische Vorstellung verkennt jedoch das Gewicht der in Rede stehenden finanziellen Interessen, die auch und sogar innerhalb der DS-GVO eine rechtliche Stütze finden sollen. Nicht zuletzt haben diese Interessen aber auch deshalb wiederum ihre Berechtigung, weil eine unausgewogene Kostenregelung die Geltendmachung der zustehenden Kontrollrechte über Gebühr einschränken oder gar aushebeln könnte. Der Drang der Vertragsparteien, sich einigen zu müssen, dürfte hierbei besonders stark ausgeprägt sein. Unterm Strich ist eine Regelung zur Übernahme von Kosten durch den Verantwortlichen anlässlich von Überprüfungen allenfalls dann gerechtfertigt, wenn diese in einem angemessenen Verhältnis zu der beauftragten Leistung stehen und transparent – nach tatsächlich anfallendem bzw. zu erwartendem Aufwand – vorab aufgeschlüsselt sind.

Conrad Sebastian Conrad
ist Senior Berater Datenschutz bei der datenschutz nord GmbH, Büro Hamburg.

Stefan R. Seiter
ist Rechtsanwalt und Senior Berater Datenschutz bei der datenschutz nord GmbH, Büro Bremen.

56 Siehe hierzu die Formulierung „festzulegen sind" in Art. 28 Abs. 3 S. 1 DS-GVO.

BITTE VORMERKEN!

40. RDV-Forum

17. November 2021 im Maternushaus Köln

45. DAFTA

Leitthema: **„Datenschutz im Umbruch: Online-Datenschutz – Internationaler Datentransfer – Schadensersatz für Datenschutzverletzungen"**

vom 18. – 19. November 2021 im Maternushaus Köln

Nadine Eichmann/Jaroslaw Norbert Nowak, LL.M.

Zum Rechtsrahmen für den transatlantischen Datenverkehr

Im Juli 2020 erklärte der Europäische Gerichtshof den Angemessenheitsbeschluss (2016/1215) der EU-Kommission zum EU-US Privacy Shield (Rechtssache C-311/118 „Schrems II“) für unwirksam mit der Folge, dass zahlreichen Datenübermittlungen in die USA die Rechtsgrundlage entzogen wurde. Zwar bezogen nationale Aufsichtsbehörden zunächst nur zögerlich Stellung, sodann bekräftigten sie jedoch mit zunehmender Vehemenz, dass Datenübermittlungen in die USA in vielen Fällen nicht datenschutzkonform möglich seien. Rund einen Monat nach dem Urteil veröffentlichte die erste Landesdatenschutzbehörde Praxishinweise und eine Checkliste zur Gestaltung transnationaler Datenübertragungen.[1] Es folgten viele weitere. Jüngst kündigten sieben Landesdatenschutzbehörden eine gemeinsame, länderübergreifende Kontrolle von Unternehmen hinsichtlich der Umsetzung der Schrems II-Entscheidung an und veröffentlichten umfangreiche Fragekataloge.[2]

Anfänglich äußerte sich auch der Europäische Datenschutzausschuss („EDSA“) nur in Form von kurzen FAQ, bevor das Gremium Ende 2020 die Einrichtung ergänzender Maßnahmen empfahl, soweit dies zur Gewährleistung des unionsrechtlichen Schutzniveaus im Drittstaat erforderlich sei. Einfluss nahmen die Empfehlungen des EDSA auch auf die überarbeiteten Standardvertragsklauseln, die am 4. Juni 2021 von der Europäischen Kommission beschlossen wurden. In der Praxis stellt sich jedoch nunmehr die Frage, ob die Vereinbarung der neu gefassten Standardvertragsklauseln für sich genommen bereits zur Zulässigkeit der Datentransfers in die USA und weitere Drittstaaten führt.

Mit dieser Frage setzen sich die Autoren in diesem Beitrag auseinander.

Nachdem zunächst die Inhalte der Schrems II-Entscheidung kurz umrissen werden, wird die Anwendbarkeit der weiteren, in der DS-GVO für Datenübermittlungen in Drittstaaten vorgesehenen, Garantien erörtert. Die Autoren stellen die Neuerungen der Standardvertragsklauseln, insbesondere im Hinblick auf eine durchzuführende Einzelfallprüfung vor, gehen auf die Kritik und die Handlungsempfehlungen des EDSA ein und schließen mit den letztlich verbleibenden Herausforderungen für Datenexporteure und -Importeure ab.

I. Das Urteil Schrems II

In seinem Urteil vom 16. Juli 2020 in der Rechtssache C-311/18 („Schrems II“) setzte sich der EuGH mit den Rechtsgrundlagen der DS-GVO für Datenübertragungen in Drittstaaten auseinander. Dem liegt die Erwägung zu Grunde, dass eine Übermittlung personenbezogener Daten in ein Drittland nach dem fünften Kapitel der DS-GVO grundsätzlich nur erfolgen darf, wenn ein Angemessenheitsbeschluss der Europäischen Kommission, Art. 45 DS-GVO, geeignete Garantien zur Sicherstellung eines angemessen Datenschutzniveaus (insbesondere die Standardvertragsklauseln), Art. 46 DS-GVO oder verbindliche interne Datenschutzvorschriften (Binding Corporate Rules), Art. 47 DS-GVO vorliegen. Daneben bestehen mit einer Einwilligung, Art. 49 Abs. 1 DS-GVO, einem überwiegenden berechtigten Interesse, Art. 49 Abs. 1 U Abs. 2 DS-GVO und zusätzlichen technischen Maßnahmen Ausnahmen, die aber nur im Einzelfall oder unter engen Voraussetzungen Anwendung finden.

1. Ungültigkeit des Angemessenheitsbeschlusses

Unter Verweis auf Erwägungsgrund 104 zur DS-GVO kommt der EuGH zu dem Ergebnis, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen in tatsächlicher Hinsicht ein Schutzniveau gewährleisten müsse, dass dem in der Europäischen Union aufgrund der durch die DS-GVO und die Charta der Grundrechte der Europäischen Union gewährten Rechte gleichwertig ist. Dabei müsse das Niveau nicht identisch sein, gefordert sei aber die gleiche Schutzhöhe.[3]

Der EuGH verweist darauf, dass die Europäische Kommission zwar ein derartig angemessenes „Schutzschild“ in den Anhängen des Angemessenheitsbeschlusses zum Privacy Shield sah, die Maßnahmen erschöpften sich jedoch in einer Prüfung des amerikanischen Handelsministeriums sowie offiziellen Zusagen und Erklärungen. Dass eine generelle Ausnahme von den Grundsätzen für den Schutz personenbezogener Daten vorgesehen war, sofern „Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss“, habe die Kommission nicht ausreichend berücksichtigt.

Vielmehr sind hinreichende Garantien für den Schutz personenbezogener Daten nach dem Wortlaut des Anhangs zum Privacy Shield nicht getroffen worden. Derartige Zusagen für Nicht-US-Bürger sieht das amerikanische Recht auch nicht vor. Nach Auffassung des EuGHs müssen sich derartige Garantien jedoch aus der gesetzlichen Grundlage ergeben, um dem Grundsatz der Verhältnismäßigkeit zu genügen.[5] So kann Section 702 des FISA (Foreign Intelligence Surveillance Act) z.B. weder entnommen werden, dass für die dort enthaltene Ermächtigung zur Durchführung von Überwachungs-

1 Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer, Stand: 25.08.2020.

2 Https://datenschutz-hamburg.de/pressemitteilungen/2021/06/2021-06-01-fragebogen-datentransfer.

3 EuGH vom 16.07.2020 – C-311/18 Rn. 94.

4 Abschnitt 1.5 des Anhangs II Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes.

5 EuGH vom 16.07.2020 – C-311/18 Rn. 180.

programmen Einschränkungen vorgesehen sind, noch das rechtstaatliche Garantien für Nicht-Amerikaner bestehen.[6]

Die amerikanische Regierung räumte zudem ein, dass betroffenen Personen aus der Europäischen Union keine Rechte zustehen, die eine gerichtliche Rechtsdurchsetzung gegenüber den amerikanischen Behörden ermöglichen.

Der EuGH kommt daher zu dem folgerichtigen Ergebnis, dass den betroffenen Personen auf Grundlage des Privacy Shields keine wirksamen und durchsetzbaren Rechtsschutzmöglichkeiten, wie in Art. 45 Abs. 2 lit. a DS-GVO vorgesehen, eingeräumt werden.

2. Standardvertragsklauseln (SCC)

Hinsichtlich der Standardvertragsklauseln (2010/87 geändert durch Beschluss 2016/2297) für die Übermittlung personenbezogener Daten in Drittländer sowie an Auftragsverarbeiter in Drittländern führt der EuGH aus, dass diese grundsätzlich mit der DS-GVO im Einklang stünden. Im Rahmen der Beurteilung des tatsächlichen Schutzniveaus im Drittstaat sind für den EuGH neben den vertraglichen Regelungen, jedoch auch die Zugriffsmöglichkeiten der Behörden eines Drittlandes von Relevanz.[7]

Soweit Datenübermittlungen in die USA betroffen sind, könnten die Standardvertragsklauseln insoweit nicht genügen, da diese aufgrund der Überwachungsmöglichkeiten der Behörden und des fehlenden gerichtlichen Rechtsschutzes kein gleichwertiges Schutzniveau bieten.[8] Es sei vielmehr die Pflicht der zuständigen Aufsichtsbehörde, eine Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn anzunehmen ist, dass die Standardvertragsklauseln nicht eingehalten werden können bzw. die Daten nicht den erforderlichen Schutz erhielten.[9]

Ein entsprechendes Vorgehen kündigten die Landesbehörden in den Folgemonaten an. Zum Leidwesen vieler Datenexporteure führte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit („BfDI") Ulrich Kelber universal aus: „demzufolge sind nicht nur die Übermittlungen unter dem durch das Urteil für unwirksam erklärten Datenschutzschild („Privacy Shield") betroffen, sondern auch alle anderen geeigneten Garantien aus Kapitel V der DS-GVO einschließlich der Verwendung von Standarddatenschutzklauseln und BCR."[10]

II. Aktuelle Rechtsgrundlagen für den internationalen Datentransfer

1. Standardvertragsklauseln

a) Entwurf der Kommission

Im November 2020 veröffentlichte die Europäische Kommission den Entwurf neu gefasster Standardvertragsklauseln, die die Rechtsprechung des EuGHs in der Rechtssache Schrems II aufgreifen und in ihrer finalen Fassung die geltenden Standardvertragsklauseln (2001/497/EG) ablösen sollten.

Die weitergehenden Regelungen der überarbeiteten Klauseln betreffen insbesondere die Bestimmungen eines Drittlandes und bindende Ersuchen von Behörden auf Offenlegung von personenbezogenen Daten, die die vertraglichen Schutzmechanismen beeinträchtigen können. Ohne zusätzliche Maßnahmen sollen die Klauseln von den Vertragsparteien gleichwohl nur abgeschlossen werden können, wenn nach eingehender Prüfung der nationalen Rechtsordnung des Drittstaates feststeht, dass die vertraglichen Garantien in dem Drittland tatsächlich eingehalten werden können.[11]

Im Hinblick auf behördliche Anfragen sehen die neu gefassten Klauseln eine Abwehr- und Mitteilungspflicht des Datenimporteurs vor. Wird dieser zur Offenlegung von personenbezogenen Daten behördlich aufgefordert, verpflichtet er sich, dies dem Datenexporteur schnellstmöglich mitzuteilen.[12] Verstößt ein solches Vorgehen gegen ein (gesetzliches) Verbot, soll der Datenimporteur mit allen ihm zur Verfügung stehenden Mitteln dagegen vorgehen und alle gegen das Ersuchen der Behörde verfügbaren Rechtsmittel ausschöpfen.

Kommt der Datenimporteur sodann in eine Lage, in der er die Vorgaben der vereinbarten Klauseln nicht mehr einhalten kann, hat er den Datenexporteur entsprechend zu informieren. Dieser muss dann entscheiden, ob die Datenübertragung beendet wird oder ob zusätzliche Maßnahmen ergriffen werden können, die geeignet sind, ein angemessenes Schutzniveau zu gewährleisten. Kommt es zu fortgesetzten Verstößen und kann die Einhaltung der Klauseln nicht spätestens innerhalb eines Monats wiederhergestellt werden, ist der Datenexporteur zur Meldung an die Aufsichtsbehörde verpflichtet.[13]

Von beiderseitigem Interesse dürfte auch sein, dass den Parteien ein Widerrufsrecht zur kurzfristigen Lösung von den Standardvertragsklauseln zusteht, sofern die Europäische Kommission einen Angemessenheitsbeschluss für das betreffende Drittland erlässt.[14]

Neu ist auch, dass die geänderten Standardvertragsklauseln nicht nur zwischen Verantwortlichen und Auftragsverarbeitern vereinbart werden können. Vielmehr wird die Komplexität moderner Verarbeitungsketten berücksichtigt, indem unterschiedliche Module bereitgestellt werden, die verschiedene Datenübermittlungsszenarien erfassen.[15] Künftig können

6 EuGH vom 16.07.2020 – C-311/18 Rn. 180.

7 EuGH vom 16.07.2020 – C-311/18 Rn. 104.

8 Siehe Ziffer II. 2. a. aa.

9 EuGH vom 16.07.2020 – C-311/18 Rn. 113.

10 BfDI, Informationsschreiben zur Auswirkung der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems II") vom 08.10.2020.

11 Erwägungsgrund 21 (EU) 2021/914 der Kommission vom 04.06.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

12 Ziffer 15 (EU) 2021/914 der Kommission vom 04.06.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

13 Ziffer 16 c) (EU) 2021/914 der Kommission vom 04.06.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

14 Ziffer 16 e) (EU) 2021/914 der Kommission vom 04.06.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

15 Erwägungsgrund 10 (EU) 2021/914 der Kommission vom 04.06.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

somit mehr als zwei Parteien die Standardvertragsklauseln vereinbaren, ungeachtet ihrer Eigenschaft als Verantwortlicher oder Auftragsverarbeiter. Ein nachträglicher Beitritt ist mit Zustimmung der anderen Parteien ebenfalls möglich.

b) Kritik des EDSA und EDSB an dem Entwurf

Der Entwurf der Standardvertragsklauseln wurde überwiegend positiv aufgenommen. Der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte („EDSB") veröffentlichten am 14. Januar 2021 ein gemeinsames Statement zu dem Entwurf der neu gefassten Standardvertragsklauseln.[16] Darin zeigten sich EDSA und EDSB erfreut, dass einige Maßnahmen, die in den Empfehlungen 01/2020 des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten enthalten waren, in den Entwurf der Standardvertragsklauseln Widerhall fanden.[17] Gleichwohl unterstrich das Gremium, dass seine Empfehlungen auch unter Geltung der Standardvertragsklauseln weiter von Relevanz seien und Anwendbarkeit beanspruchten.

Inhaltlich begrüßten EDSA und EDSB, dass die Standardvertragsklauseln klarstellende Ergänzungen zu den nationalen Rechtsvorschriften von Drittländern und Behördenanfragen mit dem Ziel des Zugriffs auf personenbezogene Daten enthalten, die zu vertragswidrigem Verhalten führen können. Zudem begrüßte der EDSA die Einrichtung eines ad-hoc Rechtsschutzmechanismus.[18]

In einigen Punkten sah der gemeinsame Ausschuss gleichwohl noch Korrekturbedarf. Hinsichtlich des Geltungsbereichs der Klauseln wurde die Klarstellung gefordert, dass der Geltungsbereich der Standardvertragsklauseln nicht gleichbedeutend mit dem Begriff der Übertragung sei.[19] Entsprechende Anpassungen wurden jedoch nicht in die Standardvertragsklauseln, die mit Durchführungsbeschluss vom 4. Juni 2021 beschlossen wurden, aufgenommen. Ziffer 1 a) der neu gefassten Standardvertragsklauseln sieht weiterhin vor, dass die Anforderungen der DS-GVO lediglich „bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden". Richtigerweise hätte der Anwendungsbereich der Standardvertragsklauseln jedoch auch auf die Verarbeitung personenbezogener Daten im Drittland erweitert werden müssen, da die Klauseln dem Datenimporteuer entsprechende Pflichten auferlegen (zu nennen ist etwa die Pflicht des Datenimporteurs zur Löschung oder Berichtigung unrichtiger Daten gemäß Ziffer 8 lit. a) der Standardvertragsklauseln).

EDSA und EDSB begrüßen die Möglichkeit des nachträglichen Beitritts weiterer Parteien bei Zustimmung aller Beteiligten, forderten aber zusätzlichen Regelungsbedarf hinsichtlich der diesbezüglichen Rahmenbedingungen (z.B. Frist, Form, Informationspflicht). Denn in der Praxis dürften sich die Fragen stellen, wie und wann die Zustimmung von den Ursprungsparteien erteilt werden muss und welche Angaben zum Zeitpunkt der Zustimmung bereits gegeben sein müssen.[20]

Von besonderer praktischer Bedeutung ist auch die vorzunehmende Beurteilung des Daten exportierenden Unternehmens. EDSA und EDSB betonen, dass bei der Prüfung allein objektive Faktoren zu berücksichtigen seien und die subjektive Wahrscheinlichkeit eines (etwa behördlichen) Zugriffs auf personenbezogenen Daten bei der Beurteilung nicht herangezogen werden könne.[21] Vor diesem Hintergrund wurde gefordert, die der Auslegung zugängliche Klausel, dass der Datenexport erfolgen könne, soweit der Datenexporteur bislang keinen Antrag auf Offenlegung der Daten erhalten habe, umzuformulieren.[22] In Teilen ist dies geschehen. In den nun beschlossenen Klauseln spielen der Inhalt und die Dauer des Vertrages, der Umfang und die Regelmäßigkeit der Datenübertragung sowie einschlägige praktische Erfahrungen mit früheren Fällen und das Fehlen beim Datenimporteur eingegangener Auskunftsersuchen von Behörden keine ausdrückliche Erwähnung und mithin keine Rolle mehr bei der Beurteilung der Gepflogenheiten und Bestimmungen im Drittland.

Konkrete Anhaltspunkte für die Auswahl und Wirksamkeit ergänzender Maßnahmen können den beschlossenen Standardvertragsklauseln nicht entnommen werden. Der EDSA führt hingegen aus, dass die Kombination vertraglicher, technischer und organisatorischer Art den Datenschutzstandard verbessern und auf diesem Wege möglicherweise eine Angleichung an den EU-Standard erreicht werden könne. Dabei sollen vertragliche und organisatorische Maßnahmen allein zwar nicht geeignet sein, den Zugriff staatlicher Stellen des Drittlands zu vereiteln.[23] In Anhang 2 der Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten nennt der EDSA jedoch einige Beispiele für zusätzliche Maßnahmen, die der Datenexporteur treffen kann.

2. Ergänzende Schutzmaßnahmen

Zusätzliche Schutzmaßnahmen sollten nach Auffassung des EDSA sowie nach Ziffer 14 lit. b) iii) der neu beschlossenen

16 EDPB-EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries.

17 EDPB-EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, Rn. 20.

18 Gemeinsame Stellungnahme 2/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, Rn. 19.

19 Gemeinsame Stellungnahme 2/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, Rn. 28.

20 Gemeinsame Stellungnahme 2/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, Rn. 46.

21 Gemeinsame Stellungnahme 2/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, Rn. 86.

22 Gemeinsame Stellungnahme 2/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, Rn. 87.

23 Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, angenommen am 10.11.2020, Rn. 48.

Standardvertragsklauseln grundsätzlich so eingerichtet werden, dass sie nicht von den Behörden des Drittstaats überwunden werden können. So ist, etwa eine Anonymisierung oder Pseudonymisierung der personenbezogenen Daten denkbar, sofern nur der Datenexporteur die Zuordnung vornehmen kann.[24]

Der Europäische Datenschutzausschuss veröffentlichte am 10. November 2020 Empfehlungen für entsprechende, ergänzende Maßnahmen. Das Gremium betont die Verantwortung jedes Datenexporteurs zur Überprüfung von Übermittlungen in Drittländer und die Pflicht sicherzustellen, dass ein vergleichbares Schutzniveau für die personenbezogenen Daten, gewährleistet ist.[25] Zur konkreten Umsetzung schlägt der EDSA folgendes sechsstufiges Verfahren vor.

Stufe 1: Dokumentation

Auf erster Stufe sollen alle Übermittlungen personenbezogener Daten in ein Drittland, wenn vorhanden, im Verarbeitungsverzeichnis, dokumentiert werden („Know your Transfers"). Als Datenübermittlung versteht der EDSA dabei jede Zugriffsmöglichkeit aus einem Drittland, auch zu Wartungszwecken. Auch Weiterübermittlungen an Subunternehmer in Drittländern werden umfasst. Die Ermittlung sämtlicher Datentransfers in Drittländer soll dem Datenexporteur dazu verhelfen, die nachfolgenden weiteren Maßnahmen zu bestimmen.

Stufe 2 und Stufe 3: Auswahl eines Transferinstruments und Prüfung der Rechtslage im Drittland

Sodann soll der Datenexporteur das Übermittlungsinstrument nach Kapitel V der DS-GVO festlegen. Hierfür hat er die Rechtslage im Drittland zu beurteilen und die Effektivität der dort vorgesehen Garantien zu überprüfen. Liegt ein Angemessenheitsbeschluss für das Drittland vor, kommt es auf die Garantien hingegen nicht mehr an. Nach Auswahl des Übermittlungsinstruments muss der Datenexporteur prüfen, ob dieses auch tatsächlich effektiv ist.[26] Die Rechtsprechung des EuGH in Schrems II aufgreifend, verlangt der EDSA in dem Drittland ein mit dem in der Europäischen Union gleichwertiges Schutzniveau, das nicht durch das Recht oder die Praxis des Drittlandes beeinträchtigt wird.[27] Eine entsprechende Formulierung findet sich nun auch in den neu beschlossenen Standardvertragsklauseln wieder.

Stufe 4: Ergänzende Maßnahmen

Kommt der Datenexporteur zu dem Ergebnis, dass das Schutzniveau in dem Drittland nicht gleichwertig zu dem in der Europäischen Union gewährleisteten Schutzniveau ist, hat er zusätzliche Maßnahmen, zu den Maßnahmen nach Art. 46 DS-GVO, auszuwählen und zu ergreifen. Welche Maßnahmen konkret in Frage kommen, hat der Datenexporteur anhand seiner bereits in den Schritten 1 bis 3 getroffenen Feststellungen zu ermitteln. In Betracht kommen neben technischen Maßnahmen auch solche vertraglicher oder organisatorischer Art. Als Beispiele für zusätzliche technische Maßnahmen nennt der EDSA im Anhang seiner Empfehlung die Datenverschlüsselung oder Pseudonymisierung vor Übermittlung in das Drittland, die Datenübermittlung an einen nach dem Recht des Drittlandes geschützten Empfänger und eine Verarbeitung durch mehrere Beteiligte, bei der die einzelnen Datenstücke ohne zusätzliche Informationen nicht mehr einer betroffenen Person zugeordnet werden können. Vertraglich sind Verpflichtungen zur Verwendung spezifischer technischer Maßnahmen und zur Einhaltung bestimmter Verfahren, Transparenzregelungen und Zustimmungserfordernisse denkbar. Der Datenexporteur kann zudem organisatorische Vorgaben in Form von internen Grundsätzen betreffend den Regelungsrahmen für Übermittlungen aufstellen, Maßnahmen in Bezug auf Transparenz und Rechenschaftspflicht vorsehen sowie solche, die auf eine Datenminimierung abzielen. Dabei kommt es wohlgemerkt auf den spezifischen Einzelfall an, weshalb eine bestimmte Maßnahme nicht stets gleich effektiv sein dürfte.

Stufe 5: Verfahrenseinleitung

Die sodann erforderlichen Schritte richten sich nach dem ausgewählten Übertragungsinstrument. Wird die Datenübermittlung auf die Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c) und d) DS-GVO gestützt und sollen zusätzliche Maßnahmen getroffen werden, die diese ergänzen, ist keine Genehmigung der Aufsichtsbehörde erforderlich. Dies gilt jedenfalls soweit die zusätzlichen Maßnahmen die Standardvertragsklauseln nicht konterkarieren und das gewährleistete Datenschutzniveau nicht beeinträchtigen.[29]

Stufe 6: Regelmäßige Neubewertung

Der Datenexporteur ist verpflichtet, das Datenschutzniveau in dem Drittland, in das er personenbezogene Daten übermittelt, sowie die von ihm getroffenen Maßnahmen regelmäßig auf ihre Angemessenheit zu überprüfen. Zudem muss er Vorkehrungen treffen, die sicherstellen, dass Datenübertragungen umgehend ausgesetzt oder beendet werden, wenn der Datenimporteuer die ihm auferlegten Pflichten verletzt oder die zusätzlich eingerichteten Maßnahmen in dem Drittland nicht mehr sicher sind.

3. Einwilligung, Art. 49 Abs. 1 lit. a) DS-GVO

Fehlt nach allem weiterhin eine Rechtsgrundlage für den Datentransfer in ein Drittland, kann eine Übermittlung personenbezogener Daten möglicherweise auf der Grundlage einer Einwilligung der betroffenen Person in die Datenübermittlung erfolgen. Es handelt sich bei Art. 49 Abs. 1 lit. a)

24 Landesbeauftragter für Datenschutz und Informationsfreiheit Baden Württemberg in Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer? Stand 25.08.2020, S. 5.

25 Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, angenommen am 10.11.2020.

26 Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, angenommen am 10.11.2020, Rn. 28.

27 Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, angenommen am 10.11.2020, Rn. 29 f.

28 Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, angenommen am 10.11.2020, Rn. 47 f.

29 Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, angenommen am 10.11.2020, Rn. 56.

DS-GVO jedoch um eine Ausnahmevorschrift, die eine qualifizierte Information der betroffenen Person vor Einwilligungserklärung vorsieht.

a) Ausnahmecharakter und Verzicht

Da die Daten nach ihrer Übertragung in das Drittland auf Grundlage von Art. 49 DS-GVO keinen der DS-GVO vergleichbaren Schutz genießen, stellen die dort genannten Maßnahmen Ausnahmetatbestände dar.[30] Dies gilt nach Erwägungsgrund 111 zur DS-GVO jedenfalls für die Tatbestände der Art. 49 Abs. 1 lit. b), c) und e) DS-GVO, da in diesen Fällen nur gelegentliche Übermittlungen legitimiert werden.[31] Liegt eine Einwilligung vor, geht zwar grundsätzlich der autonome Wille der betroffenen Person vor.[32] Nach den Datenschutzaufsichtsbehörden könnte die Grenze der Wirksamkeit aber da erreicht sein, wo geeignete Garantien für den Schutz der personenbezogenen Daten im Drittland nicht (mehr) bestehen.[33] Diese dürfte nach der Rechtsauffassung des EuGHs jedenfalls dann überschritten sein, wenn kein gleichwertiges Schutzniveau im Drittland besteht. Für den Ausnahmecharakter der Vorschrift sprechen überdies auch die Überschrift von Art. 49 DS-GVO, die „Ausnahmen für bestimmte Fälle" vorsieht und die noch strengere Regelung des Art. 49 Abs. 1 UAbs. 2 DS-GVO.[34]

Die Beschränkung der Einwilligungsfähigkeit des Betroffenen steht jedoch im Spannungsverhältnis mit dem Recht auf datenschutzrechtliche Selbstbestimmung, für das die Einwilligung in widersprüchlicher Weise das zentrale Mittel darstellt. Es stellt sich daher die Frage, ob die DS-GVO und die in ihr gewährleisteten Rechte disponibel sind und von der einzelnen betroffenen Person (mittels Einwilligung) abbedungen werden können. Gerichtlich wurde die Frage bislang nicht abschließend geklärt. Der BfDI äußerte 2019, dass er einen solchen Verzicht jedenfalls im Bereich der öffentlichen Verwaltung datenschutzrechtlich nicht für vertretbar erachtet.[35]

b) Ausdrückliche informierte Einwilligung

Eine Datenübermittlung auf Grundlage einer Einwilligung ist des Weiteren auch im Einzelfall nur zulässig, wenn die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich einwilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde. Damit werden die Anforderungen des Art. 4 Nr. 11 DS-GVO in Art. 49 Abs. 1 Satz 1 lit. a) DS-GVO konkretisiert.

Daher ist bei einem Datenexport in Drittstaaten darüber zu informieren, in welche Länder die Daten (ggf.) übertragen werden, da das Zielland Einfluss auf die Entscheidung des Betroffenen nehmen kann, ob er eine Datenübertragung gestattet oder nicht.[36] Der Datenexporteur hat dabei nicht nur darzulegen, dass in dem betreffenden Drittland kein gleichwertiges Schutzniveau für personenbezogene Daten besteht. Vielmehr hat er über die konkret bestehenden Risiken in dem Drittstaat zu informieren. Es reicht jedoch auf, die Risiken zu umreißen; Einzelheiten über die Rechtslage im Drittstaat sind nicht mitzuteilen.[37]

Das Erfordernis der „Ausdrücklichkeit" der Einwilligung in Art. 49 Abs. 1 Satz 1 lit. a) DS-GVO geht über die Anforderungen an eine Einwilligung in Art. 4 Nr. 11 DS-GVO hinaus. Nach den Aufsichtsbehörden reicht für eine qualifizierte Einwilligung in die Datenübermittlung in Dritttaaten insoweit nicht aus, dass die betroffene Person eine „sonstige eindeutige bestätigende Handlung" vornimmt.[38] Vor diesem Hintergrund ist somit ebenfalls zweifelhaft, ob die pauschale Annahme von Allgemeinen Geschäftsbedingungen, insbesondere in Form von Datenschutzerklärungen, eine ausdrückliche Einwilligung im Sinne des Art. 49 DS-GVO darstellt.

4. Datenübermittlung im berechtigten Interesse

Auch wenn einer der Erlaubnistatbestände des Art. 49 Abs. 1 U Abs. 1 DS-GVO nicht vorliegt, kann eine Datenübermittlung in ein Drittland gestattet sein, Art. 49 Abs. 1 UAbs. 2 DS-GVO. Dies erfordert allerdings das Vorliegen mehrerer kumulativer Voraussetzungen: die Übermittlung erfolgt nicht wiederholt, sie betrifft nur eine begrenzte Zahl von betroffenen Personen, ist für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich, die Interessen oder Rechte und Freiheiten der betroffenen Person überwiegen nicht, und der Verantwortliche hat alle Umstände der Datenübermittlung beurteilt und auf der Grundlage seiner Beurteilung geeignete Garantien für den Schutz personenbezogener Daten vorgesehen.[39]

Aufgrund der hohen Anforderungen an die Datenübermittlung, stellt die Ermächtigungsgrundlage des berechtigten Interesses jedoch keinen Ersatz für die Garantien nach Art. 45 ff. DS-GVO dar. Ob ein überwiegendes berechtigtes Interesse zu bejahen ist, ist stets im Einzelfall anhand der Art der personenbezogenen Daten, des Zwecks, der Verarbeitungsdauer und der Situation im Ausgangsland sowie im Zielstaat festzustellen. Erwägungsgrund 113 zur DS-GVO Satz 4 nennt beispielsweise wissenschaftliche oder historische Forschungszwecke sowie statistische Zwecke, bei denen auch die gesellschaftlichen Erwartungen an einem Wissenszuwachs zu berücksichtigen sind.

III. Fazit

Datenexporteuren stehen aufgrund der Schrems II-Entscheidung des EuGH auch nach der Neufassung der Standardvertragsklauseln weiterhin nur im geprüften Einzelfall Mittel zur Verfügung, die eine datenschutzkonforme

30 BeckOK DatenschutzR/Lange/Filip, 33. Ed. 01.08.2020, DS-GVO Art. 49 Rn. 1.

31 BeckOK DatenschutzR/Lange/Filip, 33. Ed. 01.08.2020, DS-GVO Art. 49 Rn. 2.

32 BeckOK DatenschutzR/Lange/Filip, 33. Ed. 01.08.2020, DS-GVO Art. 49 Rn. 2.

33 EDSA-Leitlinien 2/2018, S.5.

34 So auch Landesbeauftragter für Datenschutz und Informationsfreiheit Baden Württemberg in Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?, Stand 25.08.2020, S. 5.

35 BfDI, Pressemitteilung vom 16.11.2019 BfDI fordert datenschutzgerechte Kommunikation mit der Krankenkasse.

36 BeckOK DatenschutzR/Lange/Filip, 34. Ed. 01.08.2020, DS-GVO Art. 49 Rn. 7.

37 BeckOK DatenschutzR/Lange/Filip, 34. Ed. 01.08.2020, DS-GVO Art. 49 Rn. 8.

38 EDSA-Leitlinien 2/2018, 22.

39 Paal/Pauly/Pauly, 2. Aufl. 2018, DS-GVO Art. 49 Rn. 28.

Übermittlung personenbezogener Daten in einen Drittstaat ermöglichen.

Betroffene Personen können daneben zwar gemäß Art. 49 Abs. 1 Satz 1 lit. a) in die Übertragung ihrer personenbezogenen Daten in ein Drittland einwilligen. Es verbleibt jedoch insbesondere für wiederholte Datenübertragungen eine gewisse Rechtsunsicherheit, da aufgrund der systematischen Stellung der Vorschrift eine Einwilligung nur in bestimmten Ausnahmefällen Legitimationswirkung zukommen dürfte. Zudem würde eine Einwilligung in die Übermittlung personenbezogener Daten in ein Drittland, das kein der Europäischen Union gleichwertiges Datenschutzniveau bietet, den Verzicht auf die hierzulande garantierten Rechte erfordern. Zwar ist die Frage, ob die DS-GVO dispositives Recht enthält, von der Rechtsprechung bislang noch nicht beantwortet worden. Da die DS-GVO selbst jedoch nur bedingte Öffnungsklauseln vorsieht und der EuGH festgestellt hat, dass die in der DS-GVO festgelegte Schutzhöhe auch auf der Grundlage der Standardvertragsklauseln gewährleistet bleiben muss, bestehen erhebliche Bedenken, dass die Einwilligung einer betroffenen Person eine andere Bewertung rechtfertigen würde. Dafür spricht letztlich auch die eingeschränkte Öffnungsklausel des Art. 23 DS-GVO.

Die neu beschlossenen Standardvertragsklauseln enthalten einige Klarstellungen und tragen insofern zu einer ersten Steigerung der Rechtssicherheit bei. Zu begrüßen ist insbesondere, dass sich die überarbeiteten Standardvertragsklauseln an dem Prüfungsmaßstab des Art. 23 DS-GVO orientieren und damit an normativen Vorgaben. Unter Berücksichtigung der Rechtsprechung des EuGHs zu Schrems II enthalten die Klauseln ferner dokumentierte und qualifizierte Pflichten für Datenexporteure und -importeure. Neben Prüfpflichten in Bezug auf die Angemessenheit des Datenschutzniveaus ist nunmehr auch eine unmittelbare Mitteilungspflicht des Datenexporteurs an die Aufsichtsbehörde vorgesehen, sobald das Schutzniveau unterschritten wird, so dass die Kontrollmechanismen der Behörden erweitert wurden.

Die Verpflichtung des Datenimporteurs gegen Anfragen und etwaige Maßnahmen nationaler Behörden vorzugehen, belastet hingegen den Datenimporteur im Fall einer Auskunftsanfrage. Die Frage der Kostenverteilung entsprechender Prüf- und Abwehrmaßnahmen bleibt indes offen. Daher dürften anfangs vor allem kleine und mittelständische Unternehmen auf beiden Seiten zögern, die neuen Standardvertragsklauseln abzuschließen.

Kleinere und mittelständische Unternehmen dürften auch zögerlich agieren, soweit der EDSA bei Unterschreitung des in der Union gewährleisteten Datenschutzniveaus die Einrichtung zusätzlicher Maßnahmen empfiehlt. In diesem Fall soll nämlich der Datenexporteur die Rechtsordnung des Ziellandes kennen bzw. sich Kenntnis verschaffen und auf ein gleichwertiges Datenschutzniveau überprüfen. Ohne jegliche Vorgaben des Gesetzgebers oder der zuständigen Behörden geht diese Pflicht allerdings sehr weit und dürfte viele betroffene Unternehmen überfordern. Es wäre daher zu befürworten, dass offizielle Stellen eine allgemein gültige Liste über kritische datenschutzrechtliche Aspekte in Rechtsordnung und Verwaltungspraxis von Drittländern bereitstellen, die den Datenexporteuren als Grundlage der Bewertung dienen.

Bis dahin dürfte im Hinblick auf die durchzuführende Prüfung und etwaige ergänzende Schutzmaßnahmen – mangels konkreter Angaben in den Standardvertragsklauseln – nur der Rückgriff auf die Handlungsempfehlungen des EDSA bleiben. Dabei darf aber nicht außer Acht gelassen werden, dass es sich bei den Empfehlungen des EDSA um unverbindliche Vorgaben handelt, die lediglich als Auslegungshilfe herangezogen werden können. Solange den Verantwortlichen und Auftragsverarbeitern indes von legislativer oder judikativer Seite keine geeigneten Prüfmechanismen an die Hand gegeben werden, sorgen die Empfehlungen des EDSA neben den neu beschlossenen Standardvertragsklauseln noch für eine erste Rechtsklarheit. Es bleibt jedoch zu hoffen, dass diesen ersten Schritten zur Rechtssicherheit weitere folgen.

Nadine Eichmann
ist als Rechtsanwältin bei nbs partners in Hamburg tätig. Spezialisiert auf die Bereiche IT- und Datenschutzrecht berät sie zu allen juristischen Fragenstellungen, die im Wege der Digitalisierung von Unternehmensprozessen aufkommen. Zu ihrer Tätigkeit gehört neben der rechtlichen Begleitung von Systemumstellungen auch die Durchführung datenschutzrechtlicher Analysen und die Gestaltung von IT-Verträgen. Durch ihre Fokussierung auf den digitalen Bereich ist Nadine Eichmann gefragte Ansprechpartnerin für IT-Projekte und Datenschutz in Telemedien und E-Commerce.

Jaroslaw Norbert Nowak
ist als Rechtsanwalt bei nbs partners in Hamburg tätig. Aufgrund seiner langjährigen Berufserfahrung ist er ein erfahrener und qualifizierter Ansprechpartner im Handels- und Gesellschaftsrecht sowie Insolvenzrecht. Hierbei berät er auch in den Bereichen des Datenschutzes und der Compliance. Ferner liegt sein weiterer Schwerpunkt im Energierecht, wo er die Interessen von Energieversorgern und Industriekunden vertritt. Er unterstützt u.a. bei der Implementierung eines funktionierenden Managementsystems, der Durchführung von Gefährdungsanalysen und der Umsetzung von datenschutzrechtlichen Maßnahmen.

RA Jochen Zielbauer, LL.M.

Personenfotografie im nicht-journalistischen Bereich

Aktuelle Probleme und Lösungsmöglichkeiten für Unternehmen

Die Verwendung von Personenfotografien ist für viele Unternehmen, insbesondere für den Bereich der Öffentlichkeitsarbeit, sowie für Zwecke des Marketings, von enormer Bedeutung. Mit Inkrafttreten der DS-GVO sind Ungewissheiten im Hinblick auf das Verhältnis der DS-GVO gegenüber dem Kunsturhebergesetz (KUG) entstanden. Für Unternehmen, die auf eine Verwendung von Personenfotografien angewiesen sind, führt dies zu etlichen Unwägbarkeiten, da sich die Regelungen der DS-GVO in wesentlichen Punkten von denjenigen des KUG unterscheiden. Unternehmen benötigen jedoch in vielerlei Situationen Planungs- und Rechtssicherheit, sofern sie Personenfotografien für geschäftliche Zwecke verwenden wollen. Mit dem vorliegenden Beitrag werden aktuelle Probleme im Bereich der Personenfotografie für Unternehmen im nicht-journalistischen Bereich dargestellt und praktische Lösungen herausgearbeitet.

I. Der Rechtsrahmen bei der Anfertigung sowie Verwendung von Personenfotografien

Hinsichtlich des Rechtsrahmens bezüglich der Verarbeitung von Personenfotografien ist zunächst zu unterscheiden zwischen den verschiedenen in Betracht kommenden Verarbeitungsvorgängen, namentlich einerseits der Anfertigung von Personenfotografien und andererseits deren etwaiger anschließender weiterer Verwendung.

1. Die Anfertigung von Personenfotografien

Die Rechtmäßigkeit der Anfertigung von Personenfotografien bestimmt sich ausschließlich nach der DS-GVO. Insbesondere kommt eine Anwendung des KUG hier nicht in Betracht, da dieses nur eine etwaige spätere Verbreitung bzw. öffentliche Zurschaustellung regelt.[1]

Als Rechtsgrundlagen für die Anfertigung von Personenfotografien können insbesondere eine Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit. a DS-GVO, ein berechtigtes Interesse nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO sowie ein Vertrag gemäß Art. 6 Abs. 1 S. 1 lit. b DS-GVO dienen.

2. Die Verbreitung von Personenfotografien

Problematischer hingegen ist die Frage des rechtlichen Rahmens für eine weitere Verwendung von Personenfotografien, sofern diese in Form einer Verbreitung bzw. Veröffentlichung erfolgt, wie z.B. auch über Onlinedienste.

Ein solches Verwenden von Personenfotografien stellt zum einen eine Verarbeitung im Sinne von Art. 4 Nr. 2 DS-GVO dar.[2] Zum anderen fällt eine derartige Verwertungshandlung unter Umständen unter §§ 22 f. KUG, zumindest war dies bis zum In-Kraft-Treten der DS-GVO der Fall.[3] Strittig ist – nach wie vor – ob nach dem In-Kraft-Treten der DS-GVO die Regelungen des KUG oder aber diejenigen der DS-GVO auf die Verbreitung von Personenfotografien anzuwenden sind.

a) Praktische Relevanz des Meinungsstreits zur Anwendbarkeit der DS-GVO bzw. des KUG für Unternehmen

Für Unternehmen ist die Frage der Anwendbarkeit der DS-GVO oder aber des KUG vor allem deswegen von Bedeutung, da im Falle einer alleinigen Geltung der DS-GVO in vielen Fällen die Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit. a DS-GVO als Rechtsgrundlage für Datenverarbeitungen in Betracht kommt, die jedoch durch den Betroffenen gemäß Art. 7 Abs. 3 S. 1 DS-GVO jederzeit mit Wirkung für die Zukunft widerrufbar ist. Man stelle sich vor diesem Hintergrund beispielsweise den praxisrelevanten Fall einer umfangreichen Kampagne eines Unternehmens im Bereich der Öffentlichkeitsarbeit vor, bei welcher Personenfotografien zum Einsatz kommen. In einem solchen Fall hätten Betroffene, deren Abbildungen hierbei auf Grundlage einer Einwilligung gemäß der DS-GVO verwendet würden, ein Recht, diese Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Im für das jeweilige Unternehmen ungünstigsten Fall könnten diese betroffenen Personen durch Ausübung Ihres Widerrufsrechts eine solche Kampagne praktisch zu Fall bringen, wenn der Widerruf vor der betreffenden Verbreitungshandlung stattfindet. Ein Entfernen der betreffenden Abbildungen, bspw. nach erfolgtem Druck von Materialien, wäre für das betroffene Unternehmen aufgrund der damit verbundenen Aufwände bzw. Kosten in vielen Fällen keine Option. Dem jeweiligen Unternehmen könnte hierdurch ein erheblicher Schaden entstehen.[4]

1 Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, Verarbeitung personenbezogener Daten bei Fotografien, 2018, S. 4, https://www.lda.brandenburg.de/sixcms/media.php/9/RechtlicheAnforderungenFotografie.pdf

2 Wissenschaftliche Dienste des Bundestages, Veröffentlichung von Fotografien von Versammlungen und öffentlichen Veranstaltungen vom 27.09.2018, S. 7, https://www.bundestag.de/resource/blob/591826/17c71763caa37b428329641cce8a5ac2/WD-10-039-18-pdf-data.pdf

3 Landesbeauftragte für den Datenschutz Niedersachsen, Anfertigung und Veröffentlichung von Personenfotografien nach dem 25.05.2018 im nicht-öffentlichen Bereich, 2018, S. 1, https://lfd.niedersachsen.de/download/132460/Merkblatt_zur_Anfertigung_und_Veroeffentlichung_von_Personenfotografien_nach_dem_25._Mai_2018_im_nicht-oeffentlichen_Bereich.pdf.

Sind auf die Verbreitung von Personenfotografien hingegen §§ 22 f. KUG anwendbar, so kommt ein Widerruf einer Einwilligung nach ständiger Rechtsprechung nur unter bestimmten Voraussetzungen in Betracht.[5]

b) Vorzugswürdige Lösung des Meinungsstreits zur Anwendbarkeit der DS-GVO bzw. des KUG

Ausgangspunkt des Meinungsstreits ist die Frage, inwieweit Art. 85 DS-GVO eine Öffnungsklausel darstellt, so dass Abweichungen und Ausnahmen auch durch das Recht der Mitgliedsstaaten zulässig sind, oder aber inwieweit sich hieraus lediglich ein Anpassungsauftrag zur Sicherstellung eines angemessenen Ausgleichs von widerstreitenden Interessen ergibt.[6]

Zunächst ist hierbei festzuhalten, dass ein Rückgriff auf Art. 85 Abs. 2 DS-GVO zum Zwecke der Eröffnung des Anwendungsbereichs des KUG dann nicht in Betracht kommt, wenn es um Datenverarbeitungen durch Unternehmen außerhalb der in Art. 85 Abs. 2 DS-GVO genannten Zwecke geht.[7] Dies dürfte der Regelfall für Unternehmen sein, die etwa für den Bereich der Öffentlichkeitsarbeit Personenfotografien verarbeiten.[8]

Entscheidend ist daher, ob sich eine Anwendung des KUG für den nicht-journalistischen Bereich aus Art. 85 Abs. 1 DS-GVO ergeben kann.

Nach hier vertretener Auffassung ist die Ansicht, wonach Art. 85 Abs. 1 DS-GVO keine Öffnungsklausel, sondern lediglich einen Anpassungsauftrag beinhaltet, vorzuziehen. Dies ergibt sich bereits aus dem Umstand, dass Art. 85 Abs. 3 DS-GVO Mitteilungen an die Europäische Kommission nur im Hinblick auf Abweichungen und Ausnahmen auf der Grundlage von Art. 85 Abs. 2 DS-GVO vorsieht. Dass Art. 85 Abs. 1 DS-GVO ebenfalls Abweichungen bzw. Ausnahmen zulasse, diese aber eben nicht mittzuteilen sind, ist nicht einzusehen.[9] „In Einklang" gem. Art. 85 Abs. 1 DS-GVO wird entsprechendes Recht zudem nicht dadurch gebracht, dass vom Schutzniveau der DS-GVO ausdrücklich abgewichen wird bzw. entsprechende Ausnahmen vorgesehen werden. Die widerstreitenden Interessen des Datenschutzes auf der einen Seite sowie diejenigen der Meinungs- und Informationsfreiheit auf der anderen Seite können insbesondere auch dadurch in Einklang gebracht werden, dass entsprechende Abwägungsmaßstäbe auch im nationalen Recht der Mitgliedsstaaten implementiert werden.[10]

c) Zwischenergebnis

Art. 85 Abs. 1 DS-GVO stellt daher keine Öffnungsklausel entsprechend Art. 85 Abs. 2 DS-GVO dar, sondern enthält lediglich einen Anpassungsauftrag an die Mitgliedsstaaten.[11] Eine insoweit erforderliche Anpassung des KUG ist bislang nicht erfolgt.[12] Für den Bereich der Verbreitung von Personenfotografien im nicht-journalistischen Bereich überlagert die DS-GVO somit den Anwendungsbereich des KUG.[13]

II. Rechtsgrundlagen für die Verarbeitung von Personenfotografien

Im Folgenden sollen denkbare Rechtsgrundlagen gemäß der DS-GVO, auf die eine Verarbeitung von Personenfotografien gestützt werden kann, erörtert werden.

1. Das berechtigte Interesse als Rechtsgrundlage

Für Unternehmen, die insbesondere im Bereich der Öffentlichkeitsarbeit tätig sind, kommt dem berechtigten Interesse gemäß Art. 6 Abs. 1 S. 1 lit. f DS-GVO als Rechtsgrundlage im Zusammenhang mit der Verwendung von Personenfotografien besondere Bedeutung zu. Dies liegt daran, dass gerade bei Veranstaltungen, bezüglich derer ein Dokumentationsinteresse des Unternehmens besteht, oftmals eine Vielzahl an Personen beteiligt ist, und die Einholung von Einwilligungen aller dieser Teilnehmer oftmals zu erheblichen Hürden führen würde.

a) Abwägungsmaßstäbe gemäß der DS-GVO

Bei der Frage, ob ein berechtigtes Interesse als Rechtsgrundlage herangezogen werden kann bzw. im Rahmen der hierbei vorzunehmenden Abwägung können als Hilfestellung primär die im Erwägungsgrund 47 zur DS-GVO genannten Grundsätze herangezogen werden, namentlich die „vernünftigen Erwartungen der betroffenen Person", die „Beziehung zwischen der betroffenen Person und dem Verantwortlichen" sowie die Absehbarkeit einer entsprechenden beabsichtigten Verarbeitung aus Sicht des Betroffenen.

b) Abwägungsmaßstäbe gemäß dem KUG

Von Seiten der Rechtsprechung werden im Zusammenhang mit der Güterabwägung bei der Prüfung des berechtigten Interesses die §§ 22 f. KUG und die hierzu in der Rechtsprechung ergangenen Grundsätze angewendet.[14] Dies seien, so die Rechtsprechung, Gesichtspunkte, die unter Berücksichtigung einer entsprechenden europarechtsautonomen Auslegung im Rahmen der Interessenabwägung einzubeziehen sind.[15] Da es

4 Raji, ZD 2019, 61, 65.

5 BAG vom 19.02.2015 – 8 AZR 1011/13, MMR 2015, 544, 546.

6 Sundermann, K&R 2018, 441 ff.

7 Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Rechtliche Bewertung von Fotografien einer großen Anzahl von Personen nach DS-GVO außerhalb des Journalismus, 2018, S. 5, https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Wirtschaft/Inhalt/Fotografien-ausserhalb-des-Journalismus/Bewertung-Fotografien-ausserhalb-Journalismus.pdf.

8 Assmus/Winzer, ZD 2018, 508, 512

9 Raji, ZD 2019, 61, 64 f.

10 Buchner/Tinnefeld, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 85 Rn. 27.

11 Klein, Personenbilder im Spannungsfeld von Datenschutzgrundverordnung und Kunsturhebergesetz, 2017, S. 209.

12 Benedikt/Kranig, ZD 2019, 4, 6.

13 Raji, ZD 2019, 61, 65.

14 LG Frankfurt/M. vom 26.09.2019 – 2-03 O 402/18, K&R 2019, 808, 810.

15 LG Frankfurt/M. vom 13.09.2018 – 2-03 O 283/18, K&R 2018, 733, 734.

sich bei der DS-GVO um EU-Recht handelt, können die genannten Gesichtspunkte richtigerweise nicht unmittelbar, jedoch als Abwägungshilfe herangezogen werden.[16]

Folgende Regelungen des KUG sowie die hierzu abgeleiteten Grundsätze können vor diesem Hintergrund herangezogen werden:

Ist eine Person lediglich als „Beiwerk" gemäß § 23 Abs. 1 Nr. 2 KUG anzusehen, können Bilder, auf denen solche Personen erscheinen, nach KUG ohne Einwilligung verbreitet oder zur Schau gestellt werden. Entscheidend ist hier, dass der Gesamteindruck durch die abgebildete Umwelt bestimmt ist. Die abgebildeten Personen sind insofern „Beiwerk", als diese jederzeit weggelassen werden könnten, ohne dass sich der Gesamteindruck des Bildes ändern würde.[17] Es kommt darauf an, ob die einzelnen Abgebildeten nur „bei Gelegenheit" erscheinen oder ob der Einzelne aus der Anonymität herausgelöst ist.[18]

Bei Bildern von Veranstaltungen gemäß § 23 Abs. 1 Nr. 3 KUG geht es allein um die Darstellung des Geschehens, nicht aber um die Darstellung der Personen, die an dem Geschehen teilgenommen haben. Ein Teilnehmer einer solchen Veranstaltung muss damit rechnen, dass er auf Bildern, die die Veranstaltung dokumentieren, abgebildet wird.[19] Sofern der Einzelne jedoch aus der Masse der Teilnehmer „herausgelöst" wird, etwa durch Heranzoomen mittels Teleobjektiv, ist der Rechtfertigungstatbestand des § 23 Abs. 1 Nr. 3 KUG nicht erfüllt.[20]

c) Besonderheiten im Falle von Beschäftigungsverhältnissen

Im Falle von Beschäftigungsverhältnissen sollten bei Wahl des berechtigten Interesses als Rechtsgrundlage für die Datenverarbeitung spezifische Risikominderungsmaßnahmen ergriffen werden.[21] Hier spielt also ein Stück weit auch immer der Grundsatz der Fürsorgepflicht des Arbeitgebers eine Rolle, und sollte im Zusammenhang mit der Interessenabwägung mit berücksichtigt werden.

d) Zusammengefasst: Wesentliche Abwägungsmaßstäbe bei der Prüfung des berechtigten Interesses im Zusammenhang mit der Verarbeitung von Personenfotografien

Abbildungen von Personen, insbesondere im Rahmen von Veranstaltungen, bei denen diese nur als „Beiwerk" anzusehen sind, dürften im Regelfall auf Basis eines berechtigten Interesses als Rechtsgrundlage gerechtfertigt sein. Dies ergibt sich zum einen daraus, dass auf derartigen Veranstaltungen aus Sicht eines vernünftigen Dritten zumindest mit Fotografien, auf denen ein Betroffener als „Beiwerk" abgebildet ist, zu rechnen ist. Erscheint der Betroffene als aus der Anonymität „herausgelöst", wird man eher zu der Ansicht gelangen, dass derartige Aufnahmen nicht auf ein berechtigtes Interesse gestützt werden können. Insbesondere, wenn sich der Betroffene einer derartigen Aufnahme nicht bewusst ist, überwiegen dessen Rechte gegenüber denen des Verantwortlichen, da er mit einer derartigen Verarbeitung seiner personenbezogenen Daten nicht zu rechnen braucht. Will ein Verantwortlicher derartige Aufnahmen anfertigen bzw. verwenden, muss er sich ggf. auf andere Rechtsgrundlagen, wie eine Einwilligung des Betroffenen oder einen Vertrag mit diesem, stützen.

2. Die Einwilligung als Rechtsgrundlage

Die Einwilligung bietet einerseits für Unternehmen den Vorteil, dass diese – in den Grenzen des Art. 7 DS-GVO und insbesondere der Maßstäbe des Erwägungsgrundes 32 – weitgehende Verarbeitungsvorgänge zu rechtfertigen vermag. Insbesondere kann die Einwilligung grundsätzlich auch als Rechtsgrundlage für eine Verarbeitung von Personenfotografien dienen, bei der die Rechte und Freiheiten der jeweils betroffenen Person in höherem Maße betroffen sind. Dies gilt freilich nur dann, wenn die Anforderungen an eine Rechtmäßigkeit der Einwilligung erfüllt sind. Somit kann etwa die Einwilligung auch für solche Verarbeitungen Rechtsgrundlage sein, bei denen eine betroffene Person nicht lediglich als „Beiwerk" einer Veranstaltung anzusehen ist.

a) Unwirksamkeit des Widerrufs

Wegen der bereits dargestellten, unter Umständen erheblichen Auswirkungen des Widerrufs einer Einwilligung, stellt sich die Frage nach einer Möglichkeit, die Widerrufbarkeit im Einzelfall einzuschränken. Vereinzelt wird die Auffassung vertreten, dass dem Betroffenen in bestimmten Situationen der Rückgriff auf den Widerruf der Einwilligung verwehrt bleiben muss.[22] Begründet wird dies mit der bisherigen Rechtsprechung im Hinblick auf die Gültigkeit von Widerrufen einer Einwilligung gemäß § 22 KUG. Demnach ist im Falle eines Widerrufs einer Einwilligung gemäß § 22 KUG eine Abwägung im Rahmen der gegenseitigen Rücksichtnahme auf die Interessen der anderen Seite nach Maßgabe von § 241 Abs. 2 BGB vorzunehmen.[23] Eben diese Wertung der Rechtsprechung müsse auch auf den Widerruf der Einwilligung gemäß der DS-GVO angewendet werden, was sich aus dem Grundsatz von Treu und Glauben sowie arbeitsrechtlichen Rücksichtnahmepflichten ergebe.[24] Vereinzelt wird auch versucht, dieses Ergebnis, also die Einschränkung des Widerrufsrechts, durch eine teleologische Reduktion des Art. 7 Abs. 3 DS-GVO zu erreichen. Jedenfalls in denjenigen Fällen, in denen eine Einwilligung vertraglich zwingende Hauptleistung ist, könne die Möglichkeit zum Widerruf ausgeschlossen werden.[25]

16 Raji, ZD 2019, 61, 66.

17 Götting, in: Schricker/Loewenheim (Hrsg.), Urheberrecht, 6. Aufl. 2020,§ 23 KUG Rn. 81.

18 BAG vom 11.12.2014 – 8 AZR 1010/13, ZD 2015, 330, 331 f.

19 Götting, in: Schricker/Loewenheim (Fn. 17), Rn. 84.

20 LG Hamburg vom 11.01.2008 – 324 O 126/07, AfP 2008, 100, 102.

21 Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz (WP 249), S. 7, https://datenschutz-hamburg.de/assets/pdf/wp249_en.pdf.

22 Hessischer Beauftragter für Datenschutz und Informationsfreiheit, Siebenundvierzigster Tätigkeitsbericht zum Datenschutz und Erster Bericht zur Informationsfreiheit, 2018, S. 142 f., https://www.zaftda.de/tb-bundeslaender/hessen/landesdatenschutzbeauftragter-2/713-47-tb-lfd-hessen-2018-o-drs-nr-vom-24-062019/file.

23 BAG vom 11.12.2014 – 8 AZR 1010/13, NJW 2015, 2140, 2143.

24 Hessischer Beauftragter für Datenschutz und Informationsfreiheit (Fn. 22), S. 143.

25 Ernst, ZD 2020, 383, 385.

Diese Ansicht steht jedoch dem klaren Wortlaut des Art. 7 Abs. 3 DS-GVO entgegen, wonach das Recht zum Widerruf für den Betroffenen „jederzeit" besteht. Hierdurch wird deutlich, dass, sofern eine Datenverarbeitung auf die Rechtsgrundlage der Einwilligung gestützt wird, im Falle eines Widerrufs für jedwede Wertungen kein Platz ist, und die betreffende Datenverarbeitung für die Zukunft unbedingt zu unterbleiben hat.

Diese Auslegung ergibt sich zudem aus den Stellungnahmen der Artikel-29-Datenschutzgruppe, welche sich in der Kodifizierung der DS-GVO wiedergefunden haben.[26] Betont wird in diesem Zusammenhang die „Bedeutung der Einwilligung als Voraussetzung für die Autonomie und Selbstbestimmung des Einzelnen".[27] Einem derartigen Verständnis würde es zuwiderlaufen, wenn sich der Betroffene bei Erteilung seiner Einwilligung nicht sicher sein könnte, ob er von seinem Widerrufsrecht Gebrauch machen kann oder nicht, da das Widerrufsrecht insoweit gerade ein Bestandteil der autonomen und selbstbestimmten Entscheidung des Einzelnen im Hinblick auf die Verarbeitung seiner personenbezogenen Daten ist.

Der Einwilligende kann somit seine Einwilligung aus jedweden Gründen widerrufen, selbst wenn dies unter Umständen erfolgt, die aus Sicht eines Dritten interessenwidrig sein mögen. Auch für eine Interessenabwägung ist vor diesem Hintergrund kein Platz.[28] Zudem ist der Verantwortliche in diesem Fall auch gerade nicht völlig schutzlos: Eine Verarbeitung trotz eines erfolgten Widerrufs ist gleichwohl möglich, wenn die Datenverarbeitung auf eine anderweitige Rechtsgrundlage gestützt werden kann.[29]

b) Besonderheiten im Falle von Beschäftigungsverhältnissen

Geht es um eine Verarbeitung von personenbezogenen Daten im Rahmen eines Beschäftigungsverhältnisses, so ist für die Frage der Freiwilligkeit einer Einwilligung immer das gewisse Ungleichgewicht zwischen Arbeitgeber und Arbeitnehmer zu berücksichtigen. Jegliche Ausübung von Druck im Hinblick auf die Abgabe von Einwilligungen muss daher unterbleiben.[30] In der Praxis kann den insoweit gestiegenen Anforderungen an die Gewährleistung der Freiwilligkeit dadurch begegnet werden, dass der Betroffene auf die Folgenlosigkeit eines Verweigerns der Einwilligung ausdrücklich und möglichst hervorgehoben hingewiesen wird.

c) Zwischenergebnis

Die Einwilligung bietet sich wegen des flexiblen Einsatzbereichs an, um spezielle und ggf. weitreichende Verarbeitungssituationen zu rechtfertigen. Ihre maßgebliche „Schwachstelle" aus Sicht des Verantwortlichen ist jedoch die jederzeitige Widerruflichkeit, die zudem nicht eingeschränkt werden kann.

3. Der Vertrag als Rechtsgrundlage

In Betracht kommt zudem eine Heranziehung von Art. 6 Abs. 1 S. 1 lit. b DS-GVO, wonach eine Verarbeitung für die Erfüllung eines Vertrages mit dem Betroffenen gerechtfertigt sein kann.

Im Falle der Verarbeitung von Personenfotografien stellt sich jedoch hierbei die Frage, ob diese Rechtsgrundlage auch dann herangezogen werden kann, wenn der Hauptzweck der entsprechenden vertraglichen Vereinbarung die Datenverarbeitung selbst ist, und die betroffene Person – im Falle eines Vertrages – obendrein Schuldner im Hinblick auf die Bereitstellung der vertragsgegenständlichen personenbezogenen Daten wäre. Fraglich ist weiterhin, ob Art. 6 Abs. 1 S. 1 lit. b DS-GVO in derartigen Fällen nur dann Rechtsgrundlage sein kann, wenn die betroffene Person, die sich zur Bereitstellung von personenbezogenen Daten auf Basis eines Vertrages verpflichtet, hierfür eine Gegenleistung erhält.

a) Auslegung nach dem Wortlaut

Um diese Frage beantworten zu können, ist eine Auslegung des Art. 6 Abs. 1 S. 1 lit. b DS-GVO erforderlich, welche zunächst anhand des Wortlauts zu erfolgen hat.

Die Vorschrift des Art. 6 Abs. 1 S. 1 lit. b DS-GVO spricht von Verarbeitungen, die „für die Erfüllung eines Vertrages erforderlich sind". Dies lässt jedoch eine Beantwortung der oben aufgeworfenen Frage im Unklaren. Den Wortlaut könnte man einerseits dahingehend verstehen, dass es lediglich um solche Datenverarbeitungen gehen muss, die quasi „Mittel zum Zweck" bezüglich der Erbringung einer Leistung seitens des Verantwortlichen sind. Auf die synallagmatische Leistung selbst könnte sich also die Gestattungsnorm des Art. 6 Abs. 1 S. 1 lit. b DS-GVO gerade nicht beziehen.[31]

Allerdings ist jedenfalls der Wortlaut der Norm insoweit nicht eindeutig. Sofern man Art. 6 Abs. 1 S. 1 lit. b DS-GVO weit auslegt und mit der Formulierung „Erfüllung eines Vertrages" alle Datenverarbeitungen im gesamten Vertragsverhältnis erfassen möchte, vom vorvertraglichen Stadium über die Durchführung des Vertrages bis zu dessen Beendigung,[32] besteht kein Grund, die beschriebenen Datenverarbeitungen als nicht von der Gestattungsnorm umfasst anzusehen. Denn auch diese Datenverarbeitung eines Empfängers von personenbezogenen Daten bzw. eines Gläubigers im Rahmen eines entsprechenden Vertragsverhältnisses, bei dem die Übermittlung von Daten Hauptzweck ist, ist letzten Endes notwendig, um einen derartigen Vertrag zur Vollendung zu bringen.

Zu beachten ist weiter, dass Art. 6 Abs. 1 S. 1 lit. b DS-GVO jegliche Datenverarbeitungen umfasst, bei denen der Betroffene „Vertragspartei" ist. Diese weite Formulierung

26 Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, S. 27, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

27 Artikel-29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung (WP187), S. 33, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

28 A.A. Assmus/Winzer, ZD 2018, 508, 513.

29 Europäischer Datenschutzausschuss (Fn. 26), S. 29.

30 Artikel-29-Datenschutzgruppe (Fn. 21), S. 6 f.

31 Ernst, ZD 2020, 383, 385.

32 Kramer, in: Auernhammer (Hrsg.), DS-GVO/BDSG, 7. Aufl. 2020, Art. 6 Rn. 28.

lässt den Inhalt des Vertragsverhältnisses und die Konstellation der an einem entsprechenden Vertragsverhältnis Beteiligten gerade unberücksichtigt, was somit gegen eine einengende Auslegung spricht.

Was die Frage des Erfordernisses einer Gegenleistung für die Übermittlung von personenbezogenen Daten anbelangt, um eine solche Übermittlung auf die Rechtsgrundlage gemäß Art. 6 Abs. 1 S. 1 lit. b DS-GVO stützen zu können, so ist in diesem Zusammenhang das weite Verständnis des Begriffes „Vertrag" im Sinne der DS-GVO zu berücksichtigen. Es kommt jedes rechtsgeschäftliche oder rechtsgeschäftsähnliche Schuldverhältnis in Betracht,[33] so dass eine Gegenleistung, jedenfalls vom Wortlaut der Vorschrift her, insoweit keine Voraussetzung sein kann.

b) Systematische Auslegung

Nach der Rechtsprechung des EuGH „ist jede Vorschrift des Gemeinschaftsrechts in ihrem Zusammenhang zu sehen und im Lichte des gesamten Gemeinschaftsrechts, seiner Ziele und seines Entwicklungsstands zur Zeit der Anwendung der betreffenden Vorschrift auszulegen".[34] Die Vertragsfreiheit ist im primären Gemeinschaftsrecht zwar nicht selbst ausdrücklich, jedoch durch anderweitige Gewährleistungen als umfassend abgesichert anzusehen.[35] Vor diesem Hintergrund erscheint es nicht nachvollziehbar, dem Betroffenen Verfügungen über seine personenbezogenen Daten zu verbieten, auch wenn diese ggf. nicht mit einer Gegenleistung einhergehen. Die Parteien mögen Gründe dafür haben, warum sie mit einem Vertrag Rechtssicherheit im Hinblick auf die Nutzung von Personenfotografien erzielen möchten. Eine Auslegung von Art. 6 Abs. 1 S. 1 lit. b DS-GVO dergestalt, die es einem Betroffenen untersagen würde, derartige Verpflichtungen einzugehen, ist letzten Endes nicht mit einem Grundsatz der Privatautonomie vereinbar.

Den Parteien einen derartigen Spielraum bei der Vertragsgestaltung zuzugestehen, steht zudem auch nicht im Widerspruch zu der Auslegung des Europäischen Datenschutzausschuss (EDSA). Demnach reiche die bloße Bezugnahme oder Erwähnung der Verarbeitung von Daten in einem Vertrag nicht aus, um die fragliche Verarbeitung in den Anwendungsbereich von Art. 6 Abs. 1 S. 1 lit. b DS-GVO zu bringen; entscheidend sei vielmehr, was für die Erfüllung des Vertrages objektiv erforderlich sei.[36] Auch verweist der EDSA in diesem Zusammenhang auf Leitlinien der Artikel-29-Datenschutzgruppe, wonach das Merkmal der Erforderlichkeit für die Erfüllung eines Vertrags mit der betroffenen Person dann nicht erfüllt sei, wenn die Verarbeitung für die Erfüllung eines Vertrags nicht wirklich notwendig ist, sondern der betroffenen Person von dem für die Verarbeitung Verantwortlichen einseitig auferlegt wird.[37] Als Beispiel dient ein mit einem Onlinehändler abgeschlossener Kaufvertrag, welcher ebenfalls Profilerstellungen beinhaltet, die jedoch für die Erfüllung des Kaufvertrags gerade nicht erforderlich sind.[38]

Eine vergleichbare Situation ergibt sich bei Verträgen, die eine Zur-Verfügung-Stellung von personenbezogenen Daten als Hauptzweck des Vertrages zum Gegenstand haben, jedoch nicht. Da es sich hierbei eben offenkundig um den primären Inhalt des Vertrages handelt, ist weder eine einseitige Auferlegung seitens des Verantwortlichen gegeben, noch wird die Datenverarbeitung dem Betroffenen als eine Nebenbestimmung „untergejubelt".

c) Teleologische Auslegung

Gegen die Auffassung, Art. 6 Abs. 1 S. 1 lit. b DS-GVO als Rechtsgrundlage für die Bereitstellung von personenbezogenen Daten seitens des Betroffenen – auch ohne Gegenleistung – zuzulassen, könnte schließlich der Sinn und Zweck der Norm sprechen. Teilweise wird vertreten, dass ein derartiges Vorgehen unzulässig sei, da es ansonsten der Verantwortliche in der Hand hätte, durch eine vertragliche Gestaltung die Anfordernisse der Einwilligung zu umgehen, welche für derartige Konstellationen die eigentlich richtige Rechtsgrundlage sei. Darüber hinaus sei in diesem Zusammenhang eine vertragliche Bindung ohne Gegenleistung – zumindest im Kontext eines Beschäftigungsverhältnisses – als rechtsmissbräuchlich einzustufen.[39]

Gegen eine solche Auffassung ist jedoch wiederum zunächst einzuwenden, dass hierdurch zu weitgehend in die Privatautonomie und in das Recht zur informationellen Selbstbestimmung eingegriffen wird. Auch ist zu berücksichtigen, dass der Betroffene im Falle einer vertraglichen Verpflichtung zur Bereitstellung von Daten, ggf. auch ohne Gegenleistung, durch die allgemeinen Vorschriften geschützt ist. Zudem ist bei einem Vertragsschluss für den Betroffenen auch grundsätzlich ersichtlich, dass er sich dergestalt bindet, wohingegen er bei Abgabe einer Einwilligung über sein Recht zum jederzeitigen Widerruf gemäß Art. 7 Abs. 3 DS-GVO zwingend in Kenntnis zu setzen ist. Je nach Wahl der Rechtsgrundlage durch den Verantwortlichen ist somit für den Betroffenen klar, worauf er sich einlässt. Bindet er sich demnach aufgrund einer autonomen Entscheidung im Rahmen eines Vertragsverhältnisses, so ist dies nicht per se als ein Rechtsmissbrauch einzustufen.

d) Besonderheiten im Falle von Beschäftigungsverhältnissen

Im Kontext von Beschäftigungsverhältnissen ist bei Verarbeitungen von personenbezogenen Daten, die auf der Basis von Vertragsverhältnissen erfolgen sollen, immer auch § 26

33 Heinzke/Engel, ZD 2020, 189, 190.

34 EuGH vom 06.10.1982 – Rs 283/81, NJW 1983, 1257, 1258.

35 Basedow, in: Bitburger Gespräche, 2009, S. 91.

36 Europäischer Datenschutzausschuss, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Abs. 1 Buchstabe b DS-GVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, Rn. 27, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf.

37 Artikel-29-Datenschutzgruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG (WP217), S. 21, https://www.datenschutzstelle.li/application/files/2915/5914/1746/WP217_Opinion62014LegitimateInterest.pdf.

38 Europäischer Datenschutzausschuss (Fn. 36), Rn. 35.

39 Eggers, Quick Guide Bildrechte, 2. Aufl. 2019, S. 53.

BDSG mit zu betrachten, wonach bestimmte Datenverarbeitungen auf das Beschäftigtenverhältnis gestützt werden können. Problematisch ist jedoch, ob dieser auch im Falle der Zur-Verfügung-Stellung von Personenfotografien herangezogen werden kann, da oftmals eine Erforderlichkeit zur Durchführung des Beschäftigungsverhältnisses nicht bejaht werden kann.[40] Ob und unter welchen Voraussetzungen in derartigen Fällen etwa eine zusätzliche Vereinbarung zwischen Arbeitgeber und Arbeitnehmer im Hinblick auf die Verarbeitung von Personenfotografien möglich ist, bestimmt sich nach den allgemeinen bzw. arbeitsrechtlichen Bestimmungen.

e) Zwischenergebnis

Der Verantwortliche kann sich somit der Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. b DS-GVO auch in denjenigen Fällen bedienen, in denen Hauptzweck des betreffenden Vertrages die Bereitstellung der betreffenden personenbezogenen Daten seitens des Betroffenen gegenüber dem Verantwortlichen ist, selbst wenn der jeweilige Vertrag für diese Bereitstellung keine Gegenleistung vorsieht.

III. Fazit

Wie herausgearbeitet wurde, bietet die DS-GVO sowohl für die Anfertigung als auch für die Verbreitung von Personenfotografien durch die Auswahl von verschiedenen Rechtsgrundlagen für Unternehmen hinreichende Möglichkeiten, um entsprechende Datenverarbeitungen zu legitimieren. Insbesondere mittels eines Vertrages gemäß Art. 6 Abs. 1 S. 1 lit. b DS-GVO können verantwortliche Stellen Fallkonstellationen bewältigen, bei denen eine gewisse Planungssicherheit bei der Datenverarbeitung unerlässlich ist, und bei denen sich eine Einwilligung nach DS-GVO aufgrund der gegebenen Unwägbarkeiten wegen des jederzeitigen und unbedingten Widerrufsrechts des Betroffenen nicht anbietet. Unternehmen ist in jedem Fall anzuraten, sich bereits im Vorfeld einer Datenverarbeitung, beispielsweise einer umfangreichen Werbekampagne, mit den entsprechenden Vor- und Nachteilen der verschiedenen Rechtsgrundlagen vertraut zu machen und ihr weiteres Vorgehen danach auszurichten.

Jochen Zielbauer
ist derzeit als Syndikusrechtsanwalt in der Energiebranche beschäftigt. Zu seinen Beratungsfeldern gehören insbesondere das Datenschutzrecht, das IT- sowie das Urheber- und Medienrecht.

40 Assmus/Winzer, ZD 2018, 508, 511.

Basiswissen IT-Sicherheit

22.–23. September 2021 I Frankfurt/M.
Referent: Christian Semmler

Schwerpunkte:

✓ Einführung in IT-Sicherheitstechnologien
✓ Aktuelle Bedrohungen und grundlegende Abwehrstrategien
✓ Schutzziele nach DS-GVO und Bestimmung der Angemessenheit
✓ Schnittstellen und Kooperation zwischen Datenschutz- und IT-Sicherheitsbeauftragtem

Jetzt anmelden: www.datakontext.com

GDD DATAKONTEXT

Kurzbeiträge

Abdingbarkeit des Art. 32 DS-GVO durch Einwilligung

Alexander Bleckat*

In Art. 32 DS-GVO werden die Anforderungen an die technischen und organisatorischen Maßnahmen (sog. TOMs) des datenschutzrechtlich Verantwortlichen definiert. Besonderes Augenmerk soll hier auf die nach Art. 32 Abs. 1 lit. a) DS-GVO erforderliche Verschlüsselung von personenbezogenen Daten gelegt werden. Denn insbesondere die End-to-End-Verschlüsselung ist in einer Vielzahl von wirtschaftlichen Bereichen (z.B. Messenger-Dienste) nicht mehr wegzudenken und stellt einen „Trust-Faktor" für die Einhaltung von Datenschutz dar. Da die Einhaltung von TOMs mit hohen Kosten für Unternehmen verbunden ist, wäre es für diese wohl vorteilhaft, wenn diese im Rahmen der Verarbeitung von personenbezogenen Daten eines Betroffenen individuell durch Einwilligung abbedingt werden könnten. Der folgende Artikel widmet sich der Frage nach der Zulässigkeit einer solchen Einwilligung.

I. Einleitung

Die Abdingbarkeit des Art. 32 DS-GVO und somit die Abdingbarkeit der sog. TOMs korrespondiert mit der Frage, ob betroffene Personen in ein niedrigeres Schutzniveau einwilligen können als rechtlich geboten ist, wobei diese Problematik in der Praxis regelmäßig anhand der Verschlüsselung, insbesondere im E-Mail-Bereich, deutlich wird.[1] Als praxisbezogenes Beispiel kann herangezogen werden, ob ein Betroffener wirksam darin einwilligen könnte, dass ihm der datenschutzrechtlich Verantwortliche (z.B. eine Klinik) Dokumente mit personenbezogenen Daten (z.B. Befunde) unverschlüsselt oder mittels eines niedrigeren Datensicherheitsniveaus bezüglich der Verschlüsselung per E-Mail zusenden dürfte. Damit könnte der Verantwortliche nicht nur den Verschlüsselungsaufwand sparen, sondern sich auch zugleich der Haftung für etwaige „Hackerangriffe" von Dritten bzw. der Haftung für sog. „Data Breaches" (Datenpannen) entziehen. Die clientbasierten Securitykonzepte, die nur mit viel Aufwand und hohen Administrationskosten realisierbar sind,[2] würden in der E-Mail-Kommunikation für diesen Betroffenen somit wegfallen. Allein daran wird deutlich, inwiefern sich eine solche Einwilligung für den Verantwortlichen „rechnen" würde. Noch deutlicher wird dies, wenn der Verantwortliche beispielsweise von allen Kunden eine Einwilligung für eine unverschlüsselte E-Mail-Kommunikation einholt. In Anbetracht dieses Missbrauchsrisikos muss sich eingehend damit auseinandergesetzt werden, ob es sich bei den Vorgaben des Art. 32 DS-GVO um zwingende, nicht zur Disposition der betroffenen Person stehende Vorgaben handelt,[3] sodass eine Einwilligung nach§ 134 BGB unwirksam wäre.

II. Schutzzweck und Regelungsgehalt von Art. 32 DS-GVO

Aus Erwägungsgrund 83 der DS-GVO ergibt sich, dass der Verantwortliche und Auftragsverarbeiter zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung die mit der Verarbeitung verbundenen Risiken zu ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, zu treffen hat. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter müssen daher geeignete technische und organisatorische Maßnahmen durchführen, die für den Schutz gegen zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind.[4] Somit gibt Art. 32 DS-GVO den Verpflichteten die regulatorischen Leitplanken für die Umsetzung entsprechender Maßnahmen vor[5] und soll zugleich für ein angemessenes Schutzniveau für personenbezogene Daten sorgen.[6] So regelt Art. 32 Abs. 1 DS-GVO, dass eine Pseudonymisierung und Verschlüsselung personenbezogener Daten erfolgen (lit. a), die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden (lit. b), die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellt werden (lit. c) und ein Verfahren zur regelmäßigen Überprüfung, Bewertung sowie Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung bestehen

* Richter auf Probe Alexander Bleckat ist momentan bei der Staatsanwaltschaft Hannover als Staatsanwalt tätig und Mitautor des Buches „Jura geht auch anders".

1 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Vermerk: Abdingbarkeit von Art. 32 DS-GVO, https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf; S. 2 (Stand: 12.05.2021).

2 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Vermerk: Abdingbarkeit von Art. 32 DS-GVO, https://www.tecchannel.de/a/automatische-verschluesselung-mit-e-mail-gateways,1762105,2 (Stand: 12.05.2021)

3 Ebenso: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Vermerk: Abdingbarkeit von Art. 32 DS-GVO, https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf; S. 2 (Stand: 12.05.2021).

4 Kühling/Buchner/Jandt, DS-GVO, 3. Aufl. 2020, Art. 32 Rn. 3., Rn. 2; ebenso Gola/Piltz, DS-GVO, 2. Aufl. 2018, Art. 32 Rn. 3.

5 Gola/Piltz, DS-GVO, 2. Aufl. 2018, Art. 32 Rn. 3.

6 Sydow/Mantz, Europäische Datenschutzgrundverordnung, DS-GVO, 2. Aufl. 2018, Art. 32 Rn. 1.

muss (lit. d).[7] Damit stellt Art. 32 DS-GVO grundsätzlich hohe Anforderung an die Sicherheit von Verarbeitungsprozessen im Zusammenhang mit personenbezogenen Daten. Dies ist jedoch auch nachvollziehbar, da sich Betroffene darauf verlassen dürfen, dass ihre Daten bei dem Verantwortlichen sicher bzw. vor dem Zugriff von Dritten geschützt sind. Letztendlich legt Art. 32 DS-GVO dem Verantwortlichen daher im Interesse der Verarbeitungssicherheit besondere Gewährleistungspflichten auf,[8] wobei in der DS-GVO keine Ausnahme dafür vorgesehen sind.

III. Abdingbarkeit von Art. 32 DS-GVO

Die herrschende Literatur ist der Ansicht, dass Art. 32 DS-GVO nicht disponibel bzw. abdingbar ist.[9]

Dagegen sind der Hamburger Datenschutzbeauftragte und das Bayrische Landesamt für Datenschutzaufsicht der Ansicht, dass Art. 32 DS-GVO durch Einwilligung abdingbar sei und somit zur Disposition des Betroffenen stehe.[10] Gleichwohl müsse der Verantwortliche oder Auftragsverarbeiter aber die in Art. 32 DS-GVO enthaltenen verbindlichen Regeln einhalten, da Art. 32 DS-GVO eine Pflicht zur Implementierung angemessener Maßnahmen enthält und dem Verantwortlichen oder Auftragsverarbeiter gerade keine Entscheidungsbefugnis darüber einräumt, ob er diese umsetzt.[11]
Nach deren Ansicht kann der Betroffene somit in ein niedrigeres Schutzniveau einwilligen, aber der Verantwortliche oder Auftragsverarbeiter muss dennoch die in Art. 32 DS-GVO genannten Maßnahmen implementieren. Dies hat jedoch zur Folge, dass der Verantwortliche oder Auftragsverarbeiter, auch wenn er die entsprechenden Maßnahmen zu implementieren hat, grundsätzlich ein niedrigeres Datensicherheitsniveau mit Einzelnen oder sogar allen Betroffenen vereinbaren könnte. Damit könnte er sich unter Umständen Aufwand oder Kosten sparen, da er nicht mehr das in Art. 32 DS-GVO angemessene Datensicherheitsniveau hinsichtlich der eingewilligten Verarbeitungsprozesse aufrechterhalten müsste. Auch könnte er dadurch sein Haftungsrisiko für Verstöße gegen Art. 32 DS-GVO bezüglich der Datenverarbeitungsprozesse, bei denen in ein niedrigeres Datensicherheitsniveau eingewilligt wurde, minimieren. Dagegen könnte er dies nicht, wenn eine Einwilligung dem Grunde nach nicht möglich wäre.

Die besseren juristischen Argumente sprechen für die herrschende Literatur, sodass eine Einwilligung in ein niedrigeres Datenschutzniveau nicht möglich ist. Denn neben der bereits genannten Tatsache, dass die DS-GVO keine Ausnahmetatbestände für die Einhaltung der Anforderungen des Art. 32 DS-GVO kodifiziert hat, spricht auch dessen Wortlaut, der dem Verantwortlichen und dem Auftragsverarbeiter keine Wahlmöglichkeit hinsichtlich der grundsätzlichen Gewährleistungspflicht einräumt, gegen eine Abdingbarkeit.[12] Des Weiteren stehen die Möglichkeit der Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO und ihre in Art. 7 DS-GVO normierten Bedingungen systematisch im Zusammenhang mit der Frage der Zulässigkeit der Datenverarbeitung und nicht mit den spezifischen Pflichten bei der Umsetzung.[13] Darüber hinaus setzt sich die Rechtmäßigkeit der Datenverarbeitung aus dessen Zulässigkeit und der Datensicherheit als zwei kumulative Anforderungen zusammen,[14] wobei Art. 6 Abs. 1 lit. a DS-GVO nur die Zulässigkeit und nicht die Datensicherheit betrifft. Im Übrigen steht Art. 32 DS-GVO in dem Abschnitt „Sicherheit personenbezogener Daten", welcher dem Kapitel IV „Verantwortlicher und Auftragsverarbeiter" unterfällt, sodass Art. 32 DS-GVO als objektive Anforderungen des Gesetzgebers an die Datensicherheit des Verantwortlichen oder Auftragsverarbeiters zu verstehen ist, was gegen dessen Disponibilität spricht.[15]

Über diese theoretischen bzw. juristischen Argumente hinaus sprechen auch praktische Gründe gegen eine Disponibilität von Art. 32 DS-GVO. So könnten große Konzerne dessen Anforderungen an die Datensicherheit, insbesondere auch im Bereich von sensiblen Daten i.S.d. Art. 9 DS-GVO, vorsätzlich umgehen, indem Einwilligungserklärungen in ein niedrigeres Schutzniveau von den Betroffenen (ggf. sogar von allen Betroffenen) eingeholt werden. Damit würde der gesetzgeberischen Intention die Datensicherheit für personenbezogene Daten mit dem Erlass der DS-GVO zu erhöhen, ohne entsprechende Sanktionsmöglichkeiten zuwidergehandelt werden können. Auch folgt generell aus einer niedrigeren Datensicherheit ein höheres Risiko für „Hackerangriff" bzw. unberechtigten Zugriff auf personenbezogene Daten. Daher lassen auch praktische Argumente eine Abdingbarkeit des Art. 32 DS-GVO fernliegend erscheinen.

IV. Unwirksamkeit der Einwilligung

Eine Einwilligung (oder Verzichtserklärung) des Betroffenen könnte dementsprechend nach§ 134 BGB i.V.m. Art. 32 DS-GVO unwirksam sein. Dies setzt voraus, dass Art. 32 DS-GVO ein Verbotsgesetz i.S.d. § 134 BGB darstellt. Für das Vorliegen einer Verbotsnorm ist nicht erforderlich, dass das Verbot in der jeweiligen Rechtsnorm ausdrücklich ausgesprochen wird, sondern vielmehr ist der Sinn und Zweck der jeweiligen Rechtsnorm ausschlaggebend.[16] Wie bereits

7 Siehe auch: BeckOK DatenschutzR/Paulus, 35. Ed. 01.11.2019, DS-GVO Art. 32 Rn. 5.

8 Paal/Pauly/Martini, DS-GVO, 3. Aufl. 2021, Art. 32 Rn. 1.

9 Spindler/Schuster/Laue, DS-GVO, 4. Aufl. 2019, Art. 32, Rn. 21; MAH IT-R/Schwartmann/Hermann, Teil 10.5 Datenschutz und Datensicherheit im (I)IoT, Rn. 79; Kühling/Buchner/Jandt, DS-GVO, 3. Aufl. 2020, Art. 32 Rn. 40.

10 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Vermerk: Abdingbarkeit von Art. 32 DS-GVO, https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf, S. 5 (Stand: 14.05.2021); Bayrisches Landesamt für Datenschutzaufsicht mit seinem 7. Tätigkeitsbericht von 2015/2016, https://www.lda.bayern.de/media/baylda_report_07.pdf, S. 99 (Stand: 14.05.2021).

11 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Vermerk: Abdingbarkeit von Art. 32 DS-GVO, https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf, S. 5 (Stand: 14.05.2021).

12 Kühling/Buchner/Jandt, DS-GVO, 3. Aufl. 2020, Art. 32 Rn. 40.

13 Spindler/Schuster/Laue, DS-GVO, 4. Aufl. 2019, Art. 32 Rn. 20; Kühling/Buchner/Jandt, DS-GVO, 3. Aufl. 2020, Art. 32 Rn. 40.

14 Kühling/Buchner/Jandt, DS-GVO, 3. Aufl. 2020, Art. 32 Rn. 40.

15 So wohl auch Kühling/Buchner/Jandt, DS-GVO, 3. Aufl. 2020, Art. 32 Rn. 40; wohl ebenso Spindler/Schuster/Laue, DS-GVO, 4. Aufl. 2019, Art. 32 Rn. 2.

16 BeckOK BGB/Wendtland, BGB, 57. Ed. 01.02.2021, § 134 Rn. 9; MüKoBGB/Armbrüster, BGB, 8. Aufl. 2018, § 134 Rn. 41.

oben dargelegt, liegt der Sinn und Zweck des Art. 32 DS-GVO im Wesentlichen darin, dass ein angemessenes Sicherheitsniveau hinsichtlich der Verarbeitungsprozesse von personenbezogenen Daten vorliegt, um einen möglichst hohen Schutz für diese zu gewährleisten, wobei keine gesetzlichen Ausnahmen vorgesehen sind. Der Sinn und Zweck des Art. 32 DS-GVO verbietet somit Rechtsgeschäfte, die das Datensicherheitsniveau senken. Da die Einwilligung (oder Verzichtserklärung) als einseitiges Rechtsgeschäft dieses Verbot betrifft, wäre das verbotswidrige Geschäft, also in diesem Fall die Einwilligung, nach § 134 BGB nichtig.[17]

Selbst wenn die Möglichkeit einer Abdingbarkeit des Art. 32 DS-GVO angenommen und ein Verbotscharakter verneint werden sollte, dürfte in diesem Kontext dennoch fraglich sein, ob Betroffene nach Art. 7 DS-GVO wirksam darin einwilligen können, dass Verantwortliche oder Auftragsverarbeiter ganz oder teilweise auf Maßnahmen und Verfahren, die Art. 32 DS-GVO vorschreibt, verzichten dürfen. Denn, wenn man die Einwilligungsfähigkeit bejahen sollte, müssten gleichwohl die Voraussetzungen für eine wirksame Einwilligung, insbesondere eine ausreichende Informiertheit vorliegen. Dies umfasst bei Abgabe einer schriftlichen Erklärung insbesondere, dass die betroffene Person weiß, in welchem Umfang sie ihre Einwilligung erteilt.[18] Bei einer Einwilligung in ein niedrigeres Datensicherheitsniveau oder einer Verzichtserklärung bezüglich Selbiges müsste der Verantwortliche insbesondere über dessen mangelnde Haftung nach Art. 82 DS-GVO sowie über die Risiken von „Data breaches" (sog. Datenpannen), die bei einem niedrigeren Datensicherheitsniveau erhöht wären, aufklären. Der Betroffene müsste somit darüber informiert werden, dass er durch mangelnde Datensicherheit Nachteile – z.B. durch das Risiko des unberechtigten Zugriffs von Dritten („Data fishing" oder Identitätsdiebstahl) – erleiden kann.

Es dürfte jedoch zu weitgehend sein, wenn der Betroffene auch dazu verpflichtet werden sollte, dass er dem Betroffenen das verringerte Schutzniveau in technischer Hinsicht vor Abgabe seiner Einwilligung oder seines Verzichts erläutern müsste,[19] da der Betroffene dies im Zweifel mangels technischen Know-Hows – z.B. in Hinblick auf die technische Funktionsweise der Verschlüsselung von personenbezogenen Daten – nicht nachvollziehen dürfte.

Aus den obigen Ausführungen folgt somit, dass, wenn der Verantwortliche oder Auftragsverarbeiter beispielsweise dem Betroffenen Inhalte mit personenbezogenen Daten, die mit einem niedrigeren Schutzniveau hinsichtlich der Verschlüsselung versehen sind, per E-Mail zusendet und somit von den Anforderungen des Art. 32 DS-GVO abweichen möchte, er – sofern eine Abdingbarkeit angenommen werden sollte – den Betroffenen vorher zumindest auf die tatsächlichen Risiken (Identitätsdiebstahl und „Data fishing" bzw. generell einfacherer, unberechtigter Zugriff von Dritten) sowie seine mangelnde Haftung hinweisen müsste, um von einer informierten Einwilligung ausgehen zu können.

IV. Fazit

Anhand des Anforderungskatalogs an die Datensicherheit in Art. 32 DS-GVO, der keine Ausnahmen vorsieht, wird deutlich, dass der europäische Gesetzgeber ein möglichst hohes Schutzniveau für personenbezogene Daten anstrebt. Dementsprechend würde eine Einwilligung in ein niedrigeres Schutzniveau oder sogar ein Verzicht auf Datensicherheit diesem Schutzzweck zuwiderlaufen. Konsequenterweise dürften daher der Regelungsgehalt in Art. 32 DS-GVO nicht durch eine Einwilligung oder andere Individualvereinbarung abdingbar sein. Auch dürfte daher erst Recht nicht eine Umgehung des Art. 32 DS-GVO durch Allgemeine Geschäftsbedingungen möglich sein. Selbst wenn dies entgegen der herrschenden Literatur anders beurteilt werden sollte, bedarf eine informierte Einwilligung, dass der Verantwortliche oder Auftragsverarbeiter den Betroffenen über die rechtlichen und tatsächlichen Risiken aufklärt. Dagegen dürfte es jedoch zu viel verlangt sein, wenn der Verantwortliche oder Auftragsverarbeiter darüber hinaus den Betroffenen noch über den Verzicht in technischer Hinsicht aufklären müsste, da die Betroffenen dies regelmäßig nicht nachvollziehen können.

17 Jauernig/Mansel, BGB, 18. Aufl. 2021, § 134 Rn. 41.

18 Vgl. Erwägungsgrund 42 der DS-GVO.

19 A.A. wohl Bayrisches Landesamt für Datenschutzaufsicht mit seinem 7. Tätigkeitsbericht von 2015/2016, https://www.lda.bayern.de/media/baylda_report_07.pdf, S. 99: „Der Nutzer muss zudem deutlich und verständlich darüber informiert werden, welcher Übertragungsweg dem Stand der Technik entspricht und welcher nicht (...)".

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (54): Aspekte des Beschäftigtendatenschutzes im 30. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

(Berichtszeitraum: 1. Januar 2020 bis 31. Dezember 2020 vom 25. Mai 2021)

Zusammengestellt und erläutert von Prof. Peter Gola*

In seinem jüngst erschienen Tätigkeitsbericht äußert sich der BayLfD u.a. zu datenschutzrechtlichen Fragen bei der Tätigkeit einer Personalvertretung und zu dem schon „klassischen" Thema der Führung von Geburtstagslisten.

I. Personalrat

1. Mitbestimmung bei DSB-Bestellung

Noch nicht durchdringen konnte der LfD mit seinem Anliegen, den Beschäftigtendatenschutz mit einem Mitbestimmungsrecht des Personalrats bei der Benennung des behördlichen Datenschutzbeauftragten weiter zu stärken. Dieser wird in Bayern – im Gegensatz zu einen anderen Bundesländern – bislang allein durch den Verantwortlichen, regelmäßig die Leiterin oder den Leiter der Dienststelle, benannt. Hinzuweisen ist jedoch darauf, dass sich Beteiligungsrechte im Zusammenhang mit der der Bestellung zugrundeliegenden Personalmaßnahme (Einstellung, Versetzung) ergeben (vgl. Gola/Heckmann, BDSG§ 4 Rn. 11): Da der Datenschutzbeauftragte jedoch gerade auch für die Beschäftigten ein unabhängiger Ansprechpartner in datenschutzrechtlichen Fragen sein und vor allem bei datenschutzrechtlichen Konflikten mit dem Dienstherrn vermitteln soll, bietet sich nach Ansicht des BayLfD eine voll mitbestimmte Bestellung an; zumal eine Einbindung des Personalrats in das Verfahren der Benennung des behördlichen Datenschutzbeauftragten dessen Legitimation und das ihm von den betroffenen Beschäftigten entgegengebrachte Vertrauen maßgeblich steigern würde, indem der Eindruck vermindert würde, er stünde einseitig im Lager der Dienststellenleitung.

2. Auskunft an Beschäftigte aus Unterlagen des Personalrats

a) Rechtsgrundlagen

Unter Berufung auf die besondere Schweigepflicht für Mitglieder der Personalvertretung in Art. 10 Abs. 1 S. 1 des Bayerischen Personalvertretungsgesetzes, (BayPVG) soll Beschäftigten bayerischer öffentlicher Stellen zwar grundsätzlich kein Recht auf Einsicht in Personalratsunterlagen zustehen. Sie können allerdings ihr Auskunftsrecht gemäß Art. 15 DS-GVO auch im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten durch den Personalrat geltend machen. Es stellt sich dann die Frage, ob und gegebenenfalls in welchem Umfang die Schweigepflicht des Personalrats das Recht der Beschäftigten auf Auskunft einschränkt.

b) Anspruchsinhalt

Das Auskunftsrecht nach Art. 15 Abs. 1 DS-GVO umfasst zunächst die Bestätigung, ob überhaupt personenbezogene Daten der Auskunft suchenden Beschäftigten verarbeitet werden (Art. 15 Abs. 1 Halbsatz 1 DS-GVO). Ist dies der Fall, haben die Beschäftigten ein Recht auf Auskunft über diese Daten (Art. 15 Abs. 1 Halbsatz 2 Var. 1 DS-GVO) sowie über bestimmte „Metainformationen", etwa zu den Verarbeitungszwecken (Art. 15 Abs. 1 Halbsatz 2 Var. 2 DS-GVO). Beschäftigte können zudem eine Kopie ihrer verarbeiteten Daten verlangen, Art. 15 Abs. 3 DS-GVO.

c) Anspruchsverpflichteter

Die Rechte nach Art. 15 DS-GVO richten sich gegen den Verantwortlichen, auch wenn der Personalrat nach der jeweils geltenden Rechtssituation nicht als eigenständiger Verantwortlicher im Sinn von Art. 4 Nr. 7 DS-GVO, sondern als Teil der jeweiligen bayerischen öffentlichen Stelle, bei welcher er gebildet ist, anzusehen ist. Der besonderen Stellung des Personalrats sei allerdings – insbesondere im Hinblick auf die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG – organisatorisch gleichwohl Rechnung zu tragen. Dies habe unter anderem zur Folge, dass der Personalrat Auskunftsersuchen Beschäftigter bezüglich seiner eigenen Datenverarbeitungen selbstständig zu bearbeiten hat.

d) Die Schweigepflicht des Personalrats als Anspruchshindernis?

Gemäß Art. 10 Abs. 2 Nr. 3 BayDSG unterbleibt die Auskunft unter anderem, soweit „personenbezogene Daten oder die Tatsache ihrer Speicherung [...] wegen der überwiegenden berechtigten Interessen Dritter geheim gehalten werden müssen". Zur Interpretation der Vorschrift führt der LfD wie folgt aus: „Die Vorschrift schränkt die Rechte nach Art. 15 DS-GVO insgesamt ein, sowohl hinsichtlich des „eigentlichen" Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO als auch hinsichtlich des Rechts auf Kopie nach Art. 15 Abs. 3 DS-GVO. Der bayerische Gesetzgeber hat mit dieser Regelung von der Beschränkungsmöglichkeit des Art. 23 DS-GVO Gebrauch gemacht. Bei Auskunftsbegehren im Hinblick auf (mögliche) Datenverarbeitungen des Personalrats findet das in Art. 10 Abs. 2 Nr. 3 BayDSG allgemein umschriebene Ge-

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

heimhaltungsinteresse seine spezialgesetzliche Ausprägung in Art. 10 Abs. 1 Satz 1 BayPVG, der eine besondere Schweigepflicht für Mitglieder der Personalvertretung normiert. (Vgl. ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung, Stand 12/2019, Rn. 90 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Recht auf Auskunft über die eigenen personenbezogenen Daten".) Deutlich zu kurz gegriffen wäre es allerdings, wenn der Personalrat Auskunftsersuchen Beschäftigter pauschal mit einem Verweis auf Art. 10 Abs. 1 Satz 1 BayPVG ablehnen könnte. Vielmehr ist zu differenzieren: Soweit eine Schweigepflicht allein dem Schutz der betroffenen Person dient, kann diese Pflicht dem Recht der betroffenen Person auf Auskunft und auf Erhalt einer Kopie nicht entgegengehalten werden. Denn dann würde sich eine Vorschrift, die der Stärkung der Rechtsposition der betroffenen Person dienen soll, ihren Auswirkungen nach ins Gegenteil verkehren.

Auskunftsbeschränkende Wirkung kann die Schweigepflicht daher nur entfalten, soweit sie (zumindest auch) die Interessen Dritter schützt. Dies ist im Hinblick auf die Zweckrichtung der jeweils einschlägigen Schweigepflicht im Einzelfall zu beurteilen. Die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG dient zum einen zwar dem Vertraulichkeitsinteresse der Beschäftigten, zum anderen aber auch dem Zweck, die Funktionsfähigkeit des Personalrats sowie die vertrauensvolle Zusammenarbeit mit der Dienststellenleitung (vgl. Art. 2 Abs. 1 BayPVG) zu gewährleisten.

Der Anspruch nach Art. 15 Abs. 1 DS-GVO ist somit auch im Beschäftigungsverhältnis kein „Alles-oder-Nichts"-Anspruch: Die Schweigepflicht steht ihm nur so weit entgegen, wie sie im konkreten Fall reicht. Es kommt auch eine Teilerfüllung dergestalt in Betracht, dass der Personalrat diejenigen Informationen bereitstellt, die nicht von dem Anspruchshindernis erfasst sind. Eine solche Teilerfüllung ist sowohl hinsichtlich der vom Personalrat verarbeiteten Daten der betroffenen Person als auch bezüglich der zu erteilenden Metainformationen nach Art. 15 Abs. 1 Halbsatz 2 Var. 2 DS-GVO denkbar. Bei der Prüfung, ob und gegebenenfalls in welchem Umfang die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG das Auskunftsrecht nach Art. 15 Abs. 1 DS-GVO beschränkt, sollte der Personalrat insbesondere Folgendes beachten: Im Hinblick auf die eigenen personenbezogenen Daten der betroffenen Person wird die Schweigepflicht des Personalrats den Anspruch nach Art. 15 Abs. 1 DS-GVO nur in Fällen einschränken können, in denen diese Pflicht zugunsten des Personalrats selbst oder zugunsten Dritter, insbesondere der Dienststellenleitung, besteht. In Betracht hierfür kommen etwa Konstellationen, in denen die Dienststellenleitung dem Personalrat bestimmte personenbezogene Daten einer beschäftigten Person im Rahmen einer beabsichtigten Personalmaßnahme (etwa einer vorgesehenen Versetzung) „vorab" zur Verfügung stellt, die beschäftigte Person von der geplanten Maßnahme jedoch noch keine Kenntnis hat. Hier soll die Schweigepflicht nicht allein das Vertraulichkeitsinteresse der betroffenen Person schützen, sondern auch die vertrauensvolle Zusammenarbeit mit der Dienststelle gewährleisten. Die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG bezieht sich insbesondere auch auf die Meinungsäußerungen und das Abstimmungsverhalten der Personalratsmitglieder in den Sitzungen. Diese werden in aller Regel keine personenbezogenen Daten der betroffenen Person, deren Angelegenheit Gegenstand der Beratung ist, darstellen und sind insoweit von Rechten nach Art. 15 DS-GVO (einschließlich des Rechts auf Kopie) ohnehin nicht erfasst. Sofern der betroffenen Person bezüglich ihrer personenbezogenen Daten Auskunft in Form von (Teil-)Ablichtungen von Personalratsdokumenten erteilt werden kann, ist dementsprechend in besonderem Maße darauf zu achten, dass Dokumententeile, die Rückschlüsse auf Meinungsäußerungen und das Abstimmungsverhalten einzelner Personalratsmitglieder enthalten, zuvor – etwa durch Schwärzung – unkenntlich gemacht werden.

Auch hinsichtlich der in Art. 15 Abs. 1 Halbsatz 2 Var. 2 DS-GVO aufgelisteten Metainformationen ist jeweils gesondert zu prüfen, ob die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG ein Anspruchshindernis darstellt. In Betracht kommt dies insbesondere hinsichtlich der Informationen über die Herkunft der Daten nach Art. 15 Abs. 1 Buchst. g DS-GVO, so in dem Fall, dass der Personalrat personenbezogene Daten anlässlich einer Beschwerde eines anderen Beschäftigten verarbeitet.

e) Ergänzende Hinweise auf Anspruchseinschränkungen

Neben der Schweigepflicht des Personalrats können im Einzelfall auch andere Anspruchshindernisse – insbesondere nach Art. 10 Abs. 2 Nr. 1 und 2 sowie Nr. 3 Var. 1 BayDSG – in Betracht kommen. Bezüglich des Rechts auf Kopie nach Art. 15 Abs. 3 DS-GVO sieht Art. 15 Abs. 4 DS-GVO ferner ein spezifisches Anspruchshindernis vor. Diesem dürfte angesichts der Schweigepflicht der Personalratsmitglieder allerdings keine weitergehende Bedeutung zukommen: Denn soweit das Recht auf Kopie der eigenen personenbezogenen Daten ausnahmsweise die Rechte und Freiheiten anderer Personen beeinträchtigen würde (vgl. Art. 15 Abs. 4 DS-GVO), wird bereits die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG dem Auskunftsanspruch entgegenstehen. Sowohl Dienststelle als auch Personalrat haben durch organisatorische Vorkehrungen sicherzustellen, dass Auskunftsersuchen, welche (auch) die Verarbeitung personenbezogener Daten durch den Personalrat betreffen, ordnungsgemäß und insbesondere innerhalb der Frist(en) des Art. 12 Abs. 3 DS-GVO bearbeitet werden. Dabei kann auch der Personalrat den behördlichen Datenschutzbeauftragten – möglichst ohne die Nutzung personenbezogener Beschäftigtendaten – zu Rate ziehen (vgl. Art. 39 Abs. 1 Buchst. a DS-GVO (vgl. dazu im Internet: https://www.datenschutzbayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Recht auf Auskunft über die eigenen personenbezogenen Daten", S. 132).

f) Fazit

Zwar ist der Personalrat nicht selbst Verantwortlicher im datenschutzrechtlichen Sinn. Aufgrund seiner besonderen Stellung hat er allerdings Ersuchen nach Art. 15 DS-GVO –

soweit diese Datenverarbeitungen des Personalrats betreffen – eigenständig zu bearbeiten. Dabei kann er ein solches Ersuchen nicht pauschal mit einem Hinweis auf eine bestehende Schweigepflicht zurückweisen. Vielmehr hat er im Hinblick auf das jeweilige, konkrete Ersuchen – gegebenenfalls mit Unterstützung durch den behördlichen Datenschutzbeauftragten – sorgfältig zu prüfen, ob und gegebenenfalls in welchem Umfang die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG Rechte der betroffenen Person nach Art. 15 DS-GVO einschränkt."

3. Beschäftigten-Geburtstagslisten bei bayerischen öffentlichen Stellen

a) Allgemeines

Der BayLfD greift wohl aus gegebenem Anlass das schon „historische" Thema innerbetrieblicher/-behördlicher Geburtstagslisten erneut auf (vgl. hierzu Gola, Handbuch Beschäftigtndatenschutz, Rn. XX): Hierzu führt er aus: „Geburtstage von Beschäftigten geben in vielen bayerischen öffentlichen Stellen immer wieder Anlass zu einer Gratulation, zum Mitbringen eines Geburtstagskuchens oder zur Entgegennahme eines angemessen großen Stücks davon. Geburtstage werden wahrgenommen – von Kolleginnen und Kollegen, Vorgesetzten, Mitarbeiterinnen und Mitarbeitern. Sie sind Gegenstand sozialer Erwartungen. Oftmals entstehen in den Dienststellen Geburtstagslisten, die von allen Beschäftigten in einer Organisationseinheit eingesehen werden können und so für das als notwendig empfundene Maß an Transparenz sorgen. Solche Geburtstaglisten enthalten für jede eingetragene Person außer dem Namen zumindest das Datum, häufig auch das Jahr des Geburtstags. Aus datenschutzrechtlicher Sicht ist insofern zu bemerken:

b) Verantwortlichkeit

Verantwortlicher ist nach Art. 4 Nr. 7 Halbsatz 1 DS-GVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eine Beschäftigten-Geburtstagsliste wird entweder auf dienstliche Veranlassung oder in „Eigenregie" durch die Mitarbeiterinnen und Mitarbeiter geführt. Die Verantwortlichkeit einer bayerischen öffentlichen Stelle für eine dort vorgehaltene Beschäftigten-Geburtstagsliste ist jedenfalls begründet, wenn

- Vorgesetzte die Liste führen oder dies veranlassen,
- Vorgesetzte auf eine Eintragung in der Liste hinwirken oder sonst Eintragungsanreize schaffenoder
- die Liste von der Personalstelle mit den nötigen Daten beschickt wird.

Die nachfolgenden Hinweise betreffen Beschäftigten-Geburtstagslisten, die von einer bayerischen öffentlichen Stelle als Verantwortlichem geführt werden.

c) Beschäftigten-Geburtstagsliste und Personaldatenschutz

Die Führung einer Beschäftigten-Geburtstagsliste, die Beschäftigten außerhalb der personalverwaltenden Stelle zugänglich ist, findet keine Rechtfertigung in Art. 103 Satz 1 Nr. 1 Bayerisches Beamtengesetz (BayBG). Diese Vorschrift fungiert als grundlegende Verarbeitungsbefugnis für den Bereich der Personalstellen; sie ist Rechtsgrundlage im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DS-GVO und gilt nicht nur für die Beamtinnen und Beamten, sondern gemäß Art. 145 Abs. 2 BayBG grundsätzlich auch entsprechend für Tarifbeschäftigte bei bayerischen staatlichen Behörden und staatsmittelbaren Rechtsträgern. Nach Art. 103 Satz 1 Nr. 1 BayBG darf der Dienstherr Personaldaten verarbeiten, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Die Führung von Beschäftigten-Geburtstagslisten, die innerhalb einer „behördeninternen Öffentlichkeit" eingesehen werden können, ermöglicht die Gratulation in der jeweiligen Organisationseinheit und gegebenenfalls ein anlassbezogenes Gemeinschaftserlebnis. Bei alldem handelt es sich um Akte der kollegialen Beziehungspflege, nicht aber um vom Dienstherrn zu veranlassende organisatorische, personelle oder soziale Maßnahmen.

d) Einwilligung als Rechtsgrundlage

Vor diesem Hintergrund kommt als Rechtsgrundlage für Verarbeitungen im Zusammenhang mit Beschäftigten-Geburtstagslisten nur die Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO) in Betracht. Unter dem Aspekt der Datenminimierung (Art. 5 Abs. 1 Buchst. c DS-GVO) sollte die „Neuaufnahme" in eine Liste grundsätzlich auf Tag und Monat beschränkt, auf die – von nicht wenigen Menschen als sensibler empfundene – Angabe des Geburtsjahres hingegen verzichtet werden. Die Einwilligung ist wirksam, wenn sie die Anforderungen erfüllt, welche Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 Abs. 2 und 3 DS-GVO vorsehen. Eine Einwilligung muss danach insbesondere freiwillig (Art. 4 Nr. 11 DS-GVO), informiert (Art. 4 Nr. 11 DS-GVO), auf einen bestimmten Zweck (Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO) und auf eine bestimmte Verarbeitung bezogen (Art. 4 Nr. 11 DS-GVO) sowie unmissverständlich (Art. 4 Nr. 11 DS-GVO) sein. Sie wirkt grundsätzlich bis zu ihrem Widerruf (Art. 7 Abs. 3 Satz 1, 2 DS-GVO). Die öffentliche Stelle muss die Einwilligung im Rahmen ihrer Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) nachweisen können (Art. 7 Abs. 1 DS-GVO).

e) Verzeichnis der Verarbeitungstätigkeiten

Eine Verarbeitungstätigkeit mit dem Zweck „Führen von Beschäftigten-Geburtstagslisten" gehört auch in das Verzeichnis der Verarbeitungstätigkeiten. Rechtsgrundlage für diese Verarbeitungstätigkeit ist Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO. Betroffene Personen sind die Beschäftigten, die ihre Geburtsdaten in die Liste einpflegen oder einpflegen lassen. Zu den Kategorien personenbezogener Daten zählen regelmäßig der Name und der Vorname sowie das Geburtsdatum. Kategorien (dritter) Empfänger können bei einer internen Liste außer Betracht bleiben. Die Löschfrist ist an die Zugehörigkeit der betroffenen Person zu der Orga-

nisationseinheit gekoppelt, für welche die Beschäftigten-Geburtstagsliste geführt wird. Ein Eintrag ist zu löschen, wenn die betroffene Person diese Funktionseinheit – auch durch Umsetzung innerhalb einer Behörde – verlässt oder die Einwilligung widerruft. Der Verzeichniseintrag sollte so gefasst werden, dass er alle bei der öffentlichen Stelle geführten Beschäftigten-Geburtstagslisten abdeckt.

f) Informationspflichten

Die in einer Beschäftigten-Geburtstagsliste typischerweise enthaltenen Daten befinden sich regelmäßig bereits in der Sphäre des Verantwortlichen, weil sie zum Grundbestand an Beschäftigtendaten gehören. Die Nutzung von Name und Geburtsdatum im Rahmen einer Beschäftigten-Geburtstagsliste lässt sich als eine Weiterverwendung deuten, welche die Informationspflicht nach Art. 13 Abs. 3 DS-GVO auslöst. Im Regelfall werden die erforderlichen Informationen bereits durch die zu Beginn eines Beschäftigungsverhältnisses angezeigten Datenschutzhinweise erteilt sein, die eingeführte Beschäftigten-Geburtstagslisten möglichst berücksichtigen sollten. Vor der Einwilligung sollte der betroffenen Person der zusätzliche Verarbeitungszweck deutlich gemacht werden; unmissverständlich ist auf das Widerrufsrecht hinzuweisen (Art. 13 Abs. 2 Buchst. c, Art. 7 Abs. 3 Satz 3 DS-GVO). Ist dies gewährleistet, kann meist ein Kenntnisstand angenommen werden, der eine gesonderte Information entbehrlich macht (vgl. Art. 13 Abs. 4 DS-GVO).

g) Fazit

Die Führung von Beschäftigten-Geburtstagslisten durch bayerische öffentliche Stellen ist auch in der Welt der Datenschutz-Grundverordnung kein unlösbares Problem. Stets sollte aber insbesondere darauf geachtet werden, dass

- eine Verantwortlichkeit der öffentlichen Stelle organisatorisch klar geregelt ist,
- der Verarbeitung wirksame Einwilligungen zugrunde liegen,
- das Verzeichnis der Verarbeitungstätigkeiten eine entsprechende Position enthält sowie
- am Beginn eines Dienst- oder Arbeitsverhältnisses gegebene Datenschutzhinweise auch Informationspflichten hinsichtlich Beschäftigten-Geburtstagslisten mit abdecken.

Praxisfälle zum Datenschutzrecht XI: Die Kundenbefragung

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

I. Sachverhalt

Das Busreiseunternehmen B beabsichtigt, eine telefonische Erhebung bzgl. der Zufriedenheit seiner Kunden durchzuführen. Befragt werden sollen Teilnehmer an früheren Reisen. Beauftragt werden soll das Marktforschungsinstitut M. Dieses soll bzgl. der Erstellung des Fragenkatalogs beraten und bei der späteren Durchführung der Befragung unterstützen. Das Unternehmen B möchte aber die „Hoheit" über den Ablauf der Befragung behalten. Die Auswahl der zu kontaktierenden Personen erfolgt durch das Unternehmen B selbst, das die Kontaktinformationen zweckgebunden zur telefonischen Abarbeitung des Fragebogens an M weitergibt. Nach der Befragung soll M Durchschnittswerte aus den von den Befragten gegebenen „Schulnoten" bilden. Die Verwendung von Kundendaten zu Zwecken der Kundenbefragung war von B bei der Erhebung der Kundendaten noch nicht geplant. Geplant war zu diesem Zeitpunkt nur eine Verarbeitung zu Zwecken der Vertragsabwicklung. Nur über diese wurde auch informiert. Einwilligungen wurden nicht eingeholt.

Der Datenschutzbeauftragte (DSB) wird um Stellungnahme zu dem geplanten Vorhaben gebeten.

II. Musterfalllösung

1. Datenschutzrechtliche Verantwortlichkeit

Für die Beurteilung der datenschutzrechtlichen Situation ist zunächst relevant, wer für die mit der Kundenbefragung zusammenhängenden Datenverarbeitungen verantwortlich ist.

Sofern es sich bei M um einen Auftragsverarbeiter i.S.v. Art. 28 DS-GVO handelt, setzt nach hier vertretener Auffassung der Datentransfer zwischen B und M keinen gesonderten Erlaubnistatbestand voraus. Der Vorgang der Auftragsverarbeitung ist vielmehr regelmäßig als einheitlicher Verarbeitungsvorgang des Verantwortlichen anzusehen.[1] Mit anderen Worten: Datenschutzrechtlich legitimationsbedürftig ist lediglich die Datenverarbeitung als solche (hier: die Befragung unter Rückgriff auf die Kundendaten), nicht damit einhergehende Datenflüsse zwischen Auftraggeber und -nehmer. Die Rechtmäßigkeit der Verarbeitung durch den Auftragsverarbeiter bestimmt sich durch den von dem für die Verarbeitung personenbezogener Daten Verantwortlichen erteilten Auftrag.[2] Sofern B und M hingegen jeweils eigenverantwortlich sind für die von ihnen getätigten Datenverarbeitungen oder auch gemeinsam Verantwortliche (Art. 26 DS-GVO), bedürfte es hingegen eines Erlaubnistatbestandes für die Datenflüsse zwischen den Parteien.

Die Auftragsverarbeitung ist durch die Beschränkung auf eine weisungsgebundene Tätigkeit gekennzeichnet, es werden durch den Beauftragten keine eigenen Interessen im

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

1 So auch Simitis/Hornung/Spiecker/Petri, Datenschutzrecht, DS-GVO Art. 28 Rn. 33, vgl. dort auch zum Streitstand.

2 Vgl. Ehmann/Selmayr/Bertermann, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 28 Rn. 8.

Hinblick auf die verarbeiteten personenbezogenen Daten verfolgt. Führt ein Markt- oder Meinungsforschungsinstitut für Unternehmen Kunden- oder Haushaltsbefragungen durch, so handelt es sich um Auftragsverarbeitung, falls die Durchführung der Befragung sowie die Auswertung der Ergebnisse durch den Auftraggeber genau festgelegt sind.[4] Keine Auftragsverarbeitung liegt vor, sofern das Institut nur einen allgemein gehaltenen Auftrag bzgl. der zu untersuchenden Fragestellung erhält, die Details zu Fragebogeninhalt, Untersuchungsablauf und Auswertung jedoch diesem überlassen bleiben.

Hier soll M zwar bei der Fragebogenerstellung maßgeblich unterstützen, die Entwicklung des Fragebogens begründet jedoch noch keine personenbezogene Datenverarbeitung. Bzgl. der personenbezogenen Datenverarbeitung bestimmt B jedoch Zwecke wie auch Mittel: Der Zweck der Datenverarbeitung, die Zufriedenheit der Kunden zu ermitteln, wird ausschließlich durch B gesetzt. B entscheidet über den finalen Fragenbogen, den Kommunikationskanal, die anzurufenden Personen und gibt M auch die Auswertung der Ergebnisse genau vor. M demgegenüber telefoniert nur vorgegebene Telefonnummern ab und stellt auch nur von B freigegebene Fragen, handelt insofern also weisungsgebunden. Auch die Auswertung der Ergebnisse erfolgt nach Vorgaben von B, und M hat kein eigenes Interesse an den Befragungsergebnissen. M ist damit als Auftragsverarbeiter i.S.v. Art. 28 DS-GVO anzusehen, während B Verantwortlicher i.S.v Art. 4 Nr. 7 DS-GVO bleibt. Der Datentransfer zwischen B und M setzt damit nach hier vertretener Auffassung keinen gesonderten Erlaubnistatbestand voraus.

Allerdings muss der Dienstleister vor seiner Einschaltung auf seine Geeignetheit geprüft werden. Der Verantwortliche darf sich nur solcher Auftragsverarbeiter bedienen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz anwenden, so dass die Verarbeitung im Einklang mit der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet (Art. 28 Abs. 1 DS-GVO). Auch muss der Verantwortliche mit dem Auftragsverarbeiter einen Vertrag über die weisungsgebundene Tätigkeit mit in der DS-GVO festgelegten Mindestinhalten schließen (Art. 28 Abs. 3 DS-GVO).

2. Rechtmäßigkeit der Datenverarbeitung zur Kundenbefragung

a) Allgemeines

Die von M durchgeführte Befragung ist datenschutzrechtlich dem verantwortlichen Unternehmen B zuzuordnen, da M lediglich Auftragsverarbeiter ist.[5] Fraglich ist, ob B sich auf eine Rechtsgrundlage für die mit der Befragung einhergehende Datenverarbeitung berufen kann.

b) Privilegierung wissenschaftlicher Befragungen

Markt- und Meinungsforschung stellt für öffentliche und private Auftraggeber mittels wissenschaftlicher Methoden und Techniken notwendige Informationen als empirische Grundlage und zur Unterstützung wirtschaftlicher, gesellschaftlicher und politischer Entscheidungen bereit.[6] Wissenschaftliche Forschung wird von der DS-GVO aufgrund ihrer Bedeutung für die Allgemeinheit privilegiert behandelt (vgl. Art. 89 DS-GVO), ein Umstand, der sich auch auf die Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO auswirkt.[7] Mit anderen Worten: Eine Interessenabwägung wird eher zugunsten des Verantwortlichen ausfallen, wenn wissenschaftliche Forschungszwecke verfolgt werden, als wenn andere, nicht privilegierte Zwecke verfolgt werden.

Werden, wie vorliegend, Daten, die zunächst zu einem anderen Zweck erhoben wurden, für Zwecke der Markt- und Meinungsforschung zweckändernd weiterverarbeitet (sog. „Sekundärnutzung")[8], findet Art. 6 Abs. 4 DS-GVO Anwendung.[9] Auch im Rahmen der Kompatibilitätsprüfung ist dabei die Privilegierung wissenschaftlicher Forschung entsprechend zu berücksichtigen, sofern es sich um solche handelt.

Fraglich ist allerdings, ob es sich vorliegend um wissenschaftliche Forschung handelt.

Trotz der Privilegierung ist der Begriff der wissenschaftlichen Forschung weder in der DS-GVO noch im BDSG explizit definiert. Wie sich jedoch aus Erwägungsgrund 159 DS-GVO ergibt, übernimmt die DS-GVO den in Art. 179 Abs. 1 AEUV und Art. 13 S. 1 GRCh angelegten weiten Forschungsbegriff.[10] Forschung ist demnach jede „Tätigkeit mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen."[11] Auch Vorhaben der Markt- und Meinungsforschung als angewandte Forschung unterfallen prinzipiell diesem Begriff, wenn sie nach den anerkannten wissenschaftlichen Methoden der empirischen Sozialforschung durchgeführt werden.[12]

Entscheidend ist insofern insbesondere, dass die Markt- und Meinungsforschung betreibende Stelle unabhängig ist.[13] Sofern ein Auftraggeber Einfluss auf den Untersuchungsverlauf oder den Umgang mit Ergebnissen nimmt, kann man regelmäßig schon nicht mehr von einem methodischen, systematischen und nachprüfbaren Vorgehen sprechen.[14] Vorliegend kann von einer Unabhängigkeit von M im Verhältnis zu B keinerlei Rede sein. Mit Ausnahme der Beratung im Hinblick auf den Fragebogen hat M keine Möglichkeiten der Einflussnahme, und auch diesbezüglich bleibt die Letztentscheidung bei B.

Eine Privilegierung der Datenverarbeitung scheitert im Übrigen vorliegend auch an der Art der geplanten Befragung, denn Zufriedenheitsumfragen sind nach herrschender

3 Taeger/Gabel/Gabel/Lutz, DS-GVO BDSG, 3. Aufl. 2019, DS-GVO Art. 28 Rn. 17.

4 Vgl. hierzu vorstehend unter 1.

5 BT-Drs. 16/13657, 33.

6 Vgl. Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 93.

7 Vgl. Hornung/Hofmann, ZD-Beil. 2017, 1 (2).

8 Vgl. Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 94.

9 Vgl. Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 93.

10 Hornung/Hofmann, ZD-Beil. 2017, 1 (4).

11 Hornung/Hofmann, ZD-Beil. 2017, 1 (4).

12 Vgl. Gola/Heckmann/Krohm, BDSG, 13. Aufl. 2019, § 27 Rn. 17.

13 Zum Ganzen Hornung/Hofmann, ZD-Beil. 2017, 1 (4 f.).

14 BGH, Urteil v. 10.07.2018 – VI ZR 225/17.

Auffassung von der Markt- und Meinungsforschung abzugrenzen und als Werbemaßnahme einzuordnen.[15]

Die personenbezogene Datenverarbeitung im Zusammenhang mit der geplanten Kundenbefragung ist nach alledem nicht privilegiert.

c) Berechtigte Interessen

Fraglich ist, ob die Verarbeitungen im Zusammenhang mit der Befragung über eine „normale" Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f DS-GVO) gerechtfertigt sein können, also eine solche ohne Berücksichtigung privilegierter Interessen auf Seiten von B. Als Maßstab für die Datenverarbeitung zu den Zwecken der Kundenzufriedenheitsbefragung kommt Art. 6 Abs. 1 S. 1 lit. f DS-GVO vorliegend aber im Ergebnis nicht in Betracht, da die relevanten Daten zunächst für einen anderen Zweck als diesen erhoben worden sind, nämlich die Vertragsabwicklung, und nun zweckändernd weiterverarbeitet werden sollen.

Nach der DS-GVO gilt der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO). Zweckändernde Weiterverarbeitungen sind nur nach Maßgabe von Art. 6 Abs. 4 DS-GVO möglich, der eine sog. Kompatibilitätsprüfung verlangt. Ist der neue Verarbeitungszweck mit dem ursprünglichen Verarbeitungszweck kompatibel, ist die zweckändernde Weiterverarbeitung zulässig und über den ursprünglichen Erlaubnistatbestand mitabgedeckt. Weiterverarbeitungen zu einem nicht kompatiblen Zweck kommen nur auf Basis einer Einwilligung der betroffenen Person oder bei Bestehen einer entsprechenden Rechtsvorschrift in Betracht.

c) Zweckändernde Weiterverarbeitung

Maßstab für die Zulässigkeit ist nach Vorgesagtem hier also an sich Art. 6 Abs. 4 DS-GVO. Allerdings kann die Frage der Zulässigkeit einer Zweckänderung dahinstehen, sofern eine Datenverarbeitung bereits ohne Zweckänderung unzulässig ist. Mit anderen Worten: Ist eine Datenverarbeitung zu einem bestimmten Zweck unzulässig, muss sie es auch dann bleiben, wenn dieser Zweck neu hinzutritt.

Wie bereits ausgeführt, werden Kundenzufriedenheitsbefragungen von der herrschenden Meinung als Werbung eingestuft. Diese unterliegen damit den spezifischen datenschutz- und wettbewerbsrechtlichen Zulässigkeitsvoraussetzungen.

Im Hinblick auf die datenschutzrechtliche Bewertung ist zunächst zu berücksichtigen, dass nach Erwägungsgrund 47 S. 7 DS-GVO Direktwerbung zwar grundsätzlich als berechtigtes Interesse zu betrachten ist. Als Direktwerbung bezeichnet man die unmittelbare Ansprache der betroffenen Person mittels Zusendung von Briefen oder Prospekten, durch Telefonanrufe, E-Mails oder Übermittlung von SMS.[16]

Zu beachten ist allerdings auch, dass die Werbung per Telefon gegenüber Verbrauchern durch das Gesetz gegen den unlauteren Wettbewerb (UWG) in dem Sinne reglementiert wird, dass diese nur mit vorheriger ausdrücklicher Einwilligung möglich ist (§ 7 Abs. 2 Nr. 2 UWG). Nach Auffassung der Datenschutzaufsichtsbehörden schlägt diese wettbewerbsrechtliche Wertung auch auf das Datenschutzrecht durch.[17] Konkret bedeutet dies, dass wegen der wettbewerbsrechtlichen Wertung auch die datenschutzrechtliche Interessenabwägung nicht zugunsten der werbenden Stelle ausfallen kann.

Einwilligungserfordernisse des § 7 Abs. 2 UWG können auch nicht dadurch umgangen werden, dass bei einer Kundenzufriedenheitsumfrage die Kundenbefragung zuvor unter Hinweis auf eine Widerspruchsmöglichkeit schriftlich angekündigt wird.[18]

Der Datenschutzbeauftragte hat folglich darauf hinzuweisen, dass die geplante Befragung sowohl gegen Datenschutz- als auch gegen das Wettbewerbsrecht verstößt.

III. Praxishinweis

Anders als Telefonwerbung gegenüber Verbrauchern, die wettbewerbsrechtlich stets an die Einwilligung der Beworbenen gebunden ist, kann E-Mail-Werbung gegenüber Bestandskunden nach § 7 Abs. 3 UWG ausnahmsweise auch ohne Einwilligung zulässig sein, wenn alle dort genannten Voraussetzungen eingehalten werden. Nach dem KG Berlin[19] können über § 7 Abs. 3 UWG auch Kundenzufriedenheitsbefragungen per Mail legitimiert sein, sofern die in der Norm genannten notwendigen Informationspflichten eingehalten werden. Nach § 7 Abs. 3 Nr. 3 und 4 UWG darf der Kunde der werblichen Verwendung der E-Mail-Adresse nicht widersprochen haben, und der Kunde muss bereits bei Erhebung der Adresse und sodann bei jeder Verwendung klar und deutlich darauf hingewiesen werden, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

15 Vgl. Kühling/Buchner/Herbst, DS-GVO BDSG, 3. Aufl. 2020, Art. 21 DS-GVO Rn. 26.

16 DSK, Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO), Stand: Nov. 2018, Abschnitt 1.4; ebenso OVG Saarland, Beschluss v. 16.02.2021 (2 A 355/19): Bei Telefonwerbung schlägt die UWG-Wertung zur Unzumutbarkeit auch auf die datenschutzrechtliche Interessenabwägung durch; ähnlich auch der BGH zur Abwägung im Zusammenhang mit dem allgemeinen Persönlichkeitsrecht: BGH, Urteil v. 10.07.2018 – VI ZR 225/17.

17 So OLG Köln, Urteil v. 12.12.2008 – 6 U 41/08.

18 Beschluss v. 07.02.2017 – 5 W 15/17.

Rechtsgrundlagen zur Verarbeitung von Kopf- und Körpermaßen

Dr. Niels Lepperhoff*

I. Einleitung

Was haben Kostüme und Masken im Theater mit Datenschutz zu tun? Auf den ersten Blick wenig, scheint es. Bei näherer Betrachtung zeigt sich, dass die starke Zusammenarbeit zwischen Theatern sowie eine hohe Mobilität von Künstlern zu einem häufigen Austausch personenbezogener Daten führt. Die Datenverarbeitung findet zudem im Schnittpunkt des Persönlichkeitsrechts, der unternehmerischen Freiheit und der künstlerischen Freiheit statt. In der Praxis sind vielfältige Unsicherheiten hinsichtlich der anwendbaren Rechtsgrundlagen zu erkennen, und dies führt zur spürbaren Beeinträchtigung des Theaterbetriebs. Am Beispiel der Verarbeitung personenbezogener Daten zur Herstellung und Verwendung von Kostümen und Masken beleuchtet dieser Beitrag wesentliche Fragen der Zulässigkeit und zeigt erste Lösungswege auf.

Kostüme und Masken sind ein künstlerisches Element von Theaterproduktionen. Sie unterstützen die Immersion für das Publikum und transportieren künstlerische Aussagen. Es handelt sich regelmäßig um Maßanfertigungen, die an die individuellen Kopf- und Körpermaße der jeweiligen Träger angepasst werden.

Schauspieler, Tänzer, Sänger, Chormitglieder, Musiker und Statisten (im folgenden "Akteur" genannt) tragen regelmäßig Kostüme und Masken. Grundsätzlich sind Akteure bei dem aufführenden Theater angestellt ("Ensemble", "Kompagnie" usw.) oder für eine oder mehrere Produktionen beauftragt (typischerweise als "Gast" bezeichnet). Unter dem Begriff Theater werden im Folgenden alle Formen des Theaters wie z.B. Sprechtheater, Oper und Ballett verstanden. Für die Zwecke dieses Beitrags zählen Chor und Orchester dazu. Die in diesem Beitrag dargestellten Abläufe sind auf wesentliche datenschutzrechtlich relevante Schritte reduziert und stellen eher einen Idealtypus dar. Die konkrete Ausgestaltung kann abweichen.

Grob vereinfacht dargestellt, gliedert sich der Herstellungsprozess wie folgt:

- Künstlerischer Entwurf von Masken- und Kostümbildern entlang der Vorstellung des Regisseurs bzw. Maskenbildners oder Kostümbildners,
- Erhebung von Kopf- und Körpermaßen der späteren Träger
- Speicherung der Kopf- und Körpermaße unter dem Namen des Akteurs
- ggf. Anfertigung eines Gipskopfes
- Anfertigung von Kostümen sowie von Prosthetics und Perücken für die Maske
- Anprobe und Nacharbeiten
- Erstellung der Produktionsmappe
- Anlegen der Maske und Ankleiden des Kostüms für Proben und Aufführung

Die Produktionsmappe dient u.a. als "Anleitung" für die Garderobiere zum Ankleiden des Kostüms und den Maskenbildnern zum Anlegen der Maske. In der Produktionsmappe sind für jede Rolle u.a. der Name des Akteurs sowie seine Kopf- und Körpermaße enthalten. Weiterhin können Hinweise zum Ankleiden bzw. Anlegen aufgeführt sein. Kostüme tragen eingenäht den Titel der Produktion, die Rolle und den Namen aller Träger, die das Kostüm jemals getragen haben.

Die Angaben "Name der Produktion", "Rolle" und "Name des Akteurs" stellen zusammen das zentrale Ordnungskriterium dar, um alle Teile eines Kostüms zu finden, die zugehörige Maske zu identifizieren, sowie die zugehörigen Angaben in der Produktionsmappe zu finden. Es werden folglich personenbezogene Daten verarbeitet, sodass sich die Frage nach einer tragenden Rechtsgrundlage stellt.

II. Anwendbarkeit der DS-GVO

Auch wenn einzelne Verarbeitungsschritte ohne Dateisystem und nicht elektronisch stattfinden, so ist doch in Summe der Anwendungsbereich der DS-GVO und des BDSG, sofern es sich bei den Akteuren um Beschäftigte i.S.d. § 26 Abs. 8 BDSG handelt, eröffnet. Anstelle des BDSG können einzelne Theater auch unter das entsprechende Landesdatenschutzgesetz fallen. Die weitere Darstellung konzentriert sich auf die DS-GVO und das BDSG.

Die Erstellung der Produktionsmappen erfolgt regelmäßig im Zuge einer automatisierten Datenverarbeitung, d.h. mittels Computerprogramm. Eine Speicherung auf Karteikarten, die bspw. alphabetisch sortiert sind, wird als Speicherung in einem Dateisystem i.S.d. Art. 4 Nr. 6 DS-GVO zu betrachten sein. Insofern ist der Anwendungsbereich des Art. 2 Abs. 1 DS-GVO eröffnet.

Eingenähte Namen in einem Kostüm stellen, da das Nähen von Hand erfolgt, weder eine automatisierte Datenverarbeitung, noch eine Speicherung in einem Dateisystem dar. Weil ein Teil der Akteure Beschäftigte sind, eröffnet § 26 Abs. 7 BDSG den Anwendungsbereich von § 26 BDSG. Zu einem Kostüm gehört eine mittels elektronischer Verarbeitung erstellte Produktionsmappe, die ebenfalls Titel der Produktion, Rolle und Namen aller Akteure, die das Kostüm jemals getragen haben, enthält. Im Ergebnis findet die DS-GVO auch für eingenähte Namen (mittelbar) Anwendung, selbst wenn diese nicht von Beschäftigten stammen.

Die im Folgenden diskutierten Rechtsgrundlagen setzen voraus, dass die erwähnten Zwecke mit der Erhebung der personenbezogenen Daten verfolgt wurden. Sofern dieses nicht der Fall ist, wäre im Einzelfall zu prüfen, ob eine Zweckänderung gemäß Art. 6 Abs. 4 DS-GVO möglich ist.

* Der Autor ist Geschäftsführer und Gründer der Xamit Bewertungsgesellschaft mbH in Düsseldorf. Er berät Unternehmen als externer Datenschutzbeauftragter seit mehr als 10 Jahren und ist Autor zahlreicher Fachbeiträge.

III. Speicherung von Kopf- und Körpermaßen zur Herstellung

Kostüme und Masken sind einerseits ein Teil der künstlerischen Inszenierung, die sich insbesondere aus Bühnenbild, Masken, Kostümen, Performance der Akteure, Ton und Beleuchtung ergibt. Auf der anderen Seite können Kostüme und Masken eigenständige künstlerische Werke darstellen. Damit ein Kostüm die optische Wirkung erzielt, die sich der Kostümbildner erhoffte, sowie den Träger durch das Kostümdesign nicht mehr als nötig in seiner Bewegungsmöglichkeit einschränkt, ist eine Maßanfertigung erforderlich. Für eine Maske liegt die Erforderlichkeit der Maßanfertigung auf der Hand.

Eine Maßanfertigung bedeutet, dass die Kopf- und Körpermaße des Trägers für den Herstellungsprozess verarbeitet werden müssen. Zur Maßanfertigung zählen die Herstellung von Grund auf sowie die Anpassung vorhandener Kostüme oder von der Stange erworbener Kleidung, Hüte, Schuhe usw.

Als Rechtsgrundlage für Gäste drängt sich Art. 6 Abs. 1 lit. b) DS-GVO (Vertrag) auf. Um die vertragliche Leistung erbringen zu können, ist das Tragen von Maske und Kostüm erforderlich. Um Maske und Kostüm tragen zu können, müssen beide vorher hergestellt werden. Eine Interessenabwägung wäre ebenfalls denkbar (Art. 6 Abs. 1 lit. f) DS-GVO). Das Theater hat ein Interesse daran, dass Akteure durch das Tragen von Masken und Kostümen zum Kunsterlebnis der Produktion beitragen. Die künstlerische Freiheit zählt zu den Grundrechten (Art. 13 GrCh, Art. 5 Abs. 3 GG), weshalb das Interesse berechtigt ist. Eine Einwilligung scheitert an der fehlenden Freiwilligkeit. Im Übrigen würde eine nicht erteilte Einwilligung zu einem Auftritt auf der Bühne ohne Maske oder Kostüm führen. Die übrigen Erlaubnistatbestände nach Art. 6 Abs. 1 DS-GVO erscheinen offensichtlich nicht einschlägig.

Für beschäftigte Akteure kommt § 26 Abs. 1 BDSG (Durchführung des Beschäftigungsverhältnisses) anstelle von Art. 6 Abs. 1 lit. b) DS-GVO in Betracht. Diese Akteure haben einen tarifvertraglichen Anspruch auf Stellung von Kostümen (§ 25 NV Bühne, Fassung vom 28.03.2017).

Die genannten Rechtsgrundlagen tragen die Verarbeitung für die Dauer des Beschäftigungsverhältnisses oder des Vertrags bei Gästen. Nach Ende des Beschäftigungsverhältnisses bzw. des Vertrags bei Gästen wären die Kopf- und Körpermaße grundsätzlich zu löschen. Beschäftigungsverhältnisse sind häufig befristet, sodass Akteure zwischen verschiedenen Theatern wechseln. Nach dem Ende des Beschäftigungsverhältnisses ist es nicht ungewöhnlich, dass ein Akteur als Gast bei seinem ehemaligen Arbeitgeber auftritt. Im Unterschied zu Beschäftigten müssen Gäste extra anreisen, d.h. es besteht die Erforderlichkeit, so kurz wie möglich vor der Premiere mit den Proben zu beginnen. Die Herstellung von Masken und Kostümen nimmt insbesondere bei Produktionen mit mehreren Dutzend Akteuren viele Wochen in Anspruch. Aus diesem Grund liegt es im Interesse des Theaters, auf gespeicherte Kopf- und Körpermaße zurückgreifen zu können. Da eine Vermessung von Kopf und Körper vor Ort regelmäßig im Theater erfolgt, um die Maßgüte und die erforderlichen Maße zu erhalten, würde eine Erhebung vor Beginn des Probenzeitraums eine zusätzliche Anreise für Akteure mit sich bringen. Die Erfahrung zeigt, dass Akteure im Regelfall keine Zeit für eine Vermessung aufbringen wollen. Bei der Herstellung von Masken und Kostümen ist ein Theater auf die Korrektheit der Maße angewiesen. Für aufwendige Nacharbeiten bspw. bei mehreren Kostümen reicht regelmäßig die Zeit bis zur Premiere nicht aus. Weiterhin verursachen Nacharbeiten Kosten. Aus diesem Grund scheidet bspw. eine Selbstvermessung durch den Akteur als Alternative aus.

Aus den genannten Gründen hat sowohl das Theater ein berechtigtes Interesse an Speicherung der Kopf- und Körpermaße über das Ende des Vertrags bzw. Beschäftigungsverhältnisses hinaus. Diese Speicherung liegt ebenfalls im Interesse der Akteure, da aufwendige Erhebungstermine entfallen.

Wenn Akteure kurzfristig bspw. durch Krankheit ausfallen, besteht die Notwendigkeit, teilweise innerhalb von Stunden, einen "Vertreter" ("Einspringer") zu finden, der die Rolle kennt. Die Zeit reicht regelmäßig nicht aus, um im Vorfeld die Kopf- und Körpermaße zu erheben, um zu prüfen, ob der "Einspringer" in Maske und Kostüm passt, sowie um die erforderlichen Änderungen vorzunehmen. Insofern ist es für das Theater erforderlich, Kopf- und Köpermaße vorliegen zu haben. Andernfalls ist die Vorstellung abzusagen. Abgesagte Vorstellungen bedeuten nicht nur einen finanziellen Verlust, sondern für Akteure auch eine verpasste Chance, ihre Bekanntheit zu steigern. Das Interesse des Theaters ist zweifelsohne berechtigt. Der Speicherung entgegenstehende Interessen von Akteuren sind nicht erkennbar, weshalb vieles dafür spricht, dass diese Interessenabwägung die Verarbeitung über das Ende eines Beschäftigungsverhältnisses bzw. Vertrags hinaus legitimiert.

Die Aktualisierung gespeicherter Kopf- und Körpermaße erfolgt regelmäßig im Zuge von Anproben, wenn ein veränderter Kopf oder Körper als Ursache für ein Nichtpassen von Maske oder Kostüm erkannt wird.

IV. Verwendung von Kostümen

Kostüme enthalten eingenäht den Titel der Produktion, die Rolle und den Namen aller Akteure, die das Kostüm getragen haben. Zu einem Kostüm gehört ein Datenblatt, das zusätzlich für jeden Akteur die Körpermaße aufführt, für die das Kostüm angepasst worden ist. Solange eine Produktion gespielt wird, werden die zugehörigen Kostüme verwendet. Die Kombination aus Titel der Produktion, Rolle und Namen erlaubt die Zuordnung von Kostüm zum Datenblatt und umgekehrt. Diese Zuordnung ist wesentlich, da verschiedene Kostümteile zum Waschen vermischt werden. Das Ordnungskriterium "Name" erlaubt es, das richtige Kostüm für einen Akteur herauszusuchen bzw. die richtige Maske anzulegen.

Wechseln Akteure einer Rolle innerhalb einer laufenden Produktion, muss ein gänzlich neues Kostüm hergestellt werden oder das vorhandene Kostüm angepasst werden.

Vereinfacht dargestellt bedeutet ein größerer Unterschied in den Körpermaßen des neuen Akteurs zum alten Akteur, dass ein neues Kostüm anzufertigen ist. Das Anfertigen neuer Kostüme ist regelmäßig teurer und zeitaufwendiger als ein Anpassen eines vorhandenen Kostüms. Aus diesem Grund wird in der Praxis einer Anpassung den Vorzug gegeben.

Die im Datenblatt festgehaltenen Körpermaße erlauben zu prüfen, ob Personen mit ähnlichen Körpermaßen zu einem früheren Zeitpunkt das Kostüm mit Änderungen getragen haben. Diese Information ist Grundlage für die Entscheidung, ob eine Anpassung ausreicht. Der Abgleich der Maße erlaubt, sowohl die Entscheidung zu treffen als auch die Anpassung bzw. Herstellung zu beginnen, ohne dass der neue Akteur in Person anwesend sein muss oder das Kostüm anprobieren muss.

Es gibt geplante Wechsel von Akteuren mit einem längeren Vorlauf sowie ungeplante Wechsel bspw. durch Krankheit mit einem Vorlauf von wenigen Stunden. Da die Herstellung von Masken und Kostümen regelmäßig in Handarbeit teilweise für mehrere Produktionen gleichzeitig erfolgt und die Herstellungskapazitäten eines Theaters sich nicht kurzfristig steigern lassen, ist ein möglichst langer zeitlicher Vorlauf entscheidend. Eine verspätete Fertigstellung würde zu Absagen von Aufführungen führen, d.h. eine verspätete Fertigstellung ist zu vermeiden. Aus dem Kostüm ohne Datenblätter lässt sich – je nach Kostümschnitt – nicht mehr ableiten, welche Körperform benötigt wird, um das Kostüm tragen zu können.

Das Interesse des Theaters an einer frühzeitigen Entscheidung über die Anpassung oder Neuanfertigung von Kostümen ist als Ausfluss der unternehmerischen Freiheit (Art. 16 GrCh) berechtigt. Für Akteure bedeutet die Verarbeitung von Körpermaßen aus den Datenblättern eine Erleichterung, da sie nicht für die Auswahl eines möglicherweise passenden Kostüms sowie zu weiteren Anproben extra anreisen müssen. Eine Interessenabwägung (Art. 6 Abs. 1 lit. f) DS-GVO) kann folglich die Verarbeitung tragen.

Weil Körpermaße von Akteuren verarbeitet werden, mit denen keine Vertragsbeziehung und kein Beschäftigungsverhältnis mehr besteht, sind Art. 6 Abs. 1 lit. b) bzw. § 26 Abs. 1 BDSG nicht einschlägig. Dieses gilt insbesondere für die Zeit der Speicherung für eine mögliche spätere Nutzung.

Denkbar wäre die Verarbeitung auf eine Einwilligung zu stützen. Erteilt ein Akteur die Einwilligung nicht, wären seine personenbezogenen Daten zu löschen. Soll die Löschung auf den Namen beschränkt werden, ist zu prüfen, ob der Akteur in Werbematerialen für die Produktion als Mitwirkender genannt worden ist. Dieses ist regelmäßig bspw. bei Schauspielern, Sängern, Tänzern und Dirigenten der Fall. Mit dem Wissen der Mitwirkung lässt sich bei Löschung des Namens eine nachträgliche Zuordnung der Körpermaße nicht ausschließen. Deshalb müsste die Löschung auch die Körpermaße umfassen. Im Extremfall gäbe es zu einem Kostüm keine Körpermaße mehr. Damit wäre das Kostüm faktisch nicht mehr nutzbar, da aus dem Kostüm nicht ersichtlich ist, welche Maße ein Träger mitbringen sollte. Weiterhin erlangen Kostüme einen ideellen oder geschichtlichen Wert, wenn bekannte Akteure es getragen haben. Durch das Löschen der Träger würden kulturgeschichtlich bedeutende Informationen verloren gehen. Eine Einwilligung wird den wirtschaftlichen Interessen der Theater nicht gerecht und würde sich zudem nachteilig auf die Kulturgeschichte des Theaters und der Bundesrepublik auswirken.

Die übrigen Rechtsgrundlagen aus Art. 6 Abs. 1 DS-GVO sind offensichtlich nicht einschlägig.

V. Austausch von Kopf- und Körpermaßen

Zwischen Theatern findet ein häufiger Austausch an Akteuren statt. Teilweise haben Akteure einen arbeitsvertraglichen Anspruch auf Gastierurlaub, in dem sie an anderen Theatern auftreten. Dieser Austausch erlaubt es, dem Publikum ein breiteres Spektrum von Akteuren und Produktionen darbieten zu können, als es mit dem festangestellten Ensemble möglich wäre. Weiterhin ermöglicht ein kurzfristiges Engagement von Gastkünstlern, kranke Akteure zu ersetzen, sodass Vorstellungen nicht abgesagt werden müssen. Gastauftritte erhöhen für Akteure die Bekanntheit und damit ihren Marktwert. In der Folge ist ein festangestellter Akteur regelmäßig gleichzeitig auch als Freiberufler tätig. Akteure ohne Festanstellung bestreiten ihren Lebensunterhalt durch Gastauftritte.

Aus der bereits diskutierten Notwendigkeit, Maske und Kostüm maßanzufertigen, ergibt sich die Notwendigkeit, dass die Kopf- und Körpermaße zwischen Theatern ausgetauscht werden. Denkbar wäre, dass jedes Theater die benötigten Maße selber erhebt. Da wie ausgeführt die Herstellung von Masken und Kostümen u.U. vor dem Probenzeitraum beginnt, müssten Gastakteure zusätzliche Anreisen unternehmen. Während dieser Anreisen können sie jedoch nicht an anderen Proben oder Aufführungen mitwirken. Dadurch dass Akteure teilweise für mehrere Produktionen gleichzeitig tätig sind, liegt eine Nichtverfügbarkeit für Proben oder Aufführungen nicht in ihrem Interesse. Akteure, die unter den Tarifvertrag NV Bühne fallen, müssen – abgesehen von dienstfreien Tagen – jederzeit für den Arbeitgeber erreichbar sein (§ 6 Abs. 4 Arbeitseinteilung) und zu den vom Arbeitgeber festgelegten Proben und Aufführung erscheinen (§ 6 Abs. 1). Eine zusätzliche Reisetätigkeit für Anproben müsste deshalb an den dienstfreien Tagen oder während des Gastierurlaubs stattfinden. Dienstfreie Tage dienen regelmäßig der Erholung. Aus diesem Grund liegt es im Interesse der Akteure, dass Reisen zum Anprobieren oder Maßnehmen durch eine Übermittlung von Kopf- und Körpermaßen ersetzt werden.

Für Theater bedeutet ein Austausch von Kopf- und Körpermaßen eine Vereinfachung der Herstellungsabläufe und erlaubt auch ein kurzfristiges Engagement von Gästen bspw. als Ersatz im Krankheitsfall. Dieses Interesse erscheint mit Blick auf die unternehmerische Freiheit (Art. 16 GrCh) berechtigt. Da das empfangende Theater die Kopf- und Körperdaten auch selber erheben dürfte, stellt die Übermittlung lediglich eine Beschleunigung und Erleichterung dar. Gegenläufige überwiegende Interessen der Akteure sind

nicht erkennbar, sodass eine Übermittlung von Kopf- und Körpermaßen zur Anfertigung von Masken und Kostümen zwischen Theatern durch eine Interessenabwägung legitimierbar erscheint (Art. 6 Abs. 1 lit. f) DS-GVO).

Wie oben ausgeführt, verfügen Theater über eine Rechtsgrundlage, Kopf- und Körpermaße über das Ende eines Vertrags oder Beschäftigungsverhältnisses hinaus zu speichern. Aus diesem Grund hat ein Akteur zwar einen Vertrag oder ein Beschäftigungsverhältnis mit dem die Daten empfangenen Theater, jedoch nicht zwingend mit dem übermittelnden Theater. Insofern trägt Art. 6 Abs. 1 lit. b) DS-GVO regelmäßig nicht.

Wird ein Akteur von einem Theater an ein anderes Theater ausgeliehen, lässt sich die Übermittlung grundsätzlich auf § 26 Abs. 1 BDSG stützen.

Grundsätzlich ließe sich eine solche Übermittlung auch auf eine Einwilligung (Art. 6 Abs. 1 lit. a) DS-GVO) stützen. Gegen die Einwilligung sprechen Zweifel an der Freiwilligkeit. Wenn ein Theater bei einer Beauftragung die Wahl zwischen zwei Akteuren hat, von denen der eine in eine Datenübermittlung einwilligt und der andere nicht, ist es für das Theater – wie ausgeführt – effizienter, den einwilligenden Akteur zu beauftragen. Bei Nichterteilung muss ein Akteur mit wirtschaftlichen Nachteilen rechnen.

Die übrigen Rechtsgrundlagen aus Art. 6 Abs. 1 DS-GVO sind offensichtlich nicht einschlägig.

Für eine Datenübermittlung in Drittstaaten sind die Anforderungen von Art. 45 ff. DS-GVO zu berücksichtigen.

VI. Verleih von Kostümen

Theater verleihen sowohl komplette Produktionen wie auch einzelne Bestandteile von Produktionen. Die Verleihe umfassen Gegenstände wie Bühnenbild und Kostüme, jedoch keine Akteure. Beim Verleihen von Kostümen werden sowohl die eingenähten Daten wie auch die Datenblätter mitgeschickt. Das entleihende Theater benötigt die Maße aus den Datenblättern, um die Passung von Akteur zu Kostüm sowie den ggf. erforderlichen Anpassungsbedarf zu ermitteln. Vor Rückgabe der ausgeliehenen Kostüme sind Änderungen rückgängig zu machen.

Die Ausführungen zur Verwendung von Kostümen gelten für die Verwendung der Daten aus dem Kostüm und den Datenblättern analog. Zu betrachten bleibt, welche Rechtsgrundlage die Übermittlung vom verleihenden an das ausleihende Theater trägt.

Wie ausgeführt, lassen sich Kostüme nur in Kombination mit den in den Datenblättern enthaltenen Körpermaßen verwenden. Auf den ersten Blick erscheint die Kenntnis von Namen der Akteure für das entleihende Theater nicht relevant zu sein. Die Kombination aus Titel der Produktion, Rolle und Namen ermöglicht aber die Zuordnung der Kostümteile zu einem vollständigen Kostüm. Entfiele der Name, wären bspw. bei Chormitgliedern die Kostümteile nicht mehr zum richtigen Kostüm zuordenbar. Zwar wäre ein Ersetzen des Namens durch ein anderes Kennzeichnen möglich. Dagegen spricht der hohe manuelle Aufwand, aus jedem Kostüm die eingenähten Namen zu ersetzen und nach Rückgabe des Kostüms das Ersetzen wieder rückgängig zu machen. Gleiches gilt für die Datenblätter.

Sofern öffentlich bekannt ist, welcher Akteur welche Rolle gespielt hat, ließen sich die Namen vom entleihenden Theater herausfinden. Insofern erfährt das entleihende Theater durch die Übermittlung des Namens keinen neuen Sachverhalt.

Ist der Name nicht öffentlich bekannt, bspw. bei Statisten, stellt sich die Frage nach der Eingriffstiefe. Die Kenntnis eines Namens reicht regelmäßig nicht aus, um eine Person zu identifizieren. Kostüme werden weltweit verliehen. Da nicht übermittelt wird, aus welchem Land der Betroffene stammt, spricht vieles dafür, dass der Name zur Identifikation nicht ausreichend ist. In Deutschland wird deshalb zur Personenidentifizierung regelmäßig auf mindestens ein weiteres Merkmal wie z.B. das Geburtsdatum zurückgegriffen.

Somit sprechen gute Gründe dafür, dass die berechtigten Interessen des verleihenden Theaters, die Namen aus wirtschaftlichen Gründen nicht zu ersetzen, die Interessen der Akteure an Unterlassung der Namensübermittlung überwiegen. Eine Einwilligung müsste konkret gefasst werden, d.h. auch das ausleihende Theater benennen. Somit müssten vor jedem Verleih die Einwilligungen aller auf den Datenblättern genannten Akteure eingeholt werden. Dieses ist zwar denkbar, jedoch weniger praktikabel. Akteure, die nicht mehr für das ausleihende Theater tätig sind, können unerreichbar sein. Werden Einwilligungen nicht erteilt, wären die Namen zu ersetzen.

Die übrigen Rechtsgrundlagen aus Art. 6 Abs. 1 DS-GVO sind offensichtlich nicht einschlägig.

Für eine Datenübermittlung in Drittstaaten sind die Anforderungen von Art. 45 ff. DS-GVO zu berücksichtigen.

VII. Kostüme abgespielter Produktionen

Solange eine Produktion aufgeführt ("gespielt") wird, ist ein Kostüm Teil des künstlerischen Werkes und wird für Proben und Aufführungen benötigt. Wird die Entscheidung getroffen, eine Produktion einzustellen ("abgespielt"), wird ein Kostüm nicht mehr benötigt. Manche Kostüme werden in anderen Produktionen verändert oder unverändert eingesetzt. Andere werden in Museen ausgestellt oder an interessierte Theater verkauft.

Die eingenähten Angaben zu Produktion, Rolle, Namen der Träger stellen auch bei abgespielten Produktionen das Ordnungskriterium zum Zuordnen der Kostümbestandteile und des Datenblattes dar. Die Körpermaße auf dem Datenblatt sind erforderlich für eine Anpassung an neue Produktionen. Museen benötigen die Körpermaße zum Verständnis, wie das Kostüm getragen wurde, sowie zum Anfertigen von Ausstellungspuppen.

Ist der Name im Zusammenhang mit einer Produktion und Rolle nicht öffentlich bekannt, bspw. bei Statisten, reicht die Kenntnis eines Namens wegen Namensgleichheit und Namensänderungen regelmäßig nicht aus, um eine Person

zu identifizieren. Der Name wäre somit nicht als personenbezogen anzusehen. Falls der Personenbezug bejaht würde, wäre die Eingriffstiefe als gering anzusehen.

Denkbar wäre es, die Namen der Akteure durch andere Kennzeichen zu ersetzen, sodass die Funktion als Ordnungskriterium erhalten bleibt. Sofern öffentlich bekannt ist, welcher Akteur welche Rolle gespielt hat, ließen sich die Namen durch Recherche herausfinden. Es läge trotz Ersetzen des Namens keine Anonymisierung vor. Weiterhin würde eine Anonymisierung das Kostüm als geschichtlich relevanten Gegenstand entwerten.

Bedingt durch den Herstellungsprozess und die verwendeten Materialien besitzt ein Kostüm einen materiellen (Geld-)Wert. Dazu kann eine künstlerische und geschichtliche Bedeutung treten. Bestehende Kostüme dienen als Inspirationsquelle für den Entwurf neuer Kostüme. Insbesondere durch bekannte Träger oder Kostümbildner erlangen Kostüme kulturgeschichtliche Bedeutung. Eine kulturgeschichtliche Bedeutung kann sich erst im Zeitablauf entwickeln, bspw. wenn ein unbekannter Akteur im Laufe seines Wirkens berühmt wird. Von geschichtlicher Bedeutung wären nicht nur das letzte getragene Kostüm, sondern auch frühere Kostüme. Da sich Materialien und Verarbeitungstechniken über die Zeit verändern, geben Kostüme auch Zeugnis von Herstellungsprozessen ab.

Die Körpermaße werden für eine Verwendung des Kostüms benötigt. Sie stehen jedoch nicht im Zentrum der Verarbeitung, sondern sind eher als Randaspekt des Kostüms zu sehen. Sofern die Körpermaße nicht personenbezogen veröffentlicht werden, d.h. einem unbestimmten Personenkreis zur Kenntnis gegeben werden, ist von einer geringen Eingriffstiefe in das Persönlichkeitsrecht auszugehen.

Da es verschieden gelagerte Nutzungsformen abgespielter Kostüme gibt, ist die Rechtsgrundlage im Einzelfall zu prüfen. Grundsätzlich kämen eine Verarbeitung im öffentlichen Interesse bspw. zur Archivierung oder Erforschung (Art. 6 Abs. 1 lit. e) DS-GVO) sowie eine Interessenabwägung gemäß Art. 6 Abs. 1 lit. f) DS-GVO in Betracht. Eine Einwilligung wäre zwar denkbar, scheitert jedoch aus den bereits ausgeführten Gründen. Hinzu kommt, dass ein Theater ggf. nicht mehr über die Kontaktdaten der Träger des Kostüms verfügt. Insofern wäre das Einholen einer Einwilligung nicht mehr möglich.

Eine Interessenabwägung ließe sich grundsätzlich auf die geschilderten Interessen an wirtschaftlicher Nutzung inkl. Lagerung des Kostüms oder einer künstlerischen Verwendung stützen. Beide Interessen sind, wie ausgeführt, berechtigt. Da die Eingriffstiefe in das Persönlichkeitsrecht gering ist, sind keine überwiegenden gegenläufigen Interessen der betroffenen Akteure erkennbar.

Bei einer Datenübermittlung in Drittstaaten wird an Anforderungen von Art. 45 ff. DS-GVO erinnert.

VIII. Fazit

Die Verarbeitung personenbezogener Kopf- und Körpermaße ist aus einer Theaterproduktion nicht wegzudenken. Dazu zählen sowohl die Herstellung von Kostümen, deren Verleih und wirtschaftliche Verwertungen, sobald die Produktion abgespielt ist. Weiterhin ist die Übermittlung von Kopf- und Körpermaßen zwischen Theatern für die Funktionsweise der Kulturszene von hoher Bedeutung. Grundsätzlich sind Interessenabwägungen gemäß Art. 6 Abs. 1 lit. f) DS-GVO geeignet, die verschiedenen Verarbeitungen zu legitimieren, sofern personenbezogene Kopf- und Körpermaße nicht veröffentlicht werden. Auf eine Einwilligung sollte wegen Zweifeln an der Freiwilligkeit sowie praktischen Erwägungen hinsichtlich einer starken Beeinträchtigung des Herstellungsprozesses bis hin zu vermehrten Vorstellungsabsagen verzichtet werden. Die dargestellte Verarbeitung ist insbesondere in den Datenschutzinformationen für Mitarbeiter und Gastakteure darzustellen (Art. 13 und 14 DS-GVO).

So entwickeln Sie ein rechtskonformes Löschkonzept

NUR 99,99 €

Leitfaden inklusive:
✓ Checklisten
✓ Musterentwurf
✓ Vorlagen
✓ Ausfüllhinweise

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

DATAKONTEXT

Rechtsprechung

Voraussetzungen für Ausübung der Befugnisse der nationalen Aufsichtsbehörden bei grenzüberschreitender Datenverarbeitung (Ls)

(**Europäischer Gerichtshof**, Urteil vom 15. Juni 2021 – C 645/19 –)

1. **Art. 55 Abs. 1 und die Art. 56 bis 58 sowie 60 bis 66 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sind in Verbindung mit den Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass eine Aufsichtsbehörde eines Mitgliedstaats, die nach den zur Durchführung von Art. 58 Abs. 5 der Verordnung erlassenen nationalen Rechtsvorschriften befugt ist, vermeintliche Verstöße gegen die Verordnung einem Gericht dieses Mitgliedstaats zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben, von dieser Befugnis, wenn eine grenzüberschreitende Datenverarbeitung in Rede steht, Gebrauch machen darf, obgleich sie für diese Datenverarbeitung nicht die „zuständige federführende Aufsichtsbehörde“ im Sinne von Art. 56 Abs. 1 der Verordnung ist, sofern es sich um einen der Fälle handelt, in denen die Verordnung 2016/679 der Aufsichtsbehörde eine Zuständigkeit einräumt, einen Beschluss zu erlassen, mit dem festgestellt wird, dass die fragliche Verarbeitung gegen die Vorschriften der Verordnung verstößt, und die in der Verordnung vorgesehen Verfahren der Zusammenarbeit und der Kohärenz eingehalten werden.**

2. **Art. 58 Abs. 5 der Verordnung 2016/679 ist dahin auszulegen, dass die Ausübung der einer Aufsichtsbehörde eines Mitgliedstaats, die nicht die federführende Aufsichtsbehörde ist, nach dieser Vorschrift zustehenden Befugnis zur Klageerhebung bei einer grenzüberschreitenden Verarbeitung personenbezogener Daten nicht voraussetzt, dass der für die grenzüberschreitende Verarbeitung personenbezogener Daten Verantwortliche oder der Auftragsverarbeiter, gegen den die Klage erhoben wird, im Hoheitsgebiet des Mitgliedstaats der fraglichen Aufsichtsbehörde eine Hauptniederlassung oder eine andere Niederlassung hat.**

3. **Art. 58 Abs. 5 der Verordnung 2016/679 ist dahin auszulegen, dass die einer Aufsichtsbehörde eines Mitgliedstaats, die nicht die federführende Aufsichtsbehörde ist, nach dieser Vorschrift zustehende Befugnis, vermeintliche Verstöße gegen die Verordnung einem Gericht dieses Mitgliedstaats zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben, sowohl gegenüber der Hauptniederlassung des Verantwortlichen, die sich in dem Mitgliedstaat der Aufsichtsbehörde befindet, als auch gegenüber einer anderen Niederlassung des Verantwortlichen ausgeübt werden kann, sofern Gegenstand der Klage eine Datenverarbeitung ist, die im Rahmen der Tätigkeiten der Niederlassung erfolgt, und die genannte Behörde nach den Ausführungen zu Vorlagefrage 1 dafür zuständig ist, die Befugnis auszuüben.**

4. **Art. 58 Abs. 5 der Verordnung 2016/679 ist dahin auszulegen, dass, wenn eine Aufsichtsbehörde eines Mitgliedstaats, die nicht die „federführende Aufsichtsbehörde“ im Sinne von Art. 56 Abs. 1 der Verordnung ist, vor dem 25. Mai 2018, also bevor die Verordnung galt, wegen einer grenzüberschreitenden Verarbeitung personenbezogener Daten eine Klage erhoben hat, diese Klage unionsrechtlich auf der Grundlage der Vorschriften der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr aufrechterhalten werden kann, die für Verstöße gegen die in ihr enthaltenen Vorschriften, die bis zu dem Zeitpunkt begangen worden sind, zu dem die Richtlinie aufgehoben wurde, weiter gilt. Darüber hinaus kann eine solche Klage von der Aufsichtsbehörde auf der Grundlage von Art. 58 Abs. 5 der Verordnung 2016/679 wegen nach diesem Zeitpunkt begangener Verstöße erhoben werden, sofern es sich um einen der Fälle handelt, in denen die Verordnung einer Aufsichtsbehörde eines Mitgliedstaats, die nicht die „federführende Aufsichtsbehörde“ ist, ausnahmsweise die Befugnis verleiht, einen Beschluss zu erlassen, mit dem festgestellt wird, dass die betreffende Datenverarbeitung gegen die in der Verordnung enthaltenen Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten verstößt, und die in der Verordnung vorgesehenen Verfahren der Zusammenarbeit und der Kohärenz eingehalten werden, was zu prüfen Sache des vorlegenden Gerichts ist.**

5. **Art. 58 Abs. 5 der Verordnung 2016/679 ist dahin auszulegen, dass die Vorschrift unmittelbare Wirkung hat, so dass eine nationale Aufsichtsbehörde sich auf sie berufen kann, um gegen Private eine Klage zu erheben oder ein entsprechendes Verfahren fortzuführen, auch wenn die Vorschrift in der Rechtsordnung des betreffenden Mitgliedstaats nicht speziell umgesetzt worden ist.**

Unmittelbare Wirkung des unionsrechtlich verankerten Grundsatzes des gleichen Entgelts (Ls)

(**Europäischer Gerichtshof**, Urteil vom 3. Juni 2021 – C-624/19 Tesco Stores –)

Arbeitnehmer können sich in Rechtsstreitigkeiten zwischen Privaten sowohl bei „gleicher" als auch bei „gleichwertiger Arbeit" unmittelbar auf den unionsrechtlich verankerten Grundsatz des gleichen Entgelts für Männer und Frauen berufen.

(Nicht amtlicher Leitsatz)

Feststellung einer Diskriminierung muss auch bei Anerkenntnis einer Schadensersatzforderung möglich sein (Ls)

(**Europäischer Gerichtshof**, Urteil vom 15. April 2021 – C 30/19 –)

Die Art. 7 und 15 der Richtlinie 2000/43/EG des Rates vom 29. Juni 2000 zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft in Verbindung mit Art. 47 der Charta der Grundrechte der Europäischen Union sind dahin auszulegen, dass sie einer nationalen Rechtsvorschrift entgegenstehen, die ein Gericht, das mit einer Klage auf Schadensersatz wegen des Vorwurfs einer gemäß dieser Richtlinie verbotenen Diskriminierung befasst ist, daran hindert, den Antrag auf Feststellung des Vorliegens dieser Diskriminierung zu prüfen, wenn der Beklagte sich zur Zahlung des geforderten Schadensersatzes bereit erklärt, ohne jedoch das Vorliegen der Diskriminierung einzuräumen. Es ist Sache des mit einem Rechtsstreit zwischen Privatpersonen befassten nationalen Gerichts, im Rahmen seiner Befugnisse den Rechtsschutz zu gewährleisten, der den Einzelnen aus Art. 47 der Charta der Grundrechte erwächst, indem es erforderlichenfalls jede entgegenstehende Bestimmung des nationalen Rechts unangewendet lässt.

Unzulässigkeit der vollkommen anlasslosen Vorratsdatenspeicherung (Ls)

(**Europäischer Gerichtshof**, Urteil vom 2. März 2021 – C 746/18 –)

1. **Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die es Behörden zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten ermöglicht, Zugang zu einem Satz von Verkehrs- oder Standortdaten zu erlangen, die geeignet sind, Informationen über die von einem Nutzer eines elektronischen Kommunikationsmittels getätigten Kommunikationen oder über den Standort der von ihm verwendeten Endgeräte zu liefern und genaue Schlüsse auf sein Privatleben zuzulassen, ohne dass sich dieser Zugang auf Verfahren zur Bekämpfung schwerer Kriminalität oder zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit beschränken würde; dies gilt unabhängig davon, für welchen Zeitraum der Zugang zu den betreffenden Daten begehrt wird und welche Menge oder Art von Daten für einen solchen Zeitraum verfügbar ist.**
2. **Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung entgegensteht, wonach die Staatsanwaltschaft, deren Aufgabe darin besteht, das strafrechtliche Ermittlungsverfahren zu leiten und gegebenenfalls in einem späteren Verfahren die öffentliche Klage zu vertreten, dafür zuständig ist, einer Behörde für strafrechtliche Ermittlungen Zugang zu Verkehrs- und Standortdaten zu gewähren.**

Zum Recht auf eigenständige Überprüfung des Messergebnisses und eines standardisierte Geschwindigkeits-Messverfahrens

(**Bundesverfassungsgericht**, Beschluss vom 4. Mai 2021 – 2 BvR 277/19 –)

Aus dem Recht auf ein faires Verfahren folgt grundsätzlich nicht nur ein Anspruch auf Zugang zu der Bußgeldakte, sondern auch zu bei der Bußgeldbehörde vorhandenen sonstigen Informationen.

Sachverhalt:

Mit seiner Verfassungsbeschwerde wendet sich der Beschwerdeführer gegen eine Verurteilung im Bußgeldverfahren wegen einer Geschwindigkeitsüberschreitung sowie die Verwerfung der Rechtsbeschwerde als unbegründet. Die dem Ordnungswidrigkeitenvorwurf zugrundeliegende Geschwindigkeitsmessung erfolgte mittels eines standardisierten Messverfahrens mit dem Messgerät PoliScan Speed M1. Vor der Verurteilung hatte der Beschwerdeführer erfolglos Zugang zu außerhalb der Bußgeldakte befindlichen Informationen, insbesondere den Messdaten, begehrt, um eine eigenständige Überprüfung der Ordnungsmäßigkeit des Messergebnisses vorzunehmen.

Der Beschwerdeführer macht mit seiner Verfassungsbeschwerde insbesondere eine Verletzung seines Rechts auf ein faires Verfahren (Art. 2 Abs. 1 i.V.m. Art. 20 Abs. 3 GG) geltend. Er rügt unter anderem, dass ihm infolge der Entscheidungen der Fachgerichte die Möglichkeit einer eigenständigen Überprüfung des Messergebnisses und damit die Formulierung von konkreten Einwendungen gegen das standardisierte Messverfahren unzulässig erschwert worden seien. Dies stelle sich als verfassungswidrig dar.

Aus den Gründen

Die Kammer nimmt die Verfassungsbeschwerde zur Entscheidung an und gibt ihr statt, da dies zur Durchsetzung des Grundrechts des Beschwerdeführers aus Art. 2 Abs. 1 in Verbindung mit Art. 20 Abs. 3 GG angezeigt ist (§ 93a Abs. 2 Buchstabe b BVerfGG). Die Voraussetzungen für eine stattgebende Entscheidung durch die Kammer liegen vor (§ 93c Abs. 1 Satz 1 BVerfGG).

Das Urteil des Amtsgerichts und die Entscheidung des Oberlandesgerichts über die Rechtsbeschwerde verletzen den Beschwerdeführer in seinem Recht auf ein faires Verfahren (Art. 2 Abs. 1 i.V.m. Art. 20 Abs. 3 GG). Die Fachgerichte haben verkannt, dass aus dem Recht auf ein faires Verfahren für den Beschwerdeführer grundsätzlich ein Anspruch auf Zugang zu den nicht bei der Bußgeldakte befindlichen, aber bei der Bußgeldbehörde vorhandenen Informationen folgen kann. Die generelle Versagung des Begehrens des Beschwerdeführers auf Informationszugang, welches dieser im fachgerichtlichen Verfahren hinreichend geltend gemacht hat, wird deshalb der aus Art. 2 Abs. 1 in Verbindung mit Art. 20 Abs. 3 GG folgenden Gewährleistung nicht gerecht. Entgegen der Annahme der Fachgerichte handelt es sich hierbei auch nicht um eine Frage der gerichtlichen Aufklärungspflicht, sondern der Verteidigungsmöglichkeiten des Betroffenen (vgl. BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 12. November 2020 – 2 BvR 1616/18 –, Rn. 47 ff.; Beschluss der 3. Kammer des Zweiten Senats vom 28. April 2021 – 2 BvR 1451/18 –, Rn. 5). Auf dieser Fehlannahme beruht die Entscheidung des Oberlandesgerichts. Es ist auch nicht auszuschließen, dass bereits die Verurteilung des Beschwerdeführers auf dem Verstoß des Amtsgerichts Rosenheim gegen den Grundsatz des fairen Verfahrens beruht.

Beide Entscheidungen waren aufzuheben (§ 93c Abs. 2 i.V.m.§ 95 Abs. 2 BVerfGG). Die Sache ist zur erneuten Entscheidung an das Amtsgericht Rosenheim zurückzuverweisen

Vorlagepflicht zum EuGH bei Schadensersatz gem. Art. 82 DS-GVO

(**Bundesverfassungsgericht**, Beschluss vom 14. Januar 2021 – 1 BvR 2853/19 –)

Streitrelevante Fragen zur Auslegung des Geldentschädigungsanspruchs aus Art. 82 DS-GVO sind dem EuGH zur Entscheidung vorzulegen, da insofern noch keine erschöpfende Klärung durch den EuGH erfolgt ist und viele offene Rechtsfragen bestehen.

Aus den Gründen:

Die Kammer nimmt die zulässige Verfassungsbeschwerde zur Entscheidung an und gibt ihr statt, weil dies zur Durchsetzung des als verletzt gerügten Rechts des Beschwerdeführers auf den gesetzlichen Richter gemäß Art. 101. Abs. 1 Satz 2 GG angezeigt ist, § 93a Abs. 2 Buchstabe b BVerfGG. Diese Entscheidung kann von der Kammer getroffen werden, weil die maßgeblichen verfassungsrechtlichen Fragen durch das Bundesverfassungsgericht bereits entschieden sind und die Verfassungsbeschwerde danach offensichtlich begründet ist, § 93c Abs. 1 Satz 1 BVerfGG.

1. Das Amtsgericht hat das Recht des Beschwerdeführers auf den gesetzlichen Richter verletzt, indem es aufgrund der teilweisen Klageabweisung, der dadurch für den Beschwerdeführer nicht erreichten Berufungsbeschwer (§ 511 Abs. 2 Nr. 1 ZPO) und der nicht zugelassenen Berufung letztinstanzlich tätig geworden ist und entgegen Art 267 Abs. 3 AEUV von einem Vorabentscheidungsersuchen an den Gerichtshof der Europäischen Union abgesehen hat

a) Der Gerichtshof der Europäischen Union ist gesetzlicher Richter im Sinne des Art. 101 Abs. 1 Satz 2 GG (vgl. BVerfGE 73, 339 <366>; 82, 159 <192>; 126, 286 <315>; 128, 157 <186 f.>; 129, 78 <105>; 135, 155 <230 f. Rn. 177>). Unter den Voraussetzungen des Art. 267 Abs. 3 AEUV sind die nationalen Gerichte von Amts wegen gehalten, den Gerichtshof anzurufen (vgl. BVerfGE 82, 159 <192 f.>; 128, 157 <187>; 129,78 <105>). Es kann einen Entzug des gesetzlichen Richters darstellen, wenn ein nationales Gericht seiner Pflicht zur Anrufung des Gerichtshofs im Wege des Vorabentscheidungsverfahrens nach Art. 267 Abs. 3 AEUV nicht nachkommt (vgl. BVerfGE 73, 339 <366 f.>; 82, 159 <192 ff.>; 135, 155 <230 f. Rn. 177>; st Rspr).

Nach der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH, Urteil vom 6. Oktober 1982, C.I.L.F.I.T., C-283/81, EU:C:1982:335, Rn. 21; Urteil vom 15. September 2005, C-495/03, EU:C:2005:552, Rn. 33; Urteil vom 6. Dezember 2005, C-461/03, EU:C:2005:742, Rn. 16; st Rspr) muss ein nationales letztinstanzliches Gericht seiner Vorlagepflicht nachkommen, wenn sich in einem bei ihm schwebenden Verfahren eine Frage des Unionsrechts stellt, es sei denn, das Gericht hat festgestellt, dass die gestellte Frage nicht entscheidungserheblich ist, dass die betreffende unionsrechtliche Bestimmung bereits Gegenstand einer Auslegung durch den Gerichtshof war (acte éclairé) oder dass die richtige Anwendung des Unionsrechts derart offenkundig ist, dass für einen vernünftigen Zweifel keinerlei Raum bleibt (acte clair) (vgl. auch BVerfGE 82, 159 <193>; 128, 157 <187>; 129, 78 <105 f.>; 140, 317 <376 Rn. 125>; 147, 364 <378 f. Rn. 37>). Davon darf das innerstaatliche Gericht aber nur ausgehen, wenn es überzeugt ist, dass auch für die Gerichte der übrigen Mitgliedstaaten und für den Gerichtshof der Europäischen Union die gleiche Gewissheit bestünde. Nur dann darf das Gericht von einer Vorlage absehen und die Frage in eigener Verantwortung lösen (vgl. EuGH, Urteil vom 6. Oktober 1982, C.I.L.F.I.T., C-283/81, EU:C:1982:335, Rn. 16).

Diese Grundsätze gelten auch für die unionsrechtliche Zuständigkeitsvorschrift des Art. 267 Abs. 3 AEUV. Daher stellt nicht jede Verletzung der unionsrechtlichen Vorlagepflicht zugleich einen Verstoß gegen Art. 101 Abs. 1 Satz 2 GG dar (vgl. BVerfGE 126, 286 <315>; 147, 364 <380 Rn. 40>). Das Bundesverfassungsgericht überprüft nur, ob die Auslegung und Anwendung der Zuständigkeitsregel des Art. 267 Abs. 3 AEUV bei verständiger Würdigung der das Grundgesetz bestimmenden Gedanken nicht mehr verständlich erscheint und offensichtlich unhaltbar ist (vgl. BVerfGE 126, 286 <315 f.>; 128, 157 <187>; 129, 78 <106>). Durch die zurückgenommene verfassungsrechtliche Prüfung behalten die Fachgerichte bei der Auslegung und Anwendung von Unionsrecht einen Spielraum eigener Einschätzung und Beurteilung, der demjenigen' bei der Handhabung einfachrechtlicher Bestimmungen der deutschen Rechtsordnung entspricht. Das Bundesverfassungsgericht wacht allein über die Einhaltung der Grenzen dieses Spielraums (vgl. BVerfGE 126, 286 <316>). Ein „oberstes Vorlagenkontrollgericht" ist es nicht (vgl. BVerfGE 126, 286 <316>; 135, 155 <231 f.: Rn. 180>; 147, 364 <379 f.

Rn. 39>; BVerfGE 13, 506 <512>; 14, 230 <233>; 16, 328 <336>; BVerfG, Beschluss der 1. Kammer des Zweiten Senats vom 9. November 1987 – 2 BvR 808/82 –, NJW 1988, S. 1456 [1457]).

Die Vorlagepflicht nach Art. 267 AEUV zur Klärung der Auslegung unionsrechtlicher Vorschriften wird in verfassungswidriger Weise gehandhabt, wenn ein letztinstanzliches Gericht eine Vorlage trotz der – seiner Auffassung nach bestehenden – Entscheidungserheblichkeit der unionsrechtlichen Frage überhaupt nicht in Erwägung zieht, obwohl es selbst Zweifel hinsichtlich der richtigen Beantwortung der Frage hat (grundsätzliche Verkennung der Vorlagepflicht; vgl. BVerfGE 82, 159 <195 f.>; 126, 286 <316 f.>; 128, 157 <187 f.>; 129, 78 <106 f.>; 135, 155 <232 Rn. 181>; 147, 364 <380 Rn. 41>).

Gleiches gilt in den Fällen, in denen das letztinstanzliche Gericht in seiner Entscheidung bewusst von der Rechtsprechung des Gerichtshofs zu entscheidungserheblichen Fragen abweicht und gleichwohl nicht oder nicht neuerlich vorlegt (bewusstes Abweichen von der Rechtsprechung des Gerichtshofs ohne Vorlagebereitschaft; vgl. BVerfGE 75, 223 <245>; 82, 159 <195>; 126, 286 <316 f.>; 128, 157 <187 f.>; 129, 78 <106 f.>; 135, 155. <232 Rn. 182>; 147, 364 <381 Rn. 42>).

Liegt zu einer entscheidungserheblichen Frage des Unionsrechts einschlägige Rechtsprechung des Gerichtshofs der Europäischen Union noch nicht vor oder hat er die entscheidungserhebliche Frage möglicherweise noch nicht erschöpfend beantwortet oder erscheint eine Fortentwicklung der Rechtsprechung des Gerichtshofs nicht nur als entfernte Möglichkeit (Unvollständigkeit der Rechtsprechung), so wird Art. 101 Abs. 1 Satz 2 GG verletzt, wenn das letztinstanzliche Hauptsachegericht den ihm in solchen Fällen notwendig zukommenden Beurteilungsrahmen in unvertretbarer Weise überschritten hat (vgl. BVerfGE 82, 159 <195 f.>; 126, 286 <316 f.>; 128, 157 <187 f.>; 129, 78 <106 f.>; 135, 155 <232 f. Rn. 183>). Dies kann insbesondere dann der Fall sein, wenn mögliche Gegenauffassungen zu der entscheidungserheblichen Frage des Unionsrechts gegenüber der vom Gericht vertretenen Meinung eindeutig vorzuziehen sind (vgl. BVerfGE 82, 159 <195 f.>; BVerfGK 10, 19 <29>). Jedenfalls bei willkürlicher Annahme eines „acte clair" oder eines „acte éclairé" durch die Fachgerichte ist der Beurteilungsrahmen in unvertretbarer Weise überschritten (vgl. BVerfGE 135, 155 <232 f. Rn. 183>; 147; 364 <381 Rn. 43>).

In diesem Zusammenhang ist auch zu prüfen, ob sich das Gericht hinsichtlich des Unionsrechts ausreichend kundig gemacht hat. Etwaige einschlägige Rechtsprechung des Gerichtshofs der Europäischen Union muss es auswerten und seine Entscheidung hieran orientieren (vgl. BVerfGE 82, 159 <196>; 128, 157 <189>). Auf dieser Grundlage muss das Fachgericht unter Anwendung und Auslegung des materiellen Unionsrechts (vgl. BVerfGE 75, 223 <234>; 128, 157 <188>; 129, 78 <107>) die vertretbare Überzeugung bilden, dass die Rechtslage entweder von vornherein eindeutig („acte clair") oder durch Rechtsprechung in einer Weise geklärt ist, die keinen vernünftigen Zweifel offen lässt („acte eclairé"; vgl. BVerfGE 129, 78 <107>). Hat es dies nicht getan, verkennt es regelmäßig die Bedingungen für die Vorlagepflicht. Zudem hat das Fachgericht Gründe anzugeben, die dem Bundesverfassungsgericht eine Kontrolle am Maßstab des Art. 101 Abs. 1 Satz 2 GG ermöglichen (vgl. BVerfGE 147, 364 <380 f. Rn. 41>; BVerfGE 8, 401 <405>; 10, 19 <30 f.>; BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 9. Januar 2001 – 1 BvR 1036/99 –, Rn. 21; Beschluss der 3. Kammer des Ersten Senats vom 20. Februar 2008 – 1 BvR 2722/06 –; Beschluss der 3. Kammer des Ersten Senats vom 25. Februar 2010 – 1 BvR 230/09 –, Rn. 19).

Bei den in der Rechtsprechung des Bundesverfassungsgerichts genannten Fallgruppen handelt es sich um eine nicht abschließende Aufzählung von Beispielen für eine verfassungsrechtlich erhebliche Verletzung der Vorlagepflicht. Für die Frage nach einer Verletzung des Rechts auf den gesetzlichen Richter gemäß Art. 101 Abs. 1 Satz 2 GG durch Nichtvorlage an den Gerichtshof der Europäischen-Union kommt es im Ausgangspunkt nicht in erster Linie auf die Vertretbarkeit der fachgerichtlichen Auslegung des für den Streitfall maßgeblichen materiellen Unionsrechts – hier der DS-GVO – an, sondern auf die Beachtung oder Verkennung der Voraussetzungen der Vorlagepflicht nach der Vorschrift des Art. 267 Abs. 3 AEUV, die den gesetzlichen Richter im Streitfall bestimmt (vgl. BVerfGE 128, 157 <188>; BVerfG, Beschluss der 3. Kammer des Ersten Senats vom 25. Februar 2010 – 1 BvR 230109 –, Rn. 20; Beschluss der 2. Kammer des Ersten Senats vom 30. August 2010 – 1 BvR 1631/08, Rn. 48).

b) Unter Berücksichtigung dieser Grundsätze hat das Amtsgericht Art. 101 Abs. 1 Satz 2 GG verletzt, indem es von einem Vorabentscheidungsersuchen wegen der zu klärenden Frage, ob im vom Beschwerdeführer vorgetragenen Fall der datenschutzwidrigen Verwendung einer Email-Adresse und der Übersendung einer ungewollten Email an das geschäftliche Email-Konto des Beschwerdeführers nach Art. 82 Abs. 1 DS-GVO ein Schmerzensgeldanspruch des Beschwerdeführers in Betracht kommt.

aa) Das Amtsgericht hätte nicht ohne Vorabentscheidungsersuchen an den Gerichtshof der Europäischen Union entscheiden dürfen, dass sich kein Anspruch des Beschwerdeführers aus der ohne seine ausdrückliche Einwilligung erfolgten Übersendung der Email aus Art. 82 DS-GVO ergebe, weil ein Schaden nicht eingetreten sei.

Der im Ausgangsverfahren zu beurteilende Sachverhalt warf die Frage auf, unter welchen Voraussetzungen Art. 82 Abs. 1 DS-GVO einen Geldentschädigungsanspruch gewährt und welches Verständnis dieser Vorschrift insbesondere im Hinblick auf Erwägungsgrund 146 Satz 3 zu geben ist; der eine weite Auslegung des Schadensbegriffs im Lichte der Rechtsprechung des Gerichtshofs der Europäischen Union verlangt, die den Zielen der DS-GVO in vollem Umfang entspricht. Nach Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen, also diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (vgl. Art. 4 Nr. 7 DS-GVO).

Dieser Geldentschädigungsanspruch ist in der Rechtsprechung des Gerichtshofs der Europäischen Union weder erschöpfend geklärt, noch kann er in seinen einzelnen, für die Beurteilung des im Ausgangsverfahrens vorgetragenen Sachverhalts notwendigen Voraussetzungen unmittelbar aus der DS-GVO bestimmt werden. Auch in der bislang vorliegenden Literatur, die sich im Hinblick auf Erwägungsgrund 146 wohl für ein weites Verständnis des Schadensbegriffes ausspricht, sind die Details und der genaue Umfang des Anspruchs noch unklar (vgl. Gola/Piltz, in: Gola, DS-GVO, 2. Aufl., 2018, Art. 82 Rn. 12 f.; Quaas, in: BeckOK Datenschutzrecht, 34. Ed., 11/2020, Art. 82 Rn. 23 f.; Bergt, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl., 2020, Art. 82, Rn. 17 f.; Boehm, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl., 2019, Art. 82 Rn. 11 f.; Frenzel, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl., 2018, Art. 82 Rn. 10). Von einer richtigen Anwendung des Unionsrechts, die derart offenkundig ist, dass für vernünftige Zweifel kein Raum bliebe (acte clair), konnte das Amtsgericht ebenfalls nicht ausgehen. Dies gilt umso mehr, als Art. 82 DS-GVO ausdrücklich immaterielle Schäden einbezieht.

bb) Die angegriffene Entscheidung zeigt, dass das Amtsgericht die Problematik der Auslegung des Art. 82 Abs. 1 DS-GVO durchaus

gesehen hat. Es hat sodann aber verfassungsrechtlich relevant fehlerhaft eine eigene Auslegung des Unionsrechts vorgenommen, indem es sich für die Ablehnung des Anspruchs auf ein Merkmal fehlender Erheblichkeit gestützt hat, das so weder unmittelbar in der DS-GVO angelegt ist, noch von der Literatur befürwortet oder vom Gerichtshof der Europäischen Union verwendet wird.

Zur Reichweite des Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO

(**Bundesgerichtshof**, Urteil vom 15. Juni 2021 – VI ZR 576/19 –)

1. **Gem. Art. 4 Nr. 1 Halbsatz 1 DS-GVO sind „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dieser Begriff ist weit zu verstehen. Er ist nicht auf sensible oder private Informationen beschränkt, sondern umfasst alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt oder diese mit ihr verknüpft sind.**

2. **Gem. Erwägungsgrund 63 Satz 1 DS-GVO dient das Auskunftsrecht der betroffenen Person hinsichtlich der sie betreffenden personenbezogenen Daten dem Zweck, sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit zu überprüfen. Der Datenauskunftsanspruch aus Art. 15 DS-GVO erstreckt sich daher auch auf die zwischen einem Versicherungsnehmer und dem Versicherer gewechselte Korrespondenz, die Daten zum „Prämienkonto" des Versicherungsvertrags, dem Gesundheitszustand des Versicherungsnehmers, den Versicherungsschein sowie versicherungsinterne Vermerke und Kommunikation aller Art.**

3. **Des Auskunftsanspruch nach Art. 15 DS-GVO ist durch das Verlangen nach einer „vollständigen Datenauskunft" hinreichend präzisiert und beschränkt sich nicht auf Daten, die dem Betroffenen noch nicht bekannt sind. Auch die Kategorisierung als „interne Vermerke" durch die datenverarbeitende Stelle steht dem Auskunftsrecht nicht entgegen.**

4. **Rechtliche Analysen können zwar personenbezogene Daten enthalten und unterfallen auch insoweit dem Auskunftsanspruch. Die auf ihrer Grundlage vorgenommene Beurteilung der Rechtslage selbst stellt jedoch ebenso wie Daten zu Provisionszahlungen einer Versicherungsgesellschaft an Dritte keine Information über den Betroffenen dar.**

5. **Erfüllt i.S.v. § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird eine Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist.**

6. **Die Annahme eines derartigen Erklärungsinhalts setzt jedoch voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdeckt. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. In diesem Fall kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen.**

Tatbestand:

Der Kläger macht – soweit für das Revisionsverfahren von Interesse – gegen den beklagten Versicherer Ansprüche auf Datenauskunft geltend.

Sein Auskunftsbegehren hat er nunmehr auf Art. 15 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, ABl. 2016 L 119 S. 1, berichtigt in ABl. 2016 L 314 S. 72 und ABl. 2018 L 127 S. 2; im Folgenden: DS-GVO) gestützt und insoweit beantragt, die Beklagte zu verurteilen, (...)

3. dem Kläger eine vollständige – über den Umfang der Anlage K37, S. 1-4, und der Anlagen BLD1-BLD10 hinausgehende – Datenauskunft durch Überlassen in Kopie – hilfsweise in Textform – zu erteilen;

4. hilfsweise zu 3., die Vollständigkeit und Richtigkeit ihrer bislang erteilten Datenauskunft an Eides statt zu versichern;

5. vorab gemäß § 256 Abs. 2 ZPO festzustellen, dass sich der Datenauskunftsanspruch des Klägers aus Art. 15 DS-GVO i.V.m. Art. 4 DS-GVO auf sämtliche bei der Beklagten tatsächlich über den Kläger vorhandene Daten erstreckt, einschließlich der intern zur Person des Klägers und der mit ihm gewechselten Korrespondenz (einschließlich E-Mails), der internen Telefon- und Gesprächsnotizen und sonstigen internen Vermerke der Beklagten zu dem zwischen den Parteien bestehenden Versicherungsverhältnis und auch der internen Bewertungen der Beklagten zu den Ansprüchen des Klägers aus der streitgegenständlichen Versicherungspolice.

Das Landgericht hat die Berufung des Klägers – unter Abweisung der erstmals in zweiter Instanz erhobenen Zwischenfeststellungsklage als unzulässig – zurückgewiesen und dabei die Revision hinsichtlich der Frage des Umfangs des Auskunftsanspruchs nach Art. 15 DS-GVO zugelassen. Der Kläger verfolgt mit seiner Revision die Klageanträge zu 3 bis 5 weiter.

Aus den Gründen:

I. Das Berufungsgericht, dessen Urteil unter anderem in CR 2019, 505 veröffentlicht ist, hat zur Begründung seiner Ent-

scheidung, soweit für das Revisionsverfahren von Interesse, im Wesentlichen Folgendes ausgeführt:

Die Zwischenfeststeilungsklage sei bereits unzulässig. Es fehle an der nach § 256 Abs. 2 ZPO erforderlichen Vorgreiflichkeit des Rechtsverhältnisses für die Entscheidung des Rechtsstreits. Die begehrte Feststellung müsse sich auf einen Gegenstand beziehen, der über den rechtskraftfähigen Gegenstand des Rechtsstreits hinausgehe. Für eine Zwischenfeststellungsklage sei daher kein Raum, wenn mit dem Urteil über die Hauptklage die Rechtsbeziehungen der Parteien erschöpfend geregelt würden.

Die Beklagte habe den Auskunftsanspruch des Klägers aus Art. 15 DS-GVO vollständig erfüllt. Die Beklagte habe dem Kläger in einer vorprozessualen Mitteilung vom 5. April 2016 und einem weiteren Schreiben vom 13. Dezember 2018 verschiedene Auskünfte und Informationen erteilt und angegeben, dass weitere personenbezogene Daten über den Kläger nicht gespeichert bzw. verarbeitet worden seien. Der Kläger habe nicht konkret dargelegt, dass die bereits von der Beklagten erteilte Auskunft unvollständig sei und inwieweit er weitere Auskunft verlange. Zurückliegende Korrespondenz der Parteien unterfalle dem Auskunftsanspruch ebenso wenig wie Datenauskünfte zu internen Bearbeitungsvermerken oder das Prämienkonto im Rahmen des Versicherungsverlaufs. Zu weiterer Korrespondenz mit Dritten habe die Beklagte erklärt, dass eine solche nicht geführt worden sei.

Die hilfsweise begehrte eidesstattliche Versicherung könne der Kläger ebenfalls nicht verlangen, da keine Anhaltspunkte für eine Unvollständigkeit oder Unrichtigkeit der erteilten Auskunft dargetan oder ersichtlich seien.

II. Die Revision ist unzulässig, soweit sie sich gegen die Abweisung der Zwischenfeststellungsklage richtet. Soweit sie sich gegen die Zurückweisung der Berufung hinsichtlich der Klageanträge zu 3 und 4 wendet, hat die Revision Erfolg und führt zur teilweisen Aufhebung des Berufungsurteils und Zurückverweisung der Sache an das Berufungsgericht.

1. Die Revision ist nach § 543 Abs. 1 Nr. 1 ZPO statthaft und auch im Übrigen zulässig, soweit sie sich gegen die Zurückweisung der Berufung hinsichtlich der Klageanträge zu 3 und 4 wendet. Die gegen die Abweisung des Zwischenfeststellungsantrags (Klageantrag zu 5) gerichtete Revision ist dagegen nach § 552 Abs. 1 Satz 2 ZPO als unzulässig zu verwerfen. Insoweit ist sie nicht statthaft (§ 542 Abs. 1, § 543 Abs. 1 Nr. 1 ZPO), weil sie vom Berufungsgericht nicht zugelassen worden ist. Das Berufungsgericht hat in der Urteilsformel die Revision lediglich hinsichtlich der Frage des Umfangs des Auskunftsanspruchs nach Art. 15 DS-GVO zugelassen und die Zulassung in der Sache damit wirksam auf die Klageanträge zu 3 und 4, einen tatsächlich und rechtlich selbständigen Teil des Gesamtstreitstoffs, beschränkt (vgl. zu den Voraussetzungen einer Zulassungsbeschränkung nur Senatsurteil vom 2. Mai 2017 – VI ZR 262/16, VersR 2017, 959 Rn. 15 mwN). Die mit dem Klageantrag zu 5 erhobene Zwischenfeststellungskiage betrifft inhaltlich zwar ebenfalls die Frage des Umfangs des Auskunftsanspruchs nach Art. 15 DS-GVO. Sie wurde jedoch vom Berufungsgericht nicht aus materiellen, sondern aus prozessualen Gründen mangels Vorgreiflichkeit des festzustellenden Rechtsverhältnisses (§ 256 Abs. 2 ZPO) als unzulässig abgewiesen. Die Frage des Umfangs des Auskunftsanspruchs nach Art. 15 DS-GVO spielte insoweit keine Rolle. Diese Entscheidung wollte das Berufungsgericht daher ersichtlich nicht zur revisionsgerichtlichen Überprüfung stellen.

2. Soweit die Revision zulässig ist, ist sie auch begründet.

a) Die Revision wendet sich mit Erfolg gegen die Beurteilung des Berufungsgerichts, dem Kläger stehe kein weitergehender Auskunftsanspruch gemäß Art. 15 DS-GVO gegen die Beklagte zu. Mit der Begründung des Berufungsgerichts kann nicht angenommen werden, die Beklagte habe die nach dieser Vorschrift bestehenden Ansprüche des Klägers bereits vollständig erfüllt.

aa) Das Berufungsgericht geht allerdings zu Recht davon aus, dass sich der datenschutzrechtliche Auskunftsanspruch des Klägers nach dem seit dem 25. Mai 2018 unmittelbar anwendbaren Art. 15 DS-GVO beurteilt (Art. 99 Abs. 2 DS-GVO; vgl. Senatsurteil vom 27. Juli 2020 – VI ZR 405/18, BGHZ 226, 285 Rn. 12). Nach Art. 15 Abs. 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen. Gemäß Art. 15 Abs. 3 Satz 1 DS-GVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.

bb) Im Ausgangspunkt zutreffend nimmt das Berufungsgericht weiter an, dass dem Kläger nach dieser Vorschrift grundsätzlich ein Auskunftsanspruch über die bei der Beklagten als Verantwortlicher im Sinne des Art. 4 Nr. 7 Halbsatz 1 DS-GVO verarbeiteten ihn betreffenden personenbezogenen Daten zusteht. Seine Annahme, dieser Anspruch sei seitens der Beklagten bereits vollständig erfüllt, ist jedoch rechtsfehlerhaft.

(1) Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, sieht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH, Urteil vom 3. September 2020 – III ZR 136/18, GRUR 2021, 110 Rn, 43 mwN).

Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen (vgl. BGH, Urteil vom 6. März 1952 – IV ZR 45/50 und – IV ZR 16/51, BeckRS 1952, 103508 Rn. 28 f.; Bittner/Kolbe, in: Staudinger, BGB, Neubearb. 2019, § 260 Rn. 36 und § 259 Rn. 32).

(2) Nach diesen Maßstäben tragen die Erwägungen des Berufungsgerichts die Annahme einer vollständigen Erfüllung des klägerischen datenschutzrechtlichen Auskunftsanspruchs nicht. Das Berufungsgericht hat zwar unangefochten festgestellt, dass die Beklagte dem Kläger bereits gewisse Auskünfte erteilt und angegeben hat, weitere personenbezogene Daten über den Kläger seien nicht gespeichert bzw. verarbeitet worden. Der Kläger hat jedoch, wie sich aus seinem Zwischenfeststeilungsantrag und dem Sitzungsprotokoll der Berufungsverhandlung ergibt und worauf die Revision zu Recht hinweist, sein Auskunftsbegehren angesichts der bereits erteilten Auskünfte unter anderem dahingehend präzisiert, dass er weitergehende Auskünfte hinsichtlich der gesamten noch nicht mitgeteilten Korrespondenz der Parteien, einschließlich der Daten des vollständigen Prämienkontos und etwaig erteilter Zweitschriften und Nachträge zum Versicherungsschein, sowie Datenauskünfte bezüglich

sämtlicher Telefon-, Gesprächs- und Bewertungsvermerke der Beklagten zum Versicherungsverhältnis fordere. Dass die Beklagte auch hinsichtlich dieser Gegenstände des Auskunftsbegehrens erklärt hätte, bereits vollständig Auskunft erteilt zu haben, hat das Berufungsgericht nicht festgestellt. Soweit das Berufungsgericht die Auffassung vertritt, diese Auskunftsgegenstände unterfielen bereits ihrer Art nach nicht dem Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO, beruht dies – jedenfalls teilweise – auf einem fehlerhaften Verständnis des Begriffs der personenbezogenen Daten im Sinne der DS-GVO und des Zwecks des datenschutzrechtlichen Auskunftsanspruchs.

(a) Gemäß Art. 4 Nr. 1 Halbsatz 1 DS-GVO sind „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Nach dieser Definition und der Rechtsprechung des Gerichtshofs der Europäischen Union ist der Begriff weit zu verstehen. Er ist nicht auf sensible oder private Informationen beschränkt, sondern umfasst potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt. Die letztgenannte Voraussetzung ist erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist (vgl. – noch zu Art, 2 lit. a der Richtlinie 95/46/EG – EuGH, Urteil vom 20. Dezember 2017 – Rs. C-434/16, NJW 2018, 767 Rn. 33-35 mwN; Art.-29-Datenschutzgruppe, Stellungn. 4/2007, WP 136, 10 ff.; zu Art. 4 Nr. 1 DS-GVO vgl. Arning/Rothkegel in Taeger/Gabel, DS-GVO/BDSG, 3. Aufl. 2019, Art. 4 DS-GVO Rn. 8 ff. mwN; Klar/Kühling in Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Nr. 1 DS-GVO Rn. 11 ff.; Klabunde, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 10 f.). Soweit die Revisionserwiderung meint, Art. 15 DS-GVO sei im Hinblick auf den Begriff der „personenbezogenen Daten" teleologisch dahingehend zu reduzieren, dass der Personenbezug im Rahmen von Art. 15 DS-GVO voraussetze, dass es um „signifikante biografische Informationen" gehe, die „im Vordergrund" des fraglichen Dokuments stünden (so auch Harting, CR 2019, 219, 224; für eine teleologische Reduktion auch Britz/Beyer, VersR 2020, 65, 73 mwN), ist diese Auffassung mit der zitierten Rechtsprechung des Gerichtshofs der Europäischen Union, die sich zweifelsfrei auf den Begriff der personenbezogenen Daten im Sinne des Art. 15 i.V.m. Art. 4 Nr. 1 Halbsatz 1 DS-GVO übertragen lässt, ersichtlich nicht zu vereinbaren (ablehnend auch König, CR 2019, 295 Rn. 47; gegen eine Einschränkung auf Tatbestandsebene auch Lembke, NJW 2020, 1841, 1843; Schulte/Welge, NZA 2019, 1110, 1111; Brink/Joos, ZD 2019, 483, 488).

Nach Erwägungsgrund 63 Satz 1 der DS-GVO dient das Auskunftsrecht der betroffenen Person hinsichtlich der sie betreffenden personenbezogenen Daten dem Zweck, sich der Verarbeitung (zum Begriff vgl. Art. 4 Nr. 2 DS-GVO; zu dem vom sachlichen Anwendungsbereich der Verordnung erfassten Bereich der Verarbeitung vgl. Art. 2 Abs. 1, Art. 4 Nr. 6 DS-GVO) bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können.

(b) Nach diesen Grundsätzen können entgegen der Ansicht des Berufungsgerichts die zurückliegende Korrespondenz der Parteien, das „Prämienkonto" des Klägers und Daten des Versicherungsscheins sowie interne Vermerke und Kommunikation der Beklagten nicht kategorisch vom Anwendungsbereich des Art. 15 Abs. 1 DS-GVO ausgeschlossen werden.

(aa) Schreiben des Klägers an die Beklagte sind grundsätzlich ihrem gesamten Inhalt nach als personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO anzusehen. Die personenbezogene Information besteht bereits darin, dass sich der Kläger dem Schreiben gemäß geäußert hat (vgl. noch zu § 4 Abs. 1 BDSG 1990 – Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 17; zu Art. 15 DS-GVO vgl. LArbG Baden-Württemberg, BB 2020, 2169, 2174). Auch die Schreiben der Beklagten an den Kläger unterfallen dem Auskunftsanspruch insoweit, als sie Informationen über den Kläger nach den oben genannten Kriterien enthalten. Dass die Schreiben dem Kläger bereits bekannt sind, schließt für sich genommen entgegen der Auffassung des Berufungsgerichts den datenschutzrechtlichen Auskunftsanspruch nicht aus (vgl, Brink/Joos ZD 2019, 483, 485; Schmidt-Wudy, in: BeckOK DatenschutzR, 35. Ed. 1.2.2021, Art, 15 DS-GVO Rn. 52.2; aA wohl LArbG Niedersachsen, Urteil vom 9. Juni 2020 – 9 Sa 608/19, juris Rn, 66; zum gegensätzlichen Regelungsansatz hinsichtlich der Informationspflichten nach Art. 13, 14 DS-GVO vgl. Art. 13 Abs. 4, Art. 14 Abs. 5 lit. a DS-GVO und Erwägungsgrund 62). Die Beklagte soll Auskunft darüber geben, ob sie die im Schriftverkehr enthaltenen personenbezogenen Daten aktuell verarbeitet, insbesondere speichert. Die Auskunft soll den Kläger, wie bereits dargelegt, in die Lage versetzen, sich der Datenverarbeitung bewusst zu werden und deren Rechtmäßigkeit zu überprüfen. Er soll sich insbesondere vergewissern können, dass die ihn betreffenden Daten richtig sind und in zulässigerweise verarbeitet werden (vgl. EuGH, Urteil vom 20. Dezember 2017 – Rs. C-434/16, NJW 2018, 767 Rn. 57). Das etwaige Bewusstsein des Klägers, dass die fragliche Korrespondenz einst gewechselt wurde, genügt insoweit nicht. Zu beachten ist ferner, dass der Auskunftsberechtigte grundsätzlich wiederholt Auskunft verlangen kann (vgl. Erwägungsgrund 63 Satz 1, Art. 12 Abs. 5 Satz 2 DS-GVO). Dies spricht ebenfalls gegen die Auffassung des Berufungsgerichts, das Auskunftsrecht nach Art. 15 DS-GVO beschränke sich auf Daten, die dem Betroffenen noch nicht bekannt sind. Daher sind auch etwaige Zweitschriften und Nachträge zu dem Versicherungsschein, auf die sich das Auskunftsbegehren des Klägers ausweislich des Sitzungsprotokolls mit erstreckt, nicht grundsätzlich vom datenschutzrechtlichen Auskunftsanspruch ausgeschlossen, soweit die darin enthaltenen personenbezogenen Daten bei der Beklagten verarbeitet werden. Dementsprechend ist auch nicht ersichtlich, warum bei der Beklagten verarbeitete Daten über Prämienzahlungen des Klägers nicht grundsätzlich Gegenstand des Auskunftsanspruchs sein sollten.

Die Korrespondenz der Beklagten mit Dritten kann, wovon auch das Berufungsgericht ausgeht, ebenfalls auf die Person des Klägers bezogene Daten enthalten. Insoweit hat das Berufungsgericht aber unangefochten festgestellt, die Beklagte habe erklärt, dass solche Korrespondenz nicht über die bereits erteilten Auskünfte hinaus geführt worden sei. Mit dieser abschließenden Negativauskunft ist der Auskunftsanspruch des Klägers hinsichtlich dieses Auskunftsgegenstandes erfüllt.

(bb) Interne Vermerke oder interne Kommunikation bei der Beklagten, die Informationen über den Kläger enthalten, kommen als Gegenstand des Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO ebenfalls grundsätzlich in Betracht. Dies ist beispielsweise entsprechend der Beurteilung der Schreiben des Klägers bei Vermerken der Fall, die festhaften, wie sich der Kläger telefonisch oder in persönlichen Gesprächen geäußert hat (vgl. OLG Köln, VersR 2020, 81, 85; Schaffland/Holthaus, in: Schaffland/Wiltfang, DS-GVO/BDSG, Lfg. 3/21, Art. 15 DS-GVO Rn. 1d). Auch Vermerke über den Gesundheitszustand des Klägers enthalten personenbezogene Daten. Die Erwägung des Berufungsgerichts, es handele sich bei Vermerken um „interne Vorgänge der Beklagten", ist im Hinblick auf den Begriff der personenbezogenen Daten ohne Relevanz. Der Auskunftsanspruch gemäß Art. 15 Abs. 1 DS-GVO setzt offensichtlich weder nach seinem

Wortlaut noch nach Sinn und Zweck voraus, dass die fraglichen Daten extern zugänglich sind.

Soweit der Kläger Auskunft über die internen Bewertungen der Beklagten zu den Ansprüchen des Klägers aus der streitgegenständlichen Versicherungspolice verlangt, ist allerdings zu beachten, dass nach der Rechtsprechung des Gerichtshofs der Europäischen Union rechtliche Analysen zwar personenbezogene Daten enthalten können, die auf der Grundlage dieser personenbezogenen Daten vorgenommene Beurteilung der Rechtslage selbst aber keine Information über den Betroffenen und damit kein personenbezogenes Datum darstellt (vgl. EuGH, Urteil vom 17. Juli 2014 – Rs. C-141/12 und C-372/12, CR 2015, 103 Rn. 39 ff.). Daten über Provisionszahlungen der Beklagten an Dritte haben nach den vom Europäischen Gerichtshof entwickelten Kriterien ebenfalls keinen Bezug zur Person des Klägers, Sein nach dem Vorbringen der Revision auch hierauf gerichtetes Auskunftsbegehren kann der Kläger daher nicht auf die DS-GVO stützen.

cc) Die Durchführung eines Vorabentscheidungsverfahrens nach Art. 267 AEUV zur Klärung des Begriffs der personenbezogenen Daten i.S.d. Art. 15 i.V.m Art. 4 Nr. 1 DS-GVO ist nicht geboten. Soweit im derzeitigen Stadium des streitgegenständlichen Verfahrens entscheidungserheblich, ist die Auslegung dieses unionsrechtlichen Begriffs durch die Rechtsprechung des Gerichtshofs der Europäischen Union (Urteile vom 20. Dezember 2017 – Rs. C-434/16, NJW 2018, 767 Rn, 33-35 und vom 17. Juli 2014 – Rs. C-141/12 und C-372/12, CR 2015, 103 Rn. 39 ff.) eindeutig geklärt („acte clair", vgl. EuGH, Urteil vom 6. Oktober 1982 – Rs. C-283/81, NJW 1983, 1257, 1258; BVerfG, NVwZ 2015, 52 Rn. 35).

b) Die Zurückweisung der Berufung des Klägers hinsichtlich des Klageantrags 3 erweist sich auch nicht aus anderen Gründen als richtig (§ 561 ZPO).

aa) Entgegen der Rüge der Revisionserwiderung ist der Auskunftsantrag – Klageantrag zu 3 – im Sinne des § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmt und daher zulässig (zu den Anforderungen des § 253 Abs. 2 Nr. 2 ZPO im Allgemeinen vgl. Senatsurteil vom 13. Oktober 2015 – VI ZR 271/14, BGHZ 207, 163 Rn. 19 mwN). Die Frage ist als Prozessvoraussetzung vom Revisionsgericht von Amts wegen zu prüfen, unabhängig von der Beschränkung der Revisionszulassung (vgl. Senatsurteil vom 13. Oktober 2015 -VI ZR 271/14, BGHZ 207, 163 Rn. 18; BGH, Urteil vom 10. Oktober 2017 – XI ZR 456/16, NJW 2018, 227 Rn. 10; jeweils m.w.N.).

Zur Ermittlung des Klagebegehrens ist nicht allein auf den Antrag selbst abzustellen, sondern auch die Klagebegründung heranzuziehen (vgl. etwa Senatsurteile vom 1. Februar 2011 – X ZR 345/09, AfP 2011, 172 Rn. 9; vom 26. Mai 2009 – VI ZR 174/08, VersR 2009, 1269 Rn. 13; jeweils mwN). Danach besteht im Streitfall kein Zweifel, dass der Kläger nicht irgendeine „Datenauskunft" (so der Antragswortlaut) verlangt, sondern eine Auskunft über die von der Beklagten verarbeiteten, ihn betreffenden personenbezogenen Daten gemäß Art. 15 Abs. 1 DS-GVO. Auch die Reichweite dieses Begehrens ist hinreichend bestimmt. Dabei kann dahinstehen, ob insoweit nicht schon das Verlangen einer „vollständigen" Auskunft genügt, weil sich deren Umfang letztlich aus dem Gesetz ergibt (in diesem Sinne König, CR 2019, 295 Rn. 9-11; aA wohl Schulte/Welge, NZA 2019, 1110, 1112), Denn spätestens im Berufungsverfahren hat der Kläger – wie bereits ausgeführt – dargelegt, welche konkreten Auskünfte er (noch) begehrt.

bb) Soweit die Revisionserwiderung geltend macht, der Auskunftsanspruch bestehe nicht, da der Kläger Zwecke verfolge, die Art. 15 Abs. 1 DS-GVO nicht schütze, zudem stehe den geltend gemachten Ansprüchen der Einwand des mit ihrer Erfüllung verbundenen unverhältnismäßigen Aufwands für die Beklagte sowie das Geheimhaltungsinteresse der Beklagten entgegen, fehlt es bereits an entsprechenden tatsächlichen Feststellungen im Berufungsurteil. Der Senat kann auf der Grundlage der getroffenen Feststellungen nicht beurteilen, ob vorliegend unter diesen Gesichtspunkten die datenschutzrechtlichen Ansprüche des Klägers aus Art. 15 DS-GVO – etwa nach den Vorschriften in Art. 12 Abs. 5 Satz 2, Art. 15 Abs. 4 DS-GVO oder Art. 23 Abs. 1 DS-GVO i.V.m. § 29 Abs. 1 Satz 2 BDSG – beschränkt werden oder sogar entfallen könnten.

c) Ist damit der Klageantrag zu 3 noch nicht abweisungsreif, so steht der nur hilfsweise gestellte Klageantrag zu 4 noch nicht zur Entscheidung. Die von der Revisionserwiderung aufgeworfene Frage, ob § 260 Abs. 2 BGB auch auf den Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO anzuwenden oder die zuletzt genannte Vorschrift auch insoweit abschließend ist, stellt sich damit noch nicht.

Das Berufungsurteil war daher im genannten Umfang aufzuheben und die Sache insoweit zur neuen Verhandlung und Entscheidung an das Berufungsgericht zurückzuverweisen, § 562 Abs. 1, § 563 Abs. 1 Satz 1 ZPO.

Elektronische Kommunikation der Bundesrechtsanwaltskammer (Ls)

(**Bundesgerichtsho**f, Urteil vom 22. März 2021 – AnwZ (Brfg) 2/20 –)

1. **Der Bundesrechtsanwaltskammer steht ein Spielraum bei der technischen Ausgestaltung der Nachrichtenübermittlung mittels des besonderen elektronischen Anwaltspostfachs zu, sofern das gewählte System eine im Rechtssinne sichere Kommunikation gewährleistet.**

2. **Ein Anspruch von Rechtsanwälten gegen die Bundesrechtsanwaltskammer darauf, dass diese das besondere elektronische Anwaltspostfach mit einer Ende-zu-Ende-Verschlüsselung im Sinne der Europäischen Patentschrift EP 0 877 507 B1 versieht und betreibt, besteht nicht. Weder die gesetzlichen Vorgaben für die Errichtung und den Betrieb des besonderen elektronischen Anwaltspostfachs noch die Verfassung gebieten eine derartige Verschlüsselung.**

3. **Zur Sicherheit der Verschlüsselungstechnik des besonderen elektronischen Anwaltspostfachs.**

Abmahnung eines Redakteurs wegen Nicht-Anzeige einer Nebentätigkeit (Ls)

(**Bundesarbeitsgericht**, Urteil vom 15. Juni 2021 – 9 AZR 413/199 –)

1. **Eine tarifliche Regelung, nach der ein angestellter Zeitschriftenredakteur dem Verlag die anderweitige Verwertung einer während seiner arbeitsvertraglichen Tätigkeit bekannt gewordenen Nachricht anzuzeigen**

hat, soll dem Verlag regelmäßig die Prüfung ermöglichen, ob seine berechtigten Interessen durch die beabsichtigte Veröffentlichung beeinträchtigt werden. Dahinter muss das Interesse des Arbeitnehmers, die Nachricht ohne vorherige Einbindung des Verlags zu veröffentlichen, regelmäßig zurücktreten.

2. Verstößt der Arbeitnehmer gegen die Anzeigepflicht, kann dies eine Abmahnung rechtfertigen.

(Nicht amtliche Leitsätze)

Vorlage an den EuGH zum Abberufungsschutz eines Beauftragten für Datenschutz

(**Bundesarbeitsgericht**, Beschluss vom 27. April 2021 – 9 AZR 383/19 (A) –)

I. Der Gerichtshof der Europäischen Union wird gemäß Art. 267 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) um die Beantwortung folgender Fragen ersucht:

1. Ist Art. 38 Abs. 3 Satz 2 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung; im Folgenden DS-GVO) dahin auszulegen, dass er einer Bestimmung des nationalen Rechts, wie hier § 38 Abs. 1 und Abs. 2 i.V.m. § 6 Abs. 4 Satz 1 des Bundesdatenschutzgesetzes (BDSG), entgegensteht, die die Abberufung des Datenschutzbeauftragten durch den Verantwortlichen, der sein Arbeitgeber ist, an die dort genannten Voraussetzungen knüpft, unabhängig davon, ob sie im Wege der Erfüllung seiner Aufgaben erfolgt?

Falls die erste Frage bejaht wird:

2. Steht Art. 38 Abs. 3 Satz 2 DS-GVO einer solchen Bestimmung des nationalen Rechts auch dann entgegen, wenn die Benennung des Datenschutzbeauftragten nicht nach Art. 37 Abs. 1 DS-GVO verpflichtend ist, sondern nur nach dem Recht des Mitgliedstaats?

Falls die erste Frage bejaht wird:

3. Beruht Art. 38 Abs. 3 Satz 2 DS-GVO auf einer ausreichenden Ermächtigungsgrundlage, insbesondere soweit er Datenschutzbeauftragte erfasst, die in einem Arbeitsverhältnis zum Verantwortlichen stehen?

Falls die erste Frage verneint wird:

4. Liegt ein Interessenkonflikt i.S.v. Art. 38 Abs. 6 Satz 2 DS-GVO vor, wenn der Datenschutzbeauftragte zugleich das Amt des Vorsitzenden des in der verantwortlichen Stelle gebildeten Betriebsrats innehat? Bedarf es für die Annahme eines solchen Interessenkonflikts einer besonderen Aufgabenzuweisung innerhalb des Betriebsrats?

II. Das Revisionsverfahren wird bis zur Entscheidung des Gerichtshofs der Europäischen Union über das Vorabentscheidungsersuchen ausgesetzt.

Sachverhalt:

Zur Klärung der Frage, ob die Anforderungen des Bundesdatenschutzgesetzes (BDSG) an die Abberufung eines betrieblichen Datenschutzbeauftragten im Einklang mit der europäischen Datenschutz-Grundverordnung (DS-GVO) stehen, hat der Neunte Senat des Bundesarbeitsgerichts ein Vorabentscheidungsersuchen an den Gerichtshof der Europäischen Union gerichtet.

Der Kläger ist der von der Arbeit teilweise freigestellte Vorsitzende des bei der Beklagten gebildeten Betriebsrats. Mit Wirkung zum 1. Juni 2015 wurde er zusätzlich zum betrieblichen Datenschutzbeauftragten der Beklagten und – parallel dazu – drei weiterer Konzernunternehmen bestellt. Die Beklagte berief den Kläger (ebenso wie die drei weiteren Konzernunternehmen) mit Schreiben vom 1. Dezember 2017 und – nach Inkrafttreten der DS-GVO – mit weiterem Schreiben vom 25. Mai 2018 als Datenschutzbeauftragten ab. Mit seiner Klage hat der Kläger geltend gemacht, seine Rechtsstellung als Datenschutzbeauftragter bestehe unverändert fort. Die Beklagte hat die Auffassung vertreten, es drohten Interessenkonflikte, wenn der Kläger zugleich Datenschutzbeauftragter und Betriebsratsvorsitzender sei. Dies führe zu einer Unvereinbarkeit beider Ämter, die einen wichtigen Grund zur Abberufung des Klägers darstelle.

Die Vorinstanzen haben der Klage stattgegeben. Für die Entscheidung, ob die Beklagte den Kläger wirksam von seinem Amt als betrieblicher Datenschutzbeauftragter abberufen hat, kommt es auf die Auslegung von Unionsrecht an, die dem Gerichtshof der Europäischen Union vorbehalten ist. Das nationale Datenschutzrecht regelt in § 38 Abs. 2 i.V.m. § 6 Abs. 4 Satz 1 BDSG, dass für die Abberufung eines betrieblichen Datenschutzbeauftragten ein wichtiger Grund i.S.v. § 626 BGB vorliegen muss. Damit knüpft es die Abberufung eines Datenschutzbeauftragten an strengere Voraussetzungen als das Unionsrecht, nach dessen Art. 38 Abs. 3 Satz 2 DS-GVO die Abberufung lediglich dann nicht gestattet ist, wenn sie wegen der Aufgabenerfüllung des Datenschutzbeauftragten vorgenommen wird. Einen wichtigen Grund zur Abberufung verlangt das europäische Recht nicht.

Der Neunte Senat des Bundesarbeitsgerichts hält unter Zugrundelegung der bisherigen Rechtsprechung vorliegend keinen wichtigen Abberufungsgrund für gegeben. Deshalb hat er sich nach Art. 267 AEUV mit der Frage an den Gerichtshof gewandt, ob neben der Regelung in Art. 38 Abs. 3 Satz 2 DS-GVO mitgliedstaatliche Normen anwendbar sind, die – wie § 38 Abs. 2 i.V.m. § 6 Abs. 4 Satz 1 BDSG – die Möglichkeit der Abberufung eines Datenschutzbeauftragten gegenüber den unionsrechtlichen Regelungen einschränken.

Sollte der Gerichtshof die Anforderungen des BDSG an eine Abberufung für unionsrechtskonform erachten, hält der Senat es zudem für klärungsbedürftig, ob die Ämter des Betriebsratsvorsitzenden und des Datenschutzbeauftragten in einem Betrieb in Personalunion ausgeübt werden dürfen oder ob dies zu einem Interessenkonflikt i.S.v. Art. 38 Abs. 6 Satz 2 DS-GVO führt.

Zum Beseitigungsanspruch des Betriebsrats

(**Bundesarbeitsgericht**, Beschluss vom 23. März 2021 – 1 ABR 31/19 –)

Ein dem Betriebsrat bei der Verletzung eines Mitbestimmungsrechts nach§ 87 Abs. 1 BetrVG gegen den Arbeitgeber zustehender Beseitigungsanspruch erfasst nur die Beendigung des betriebsverfassungswidrigen Zustands, nicht aber die Rückgängigmachung sich aus der Verletzung des Mitbestimmungsrechts ergebender Folgen.

Sachverhalt:

Die Arbeitgeberin betreibt einen Flughafen. Sie beschäftigt etwa 1.800 Mitarbeiter. Antragsteller ist der bei ihr gebildete Betriebsrat.

Die Betriebsparteien schlossen am 25. Juni 2010 die „Rahmenbetriebsvereinbarung 02/2010 zur Einführung und Anwendung von informations- und kommunikations-technischen Systemen (ICT-Systeme) für Arbeitsplätze der F GmbH“ (BV 2010).

Die Arbeitgeberin nutzt im Betrieb für die E-Mail-Kommunikation der Arbeitnehmer das Softwareprogramm „Outlook“, für das ein Exchange-Server Dienste zur Verfügung stellt. Der Einführung und Anwendung der hierfür erforderlichen Anwendungen stimmte der Betriebsrat auf der Grundlage der BV 2010 zu.

Am 27. Mai 2015 vereinbarten die Beteiligten die „Rahmenbetriebsvereinbarung 01/2015 zur Nutzung von Kommunikationssystemen der F GmbH“ (BV 2015), die nach ihrem § 1 Nr. 1 für alle Arbeitnehmer „im Sinne des BetrVG“ gilt. Nach § 1 Nr. 2 BV 2015 sind unter Kommunikationssysteme „alle Systeme (Hardware, Software und Infrastruktur)“ zu verstehen, „die für den mittel-, orts- und zeitunabhängigen Austausch von Informationen (Audio, Video, Daten)“ genutzt werden. § 4 Satz 1 BV 2015 sieht vor, dass die Arbeitgeberin ihren Beschäftigten bei Bedarf einen E-Mail-Account zur Erfüllung der dienstlichen Aufgaben zur Verfügung stellt. Nach § 7 BV 2015 gelten „im Übrigen … die Vereinbarungen der … ICT-RBV 02/2010 entsprechend“.

Die Arbeitgeberin leitete im Herbst 2017 eine interne Untersuchung zur Klärung strafrechtlich relevanter Vorwürfe u.a. gegen einen ihrer damaligen Geschäftsführer ein. Die Ermittlungen wurden von einer Wirtschaftsprüfungsgesellschaft und einer Rechtsanwaltskanzlei unterstützt. Im Rahmen der Untersuchung überprüfte die Arbeitgeberin die E-Mail-Postfächer des Geschäftsführers, verschiedener leitender Angestellter und weiterer Arbeitnehmer, sicherte E-Mails – um deren Löschung zu verhindern – und leitete sie zum Zwecke der Auswertung an die Wirtschaftsprüfungsgesellschaft und die Rechtsanwaltskanzlei weiter.

Der Betriebsrat hat die Ansicht vertreten, ihm habe bei der Auswertung, Sicherung und Weiterleitung des E-Mail-Verkehrs der Arbeitnehmer ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG zugestanden. Dieses habe er weder durch die BV 2010 noch durch die BV 2015 abschließend ausgeübt. Zur – ggf. noch nachträglichen – Ausübung dieses Mitbestimmungsrechts, zumindest aber für die Geltendmachung von Beseitigungsansprüchen wegen dessen Verletzung benötige er die Namen der betroffenen Arbeitnehmer sowie den Grund für die Überprüfung ihrer E-Mails. Auch § 12 BV 2010 stütze sein Auskunftsbegehren. Die Arbeitgeberin sei zudem verpflichtet, den durch die Weiterleitung von personenbezogenen Daten der Arbeitnehmer an die beiden beauftragten Firmen entstandenen, mitbestimmungswidrigen Zustand zu beseitigen und künftig die Auswertung von E-Mails der Arbeitnehmer sowie ihre Speicherung oder Weiterleitung an Dritte zu unterlassen.

Die Arbeitgeberin hat beantragt, die Anträge abzuweisen.

Das Arbeitsgericht hat den Anträgen stattgegeben. Das Landesarbeitsgericht hat auf die Beschwerde der Arbeitgeberin – unter ihrer Zurückweisung im Übrigen – den Antrag zu 2. abgewiesen. Mit ihren Rechtsbeschwerden verfolgen die Beteiligten ihre jeweiligen Begehren weiter.

Aus den Gründen:

B. Die Rechtsbeschwerde der Arbeitgeberin ist begründet, die Rechtsbeschwerde des Betriebsrats hingegen unbegründet. Anders als vom Landesarbeitsgericht angenommen, bleiben alle Anträge des Betriebsrats erfolglos.

I. Die Rechtsbeschwerde der Arbeitgeberin hat Erfolg.

1. Die Zulässigkeit der von der Arbeitgeberin gegen den antragstattgebenden Beschluss des Arbeitsgerichts erhobenen Beschwerde – die vom Senat als Verfahrensfortführungsvoraussetzung von Amts wegen zu prüfen ist (vgl. BAG 20. März 2018 – 1 ABR 50/16 – Rn. 8) – begegnet keinen Bedenken…

a) Das Unterrichtungsverlangen ist – nach gebotener Auslegung – zulässig.

aa) Wie der Antragswortlaut sowie das Vorbringen des Betriebsrats zeigen, begehrt der Betriebsrat nicht nur die Mitteilung der Namen derjenigen Arbeitnehmer, deren Exchange-Postfächer von der Arbeitgeberin in der ab November 2017 bei ihr begonnenen internen Untersuchung zur Klärung etwaiger strafrechtlicher Handlungen durch ihren ehemaligen Geschäftsführer überprüft, gesichert und ausgewertet oder von ihr gesichert und an die beauftragte Wirtschaftsprüfungsgesellschaft oder die Rechtsanwaltskanzlei übermittelt wurden. Vielmehr möchte er die Namen von allen Arbeitnehmern – ausgenommen der leitenden Angestellten – wissen, deren elektronischer Schriftverkehr von einer der im Antrag beschriebenen Behandlung durch die Arbeitgeberin betroffen war, unabhängig davon, ob die Beschäftigten die betroffene E-Mail selbst versandt haben oder lediglich ihr Empfänger (ggf. auch nur im Rahmen eines offenen oder verdeckten Verteilers) waren. Unerheblich ist auch, ob sich der elektronische Schriftverkehr der Arbeitnehmer im E-Mail-Account des ehemaligen Geschäftsführers, eines leitenden Angestellten oder eines anderen Arbeitnehmers befand. Entscheidend ist lediglich, dass die Arbeitgeberin im Rahmen der internen Untersuchung über die Vorwürfe gegen ihren früheren Geschäftsführer mit einer von einem Arbeitnehmer verschickten oder an ihn gesendeten E-Mail wie im Antrag zu 1. umschrieben verfahren ist. Nach dem Vortrag des Betriebsrats ist dies der Fall, wenn die Arbeitgeberin die betreffende E-Mail selbst „überprüft“ – also inhaltlich zur Kenntnis genommen –, „ausgewertet“, d.h. ihren Inhalt auf eine Relevanz für die zu untersuchenden Vorfälle geprüft, und „gesichert“, mithin – in welcher Form auch immer – auf ein anderes Speichermedium oder an einen anderen Speicherort übertragen hat. Daneben genügt es auch, wenn die Arbeitgeberin die betroffene E-Mail lediglich gesichert und zum Zwecke der Auswertung an die von ihr bei der Ermittlung hinzugezogene – im Antrag namentlich benannte – Wirtschaftsprüfungsgesellschaft oder die Rechtsanwaltskanzlei weitergeleitet hat.

bb) Darüber hinaus möchte der Betriebsrat für jeden der Arbeitnehmer, deren elektronischer Schriftverkehr wie im Antrag bezeichnet behandelt wurde, erfahren, aus welchem Grund dies erfolgt ist. Wie das Landesarbeitsgericht zutreffend – und vom Betriebsrat unwidersprochen – angenommen hat, zielt dieses Begehren nicht darauf ab, die tatsächlichen Umstände zu erfahren, aus denen sich ein etwaiger Verdacht auf eine Straftat ergeben haben könnte, sondern nur den „Anlass“, der dazu geführt hat, dass die E-Mail von der Arbeitgeberin überprüft, ausgewertet und gesichert oder von ihr gesichert und an die mit der begleitenden Ermittlung beauftragte Wirtschaftsprüfungsgesellschaft oder die entsprechend beauftragte Rechtsanwaltskanzlei übermittelt wurde. Diesem Auskunftsverlangen ist daher bereits dann Genüge getan, wenn die Arbeitgeberin angibt, ob gegen den betreffenden Arbeitnehmer ein Anfangsverdacht bestand oder sich die auf ihn beziehende E-Mail im Postfach eines verdächtigten Mitarbeiters befand.

cc) Mit diesem Inhalt ist der Antrag zu 1. zulässig, insbesondere hinreichend bestimmt i.S.v. § 253 Abs. 2 Nr. 2 ZPO…

b) Der Antrag zu 1. ist erfolglos. Die Arbeitgeberin ist nicht verpflichtet, die streitbefangenen Auskünfte zu erteilen.

aa) Die vom Betriebsrat geltend gemachten Aufgaben tragen keinen Anspruch nach § 80 Abs. 2 Satz 1 Halbs. 1 BetrVG auf die begehrten Informationen.

(1) Nach dieser Norm hat der Arbeitgeber den Betriebsrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten. Hieraus folgt ein entsprechender Anspruch des Betriebsrats, soweit die begehrte Information zur Aufgabenwahrnehmung erforderlich ist. Anspruchsvoraussetzung ist damit zum einen, dass

überhaupt eine Aufgabe des Betriebsrats gegeben ist, und zum anderen, dass im Einzelfall die begehrte Information zur Wahrnehmung der Aufgabe erforderlich ist. Dies hat der Betriebsrat darzulegen (BAG 12. März 2019 – 1 ABR 48/17 – Rn. 23 m.w.n., BAGE 166, 98). Erst anhand dieser Angaben können der Arbeitgeber und im Streitfall das Arbeitsgericht prüfen, ob die Voraussetzungen einer Auskunftspflicht sowie eines damit korrespondierenden Auskunftsanspruchs vorliegen. Ein allgemein gehaltener Hinweis des Betriebsrats auf seine gesetzlichen Aufgaben unter Wiederholung des Gesetzeswortlauts ist nicht ausreichend. Stützt sich der Betriebsrat auf eine Überwachungsaufgabe nach § 80 Abs. 1 Nr. 1 BetrVG muss er die konkrete normative Vorgabe, deren Durchführung er überwachen will und die sein Auskunftsverlangen tragen soll, aufzeigen. Dies gilt insbesondere, wenn er sich auf ein normativ geltendes Regelwerk mit mehreren und unterschiedlichen (Schutz-)Bestimmungen zugunsten der Arbeitnehmer bezieht. Es ist nicht Aufgabe des Gerichts, ohne solche Angaben von Amts wegen zu prüfen, welche Aufgaben den Auskunftsanspruch stützen und aus welchen Gründen die verlangte Information für die Durchführung dieser Aufgabe benötigt werden könnte (vgl. BAG 9. April 2019 – 1 ABR 51/17 – Rn. 12 f. m.w.N., BAGE 166, 269).

(2) Ausgehend hiervon kann sich der Betriebsrat für sein Auskunftsbegehren nicht auf seine nach § 80 Abs. 1 Nr. 1 BetrVG bestehende Aufgabe berufen, die Einhaltung des § 26 Abs. 1 Satz 2 BDSG zu überwachen.

(a) Der Betriebsrat hat geltend gemacht, er müsse die Beachtung der datenschutzrechtlichen Vorgaben für die Rechtmäßigkeit der Verarbeitung von Beschäftigtendaten zum Zwecke der Aufdeckung von Straftaten nach § 26 Abs. 1 Satz 2 BDSG überprüfen. Damit hat er eine für sein Unterrichtungsverlangen nach § 80 Abs. 2 Satz 1 Halbs. 1 BetrVG benötigte Überwachungsaufgabe i.S.v. § 80 Abs. 1 Nr. 1 BetrVG konkret aufgezeigt. Bei § 26 Abs. 1 Satz 2 BDSG handelt es sich um eine zugunsten der Arbeitnehmer geltende gesetzliche Vorschrift (vgl. schon BAG 17. März 1987 – 1 ABR 59/85 – zu B II 2 der Gründe, BAGE 54, 278). Soweit der Betriebsrat ergänzend auch die seit dem 25. Mai 2018 geltende Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DS-GVO) angeführt hat, ermöglicht dieser Verweis – sollte ihm denn ein eigenständig weitergehender Inhalt zukommen – hingegen keine Prüfung, welche der dort vorgesehenen Schutzbestimmungen zugunsten der Arbeitnehmer er hinsichtlich ihrer Durchführung oder Einhaltung zu überwachen beabsichtigt.

(b) Die vom Betriebsrat begehrten Auskünfte sind aber nicht erforderlich i.S.v. § 80 Abs. 2 Satz 1 Halbs. 1 BetrVG, um die Einhaltung des § 26 Abs. 1 Satz 2 BDSG zu überprüfen.

(aa) Ausweislich der Gesetzesbegründung regelt § 26 Abs. 1 BDSG – ebenso wie der bis zum 24. Mai 2018 geltende § 32 Abs. 1 BDSG (aF) –, zu welchen Zwecken und unter welchen Voraussetzungen personenbezogene Daten im Beschäftigungsverhältnis verarbeitet werden können, wenn dies zum „Zweck des Beschäftigungsverhältnisses" erfolgt, wobei Satz 2 die Voraussetzungen für die Verarbeitung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten, die im Beschäftigungsverhältnis begangen worden sind, normiert (vgl. BT-Drs. 18/11325 S. 97). Danach dürfen personenbezogene Daten von Beschäftigten zur Aufdeckung von Straftaten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. § 26 Abs. 1 Satz 2 BDSG erfordert – wie seine inhaltsgleiche Vorgängerregelung in § 32 Abs. 1 Satz 2 BDSG aF – trotz des insoweit missverständlichen Wortlauts der Norm („dass die betroffene Person … eine Straftat begangen hat") nicht, dass von einer auf ihrer Grundlage vorgenommenen Kontrollmaßnahme ausschließlich Arbeitnehmer betroffen sein können, hinsichtlich derer es bereits einen konkretisierten Verdacht gibt. Der Kreis der Verdächtigen muss zwar möglichst eingegrenzt sein; es ist aber nicht zwingend notwendig, die Maßnahme in einer Weise zu beschränken, dass von ihr ausschließlich Personen erfasst werden, bezüglich derer bereits ein konkretisierter Verdacht besteht (vgl. zu § 32 Abs. 1 Satz 2 BDSG aF BAG 22. September 2016 – 2 AZR 848/15 – Rn. 30, BAGE 156, 370).

(bb) Für die Einhaltung der Voraussetzungen des § 26 Abs. 1 Satz 2 BDSG kommt es damit nicht darauf an, wie die Arbeitnehmer, die von einer zum Zwecke der Strafverfolgung erfolgten Datenverarbeitung der Arbeitgeberin betroffen sind, heißen. Auch die vom Betriebsrat erstrebte Auskunft, aus welchem Grund die E-Mails der Arbeitnehmer wie im Antrag zu 1. beschrieben behandelt wurden, ist nicht geeignet – und daher auch nicht erforderlich –, um festzustellen, ob die Arbeitgeberin die Vorgaben dieser Norm beachtet hat. Mit der bloßen Angabe, ob es gegen den betroffenen Arbeitnehmer einen gegen ihn gerichteten Verdacht gab oder sich eine auf ihn bezogene E-Mail im Postfach eines verdächtigten Mitarbeiters befand, kann der Betriebsrat weder erkennen, ob – und ggf. welche, von der Arbeitgeberin dokumentierte – tatsächliche Anhaltspunkte einen Anfangsverdacht (vgl. dazu BAG 20. Oktober 2016 – 2 AZR 395/15 – Rn. 25, BAGE 157, 69) für eine Straftat begründet haben, noch, ob die von ihr durchgeführte Datenverarbeitung zu deren Aufdeckung erforderlich und im Hinblick auf die schutzwürdigen Interessen der hiervon betroffenen Arbeitnehmer geeignet sowie angemessen war.

(3) Der Betriebsrat vermag sein Unterrichtungsverlangen nach § 80 Abs. 2 Satz 1 Halbs. 1 BetrVG auch nicht auf ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG zu stützen.

(a) Soweit er vorbringt, er benötige die Auskünfte zur Prüfung eines ihm bei der Kontrolle und der Auswertung des E-Mail-Verkehrs der Arbeitnehmer zustehenden Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG, kann vorliegend dahinstehen, ob eine solche Aufgabe des Betriebsrats (noch) besteht. Denn jedenfalls erschließt sich nicht, wieso er die mit dem Unterrichtungsverlangen geforderten Informationen für die Vorbereitung einer – ggf. „nachträglichen" – Ausübung seines Mitbestimmungsrechts benötigt. Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG knüpft an die Einführung und Anwendung von technischen Einrichtungen an, die geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Die vom Betriebsrat verlangten Auskünfte beziehen sich weder auf die technischen Einzelheiten einer von der Arbeitgeberin angewendeten Überwachungseinrichtung noch auf das konkrete technische Vorgehen der Arbeitgeberin bei der Überprüfung, Speicherung und Sicherung des elektronischen Schriftverkehrs der Arbeitnehmer. Es ist weder ersichtlich noch dargetan, welchen Erkenntnisgewinn sich der Betriebsrat aus den Namen der von der E-Mail-Auswertung betroffenen Arbeitnehmer und aus der Angabe, warum ihr elektronischer Schriftverkehr Gegenstand der im Antrag zu 1. beschriebenen Behandlung durch die Arbeitgeberin war, für die Ausübung seines – von ihm ohnehin schon angenommenen – Mitbestimmungsrechts verspricht.

(b) Entsprechendes gilt, soweit der Betriebsrat sich darauf beruft, er benötige die begehrten Informationen, um Beseitigungsansprüche wegen Verletzung seines Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG geltend zu machen.

Rechtsweg im Konkurrentenstreit um ein öffentliches Amt (Ls)

(**Bundesverwaltungsgericht**, Beschluss vom 17. März 2021 – 2 B 3.21 –)

1. **Der von der Rechtsprechung aus Art. 33 Abs. 2 GG entwickelte Bewerbungsverfahrensanspruch ist weder von vornherein öffentlich-rechtlich noch bürgerlich-rechtlich zu verorten.**
2. **Die Gerichte für Arbeitssachen sind für Konkurrentenstreitverfahren zuständig, bei denen sich allein Arbeitnehmer und Selbstständige um die Besetzung einer Stelle im Arbeitsverhältnis des öffentlichen Dienstes bewerben.**
3. **Der Bewerbungsverfahrensanspruch aus Art. 33 Abs. 2 GG hat – für alle Mitbewerber – einen einheitlichen öffentlich-rechtlichen Charakter i.S.v. § 40 Abs. 1 Satz 1 VwGO, wenn entweder ein Beamter um Rechtsschutz nachsucht (unabhängig davon, ob die Stelle als Statusamt oder nach Tarifvertrag besetzt werden soll) oder wenn sich ein – auch nicht beamteter – Mitbewerber gegen die Auswahlentscheidung zugunsten eines Beamten wendet.**

Anspruch eines fristlos gekündigten Personalratsmitglieds auf Erlass einer einstweiligen Verfügung zwecks Gestattung bzw. Duldung der weiteren Amtsausübung (Ls)

(**Bundesverwaltungsgericht**, Beschluss vom 4. Februar 2021 – BVerwG 5 VR 1.20 –)

1. **Ein dem Personalrat angehörender Arbeitnehmer, der nach der außerordentlichen Kündigung seines Arbeitsverhältnisses ein Kündigungsschutzverfahren einleitet, darf in der Ausübung seines Personalratsamtes nicht behindert werden, wenn die angegriffene Kündigung offensichtlich unwirksam ist.**
2. **Bei nicht offensichtlicher Unwirksamkeit der Kündigung ist das außerordentlich gekündigte Personalratsmitglied grundsätzlich aus rechtlichen Gründen im Sinne des § 31 Abs. 1 Satz 2 BPersVG an der Ausübung seines Amtes verhindert.**
3. **Eine offensichtlich unwirksame Kündigung liegt vor, wenn sich schon aus dem eigenen Vortrag des Arbeitgebers ohne Beweiserhebung und, ohne dass ein Beurteilungsspielraum gegeben wäre, jedem Kundigen die Unwirksamkeit der Kündigung geradezu aufdrängen muss. Die Unwirksamkeit der Kündigung muss also ohne jeden vernünftigen Zweifel in rechtlicher und tatsächlicher Hinsicht offen zu Tage liegen.**

Zur Ausrüstung des Betriebsrats mit Videokonferenztechnik (Ls)

(**Landesarbeitsgericht Berlin-Brandenburg**, Urteil vom 14. April 2021 – 15 TaBVGa 401/21 –)

Der Arbeitgeber hat dem Betriebsrat eine technische Ausstattung zur Verfügung zu stellen, die diesem die Durchführung von Sitzungen und Beratungen in Form einer Videokonferenz ermöglicht. Es handelt sich um erforderliche Informationstechnik, die der Arbeitgeber nach § 40 Abs. 2 Betriebsverfassungsgesetz zur Verfügung stellen muss, um der Mitarbeitervertretung dieses gesetzlich zulässige Beschlussfassungsverfahren zu ermöglichen.

(Nicht amtlicher Leitsatz)

Zur Zulässigkeit videobeochteter Klausuren wegen Corona (I) (Ls)

(**Oberverwaltungsgericht Nordrhein-Westfalen**, Beschluss vom 4. März 2021 – 14 B 278/21 –)

Die in der Corona-Prüfungsordnung der Fernuniversität Hagen als Alternative vorgesehene Möglichkeit, neben Präsenzprüfungen, die zurzeit nicht durchgeführt werden, videobeaufsichtigte häusliche Klausurprüfungen durchzuführen, ist nach Datenschutz-Grundverordnung eine Datenverarbeitung, die zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist, da die Aufzeichnung und vorübergehende Speicherung im Hinblick darauf, die teilnehmenden Prüflinge von Täuschungsversuchen abzuhalten, und im Hinblick auf ein sich im Verlauf der Prüfung ergebendes Bedürfnis nach Beweissicherung in der Sphäre des Prüflings, auch trotz einer vom Prüfling geltend gemachten Störung des ordnungsgemäßen Prüfungsablaufs, geeignet und erforderlich ist.

(Nicht amtlicher Leitsatz)

Eignung einer audio-visuellen Übertragung (Videoaufsicht) zur Vermeidung von Täuschungsversuchen bei Prüfungen (Ls)

(**Oberverwaltungsgericht Schleswig-Holstein**, Beschluss vom 3. März 2021 – 3 MR 7/21 –)

1. **Dem Rechtsschutzsuchenden fehlt das Rechtsschutzinteresse, wenn er seine Rechtsstellung mit der begehrten gerichtlichen Entscheidung derzeit nicht verbessern kann.**
2. **Eine audio-visuelle Übertragung (Videoaufsicht) ist zur Vermeidung von Täuschungsversuchen bei Prüfungen geeignet gemäß nachstehendem § 7 – 2021 der Corona-**

Ergänzungssatzung Elektronische Prüfungen und zur Prüfungsaufsicht bei elektronischen Prüfungen gestattet.

Prüfungsaufsicht bei elektronischen Prüfungen

(1) Zur Unterbindung von Täuschungshandlungen während einer elektronischen Prüfung können die Studierenden verpflichtet werden, die Kamera- und Mikrofonfunktion der zur Prüfung eingesetzten Kommunikationseinrichtungen zu aktivieren (Videoaufsicht). Die Videoaufsicht ist im Übrigen so einzurichten, dass der Persönlichkeitsschutz und die Privatsphäre der Betroffenen nicht mehr, als zu den berechtigten Kontrollzwecken erforderlich, eingeschränkt werden.

(2) Die Videoaufsicht erfolgt durch Aufsichtspersonal der Hochschule. Eine automatisierte Auswertung von Bild- oder Tondaten der Videoaufsicht ist unzulässig.

(3) Eine Aufzeichnung der Prüfung oder anderweitige Speicherung der Bild- oder Tondaten ist nicht zulässig. § 6 Abs. 2 Satz 2 gilt entsprechend.

(4) Der Ablauf und die wesentlichen Inhalte der elektronischen Prüfung werden von einer prüfenden oder beisitzenden Person protokolliert.

Anmerkung von Rechtsanwalt Dr. Felix Neumann, M.A.*

Elektronische Fernprüfungen haben sich in der Coronapandemie als Möglichkeit erwiesen, den Prüfungsbetrieb aufrecht zu erhalten. Um die Chancengleichheit zu gewährleisten, werden diese Onlineklausuren regelmäßig durch eine audiovisuelle Prüfungsaufsicht flankiert, die jedoch eine Vielzahl datenschutzrechtlicher Fragen aufwirft. Vorliegend entschied das Oberverwaltungsgericht Schleswig, dass eine solche Videoaufsicht unter bestimmten Voraussetzungen verhältnismäßig ist.

Der Antragsteller, ordentlich immatrikulierter Student der Antragsgegnerin im 3. Fachsemester, wendet sich gegen die in § 7 der Satzung der Christian-Albrechts-Universität zu Kiel zur Ergänzung der Corona-Satzung Studien- und Prüfungswesen – 2020 zur Durchführung elektronischer Prüfungen – 2021 (Corona-Ergänzungssatzung Elektronische Prüfungen – 2021) enthaltene, Regelung zur Prüfungsaufsicht bei elektronischen Prüfungen.

I. Hintergrund

Der vorliegende Beschluss des OVG Schleswig fügt sich in eine Reihe erster Eilentscheidungen der Verwaltungsgerichtsbarkeit rund um die Thematik von Onlineklausuren ein, die eine Vielzahl von Rechtsfragen aufwerfen.[1] Der Kern des vorliegenden Verfahrens bildete die Frage der datenschutzrechtlichen Zulässigkeit einer audiovisuellen Prüfungsaufsicht. Das Spannungsfeld wurde dabei einerseits determiniert durch das Recht auf Chancengleichheit, die Vermeidung von Täuschungsversuchen und die Aufrechterhaltung des Prüfungsbetriebs (Art. 3 Abs. 1, 12 Abs. 1 GG). Andererseits stehen diesen Geboten das Recht auf informationelle Selbstbestimmung bzw. auf Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG), der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO) und das Recht auf Unverletzlichkeit der Wohnung (Art. 13 GG) gegenüber.

Um sich dieser Thematik zu nähern, sind grundsätzlich drei Eingriffsstufen audiovisueller Prüfungsaufsicht voneinander zu unterscheiden.[2] Nur geringe Eingriffe bestehen bei solchen Maßnahmen, die keine Echtzeitüberwachung des Prüflings, sondern lediglich die Identifizierung auf einer Prüfungsmaske vorschreiben und gleichzeitig technische Möglichkeiten integrieren, die es verhindern, dass weitere Bildschirme oder Zwischenablagen auf dem Computer geöffnet werden können. Die zweite Stufe, die auch Gegenstand der hier besprochenen Entscheidung ist, wird geprägt durch eine dauerhafte audiovisuelle Überwachung der Studierenden, die auch Einblicke in die privaten Wohnräume ermöglicht. Diese zweite Eingriffsschwelle (sog. menschliches Proctoring) unterscheidet von der dritten Stufe (sog. automatisiertes Proctoring) dadurch, dass eine menschliche Aufsichtsperson durch Zuschaltung des Mikrophones bzw. der Computerkamera – regelmäßig durch Verwendung eines Onlinekonferenzprogramms – die Aufsicht durchführt. Bei der dritten Stufe ersetzen hingegen vollautomatische Programme die menschliche Kontrolle. Während die erste Stufe regelmäßig zulässig und die letztere Überwachungsvariante grundsätzlich unzulässig ist, kommt es bei der mittleren Eingriffsschwelle entscheidend auf deren Ausgestaltung und die datenschutzrechtlichen Flankierungen im Einzelfall an.

Dabei können folgende Maßstäbe einen Ausschlag zugunsten einer Zulässigkeit gegeben: Von einer Konformität ist umso eher auszugehen, je stärker die Onlineüberwachung den bei Präsenzklausuren eingesetzten Methoden ähnelt.[3] Wenn das in der Onlineklausur verwendete Programm keine weiteren, nicht notwendigen Datenmaßnahmen durchführt, wie bspw. ein Auslesen der Browserhistorie, so schlägt ebenso dies ebenfalls zugunsten der Prüfungsaufsicht aus.[4] Gleichzeitig sollte eine Vor-Ort-Prüfung nach Möglichkeit angeboten werden, keine Aufzeichnung der Prüfung oder eine Übermittlung der Daten an Dritte erfolgen und die Bildschirm- bzw. Raumüberwachung nur soweit erfolgen, wie es zwingend für das jeweilige Prüfungsformat erforderlich ist.[5]

II. Bewertung

Gemessen an diesen abstrakten Kriterien ist der Eilentscheidung des Gerichts in Bezug auf die grundrechtliche Abwägungsentscheidung prinzipiell zuzustimmen.

Die Verordnung verbietet nämlich eine automatisierte Auswertung der erzeugten Bild- oder Tondaten. Die Aufsicht erfolgt nur durch das Hochschulpersonal mittels der Kamera- und Mikrophonfunktion und ist somit vergleichbar mit der Eingriffsintensität einer Präsenzprüfung bzw. der Teilnahme an einem Onlinemeeting. Auch die Aufzeichnung der Prüfung oder anderweitige Speicherung der Bild- oder Tondaten ist nach der Verordnung nicht zulässig, wodurch insbesondere dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c) DS-GVO Genüge getan wird.

Ebenso spricht für die datenschutzrechtliche Konformität der Verordnung, dass die Teilnahme nach § 9 Abs. 1 Corona-Ergänzungssatzung i.S.v. Art. 6 Abs. 1 S. 1 lit. a) DS-GVO freiwillig ist, denn es sollen nach Möglichkeit nichtelektronische Klausuren im gleichen Zeitraum angeboten werden, sodass die Satzung tatsächlich rechtskreiserweiternd wirkt. Hiergegen kann auch nicht eingewandt werden, dass die Einwilligung wegen des Machtgefälles zwischen den Studierenden und der Universität prinzipiell auszuschließen ist, denn eine solche Auslegung ist dem Wortlaut des Erwägungsgrunds Nr. 43 DS-GVO nicht zu entnehmen.[6]

Im Rahmen des Hauptsacheverfahrens sollte das Gericht jedoch die Gültigkeit der Rechtsgrundlage stärker in den Blick nehmen. Die indirekte Argumentation des Gerichts, dass Onli-neprüfungen keinen so starken Grundrechtseingriff darstellen, dass diese nicht im Rahmen eines förmlichen Gesetzes, sondern ohne dezidierte Vorgaben in einer Hochschulsatzung geregelt werden können, überzeugt nicht. Elektronische Klausuren finden nämlich nicht an einem neutralen Ort, sondern in der eigenen Wohnung statt.[7] Auch die überwiegende Anzahl der Bundesländer hat dies bereits anders entschieden und explizite formellgesetzliche Regelungen für Onlineprüfungen geschaffen.[8]

Fraglich ist zudem, ob es wirklich im vorliegenden Fall einer Eilentscheidung des Präsidiums bedurfte und die Regelungen zur elektronischen Prüfung nicht durch den Senat, wie von § 5 Abs. 1 S. 3 Corona-HEVO i.V.m. §§ 21 Abs. 1 S. 3 Nr. 2, 22 Abs. 8 S. 1 HSG vorgesehen, hätten etabliert werden müssen.[9] Inwieweit ein feststehender Prüfungszeitraum bzw. eine seit einem Jahr bestehende Pan-

demielage nicht vorhersehbar und planbar, sondern eilbedürftig waren, erschließt sich einem Außenstehenden nicht.

Auch die mit diesem Punkt verbundene Frage, dass die Universität eine Onlineklausur ohne Überwachung beim Erlass der angegriffenen Norm nicht gewollt habe, weshalb das Gericht bereits die Zulässigkeit des Eilantrags vereinte, bedarf einer weiteren Prüfung in der Hauptsache. Alternative Prüfungsmodelle, wie z.B. Open-Book-Klausuren, können abhängig vom didaktischen Ziel im jeweiligen Fach, eine sinnvolle Alternative ohne Überwachung darstellen.[10]

Vage bleibt die Verordnung, ebenso wie die ihr in vielen Punkten identische Bayerische Fernprüfungserprobungsverordnung, in Bezug auf konkrete Vorgaben, wie der Persönlichkeitsschutz und die Privatsphäre der Betroffenen nicht mehr als zu den berechtigten Kontrollzwecken eingeschränkt werden soll.[11]

III. Praxisfolgen

Mit dieser Eilentscheidung sind die Fragen des Verfahrens nicht abschließend geklärt, denn die Hauptsacheentscheidung steht noch aus, in der mit einer tiefgreifender Prüfung der Rechtsprobleme zu rechnen ist. Zudem werden trotz der aktuell fortschreitenden Impfkampagne die Rechtsfragen rund um die Onlineprüfungen nicht verschwinden. Durch den Vorteil der zeitlichen und räumlichen Flexibilität ist vielmehr zukünftig mit einer Mischung aus Präsenz- und Digitalprüfungen zu rechnen. Ebenso haben die Datenschutzbehörden begonnen, sich des Themas anzunehmen, und haben erste Fragebögen an die Hochschulen versandt. Diesen Schreiben war zu entnehmen, dass die Behörden insgesamt strenge Maßstäbe an Online-prüfungsformate anlegen und mit den Hochschulen sowie Wissenschaftsministerien im Gespräch darüber bleiben werden, wie elektronische Prüfungen datenschutzkonform durchgeführt werden können.[12]

Die Länder wären folglich gut beraten, ihre Hochschulgesetzte nun umfassend zu überarbeiten und detailreichere sowie einheitliche Vorgaben für alle Hochschulen zu schaffen. Insbesondere sollte geregelt werden, das digitale Prüfungsformate, die zu einer automatisierten Überwachung führen, Daten dauerhaft speichern bzw. an Dritte übermitteln, nicht zulässig sind. Auch dürfte eine umfassendere Aufklärung sowie Einbindung der Prüflinge zu mehr Akzeptanz beitragen.[13] So sollten einerseits die Aufsichtspersonen datenschutzrechtlich geschult werden, wie Persönlichkeitseingriffe vermieden werden können. Andererseits sollte eine Sensibilisierung der Studieren stattfinden, wie diese ihre persönlichen Daten und Räume schützen können. Einen Beitrag im Rahmen einer solchen Aufklärung bei Onlineklausuren könnten speziell gestaltete Datenschutzerklärungen leisten.[14] Aus der datenschutzrechtlichen Perspektive wäre es zudem zu begrüßen, wenn die Hochschulen langfristig eigene Plattformen und Programme entwickeln würden, anstatt auf kommerzielle Anbieter zurückzugreifen, die sich ihre vermeintlichen kostenfreien Produkte mit der Preisgabe der Daten bezahlen lassen.

Letztendlich kommt es entscheidend auf den konkreten Abwägungsvorgang und den Ausgleich der widerstreitenden Grundrechte an, sodass die Aussage des rheinland-pfälzischen Landesdatenschutzbeauftragten auch nach der Pandemie seine Gültigkeit behalten wird: „[Das] Datenschutzrecht gilt, aber seine Anwendung in Zeiten der Pandemie ist mit Augenmaß und Fingerspitzengefühl zu gewährleisten."[15]

* Der Autor ist Rechtsanwalt in der Kanzlei SchulteRiesenkampff in Frankfurt am Main.

1 OVG Münster, Beschl. v. 04.03.2021 – 14 B 2781/21.NE, NJW 2021, 1414 ff.; OVG Lüneburg, Beschl. v. 02.09.2020 – 2 ME 349/20, NVwZ-RR 2021, 58 ff.; VG Frankfurt (Oder), Beschl. v. 11.05.2021 – VG 1 L 124/21, BeckRS 2021, 11914; VG Leipzig, Beschl. v. 02.02.2021 – 7 L 41/21, BeckRS 2021, 1093.

2 Zu diesen Stufen: Albrecht/Grath/Uphues, ZD 2021, 80, 80.

3 Albrecht/Grath/Uphues, ZD 2021, 80, 81.

4 LfDI Baden-Württemberg, Pressemitteilung v. 14.04.2021, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/04/20210414_PM_Proctoring.pdf, abgerufen am 31. Mai 2021.

5 Albrecht/Grath/Uphues, ZD 2021, 80 ff.; Birnbaum, NJW 2021, 1356 ff.; LfDI Baden-Württemberg (Fn. 4); Roßnagel, ZD 2020, 296, 299; Sandberger, OdW 2020, 155, 159 ff.

6 Albrecht/Grath/Uphues, ZD 2021, 80, 82; Fehling, OdW 2020, 137, 146 f.; a. A.: Birnbaum, NJW 2021, 1356, 1357; Ernst, ZD 2017, 110, 111 f. Diff. Hoeren, Gutachten zur datenschutzrechtlichen Zulässigkeit von Überwachungsfunktionen bei Online-Klausuren, https://www.itm.nrw/wp-content/uploads/RiDHnrw_11.06.20_Gutachten-zur-datenschutzrechtlichen-Zulässigkeit-von-Überwachungsfunktionen-bei-Online-Klausuren.pdf, abgerufen am 31.05.2021.

7 Ebenso: Birnbaum, NJW 2021, 1356, 1357; Botta, Grundrechtseingriffe durch Online-Proctoring, https://verfassungsblog.de/grundrechtseingriffe-durch-online-proctoring/, abgerufen am 31. Mai 2021; Fischer/Dietrich, NVwZ 2020, 657, 661; Sandberger, OdW 2020, 155, 161; a. A.: Albrecht/Grath/Uphues, ZD 2021, 80, 82.

8 Hierzu: Birnbaum, NJW 2021, 1356, 1357.

9 Birnbaum, NJW 2021, 1356, 1357 f.

10 Albrecht/Grath/Uphues, ZD 2021, 80, 81; Schwartmann, Hochschulen bewegen sich auf Glatteis, https://www.forschung-und-lehre.de/recht/hochschulen-bewegen-sich-auf-glatteis-3420/, abgerufen am 31.05.2021.

11 Beide Verordnungen sind abrufbar unter: https://www.uni-kiel.de/gf-praesidium/de/recht/amtl-bekannt/amtliche-bekanntmachung-2021-1/1-Corona-Ergaenzungssatzung-Elektronische-Pruefungen-2021.pdf; https://www.gesetze-bayern.de/Content/Document/BayFEV, abgerufen am 31. Mai 2021.

12 LfDI Baden-Württemberg (Fn. 4).

13 Fischer/Dietrich, NVwZ 2020, 657, 662.

14 Fehling, OdW 2020, 137, 148.

15 Kugelmann, Gesundheitsnot kennt Datenschutzgebot, https://verfassungsblog.de/gesundheitsnot-kennt-datenschutzgebot/, abgerufen am 31.05.2021.

Gezieltes Fotografieren fremder Personen in der Öffentlichkeit ist unzulässig (Ls)

(**Amtsgericht Hamburg**, Beschluss vom 3. Juli 2020 – 163/Gs656/20 –)

Ein gezieltes Fotografieren von fremden Personen ist auch dann unzulässig, wenn die Verwendung ausschließlich privaten Zwecken dienen soll.

Tätigkeit des DSB nach Art. 39 DS-GVO mit RDG vereinbar (Ls)

(**Anwaltsgerichtshof Nordrhein-Westfalen**, Beschluss vom 12. März 2021 – 1 AGH 9/19 –)

Die Tätigkeit eines Datenschutzbeauftragten i. R. d. Art. 39 DS-GVO steht nicht im Konflikt zum Rechtsdienstleistungsgesetz (RDG). Art. 39 DS-GVO umfasst ausdrücklich die Rechtsberatung im Datenschutz. Also ist diese nach § 3 RDG auf Grund Zulassung in einem anderen Gesetz zulässig. Selbst wenn dies nicht so wäre, würde dies eine zulässige Nebentätigkeit i.S.d. § 5 RDG darstellen.

(Nicht amtliche Leitsätze)

Online-Kompaktkurse im Datenschutz 2021

Datenschutzorganisation gestalten

Thema	Referent/in	Termin*
Datenschutz-Leit- und Richtlinien	Dr. Frank Fenner Thomas Müthlein	21.09.2021
Den Umgang mit Betroffenenrechten organisieren	Dr. Frank Fenner	26.10.2021
Den Umgang mit Datenschutz-Pannen organisieren	Dr. Frank Fenner	10.11.2021
Awareness schaffen – Datenschutz-Richtlinien zum Leben erwecken	Dr. Frank Fenner	07.12.2021

Praxishilfen zur Bearbeitung typischer Datenschutzfälle

Thema	Referent/in	Termin*
Hilfe, eine Betroffenenanfrage	Erida Mezini	15.09.2021 04.11.2021
Hilfe, eine Datenschutz-Panne	Philipp Lehmann	23.09.2021 02.12.2021
Kurz und kompakt: Datenschutz-Folgenabschätzung	Evelyn Seiffert	30.09.2021 14.12.2021
Best Practices: Löschen nach der DS-GVO	Sascha Kremer	07.10.2021 08.12.2021
Hilfe, ein AV-Vertrag	Pascal Longerich	25.10.2021
Geschäftsgeheimnisschutz in der Praxis: Know-how-Schutz und Synergien aus dem Datenschutz	Sascha Kremer	28.10.2021

Spezialwissen

Thema	Referent/in	Termin*
Datenschutz in der Kita	Georg Karl Bittorf	02.09.2021 01.12.2021
Datenschutz im Seniorenzentrum	Georg Karl Bittorf	09.09.2021 25.11.2021
Datenschutz und Datensicherheit bei digitalen Gesundheits-anwendungen gem. der neuen DiGA-Verordnung	Jun.-Prof. Dr. Werner Schäfke-Zell Dipl.-Inf. Marius Post	16.09.2021
Unbeabsichtigte Datenschutzverstöße im Personalbereich	Petra Eul-Löh	21.09.2021
Das „datenschutzkonforme" Produkt – Berücksichtigung datenschutzrechtlicher Anforderungen bei Produktentwicklung und Softwarebeschaffung	Dr. Sebastian Buss, LL.M.	22.09.2021
... und es hat Zoom gemacht ... Datenschutzfreundlichere Zoom-Videokonferenzen	Petra Eul-Löh	29.09.2021
IT-Sicherheit in der Arzt-Praxis	Prof. Dr. Rainer W. Gerling	30.09.2021
Sichere und datenschutzkonforme Videokonferenzen	Michael Atzert	07.10.2021
Microsoft 365/Office 365 datenschutzrechtlich bändigen	Prof. Dr. Rainer W. Gerling	13.10.2021
Datenschutz im Verein	Georg Karl Bittorf	19.10.2021

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

90 Minuten praxisgerecht aufbereitetes Datenschutzwissen

NUR 119,– €

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

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Berichte, Informationen, Sonstiges

Verliebt am Arbeitsplatz

Aus dem aktuellenTB des BdgLfDI

Eine Arzthelferin einer brandenburgischen Arztpraxis speicherte die dort hinterlegte Telefonnummer eines Patienten in ihrem Mobiltelefon und kontaktierte ihn daraufhin privat. Diese Vorgehensweise missfiel nicht nur der Ehefrau des Patienten, die von dem Chatverlauf Wind bekam. Letztendlich involvierte daraufhin der Patient die LfDI; die ein Bußgeld in dreistelliger Höhe gegen die Arzthelferin wegen der unrechtmäßigen Verarbeitung personenbezogener Daten verhängte. Der Patient hätte darin einwilligen müssen, dass die Telefonnummer, die er in der Praxis zweckbestimmt zu Behandlungszwecken hinterlegt hatte, von der Arzthelferin privat verwendet wird. Jedoch bleibt bei der Schilderung des Geschehens manche Frage offen. Wusste die Arzthelferin von der ehelichen Bindung des Patienten? Vielleicht hatte sie auch berechtigten Anlass zu einer vermuteten Einwilligung in die Kontaktaufnahme? Und was wäre, wenn sie sich – datenschutzgeschult – einer aus dem Telefonbuch entnommenen Nummer bedient hätte?

Forum Privatheit: EU-Kommission hat aus den Schwächen der DS-GVO gelernt: Entwurf der KI-Verordnung regelt Gefahren für Grundrechte deutlich konkreter

Die DS-GVO hat in Sachen Grundrechtsschutz eine Vorreiter-Rolle gespielt, viele Staaten sind mittlerweile ihrem Beispiel gefolgt. Ihre Grundsätze sind Bedingungen für eine lebenswerte, digitale Gesellschaft. Doch bisherige Rechtslücken werfen viele Fragen auf – und werden vor allem von mächtigen Datenverarbeitern, wie globalen Konzernen, ausgenutzt.

„Der größte Erfolg der Datenschutz-Grundverordnung ist, dass sie die Werte zum Ausdruck bringt, auf die sich die Mitgliedstaaten der Europäischen Union für ihren Weg in die digitale Gesellschaft geeinigt haben. Ihre Grundsätze, um die Grundrechte auf Datenschutz und Selbstbestimmung auszugestalten, sind Bedingungen für eine lebenswerte Gesellschaft“, so Alexander Roßnagel, Sprecher des Forschungsverbunds „Forum Privatheit“ Denn die DS-GVO fordere eine ausreichende Transparenz der Datenverarbeitung für die betroffenen Personen, die Bindung der Datenverarbeitung auf die Zwecke einer legitimen Datenerhebung, die Minimierung des Personenbezugs der Daten auf das zur Zweckerreichung Notwendige und die Gewährleistung von Datenschutz durch die technisch-organisatorische Gestaltung der Verarbeitungssysteme. „Damit zeigt die Verordnung einen dritten Weg der weltweiten Digitalisierung auf – zwischen der Kontrolle des Alltagslebens in China und der Datenausbeutung des kalifornischen Digitalkapitalismus“, konstatiert Roßnagel. Diesen Weg wollten mittlerweile viele Staaten der Welt mitgehen und gäben sich Datenschutzgesetze, die an der Datenschutz-Grundverordnung orientiert sind.

Die Intention war gut – doch bisher bleibt Manches hinter den Erwartungen zurück. Drei Jahre Datenschutzpraxis lassen auch Schwachstellen der Datenschutz-Grundverordnung immer deutlicher werden. Sie hat zum einen nicht zu einer einheitlichen Datenschutzpraxis in der Europäischen Union geführt: Die Abstraktheit vieler Regelungen lässt Raum für unterschiedliche Interpretationen, und die vielen Öffnungsklauseln eröffnen Spielräume für divergierende Gesetze in den Mitgliedstaaten. Hinsichtlich der Abstimmung der unabhängigen Aufsichtsbehörden hat sie komplizierte Verfahren vorgesehen, die eine einheitliche Zielsetzung und einen Kulturwandel voraussetzen, der (noch) fehlt. Zum anderen hat sie die notwendige Modernisierung des Datenschutzes angesichts der Herausforderungen von modernsten Informationstechniken wie Big Data, Internet der Dinge oder Künstlicher Intelligenz verfehlt: Sie enthält überwiegend abstrakte, technik- und risikoneutrale Regelungen, die in der Praxis nur schwer und hochumstritten zu konkretisieren sind. Beispiele hierfür sind etwa die notwendige Abwägung bei datengetriebenen Geschäftsmodellen zwischen berechtigten Interessen des Verantwortlichen und schutzwürdigen Interessen der betroffenen Person, ohne dass die Verordnung hierfür geeignete Kriterien vorgibt. Ein anderes Beispiel sind die unzähligen Streitverfahren über den Umfang des Auskunftsanspruchs. Die mangelnde Bestimmtheit vieler Regelungen der Verordnung bindet täglich Millionen von Arbeitsstunden und behindert Innovationen und Investitionen.

In Lücken, die das Recht lässt, dringt immer gesellschaftliche Macht ein. Solche Lücken werden vor allem von globalen Konzernen und anderen mächtigen Datenverarbeitern genutzt, um ihre Interessen – oft zu Lasten der betroffenen Personen – durchzusetzen. Defizite in der Gesetzgebung nachträglich auszugleichen, verursacht sehr viel Arbeit für die Aufsichtsbehörden. Fortschritte in der Datenschutzpraxis zeigen sich vor allem dort, wo der Europäische Datenschutzausschuss, die Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder oder einzelne Aufsichtsbehörden für Rechtsklarheit gesorgt haben – aber immer unter dem Risiko, dass diejenigen, die damit nicht einverstanden sind, die Gerichte anrufen. Dies hätte oft durch wenige risikoorientierte Festlegungen des Unionsgesetzgebers vermieden werden können.

„Die europäische und die deutsche Gesetzgebung sollte für künftige Digitalisierungsprojekte aus den Erfahrungen mit der Datenschutz-Grundverordnung lernen“, meint Forum Privatheit-Sprecher Alexander Roßnagel.

Dieser Wunsch scheint zumindest bei der Europäischen Kommission angekommen zu sein. In ihrem Entwurf für eine Verordnung zur Regulierung künstlicher Intelligenz hat sie die

strikte Technik- und Risikoneutralität in der Regulierung aufgegeben und regelt bereichs- und anwendungsspezifisch, wie Risiken für Grundrechte durch Künstliche Intelligenz abgewehrt werden können.

„Forum Privatheit": Pressemitteilung v. 02.06.2021

BDSG feiert 45-jähriges Jubiläum

Der BfDI Professor Ulrich Kelber erinnert zum 45-jährigen Jubiläum des Bundesdatenschutzgesetzes (BDSG) an Erfolge beim Schutz des Grundrechts auf informationelle Selbstbestimmung: „Gerade während des letzten Jahres konnten wir beobachten, dass Datenschutzgesetze sich erst recht in der Krise bewähren.

Schon als der Bundestag am 10. Juni 1976 das Bundesdatenschutzgesetz beschlossen hat, ging es darum, die Bürgerinnen und Bürger vor dem Missbrauch ihrer personenbezogenen Daten zu schützen. An soziale Netzwerke, Staatstrojaner und biometrische Videoüberwachung haben vermutlich die wenigsten Abgeordneten gedacht. Die Herausforderungen für das BDSG wachsen jedes Jahr weiter.

2017 wurde bereits die dritte Fassung des BDSG beschlossen. Dies wurde notwendig, um das Gesetz mit der seit 2018 wirksamen europäischen Datenschutz-Grundverordnung (DS-GVO) zu harmonisieren. Es ergänzt und präzisiert die DS-GVO dort, wo nationale Regelungen der EU-Staaten überlassen sind. Dazu zählen zum Beispiel die Verarbeitung von Beschäftigtendaten oder die Bestellung von Datenschutzbeauftragten. Aktuell findet eine planmäßige Evaluierung des Gesetzes statt, um weitere Anpassungen vorzunehmen."

Der BfDI äußert zum Jubiläum des Gesetzes einen Wunsch: „Es wäre schön, wenn Regierung und Parlament bei zukünftigen Anpassungen des BDSG ähnlich viel Weitsicht beweisen, wie es der Bundestag 1976 getan hat. Die Pandemie wird nicht die letzte Krise sein, in der es darauf ankommt, die Bürgerinnen und Bürger vor denen zu schützen, die ihre Geheimnisse missbrauchen wollen."

BfDI: Pressemitteilung v. 10.06.2021

22. Euroforum Datenschutzkongress

Am 19. und 20. Mai dieses Jahrs fand der 22. Euroforum Datenschutzkongress statt. Erstmals in ihrer Geschichte wurde die Veranstaltung dabei in digitaler Form durchgeführt.

Ein Themenschwerpunkt der Veranstaltung war der Drittlandtransfer personenbezogener Daten und die Konsequenzen aus der diesbezüglichen „Schrems II"-Entscheidung des Europäischen Gerichtshofs (EuGH). Den Auftakt zum Thema Drittlandtransfer bildete ein Impulsreferat von Max Schrems selbst. Mit seinen Klagen beim EuGH kippte der Datenschutzaktivist zunächst das Safe-Harbor-Abkommen und zuletzt auch dessen Nachfolger, das Privacy Shield Abkommen. Die letzterwähnte EuGH-Entscheidung hat weitreichende Konsequenzen für Drittlandtransfers, und dies nicht nur dann, wenn diese bislang aufgrund des Privacy Shield Abkommens erfolgten, sondern auch bei Einsatz der Standarddatenschutzklauseln der EU-Kommission (EU-Standardvertragsklauseln). Nach dem Urteil des EuGH reichen bei Datenübermittlungen in sog. Drittländer die Standardvertragsklauseln ohne zusätzliche Maßnahmen nicht mehr ohne Weiteres aus.

Dr. Anna Zeiter, Chief Privacy Officer eBay Inc., erklärte, dass man sich bei eBay in Europa eng an die Empfehlungen des Europäischen Datenschutzausschusses (EDSA) zum Thema „Schrems II" halten, und betonte den immensen Aufwand, der mit der Umsetzung der Vorgaben einhergehe. Die geforderte Überprüfung, ob die übermittelten Daten im Drittland einem dem EWR im Wesentlichen gleichwertigen Schutzniveau unterliegen, sei insbesondere von kleineren Stellen gar nicht leistbar, so Zeiter.

Dr. Axel Frhr. von dem Bussche, TaylorWessing, gab im Rahmen eines Forums Hinweise zur Umsetzung der „Schrems II"-Entscheidung in der Praxis und erläuterte insbesondere die einzelnen Verfahrensschritte der diesbezüglichen Empfehlungen des EDSA. Fraglich sei aus seiner Sicht, ob bei der Bewertung des Schutzniveaus im Zielland des Datentransfers (Schritt 3 der Empfehlungen des EDSA) das abstrakte oder das konkrete Risiko zugrunde zu legen sei. Während nach dem EDSA bei Bewertung des Datenschutzniveaus kein risikobasierter Ansatz gelten, vielmehr die abstrakte Gefahr im Zielland maßgeblich sein solle, verstehe er selbst die EuGH-Entscheidung so, dass eine „case to case"-Bewertung, also eine Beurteilung des konkreten Datentransfers vorzunehmen sei. Von dem Bussche empfahl Unternehmern dringend, mit der Umsetzung der „Schrems II"-Entscheidung umgehend zu beginnen und nicht zuzuwarten. Bei Erstellung des Umsetzungsplans sei zu berücksichtigen, dass es sich nicht um ein Projekt handele, dass kurzfristig abgeschlossen werden könne. Es handele sich um einen andauernden Prozess, der potenziell mehrere Jahre in Anspruch nehme.

Dr. Claus-Dieter Ulmer, Global Data Privacy Officer der Deutschen Telekom AG, stellte das Projekt GAIA-X vor. Dieses hat den Aufbau einer leistungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Dateninfrastruktur für Europa zum Ziel und wird von Vertretern aus Wirtschaft, Wissenschaft und Verwaltung aus Deutschland und Frankreich, gemeinsam mit weiteren europäischen Partnern getragen. GAIA-X werde häufig im Sinne eines europäischen Rechenzentrums fehlverstanden. Zielsetzung des Projekts sei, strukturelle Grundlagen und Standards für ein digitales Ökosystem nach europäischen Maßstäben zu schaffen. Die Datenverarbeitung solle ausschließlich in der EU bzw. im EWR erfolgen. Anbieter aus anderen Ländern dürften die Standards aber nutzen.

Neben dem Drittlandtransfer lag ein weiterer inhaltlicher Schwerpunkt des 22. Euroforum Datenschutzkongresses auf der Bedeutung des Datenschutzes in Zeiten beschleunigter Digitalisierung. Sowohl der Auftaktvortrag von

Prof. Dr. Johannes Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, am ersten Veranstaltungstag als auch der Vortrag von Prof. Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, am zweiten Veranstaltungstag befassten sich mit dieser Thematik. Als „Sauerteig in der Digitalisierungsbäckerei" bezeichnete Kelber in diesem Zusammenhang den Datenschutz und kritisierte scharf die aus seiner Sicht aktuell sichtbare Tendenz, ohne jegliche belastbare Belege den Datenschutz als Hindernis bei der Pandemiebekämpfung zu verunglimpfen. Als „Innovationstreiber" bewertete Jutta Löwe, Group Data Protection Officer, Brenntag Holding, den Datenschutz. Als Beispiel nennt sie die Einführung eines durchgehend digitalen Einkaufsprozesses von Gefahrstoffen mittels Einsatzes von eSignaturen anstelle von mit diversen Datenschutzimplikationen verbundenen Ausweiskopien.

Marit Hansen, LfD Schleswig-Holstein, berichtete über den aktuellen Stand des Verfahrens zum Erlass einer ePrivacy Verordnung. Diese fast unendliche Geschichte sei nunmehr doch noch in die nächste Runde gelangt, indem sich der EU-Ministerrat nach langer Zeit im Februar auf eine gemeinsame Position verständigen konnte. Damit könne jetzt das Trilogverfahren zwischen Rat, EU-Parlament und EU-Kommission beginnen. Für richtig erachtete Hansen, dass der Bundesgesetzgeber parallel zum Verfahren zum Erlass einer ePrivacy Verordnung begonnen habe, mittels der geplanten Schaffung eines Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG) das Telekommunikations- und Onlinedatenschutzrecht auf nationaler Ebene zu novellieren. Die ePrivacy Verordnung habe nicht länger abgewartet werden können, so Hansen. Sofern sich später Konflikte zwischen nationalem und europäischem Recht ergäben, könnten diese durch entsprechende Nacharbeit behoben werden.

RAin Yvette Reif, LL.M.

Literaturhinweise

Flemming Moos/Jens Schuftig/Marian Alexander Arning (Hrsg.), **Praxishandbuch DS-GVO – einschließlich BDSG und spezifischer Anwendungsfälle**, R&W Fachmedien Recht und Wirtschaft, Frankfurt, 2. Aufl. 2021, 1.414 S., 199,– €

Bezogen auf die Unternehmenspraxis bietet das Handbuch sowohl eine umfassende Darstellung des Datenschutzrechts (DS-GVO und BDSG) als auch Schwerpunktkapitel zu wichtigen Fragen wie Cloud Computing, Web Tracking, Customer Relationship Management und Künstliche Intelligenz. DS-GVO und BDSG zeichnen sich einerseits durch umfassende Regelungen aber andererseits notwendigerweise abstrakte Vorgaben aus, die sodann wieder durch die Datenschutzbehörden präzisiert werden. Letztlich bleibt es jedoch den Unternehmen selbst überlassen, pragmatische und praxistaugliche Lösungen zu entwickeln. Vor diesem Hintergrund richtet sich das Praxishandbuch mit seinen 21 Kapiteln an alle Datenschutzpraktiker. Seine 15 Autoren/-innen liefern umfassende Lösungen für die Vielzahl an Fragestellungen, die sich im Unternehmen bei der Einhaltung der datenschutzrechtlichen Anforderungen ergeben. Dabei geht es nicht nur um die Implementierung eines Datenschutzmanagementsystems. Das Handbuch dient auch als Ratgeber bei der Bewältigung datenschutzrechtlicher Fragen, für die es pragmatische, aber zugleich rechtssichere Lösungen bietet. Durch die vielen Praxishinweise, kleinen Checklisten und Beispiele ist es ein rundum gelungener Titel zum Datenschutz das den Zusatz „Praxishandbuch" verdient.

(Schriftleitung)

Dennis-Kenji Kipker/Friederike Voskamp (Hrsg.), **Sozialdatenschutz in der Praxis**, Handbuch, Nomos Verlag Baden-Baden, 2021, 582 S., 79,– €

Das Sozialdatenschutzrecht ist durch die Datenschutz-Grundverordnung, das neue Bundesdatenschutzgesetz und die angepassten Regelungen in SGB I und X in vielen Teilen vollkommen neu verfasst.

Das von Kipker/Voskamp unter Mitwirkung von mehr als in Dutzend weiteren Autoren-/innen herausgsgebene neue Handbuch geht auf alle wichtigen Umsetzungsprobleme ein und klärt die Abgrenzung der allgemeinen Grundsätze von den bereichsspezifischen Datenschutzvorschriften. Es begnügt sich dabei nicht mit einem abstrakten Problemaufriss, sondern löst ganz konkret datenschutzrechtlich relevante Sachverhalte in der täglichen Praxis; wobei die nach den Schwerpunktbereichen:

– **Verantwortlichkeit**, Betroffenenrechte und Kontrollmaßnahmen, z.B. Auskunftsrecht; Schweigepflicht und Offenbarungsbefugnisse, gerichtlicher Rechtsschutz; Recht auf Berichtigung/Löschung, Schadensersatzansprüche, Auftragsverarbeitung; Informations- und Dokumentationspflichten

– Digitalisierung, z.B. Websites, Kommunikation per E-Mail, E-Postbrief, Krankmeldungen, Dienstpläne, Fotos bei

Patienten/Kunden/Betreuten, Smartphone-Apps, Wellness- und Gesundheits-Apps, Telemedizin, Elektronische Gesundheitskarte; Patientendaten-Schutz-Gesetz (PDSG), Elektronische Gesundheitskarte, Elektronische Patientenakte.

– Forschung, z.B. Auskunftsrechte; Einwilligungs- und Genehmigungserfordernisse, Forschung mit Primär-, Sekundär- und verknüpften Daten; Einsatz von Algorithmen und künstlicher Intelligenz, Auswirkungen der COVID-19-Pandemie.

– Grundsicherung, z.B. Zulässigkeit und Grenzen von Hausbesuchen, Einsatz Dritter durch das Jobcenter zur Überprüfung der Angaben der Leistungsbezieher-/innen; Datenweitergabe an das Jobcenter durch andere Behörden, Banken, Online-Dienste und an Dritte (z.B. Vermieter).

– Kinder- und Jugendhilfe, z.B. Datenerhebung und -übermittlung, Schweigepflicht und Offenbarungsbefugnisse; Datenschutz bei freien Trägern, Akteneinsicht; Datenschutz bei Kindeswohlgefährdung.

– Sozialversicherung, z.B. Qualitätsprüfungen in der Pflegeversicherung; MDK-Gutachten, Selektivverträge, insbesondere Abrechnung; Unfallversicherung, Akteneinsichtsrecht beim Gutachter, Rentenversicherungsnummer, Versicherungskonto

geordneten Themenbereiche das weite Feld der Sozialdatenverarbeitung überschaubar und beispielbezogen abbilden.

(Schriftleitung)

Lukas Zeyher, **Strafprozessuale Beweisverwertung von privatem Videomaterial am aktuellen Beispiel der Dashcam**, Duncker&Humblot, Berlin, Schriften zum Prozessrecht (PR), Band 277, 2021, 226 S., 71,90 €

Der in unserem Alltag mittlerweile allgegenwärtige Einsatz privater Videoaufzeichnungsgeräte spiegelt sich in jüngerer Zeit auch im Straßenverkehr wider. Konkret geht es hier um sog. Dashcams, die das Geschehen rund um das eigene Kraftfahrzeug aufzeichnen und so als Beweismittel im Prozess in Betracht kommen. Während sich der BGH im Jahr 2018 zur zivilprozessualen Verwertbarkeit dieser Aufnahmen bereits geäußert und diese grundsätzlich bejaht hat, steht eine höchstrichterliche Entscheidung auf strafprozessualer Ebene noch aus. Die Arbeit beantwortet diese Frage, indem sie das allgemeine Meinungsbild rund um die Konsequenzen privater Beweiserhebung für die Beweisverwertung darstellt, dieses kritisch beleuchtet und anschließend auf mittels Dashcam gefertigte private Videoaufzeichnungen überträgt. Anhand dieser Erkenntnisse werden die bisher zu dieser Frage ergangenen Entscheidungen des AG Nienburg aus dem Jahr 2015 und des OLG Stuttgart aus dem Jahr 2016 analysiert, ehe in einem Fazit die Erkenntnisse der Arbeit zusammengefasst werden.

(Schriftleitung)

Maike Flink, **Beschäftigtendatenschutz als Aufgabe des Betriebsrats – Kompetenzen und Verantwortung des Betriebsrats für den Datenschutz**, Duncker&Humblot, Berlin, Schriften zum Sozial- und Arbeitsrecht (SAR), Band 366, 2021, 321 S., 89,90 €

Die Arbeit behandelt die datenschutzrechtliche Rolle des Betriebsrats, wobei aufbauend auf einer Darstellung der rechtlichen Grundlagen des Beschäftigtendatenschutzes das Zusammenspiel von Datenschutz- und Betriebsverfassungsrecht beleuchtet wird. Dies bildet die Grundlage für die Herausarbeitung der dem Betriebsrat auf diesem Gebiet zustehenden Kompetenzen, seiner Gestaltungsmöglichkeiten, sowie der ihn treffenden Verantwortung. Zentrale Fragen sind dabei, welche inhaltlichen Anforderungen an datenschutzrechtliche Betriebsvereinbarungen zu stellen sind, ob der Betriebsrat selbst datenschutzrechtlich Verantwortlicher ist, welchen Grenzen er selbst bei der Verarbeitung personenbezogener Beschäftigtendaten unterliegt und wie sein Verhältnis zum betrieblichen Datenschutzbeauftragten ausgestaltet ist. Ziel ist es, die datenschutzrechtliche Rolle des Betriebsrats inhaltlich zu konturieren, um die künftige Zusammenarbeit von Mitarbeitervertretung und Arbeitgeber zu erleichtern. Von aktueller Relevanz sind die unter Kapitel E erfolgten Ausführungen zur Verantwortung des Betriebsrats im Rahmen des Datenschutzrechts und seine evtl. Rolle als Verantwortlicher nebst seinem Verhältnis zum betrieblichen Datenschutzbeauftragten angesichts der diesbezüglich erfolgten Entscheidungen des Gesetzgebers.

(Schriftleitung)

Flemming Moos (Hrsg.), **Datenschutz und Datennutzung – Verträge – Datenschutzklauseln – Datenschutzerklärungen**, Verlag Dr. Otto Schmidt, Köln, 3. Aufl. 2021, 1500 S., 139,– € (inklusive Online-Nutzung aller Muster und ausgewählter Muster mit Lawlift-Funktion)

Das von Moos und 28 weiteren Autoren und Autorinnen verfasste, und nunmehr in dritter und aktualisierter Auflage vorgelegte Formularhandbuch bietet praktische Hilfestellung zwischen gesetzlichen Pflichten und unternehmerischen Anforderungen an Datennutzung und Datenschutz im Unternehmen, indem es in über 50 praxiserprobte Musterverträge, Klauseln und Vereinbarungen ein ideales Werkzeug für die tägliche Arbeit von Datenschutzbeauftragten, Unternehmensjuristen, Rechtsabteilungen und Rechtsanwälten mit Schwerpunkt im Datenschutzrecht bietet. Praktiker finden eine optimale Hilfe bei der Erstellung eigener oder Prüfung vorgelegter Vertragstexte in allen wichtigen Bereichen des Datenschutzrechts. Die Themengebiete sind wie folgt gegliedert: Verträge zur Datenschutzorganisation, Datenschutzverträge; Datennutzungsverträge, Unternehmensrichtlinien und Betriebsvereinbarungen; Verträge über internationale Datentransfers; Datenschutzklauseln, Datenschutzerklärungen und Einwilligungen. Wichtige Vertragsmuster werden auch in englischer Sprache angeboten.

Dabei geht es u.a. konkret um Arbeitsverträge mit einem internen und einem externen Datenschutzbeauftragten, die Übermittlung personenbezogener Daten in Drittländer und EU-Standarddatenschutzklauseln oder verbindliche Unternehmensregelungen.

(Schriftleitung)

Neuerscheinungen

Aufsätze

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

Baeck, Ulrich/Hilgers, Elena/Winzer, Thomas, **Das Betriebsrätemodernisierungsgesetz – der Regierungsentwurf als Update für das BetrVG?** NZA 2021, S. 620
Dieser und weitere nachfolgend aufgeführte Beiträge von Eicke, Möllenkamp, Schiefer und Schulze erläutern die Neuregelungen des Betriensrätemodernisierungsgesetzes und die sich hieraus ergebenden neuen Befugnisse der Mitarbeitervertretung bei neuen Arbeitsformen.

Bergwitz, Christopher, **Der Abfallbeauftragte – das unbekannte Wesen,** NZA 2021, S. 54
Von Interesse sind die zu Aufgaben und Rechtsstellung des Datenschutzbeauftragten bestehende Parallelen.

Eicke, Anne, **Die wichtigsten Neuerungen durch das Betriebsrätemodernisierungsgesetz,** ArbRAktuell 2021, S. 313

Gola, Peter, **Das Verbandsklagegesetz-E und betriebliche Datenschutzbeauftragte**, DuD 2021, S. 472
Mit dem Bundestag vorliegenden Gesetzesentwurf stellt sich u.a. erneut die Frage, ob das Handeln bzw. Nicht-Handeln betrieblicher Datenschuzbeauftragter, zur Haftung des Arbeitgebers führen kann.

Henseler, Maren/Köllmann, Thomas, **Die Rechte des Betriebsrats im Zusammenhang mit betrieblichen Entgeltlisten – Reichweite, Grenzen und praktische Implikationen,** BB 2021, S. 94
Der Beitrag würdigt die diesbezügliche aktuelle Rechtsprechung des BAG.

Machmann, Frank, **Der Arbeitgeber als Verantwortlicher für den Datenschutz im Betriebsratsbüro (§ 79 a BetrVG)?,** NZA 2021, S. 834
Der Beitrag erörtert den Konflikt aus der Stellung des Betriebsrats als Teil der verantwortlichen Stelle, d.h. dass der Arbeitgeber auch Verantwortlicher für die personenbezogenen Daten bei der Mitarbeitervertretung ist, die diese aber eigenständig verarbeitet.

Mesch, Gerrit/Folkerts, Elena, **Aufnahme von Bewerbern in einen „Talentpool“,** ZD 2021, S. 252
Beleuchtet wird die Zulässigkeit solcher digitaler Bewerberdatenbanken.

Möllenkamp, Olaf, **Das Betriebsrätemodernisierungsgesetz 2021 – Regelungsinhalte und Praxisauswirkungen**, DB 2021, S. 1198

Röß, Simon, **Die Auskunftspflicht von Arbeitnehmern bei der Aufklärung einer Straftat durch den Arbeitgeber**, NZA 2021, S. 675
Der Verfasser erörtert, ob es der Milderung von Sanktionen gemäß § 17 Abs. 1 Nr. 5 VersanG-E um ein subjektives Recht des Arbeitnehmers handelt und ob der Betriebsrat Mitbestimmungsrechte haben würde, was er mit Blick auf § 94 Abs. 1 S. 1 BetrVG bejaht.

Schiefer, Bernd/Worzalla, Michael, **Das Betriebsrätemodernisierungsgesetz – eine „Mogelpackung“?** NZA 2021, S. 817

Schulze, Marc-Oliver, **Der Entwurf des Betriebsrätemodernisierungsgesetzes,** ArbR Aktuell 2021, S. 211

Stück, Volker, **Entwurf für ein Verbandssanktionengesetz**, ZD 2021, S. 307
Der Beitrag stellt das von der Bundesregierung geplante neue Unternehmensstrafrecht und die daraus folgenden unternehmensbezogenen Konsequenzen dar.

Wybitul, Tim/Venn, Nikolai, **Verteidigung von Unternehmen gegen Geldbußen nach Art. 83 DS-GVO – Streit um rechtliche Voraussetzungen für Unternehmenssanktionen**, ZD 2021, S. 343
Der Beitrag erörtert die diesbezüglich zur Zeit strittige Rechtslage.

„Stopp! Gaffen tötet" – App soll Leben retten

Fotos von Unfällen zu machen ist geschmacklos. Sie sind zudem gefährlich, weil Handyfotografen den Weg zum Unfallort blockieren und den Einsatz der Rettungskräfte stören. „Gaffen tötet" ist eine drastische und traurige Wahrheit, weil schon wenige Minuten Verzug bei der Unfallrettung Leben kosten können. Weil dieses Verbot Gaffer nicht scherte, wurde es einem Polizisten zu viel. Nach einem tödlichen Unfall auf der A6 zwischen Roth und Nürnberg griff zu einer drastischen Maßnahme, nachdem die Aufforderung nicht zu fotografieren nicht fruchtete. Mit den Worten „Willst du die Leiche sehen?" bot er Gaffern eine Schockbehandlung an. Rechtlich angemessen ist diese Reaktion nicht. Wie man Schaulustige am Gaffen und Fotografieren hindern kann und dabei die Grenzen des rechtlich gebotenen wahrt, zeigt ein Projekt der Johanniter-Unfallhilfe. Wenn deren Einsatzkräfte an einen Unfallort kommen, kann es Handyfotografen künftig passieren, dass die Warnung „Stopp! Gaffen tötet!" auf dem Display ihres Smartphones erscheint. Dazu werden QR-Codes auf Rettungswagen geklebt. Wird der QR-Code aufgenommen, dann werden die fotografierenden Gaffer per automatischer Umleitung auf eine Website geleitet und sehen dort einen Warnhinweis zu den Gefahren des Gaffens. Wie das konkret aussieht, zeigt ein Video[1] der Johanniter-Unfallhilfe. Viele „smarte" Ideen sind oft nichts anderes als ein freundliches Synonym für datenschutzrechtlich fragwürdige Spielereien. Die Johanniter zeigen, dass es auch anders geht.

1 Https://www.youtube.com/watch?v=rBCupH0L7t4

E-LEARNING

Mitarbeiter online sensibilisieren:

In 45 Minuten Datenschutzrisiko mindern

nur 14,90 € Einstiegspreis pro Schulung

Jetzt kostenlos testen:
elearning-mit-zertifikat.de

UNIVADO

DATAKONTEXT

powered by GDD

Foto: peshkova - Adobe Stock

Der einfache Weg zum organisierten Datenschutz!

DATA AGENDA Datenschutz Manager

Der Experte an Ihrer Seite!

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

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

DATAKONTEXT